



CLI Application Guide Avaya VPN Gateway

9.0
NN46120-101, 04.02
August 2012

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: <http://www.avaya.com/support>. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/](http://support.avaya.com/licenseinfo/) ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation(s) and Product(s) provided by Avaya. All content on this site, the documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is

protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://www.avaya.com/support/Copyright/>.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: <http://www.avaya.com/support>

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: <http://www.avaya.com/support>

Contents

Chapter 1: Preface	11
Who Should Use This Book	11
Related Documentation	11
Product Names	12
How This Book Is Organized	12
Customer service	13
Getting technical documentation	14
Getting product training	14
Getting help from a distributor or reseller	14
Getting technical support from the Avaya Web site	14
Chapter 2: New in this release	15
Features	15
IPsec Two Factor authentication for Avaya VPN Gateway	15
Android L2TP/IPsec support	15
AES 256 support for IPsec	16
Java RDP upgrade support	16
Net Direct Mac OS X support	16
Secure Portable Office (SPO) support	16
Other Changes	17
Chapter 3: VPN Introduction	19
Secure Access from a Remote Location	19
VPNs	19
Secure Service Partitioning	20
Clientless Mode	20
Web Portal	20
The Net Direct Client	21
PDA Support	22
Transparent Mode	23
Avaya SSL VPN Client	24
Avaya IPsec VPN Client (formerly Contivity VPN Client)	24
Installed Version of Net Direct	24
VPN Client Summary	25
Authentication and Access Control	25
External Database Authentication	25
Local Database Authentication	25
Access Rules	26
Licenses	26
SSL License	26
IPsec License	26
Secure Service Partitioning License	27
Portal Guard License	27
TPS License	27
Demo License	27
Virtual Desktop License	27

Emergency Remote Access License.....	27
Secure Portable Office License.....	28
Obtaining Licenses.....	28
License Key.....	28
License Pool (SSL and IPsec Users).....	28
Secure Portable Office.....	29
Secure Service Partitioning.....	29
Obtaining the MAC Address.....	30
Paste the License Key.....	30
Managing New IPSec Logins during Maintenance.....	31
If a Cluster Member Fails.....	32
Chapter 4: Clientless Mode.....	35
Configure VPN from Wizard Settings.....	35
Import Signed Certificate to the AVG.....	36
Map Signed Server Certificate to VPN.....	37
Assign a Fully Qualified Domain Name.....	38
Configure VPN from Scratch.....	38
Import Signed Certificate.....	38
Create a VPN.....	39
Update DNS Server.....	41
Select Authentication Method(s).....	41
Configure User Access Groups and Access Rules.....	41
Configure Group-Specific Linksets.....	41
Configure Access through the Net Direct Client.....	41
Configure Tunnel Guard.....	42
Enable WholeSecurity Scan.....	42
Customize the Portal.....	42
HTTP to HTTPS.....	42
DNS Round Robin Load Balancing.....	42
Add IP Addresses.....	43
VPN with Application Switch.....	44
Configure the AVG.....	45
Configure the Application Switch.....	46
Chapter 5: The Portal from an End-User Perspective.....	51
Accessing the Portal Web Page.....	51
The Portal Web Page.....	52
Java Applet/ActiveX Control Icons.....	53
General Capabilities.....	54
The Home Tab.....	54
The Files Tab.....	56
The Tools Tab, System Information.....	57
The Tools tab, Clear Login Cache.....	58
The Tools tab, Change User Password.....	59
The Tools tab, Edit Bookmarks.....	60
The Tools Tab, Change Language.....	61
The Full Access Page.....	61
The Advanced Tab, Telnet/SSH Access.....	63

The Advanced Tab, HTTP Proxy	65
The Advanced Tab, FTP Proxy	68
The Advanced Tab, Port Forwarders	69
The Download Tab	77
Logging out from the Portal	77
Chapter 6: Bandwidth Management	79
User traffic	79
IPsec Passthrough	79
Hard and soft limit	80
Configure BWM	80
Enabling BWM	80
Configuring BWM policy	80
Configure IPsec Passthrough	81
Enabling IPsec Passthrough	82
Configuring bandwidth policy	82
Configuring IPsec servers	83
Listing the IPsec servers	83
Inserting the IPsec servers	84
Moving the IPsec servers	84
Chapter 7: Net Direct	87
About the Net Direct Client	87
Supported Operating Systems	88
Net Direct Modes	88
Mobility	89
Server Configuration	90
Create IP Pool	90
Enable Net Direct	97
Configure Net Direct Link	101
Configure Windows Administrator User Name/Password	102
Configure Link for Downloading Installed Version	103
License Text and Banner	104
Enable Full Access	106
Net Direct from a User Perspective	106
Downloadable Version (Windows)	106
Installed Version (Windows)	109
Downloadable Version (Mac OS X and iMac)	112
Start Net Direct Outside Portal	114
Start Net Direct Outside Portal with Auto-Login	115
Chapter 8: Authentication Methods	117
External Database Authentication	117
Local Database Authentication	117
Client Certificate Authentication	118
Login Service List Box	118
Secondary and Two Factor authentication	118
RADIUS Authentication	119
LDAP Authentication	123
Search the LDAP Dictionary Information Tree (DIT)	128

NTLM Authentication.....	130
Netegrity SiteMinder Authentication.....	132
RSA ClearTrust Authentication.....	137
RSA SecurID Authentication.....	143
Configure the RSA Server Settings.....	143
Configure the RSA Authentication Method.....	144
Local Database Authentication.....	147
Client Certificate Authentication.....	149
Generate Unique Client Certificates.....	149
Chapter 9: Groups, Access Rules and Profiles.....	157
Group Parameters.....	157
Linksets.....	158
User Type.....	158
Access Rules.....	158
Default Group.....	159
Extended Profiles.....	159
Number of Login Sessions.....	159
Idle Timeout.....	160
Maximum Session Length.....	160
IP Pool.....	160
Tunnel Guard rules.....	160
IPsec Tunnel Access.....	161
IE Cache Wiper.....	161
Citrix Metaframe Support.....	161
Net Direct Access.....	162
Windows Administrator User Name/Password.....	162
Multiple Groups.....	162
ID or Name?.....	163
SPO Access.....	163
Bandwidth policy.....	164
AAA Configuration Order.....	164
Extended Profiles.....	165
Network, Service and Path Configuration.....	165
Create Network Definitions.....	165
Create Service Definition.....	169
Create Path (Appspec) Definition.....	170
Group Configuration.....	172
Example 1: Access to Specific Services on Specific Intranet Hosts.....	172
Example 2: Access Allowed to All Services on Hosts in a Specific Subdomain	175
Example 3: Access Allowed to the Complete Intranet, Except for Hosts in a Specific Subdomain ..	176
Specifying the Secure Portable Office Software Index.....	178
Configuring bandwidth policy.....	181
Working with Extended Profiles.....	182
Base Profiles and Extended Profiles.....	182
When is the Extended Profile Applied?.....	182
Linksets.....	183
Access Rules.....	183

User Type.....	183
Multiple Groups.....	183
Client filters.....	185
Example 1: Define the Staff Group.....	186
Example 2: Define the Engineer Group.....	193
Extended Profile for Users with Client Certificate.....	198
Extended Profile for Users with IE Cache Wiper.....	199
Configuring bandwidth policy.....	201
Extended profiles for users with NAP.....	201
Chapter 10: Group Links.....	203
Link Types.....	203
Linksets.....	204
Linkset Name.....	204
Linkset Text.....	204
Autorun Support.....	205
Configuration Examples.....	205
WTS and Citrix Setup.....	205
Create a Linkset for File Server Access.....	207
Set Net Direct as Prerequisite.....	213
Other Link Types.....	216
Chapter 11: Customize the Portal.....	249
Default Appearance.....	249
Change Color Theme.....	249
Change the Colors.....	250
Common Colors.....	250
Change the Banner Image.....	251
Change Company Name.....	252
Change Icon Mode.....	253
Change Number of Link Columns.....	253
Change Link Area Width.....	254
Hide Enter URL Field.....	254
Change the Static Text.....	254
Change Static Text on Login Page.....	255
Change Portal Language.....	256
Check the New Appearance.....	258
Automatic Redirection to Internal Site.....	259
Upload Custom Content.....	261
Chapter 12: HTTP to HTTPS Redirection.....	265
Configure HTTP to HTTPS Redirection.....	265
Chapter 13: Configure Tunnel Guard.....	269
How is Tunnel Guard Activated?	269
Tunnel Guard SRS Rules.....	269
Configuration Using Wizard.....	270
Test Tunnel Guard Using Wizard Settings.....	272
Configure SRS Rules.....	275
Making API Calls.....	275
Configuration from Scratch.....	276

Enable Tunnel Guard.....	276
Configure Tunnel Guard SRS Rules.....	278
Configure Linksets.....	278
Configure a Network.....	280
Configure a Group.....	281
Create Client Filters.....	282
Configure Extended Profiles.....	283
Test the Example Configuration.....	286
Chapter 14: Network Access Protection.....	289
NSG NAP architecture.....	289
System Health Agent.....	290
Configuring NAP.....	290
Chapter 15: WholeSecurity.....	293
How Does it Work?.....	293
Configuration.....	293
Requirements.....	293
Configure a Deployment in WholeSecurity.....	294
Enable WholeSecurity on the AVG.....	294
Configure an Anonymous Group.....	295
Chapter 16: Virtual Desktop.....	299
Starting vdesktop.....	299
Access vdesktop using CLI.....	299
Chapter 17: Secure Portable Office (SPO) Client.....	305
Configuring SPO General Settings.....	305
Importing logo.....	306
Importing system tray icon.....	307
Adding a Backup Server.....	308
Importing a SPO client Software Image.....	308
Administrating third-party applications.....	309
Chapter 18: Secure Service Partitioning.....	313
802.1Q VLAN Tags.....	313
License Keys.....	314
Connection Example.....	314
Configuration Example.....	315
Initial Setup.....	316
Configure the Interfaces.....	316
Configure VPN 1.....	320
Configure VPN 2.....	335
Update DNS Server.....	335
Remaining Configuration.....	335
Chapter 19: Branch Office Tunnels.....	337
Clustering Branch Office Tunnels.....	337
Scalability and Load Balancing.....	337
Connection Example.....	338
Configuration Example.....	339
Initial Setup.....	339
Basic VPN Setup.....	340

Secure Service Partitioning.....	340
Configure Branch Office Tunnel.....	340
Information Menu.....	346
Statistics Menu.....	347
Chapter 20: Layer 2 Tunneling Protocol.....	349
Configure L2TP.....	349
Configuring L2TP.....	349
Chapter 21: Transparent Mode.....	355
What is Transparent Mode?.....	355
Avaya SSL VPN Client.....	355
Server Configuration.....	356
Client Configuration.....	359
Avaya IPsec VPN Client.....	368
Server Configuration.....	368
Client Configuration.....	380
Transparent Mode Without Portal.....	382
Configure a VPN.....	382
Transparent Mode without Portal but with Application Switch.....	386
Configure the AVG.....	386
Configure the Application Switch.....	387
Chapter 22: Configure Portal Guard.....	393
HTTP to HTTPS Rewrite.....	393
Initial Setup.....	393
Add a Signed Server Certificate to the AVG.....	394
Update DNS Server.....	394
License Key.....	394
Configure a Default Group.....	395
Configure Portal Acceleration.....	395
Glossary.....	397

Chapter 1: Preface

This guide contains example configurations and describes how to use the Avaya VPN Gateway (AVG) when using it for VPN deployment. For instructions about how to deploy SSL acceleration, see the *Application Guide for SSL Acceleration*.

Who Should Use This Book

This guide is intended for network installers and system administrators who configure and maintain a network. This guide is based on assumption that you are familiar with Ethernet concepts and IP addressing. All IP addresses are examples and should not be used as-is.

Related Documentation

For complete documentation to install, configure, and use the many features of the AVG, see the following manuals:

- *Avaya VPN Gateway Command Reference* (NN46120-103). Describes each command in detail. The commands are listed for each menu, according to the order they appear in the Command Line Interface (CLI).
- *Avaya VPN Gateway Application Guide for SSL Acceleration* (NN46120-100). Provides examples on how to configure Secure Socket Layer (SSL) Acceleration through the CLI.
- *Avaya VPN Gateway CLI Application Guide* (NN46120-101). Provides examples on how to configure VPN deployment through the CLI.
- *Avaya VPN Gateway BBI Application Guide* (NN46120-102). Provides examples on how to configure VPN deployment through the Browser-Based Interface (BBI).
- *Avaya VPN Gateway User Guide* (NN46120-104). Describes the initial setup procedure, upgrades, operator user management, certificate management, troubleshooting and other general operations that apply to both SSL Acceleration and VPN.
- *Avaya VPN Gateway Administrator Guide* (NN46120-105). VPN management guide intended for end-customers in a Secure Service Partitioning configuration.
- *Avaya VPN Gateway Configuration - Secure Portable Office Client* (NN46120-301). Gives the feature list and provides general information about Secure Portable Office (SPO) based VPN client.

- *Avaya VPN Gateway VMware Getting Started Guide* (NN46120–302). Describes how to install, configure, and deploy the Avaya VPN Gateway VMware appliances.
- *Avaya VPN Gateway Release Notes* (NN46120-400). Lists new features available in version and provides up-to-date product information.
- *Avaya VPN Gateway Troubleshooting Guide* (NN46120-700). Describes the prerequisites and various tools used to troubleshoot the Avaya VPN Gateway (AVG).

You can download these manuals; (see [Customer service](#) on page 13.

Product Names

The software described in this manual runs on various hardware models. The generic terms Avaya VPN Gateway, VPN Gateway, or AVG are used to refer to the following hardware models:

- Avaya VPN Gateway 3050–VM (AVG 3050–VM)
- Avaya VPN Gateway 3070–VM (AVG 3070–VM)
- Avaya VPN Gateway 3090–VM (AVG 3090–VM)

Similarly, all references to the old product name—iSD-SSL or iSD—in commands or screen output to the preceding hardware models.

 **Note:**

SSL Accelerator (formerly Alteon SSL Accelerator) is now discontinued.

How This Book Is Organized

[VPN Introduction](#) on page 19. Introduces the main features of the VPN Gateway software.

[Clientless Mode](#) on page 35. Describes how to set up a VPN for clientless mode, that is, accessible with the available browser.

[The Portal from an End-User Perspective](#) on page 51. Describes the Portal Web page.

[Bandwidth Management](#) on page 79. Describes how to configure Bandwidth Management.

[Net Direct](#) on page 87. Describes how to configure the system for use with the Net Direct, a VPN client downloadable for each Portal session.

[Authentication Methods](#) on page 117. How to configure a VPN to use external authentication servers (for example, RADIUS), local database authentication, or client certificate authentication.

[Groups, Access Rules and Profiles](#) on page 157. Describes how to define groups with access rules and profiles. The access rules define the user's access rights to various intranet resources.

[Group Links](#) on page 203. How to define hypertext links on the Portal's Home tab.

[VPN Introduction](#) on page 19. How to customize the Portal, for example, language version, logo, company name, colors, and static texts.

[HTTP to HTTPS Redirection](#) on page 265. How to configure the AVG for redirection of HTTP requests to HTTPS.

[Configure Tunnel Guard](#) on page 269. How to configure Tunnel Guard to check the client PCs status.

[Network Access Protection](#) on page 289. How to configure Network Access Protection for system health validated access to private network.

[WholeSecurity](#) on page 293. How to enable a WholeSecurity scan of client PCs.

[Secure Service Partitioning](#) on page 313. How to configure hosting of multiple VPNs, a feature especially for Internet Service Providers (ISPs).

[Branch Office Tunnels](#) on page 337. How to configure IPsec-based branch office tunnels.

[Layer 2 Tunneling Protocol](#) on page 349. Describes how to configure Layer 2 Tunneling Protocol.

[Transparent Mode](#) on page 355. How to set up a VPN for access with the Avaya SSL VPN client or the Avaya IPsec VPN client (formerly Contivity VPN client).

[Configure Portal Guard](#) on page 393. Describes how to convert a regular HTTP site to generate HTTPS links.

[Secure Portable Office \(SPO\) Client](#) on page 305. Describes how to access various applications of the SPO client when it is integrated with the AVG server.

Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

- [Getting technical documentation](#) on page 14
- [Getting product training](#) on page 14
- [Getting help from a distributor or reseller](#) on page 14
- [Getting technical support from the Avaya Web site](#) on page 14

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Chapter 2: New in this release

The following section details what's new in *Avaya VPN Gateway CLI Application Guide* (NN46120-101) for Release 9.0.

Features

See the following section for information about feature changes:

IPsec Two Factor authentication for Avaya VPN Gateway

Release 9.0 adds a two factor authentication method for authentication between servers and clients. When assigning authentication servers, you have the option to specify a second authentication server to use after the first one succeeds.

IPsec Two Factor authentication adds more robust security by using client certificate authentication as first factor to represent "what user-has" and using other authentication methods as second factor, "what user-knows".

Configuring a new certificate authentication server automatically supports IPsec Two Factor authentication. IPsec Two Factor authentication supports only certificate authentication as primary servers and local, RADIUS or LDAP as secondary servers.

Refer to the following sections for more information:

- [Secondary and Two Factor authentication](#) on page 118
- [Configuring IPsec Two Factor authentication](#) on page 155

Android L2TP/IPsec support

Avaya VPN Gateway Release 9.0 adds support for clients connecting via L2TP/IPsec from Android devices. Android versions 2.x, 3.x, and 4.x are supported and an additional license key is not required.

 **Note:**

For supported Android versions, refer to the compatibility matrix, *AVG 9.0 Release Notes* (NN46120-400).

AES 256 support for IPsec

Avaya VPN Gateway Release 9.0 adds AES 256 support for IPsec.

Java RDP upgrade support

Release 9.0 upgrades JavaRDP client for better support of the latest Windows Terminal server. A new optional field was added for WTS links, KeyMap URL, a URL path that points to a custom key code definition file.

Net Direct Mac OS X support

Release 9.0 supports Net Direct on Mac OS X 10.7 (Lion).

Secure Portable Office (SPO) support

Release 9.0 adds Ceedo support on all Windows 64 bit platforms in virtualized mode.

Beginning with Release 9.0, you can download one of the two versions of SPO:

- Avaya Basic— contains basic software with Avaya 2050 IP Softphone and JRE 7.
- Avaya Contact Center (ACC)— contains all the applications and software of Avaya Basic with the addition of Avaya Contact Center Express Desktop 5.0 and Avaya One-X Client.

Both SPO version (Basic and ACC) use security restrictions on Ceedo environment. Next host resources are blocked inside Ceedo:

- Access to network shares and drives
- Access to printing
- Drag and drop
- Clipboard access

For more information on the Release 9.0 support, refer to *Configuration — Secure Portable Office Client Avaya VPN Gateway* (NN46120-301).

Other Changes

- Please note, while the Avaya Endpoint Access Control Agent (formerly Tunnel Guard) can be configured through both the BBI and CLI, the CLI configuration is performed under the former Tunnel Guard context.

New in this release

Chapter 3: VPN Introduction

This chapter introduces the Virtual Private Network (VPN) subsystem included in the Avaya VPN Gateway (AVG) software.

The VPN subsystem is added to the SSL acceleration system, which makes it possible to combine SSL acceleration and VPN. For more information about SSL acceleration, see *Application Guide for SSL Acceleration*.

Secure Access from a Remote Location

VPNs allow remote users—mobile workers, telecommuters or partners—to access protected intranet or extranet resources such as applications, mail, files, or web pages. Data is sent through a secure connection, either SSL (Secure Sockets Layer) or IPsec (Internet Protocol Security). What resources are accessible to the remote user is determined by the access rules configured for the group where the user is a member.

Users can access intranet in clientless mode, transparent mode, or both:

- Clientless mode. From any computer connected to the Internet. The remote user connects to the VPN Portal through a secure SSL connection through the web browser. After it is authenticated, the user can access the resources through the Portal tabs (see [Web Portal](#) on page 20). Clientless mode also enables download of the Net Direct client, a simple and secure method to access intranet resources through the remote user's applications.
- Transparent mode. From a computer with the Avaya SSL VPN client or the Avaya IPsec VPN client (formerly the Contivity VPN client) installed. The term transparent implies that remote users have network access as if they were actually connected to the corporate intranet (see [Transparent Mode](#) on page 23).

VPNs

You can configure up to 250 VPNs for each cluster of VPN Gateways. A VPN is typically defined for access to an intranet, parts of an intranet, or to an extranet. For each VPN, you can define how the user is authenticated, which user access groups are authorized to access the VPN, and the access rules that apply to each user group.

Each VPN have one or more assigned IP addresses. To access resources in the VPN, the remote user connects to the IP address or the corresponding DNS name—either through the browser or through a preinstalled VPN client.

Secure Service Partitioning

Because the SSL VPN software provides the ability to partition a cluster of VPN Gateways into separate VPNs, Internet Service Providers (ISPs) can host multiple VPN customers on a shared Remote Access Services (RAS) platform.

To enable the Secure Service Partitioning feature, you must obtain a license key from Avaya. For more information about the Secure Service Partitioning feature, see [Secure Service Partitioning](#) on page 313

Clientless Mode

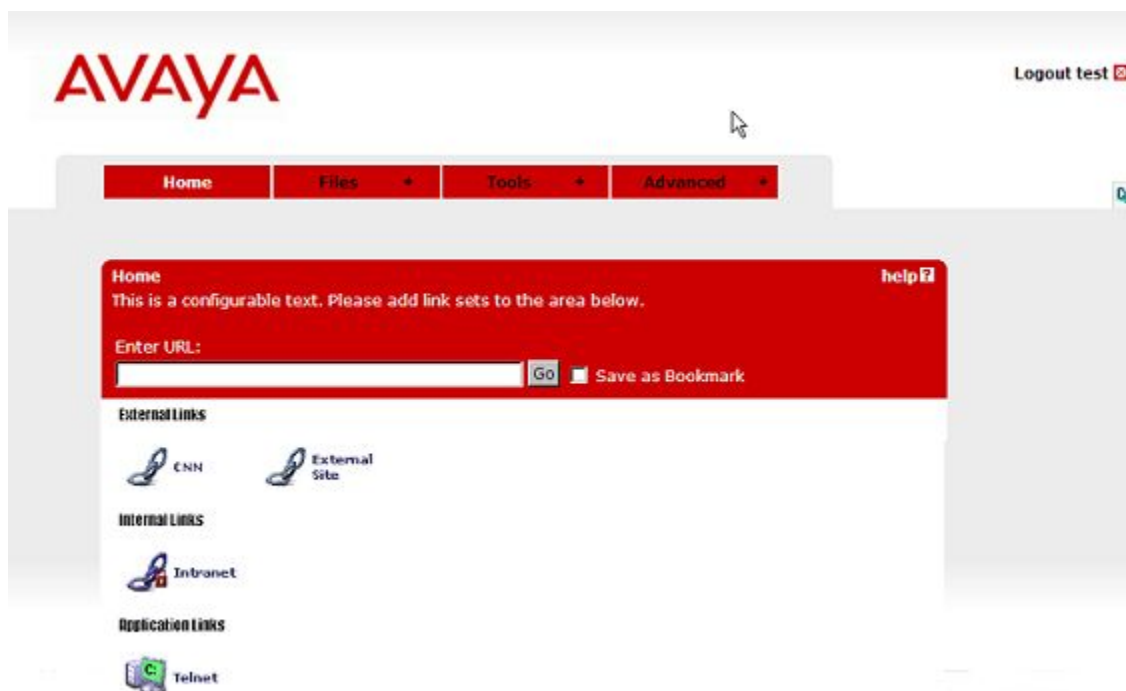
For a partner or mobile worker to access intranet resources from any computer with Internet connectivity (for example an Internet café), access is possible through the clientless mode. No manual software installation is required.

In clientless mode, all interaction with the intranet is through the web Portal through HTTP, Java Applets, and ActiveX controls, which gives the client full HTTP access to the intranet. It also provides FTP and SMB (Windows file shares) access from the browser. All network traffic between the client and the VPN Gateway is sent through a secure SSL connection.

Clientless mode capabilities include intranet browsing, file server access through the Portal, Telnet/SSH access occurs, and application tunneling (port forwarding).

Web Portal

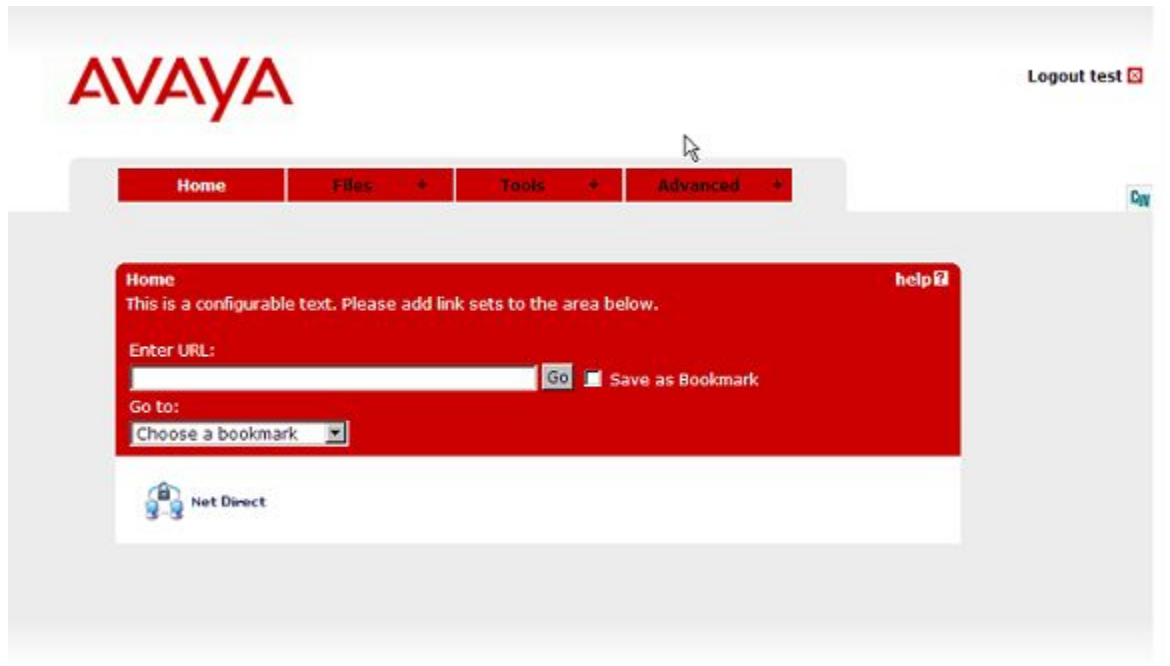
In clientless mode, the remote user connects to the VPN through the web browser. Each VPN has a web Portal where the remote user can access intranet resources from various tabs.



For a detailed description of the Portal, see [The Portal from an End-User Perspective](#) on page 51.

The Net Direct Client

Net Direct provides end-users with clientless SSL access to the intranet. By clicking a link on the Web Portal, the Net Direct client is downloaded, installed, and run on the remote user's PC. While Net Direct runs in the background, remote users can access intranet resources through their native applications – without the need to manually install VPN client software.



Cached Version

To reduce network traffic and start up time, a cached version of Net Direct is also available as a configurable option. If enabled, Net Direct leaves some components from the first installation on the client machine when the user exits the Portal session. These components are retrieved from the server only when they become outdated.

Installed Version

The Net Direct client is also available as a setup.exe file that you install permanently on the remote users' machines. See [Installed Version of Net Direct](#) on page 24.

PDA Support

Clientless mode includes PDA (Personal Digital Assistant) support. To browse to the PDA page, enter the Portal address followed by **/pda**, for example, **https://vpn.example.com/pda**. The Portal logon page appears:

After you log on, the PDA Portal appears. The PDA Portal layout is a simplified version of the Web Portal from which you can browse the intranet and access the file server to download files. You can change the company name if desired.

The preceding example shows the **Home** tab with two linksets with one link each.

*** Note:**

When you configure an SMB (Windows file share) link to appear on a PDA Portal, you must specify a shared network folder.

For instructions to configure the VPN Gateway for clientless mode, see [Clientless Mode](#) on page 35.

Transparent Mode

As opposed to clientless mode, transparent mode requires the user to install VPN software, either the Avaya SSL VPN client or the Avaya IPsec VPN client (formerly the Contivity VPN client). The VPN Gateway becomes the VPN server.

The term transparent is mainly relevant from a user perspective. It means that the remote user experiences network access as if they are physically connected to the corporate intranet. No Portal interaction is required. Transparent mode supports access to the intranet through legacy TCP- and UDP-based client applications.

Avaya SSL VPN Client

The Avaya SSL VPN client is permanently installed on the remote user's machine. The SSL VPN client is available in two versions:

- LSP (Layered Service Provider) client. Compatible with Windows 98, ME, NT (with IE 5 or later) 2000 and XP. This client does not support UDP.
- TDI (Transport Driver Interface) client. Compatible with Windows 2000 and XP. This client supports UDP and TCP.

SSL VPN Client version 1.5.0.15 or later supports PC with dual CPU processors and hyper-threading.

The SSL VPN client is instructed to connect and intervene as soon as the remote user initiates a TCP or UDP connection to the intranet. Depending on the client's configuration, the request can either be directed to the VPN Gateway through a secure SSL tunnel or directly to the requested destination.

For more information about the SSL VPN client, along with configuration instructions, see [Avaya SSL VPN Client](#) on page 355 in [Transparent Mode](#) on page 355.

Avaya IPsec VPN Client (formerly Contivity VPN Client)

Install and configure the Avaya IPsec VPN Client on the remote user's machine with the desired authentication option along with the IP address or domain name of the AVG cluster.

When the IPsec VPN client starts on the remote user's machine and the user is authenticated to the VPN Gateway, requests made by the remote user are tunneled to the VPN Gateway through a secure IPsec connection.

For more information about the Avaya IPsec VPN client along with configuration instructions, see the section [Avaya IPsec VPN Client](#) on page 368 in [Transparent Mode](#) on page 355.

Installed Version of Net Direct

As mentioned previously, the Net Direct client is available as a setup.exe file that you install permanently on the remote user's machines. No Portal logon is required. The user logs on through the user interface provided by the installable Net Direct client. To install the Net Direct client, users must have administrator rights on their PC.

For more information, including instructions to configure the VPN Gateway for use with the Net Direct client, see [Net Direct](#) on page 87.

VPN Client Summary

The AVG software supports several types of VPN clients. The following table summarizes the supported operating systems and protocols for available VPN clients.

VPN Client	Security Protocol	Network Protocols	Operating Systems	Requires preinstallation
Net Direct (downloadable client)	SSL	All IP protocols	Windows 2000, XP, Linux, Macintosh, Vista, 7	No
Net Direct (installable client)	SSL	All IP protocols	Windows 2000, XP, Vista, 7	Yes
Avaya VPN Client 10.06	SSL and IPsec	All IP protocols	Windows XP, Vista, Win 7 (32 and 64 bit)	Yes

Authentication and Access Control

To achieve secure authentication and access control, the AVG can use both external authentication servers and the VPN Gateway built-in local database. The same mechanisms are used for both clientless and transparent mode. Authentication can also be achieved by client certificate authentication.

External Database Authentication

Companies with external authentication servers (RADIUS, LDAP, NTLM, RSA SecurID, RSA ClearTrust, and Netegrity SiteMinder) can use these servers for authentication without modification. Which server and fallback order to use is defined on the VPN Gateway.

Local Database Authentication

If no external authentication server exists, or if speedy deployment is required, the VPN Gateway can be an authentication server. It can store thousands of user authentication entries each defining user name, password, and the name of access groups.

Access Rules

Each user maps to one or more access groups stored. Access rules are associated with the group defined in the user's access rights to resources on the corporate intranet. The access rules permit or deny access to servers based on a combination of criteria:

- Destination host or network
- Ports or protocol
- Path (for HTTP, SMB and FTP file browsing)
- Source IP address (if extended profiles are used)
- Authentication method (if extended profiles are used)
- Access method (if extended profiles are used)
- Client PC properties (if extended profiles are used)
- Maintenance status of the VPN Gateway

In [Groups, Access Rules and Profiles](#) on page 157 you find instructions to define groups, access rules, and profiles.

Licenses

The following licenses are available to enhance the capabilities of the Avaya VPN Gateway (AVG) software.

SSL License

To enable the VPN feature for more than 50 concurrent SSL users, you must obtain a license key from Avaya. SSL users are those who connect to the VPN Gateway through Web browsers or through the Avaya SSL VPN client. License upgrades are available for 50, 100, 250, 500, 1000, and 2000 users.

IPsec License

To enable the VPN feature for more than 50 concurrent IPsec users, you must obtain a license key from Avaya. IPsec users are users who connect to the VPN Gateway through the Avaya IPsec VPN client (formerly Contivity). License upgrades are available for 250, 500 and 1000 users. For the ASA 310 and ASA 410 models, only demo licenses are available.

Secure Service Partitioning License

To enable the Secure Service Partitioning license, you must obtain a license key from Avaya. For instructions to configure the Secure Service Partitioning feature, see [Secure Service Partitioning](#) on page 313.

Portal Guard License

To enable the Portal Guard feature, you must obtain a license key from Avaya. For instructions to configure the PortalGuard feature, see [Configure Portal Guard](#) on page 393.

TPS License

No license is required to enable full TPS capacity.

Demo License

To try out the preceding features, you must obtain a 30-day demo license from Avaya upon request. See [Customer service](#) on page 13 for contact information.

Virtual Desktop License

To enable the virtual desktop feature, you must obtain a license key from Avaya. See [Virtual Desktop](#) on page 299 for more information.

Emergency Remote Access License

An Emergency Remote Access (ERA) license provides remote access in a secure way. The ERA license is valid for 60 days. License upgrades are available for 500, 1000, 2000, and 5000 users.

 **Note:**

You can extend the license validity period by contacting Avaya support (www.avaya.com/support).

Secure Portable Office License

To enable the Secure Portable Office (SPO) feature, you must obtain a license key from Avaya.

For more information on SPO feature, see [Secure Portable Office \(SPO\) Client](#) on page 305.

Obtaining Licenses

For more information about obtaining licenses and applying them to the device, see <http://support.avaya.com>.

*** Note:**

The keycode can be applied to the device through BBI. For additional information, see BBI Application Guide.

License Key

To obtain the license key from Avaya, you must provide the MAC address of each VPN Gateway device on which a VPN license is installed (see instructions on next page). This applies to all available licenses.

License Pool (SSL and IPsec Users)

All VPN Gateways that run in a cluster contribute to the license pool. For example, if the cluster consists of two VPN Gateways, where each device has an IPsec license installed that is valid for 500 users, the cluster shares a license pool of 1000 concurrent IPsec users. When the remote user connects to the AVG cluster, a license for the current user session is allocated from the license pool-not from a specific VPN Gateway. The distribution of users on the two devices is independent of the licenses installed on each device.

If a user logs on through IPsec and no IPsec user license is available, an SSL user license will instead be used (if available).

If a Cluster Member Fails

If a cluster member fails, it continues to contribute to the license pool for a period of 30 days. After that, the cluster is no longer be aware of the license loaded to the faulty device. Using

the preceding example, the license pool can consist only of a 500 user license after the 30 days grace period.

If the cluster consists of three VPN Gateways – one with a 1000 user license and the two other devices with the default 50 user license – the license pool will consist only of a 100 user license (after 30 days) if the VPN Gateway with the 1000 user license fails.

An alarm message (see step [3](#) on page 30) will be generated if the devices in a cluster do not have the same license loaded. In the SSL/IPsec user license case, you can ignore this message safely. In the Secure Service Partitioning case however (see following sections), the licenses must be the same on all devices.

Also see the section [If a Cluster Member Fails](#) on page 32.

Secure Portable Office

The Secure Portable Office feature does not work properly in a cluster unless this feature is enabled by license key on every device in the cluster.

Secure Service Partitioning

The Secure Service Partitioning feature will not work properly on all devices unless this feature is unlocked on every VPN Gateway in the cluster, using a unique Secure Service Partitioning license key.

Hardware Limits

Loaded licenses in a cluster might add up to a high number of allowed users. Each device type, however, has a hardware limit that determines how many concurrent user sessions it can accept.

- Avaya VPN Gateway 3090–VM: 5000 SSL concurrent users. The single node host license limit is 5000.

 **Note:**

The 3090-VM requires the Enterprise VMware license or VMware ESX 4.1 and above license to enable 8-core in Guest OS environment.

- Avaya VPN Gateway 3070–VM: 1000 concurrent users.
- Avaya VPN Gateway 3050–VM: 250 concurrent users

For example, if the cluster consists of two Avaya VPN Gateways, each with a 5000 user license, make sure that the cluster is properly load balanced to avoid an uneven session distribution.

Obtaining the MAC Address

1. Connect to the VPN Gateway through serial cable or through Telnet/SSH to the AVG real IP address.
2. Find out the AVG MAC address from the Information menu.

If you install or join a new VPN Gateway, you can find the MAC address from the Setup menu by entering `/info/local`.

3. Contact Avaya Support and provide the MAC address. You will be given the license key for the desired feature/number of users.

Contact information is in [Customer service](#) on page 13.

Paste the License Key

1. To paste the license key, go to the iSD Host menu for the desired VPN Gateway.

```
>> Main# cfg/sys/host
Enter Host number: 1
>> iSD host 1# license

Paste the license, press Enter to create a new line,
and then type "..." (without the quotation marks)
to terminate.
> -----BEGIN LICENSE-----
> U2FsdGVkX19HJpnd8KL4iImtRzKvZy
> +iANDzxog22+vq6Qx4aawSl4EUQio6T3Pq
> > 1XYlsMMFJpYW/vl3osvNPXhzcLV2E7hNHlqirkyx5aLHY
> +2xYpK/BTTrMZfJbbhR
> > 86OQvdBMyer53xgq6Kk/5BvoFcQYvEC/
> yWrKyrMzr4XPtAr3qmuX8UxLqJwA2de6
> > 0x7PUrp6tVI=
> -----END LICENSE-----
> ...
License loaded
```

2. To load a license key to another VPN Gateway in the cluster, go to the Host menu for that device and paste the license key in the same way.

This must be another license key, because each key is generated from the VPN Gateway MAC address.

3. For the license keys to take effect, log out from the CLI and log back in.

*** Note:**

If there are several VPN Gateways in the cluster and they do not have the same license loaded, a warning message will be generated.

You can view the message in the Alarm list and the System log.

```
>> Main# info/events/alarms

** (alarm) Active Alarm List
*****
---
Id: 1
Severity: warning
Name: license
Time: Wed 2006-04-28,16:27:21+0100
Sender: license_server
Cause: license_not_loaded
Description: "All iSDs do not have the same license
loaded"
```

Managing New IPSec Logins during Maintenance

The option "Disable new IPSec logins" allows maintenance of the VPN Gateway without forcing current users to log-off. During the maintenance interval, new IPSec logins to the node can be redirected to the other nodes.

1. Select the configured Host.

```
/cfg/sys/host <host_ID>
```

The cluster host menu is displayed.

```
[Cluster Host 1 Menu]
type          - Set type of the host
ip            - Set IP address
sysName       - Set sysName
sysLocatio    - Set sysLocation
license       - Set License
gateway       - Set default gateway address
routes        - Routes menu
ipsec         - Host IPsec menu
interface     - host interface menu
port          - host port configuration menu
ports         - Display physical ports
hwplatform    - Display hardware platform
halt          - Halt the host
reboot        - Reboot the host
```

```
delete      - Remove Cluster Host
```

2. Select the IPsec menu item.

```
>> Cluster Host <host_ID> # ipsec
```

The IPsec menu is displayed.

```
[Host IPsec Menu]
dfbit      - Set IPsec DF bit
blocklogin - Block IPsec logins
```

3. Set the blocklogin state.

```
Host IPsec# blocklogin
Current value: off
Permit/Block IPsec logins:
on   off
Permit/Block IPsec logins:
```

If a Cluster Member Fails

If a cluster member fails it will continue to contribute to the license pool for a period of 30 days. When the 30 days expires, the cluster will no longer be aware of the license loaded to the faulty device. If the device must be replaced, proceed as follows:

1. Contact your reseller at Avaya for information about replacing a device and license.

After you obtain a new device and a new license, continue with the following steps.

2. Dump the information configured for the faulty device (host).

```
>> Main# cfg/sys/host 2/dump

Dump private/secret keys (yes/no) [no]: <press ENTER
to accept>

Collecting data, please wait...
```

3. Copy and save the data to a text editor.
4. Delete the faulty host from the cluster.

```
>> Main# cfg/sys/host 2/delete  
Cluster Host 2 will be deleted when changes are  
applied.
```

5. Connect the new device to the network and join it to the cluster.

For instruction to join an AVG to an existing cluster, see the "Initial Setup" chapter in the User's Guide. Assign the IP address of the failed device to the new device.

6. Load the license to the new device as described in the previous section.

You need a new license because the new device has a different MAC address.

7. To restore the host configuration, paste the configuration that was previously dumped.

```
>> Main# cfg/sys/host 2/paste  
Enter global key/secret import password:  
<press ENTER to skip>  
>> Cluster Host 1#  
<paste the configuration at this prompt>
```

8. Apply the changes.

Chapter 4: Clientless Mode

This chapter describes how to configure the Avaya VPN Gateway (AVG) for clientless mode. Clientless mode requires no reconfiguration of the client web browser, nor do you need to install any VPN client software on the remote user's machine.

This section describes the flow when a remote user requests a resource on the intranet. To access the Portal, the remote user types the AVG's Portal IP address or fully qualified domain name in the available browser. The Portal's capabilities are shown in the Intranet cloud in the following figure.

To maintain the AVG configuration (for example, add users, change access rules etc), the operator connects to the AVG's management IP address (MIP). To access the command line interface (CLI), the operator connects to the MIP through Telnet or SSH. To access the browser-based management interface (BBI), the operator connects to the MIP through the browser.

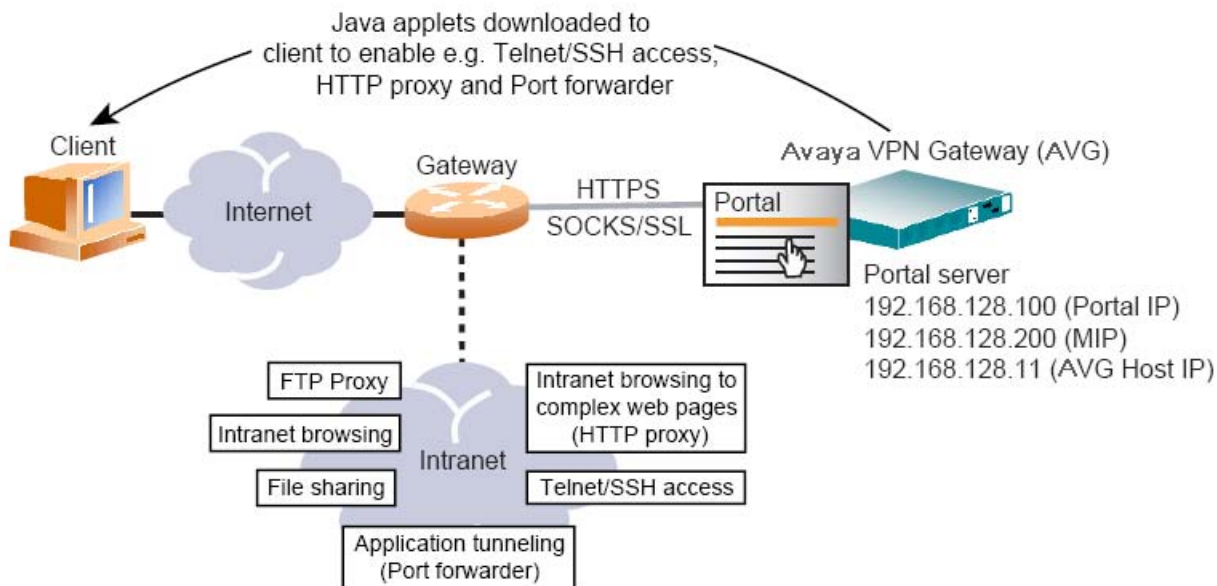


Figure 1: VPN in Clientless Mode

Configure VPN from Wizard Settings

If you run the VPN Quick Setup wizard during the initial setup, the AVG cluster is automatically configured with all the required settings for a fully functional VPN Portal (clientless mode), and support for the Avaya SSL VPN client (transparent mode). This setup is mainly for testing, but you can easily let your proper VPN evolve from these settings.

Configure the following settings:

- A VPN with the number 1.
- A server of the portal type with a Portal IP address. This is the address to which the remote user connects to access the Portal. The portal server is in stand-alone mode, which is required when using the VPN feature without a Application Switch.
- Install a test certificate to use with the portal server.
- You can add one or several domain names to the DNS search list, which means that the remote user can enter a short name in the Portal's URL and host name fields (for example, `inside` instead of `inside.example.com` if `example.com` is added to the search list).
- The authentication method to Local database and you have one test user configured. The test user belongs to a group called

`trusted`

, whose access rules allow access to all networks, services, and paths.

After you test the portal, change the settings made by the wizard. You probably want more than one user and one access group configured and you must define the relevant access rules for each group. Substitute the test certificate for a real certificate, signed by a CA authority. Furthermore, you may want to use an external authentication database instead of or, as a complement, to the local database.

The following sections describe how to import a signed server certificate, map it to the VPN, and configure a DNS name.

For information about how to perform an initial setup, see the "Initial Setup" chapter in the *Users Guide*.

Import Signed Certificate to the AVG

This instruction assumes that you have a real server certificate available, signed by a CA authority. You can import the certificate to the AVG as a file, through the CLI, or paste into the CLI as text.

1. Specify the certificate number to use when importing the server certificate.

The VPN Quick Setup wizard assigns certificate number 1 to a self-signed test certificate. You can either overwrite the test certificate by specifying certificate number 1 for the new certificate or create a new certificate number (recommended).

```
# /cfg/cert 2
Creating Certificate 2
```

2. Import the new certificate.

```
>> Certificate 2#import

Select protocol (tftp/ftp/scp/sftp) [tftp]:ftp

Enter hostname or IP address of server:192.168.128.1

Enter filename on server:new_cert.pfx

Retrieving new_cert.pfx from 192.168.128.1

FTP User (anonymous):john

Password:<password>

received 2392 bytes

Enter pass phrase:<passphrase if required>

Key added.

Certificate added.

Use 'apply' to activate changes.
```

3. Apply the changes.

```
>> Certificate 2#apply

Changes applied successfully.
```

The certificate is now imported to the VPN Gateway and you can map it to the server of the desired VPN.

The "Certificates and Client Authentication" chapter in the *Users Guide* provides all the information you need to generate certificate signing requests, add certificates to the AVG, generate and revoke client certificates, and configure the AVG to require client certificates.

Map Signed Server Certificate to VPN

When you import the signed server certificate to the AVG, map it to the portal server of the desired VPN. The certificate (1) that currently maps to your portal server is a test certificate. Type the number that corresponds to the signed certificate that you added to the AVG.

```
# /cfg/vpn 1/server/ssl

>> SSL Settings#cert

Current value: 1
```

```
Enter certificate number: (1-1500)
```

```
2
```

Assign a Fully Qualified Domain Name

Assign a Fully Qualified Domain Name (FQDN) to the portal server. Register the domain name you specify in DNS to resolve to the virtual server IP address you specified in VPN quick setup wizard. The FQDN for the portal server corresponds to the URL that remote users type in the address field of their web browser to access the Portal login page.

```
# /cfg/vpn 1/server  
  
>> Server 1#dnsname  
  
Current value:" "  
  
Enter fully qualified DNS name of VIP:vpn.example.com  
(example of FQDN)
```

After you create your portal, you must update your DNS server, configure one or more authentication methods, add user groups with access rules, configure group links, and customize the web Portal page. You may also want to configure the Tunnel Guard client security feature and HTTP to HTTPS redirection.

For a list of remaining tasks and where to find the necessary documentation, see [Update DNS Server](#) on page 41

Configure VPN from Scratch

If you did not run the VPN quick setup wizard during the initial setup, this section describes how to configure the VPN from scratch. Even if you did run the VPN quick setup wizard, reading through this section helps you understand which settings you need for a fully functional Portal.

Import Signed Certificate

For instructions to import a signed certificate to be used as the AVG server certificate, see [Import Signed Certificate to the AVG](#) on page 36

Create a VPN

1. Create a VPN and enter the Portal IP address.

This step creates a VPN. You can have several VPNs, where each VPN identifies a unique Portal. Thus, you can have several different Portals, for example, with different layout and links. A portal server is automatically created along with the VPN. The portal server is connected to the Portal IP address(es) and listens to TCP port 443 (https) by default.

Creating several VPNs is especially useful to service providers (ISPs). For hosting customers with their own Portals, which are securely separate from one another (see [Secure Service Partitioning](#) on page 313).

```
# /cfg/vpn 1

Creating VPN 1

VPN name: Name

Enter server ips (comma separated):<Portal IP address>
```

2. Enable standalone mode.

This step sets the portal server to standalone mode, which is required if the VPN Gateway is not connected to a Application Switch.

```
>> VPN 1#standalone

Current value: off

Standalone mode (on/off):on
```

3. Specify the certificate to be used by the portal server.

You are prompted to type the index number of an existing certificate. To view all certificates currently added to the AVG cluster, press TAB. For more information about how to add a certificate to the AVG, see the "Certificates and Client Authentication" chapter in the *Users Guide*.

```
>> VPN 1#server/ssl/cert

Current value: unset

Enter certificate number: (1-1500)

1
```

*** Note:**

If the certificate you specify is a chained certificate, you must first add the CA certificates up to and including the root CA certificate, and then specify the CA certificate chain of the server certificate. For more information about how to construct the server certificate chain, see the **cachain** command in the *Command Reference*.

4. Assign a Fully Qualified Domain Name (FQDN) to the portal server.

Register the domain name you specify in DNS to resolve to the virtual server IP address you specified in the previous step. The FQDN for the portal server corresponds to the URL that remote users will type in the address field of their web browser to access the Portal login page when the VPN is fully deployed.

```
>> SSL Settings#../dnsname

Current value:

" "

Enter fully qualified DNS name of VIP:vpn.example.com
(example of FQDN)
```

5. Configure the DNS settings for the portal server.

Specify a DNS search domain. The search domain(s) you specify is automatically appended to the host names a remote user types in the various address fields on the Portal (if a match is found).

```
>> Server#../adv/dns

>> DNS Settings#search

Current value: " "

Enter search domains (separated by comma):example.com
```

6. Apply your changes.

```
>> DNS Settings#apply

Changes applied successfully
```

After you create the portal, you must update your DNS server, configure one or more authentication methods, add user groups with access rules, configure group links, and customize the web Portal page. You may also want to configure the Tunnel Guard client security feature and HTTP to HTTPS redirection.

Update DNS Server

Update the local DNS server with the domain name used for the VPN, and be configured to perform reverse DNS lookups.

Select Authentication Method(s)

There are several external authentication methods available (RADIUS, LDAP, NTLM, Netegrity SiteMinder, RSA SecurID, and RSA ClearTrust). You can configure the AVG cluster for client certificate authentication. To test the Portal, configure the local database authentication method with one or several test users. For more information about how to configure authentication methods, see [Authentication Methods](#) on page 117.

Configure User Access Groups and Access Rules

The user's group membership determines which resources can be accessed from the Portal. The access rules associated with a group govern which networks, services, and paths the group member has access to. See [Groups, Access Rules and Profiles](#) on page 157 for configuration instructions.

Configure Group-Specific Linksets

You can configure hypertext links to intranet and Internet web pages and server applications. Links appear on the Portal's Home tab. Which links appear for the logged on user depends on the user's group membership and which linksets map to the user group. For instructions to configure linksets and links, see [Group Links](#) on page 203.

Configure Access through the Net Direct Client

Net Direct eliminates the need to install VPN client software on all remote user machines. Net Direct installs a slim version of the Avaya SSL VPN client, the Net Direct client, when the remote user clicks a Net Direct link on the Portal's **Home** tab. When the user exits the Portal session, the exit of Net Direct depends upon the "portal bind". For instructions to configure access using the Net Direct client, see [Net Direct](#) on page 87.

Configure Tunnel Guard

Tunnel Guard verifies whether the required components (for example, executables, DLLs, and configuration files) are installed and active on the remote user's machine. For instructions on configuring Tunnel Guard, see [Configure Tunnel Guard](#) on page 269.

Enable WholeSecurity Scan

Using the Symantec WholeSecurity Confidence Online software, perform a scan of client PCs before the user logs on to the VPN. When remote users connect to the VPN, they are automatically redirected to a WholeSecurity Confidence Online server on the intranet. The Confidence Online software is downloaded to the endpoint machine and performs a scan to identify any eavesdropping threats, including Trojan horses, remote controls, keystroke loggers, and worms. See [WholeSecurity](#) on page 293.

Customize the Portal

Customize the Portal with respect to logo, language, color, and static texts. For instructions to customize the Portal, see [Customize the Portal](#) on page 249.

HTTP to HTTPS

To configure the AVG to automatically transform an HTTP client request to the required HTTPS request, see [HTTP to HTTPS Redirection](#) on page 265.

DNS Round Robin Load Balancing

The example in this section uses round-robin load balancing performed by a DNS server. To distribute client traffic evenly between two VPN Gateways in a cluster.

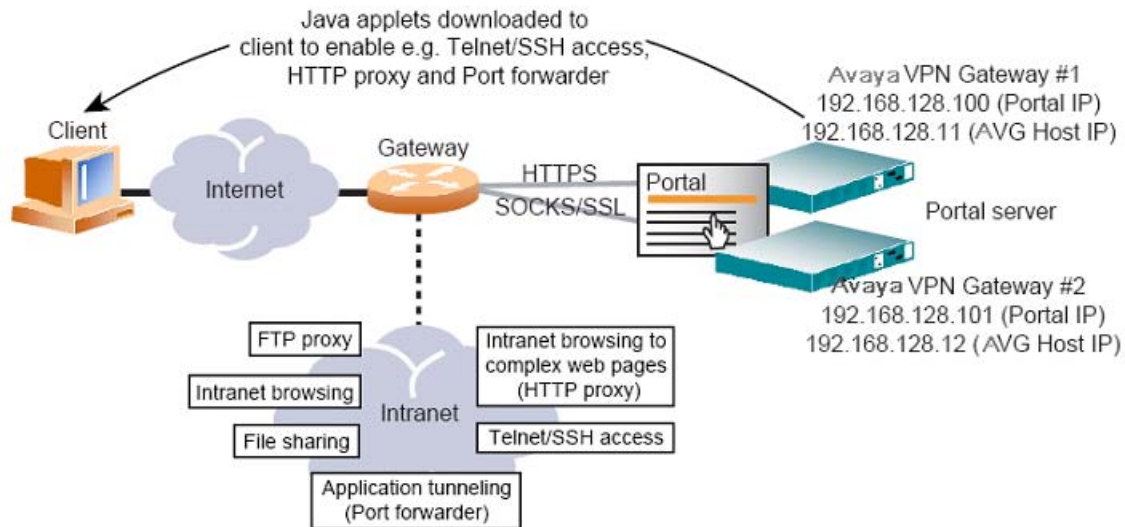


Figure 2: DNS Round Robin Balancing of two AVGs

To realize DNS round-robin load balancing, you typically add the same number of Portal IP addresses as VPN Gateways in the cluster. For instructions to join a VPN Gateway to an existing cluster, see the "Initial Setup" chapter in the *Users Guide*.

In the DNS server configuration, specify that the fully qualified domain name assigned to the Portal resolves to the Portal IP addresses configured with the `/cfg/vpn # /ips` command. You must also configure the DNS server to perform round robin load balancing and reverse DNS lookups.

If one VPN Gateway in the cluster fails the virtual server IP address currently assigned to that VPN Gateway migrates to another AVG in the cluster. This means that traffic directed to that IP address (by means of the DNS round-robin configuration) still reaches the destination.

Add IP Addresses

1. Add a new IP address to the VPN.

Add as many IP addresses as there are VPN Gateways in the cluster. The IPs are floating, that is, belong to the cluster rather than to one AVG.

```
# /cfg/vpn 1/ips
Current value: 192.168.128.100
Enter server ips (comma separated):
192.168.128.100,192.168.128.101
```

2. Apply the changes.

```
>> VPN 1#apply
```

Rewriting portal domain name

Portal Domain Name rewrite is available only on a DNS configuration. Portal Domain Name rewrite provides persistent connection within a cluster to support intercluster load balance. After the initial contact, the persistent connection is available. On failover, the intercluster session is not available. To maintain persistent connection when multiple AVG boxes are clustered separately in different locations, the administrator can configure the secondary DNS name associated to each cluster. After the initial contact, the AVG automatically replaces the primary DNS with the secondary DNS and further packets reach the same cluster.

To configure the secondary DNS in each cluster, perform the following:

1. Specify the rewrite domain name.

```
>> Main# cfg/vpn 1/server/portal/dnrewrite  
Current value: ""  
Enter a FQDN to rewrite to:
```

2. Apply changes.

```
>> Portal Settings# apply
```

VPN with Application Switch

When the VPN Gateway is used for SSL acceleration, it typically requires support of a Application Switch for traffic redirection. With this setup, do not enable stand-alone mode. You can assign only one VIP to the virtual SSL server and map this VIP to the Application Switch.

This configuration example, as shown in the following figure, is based on the assumption as shown in the following is based on the assumption that you have two VPN Gateways in the cluster, and that the AVGs connect to a Application Switch.

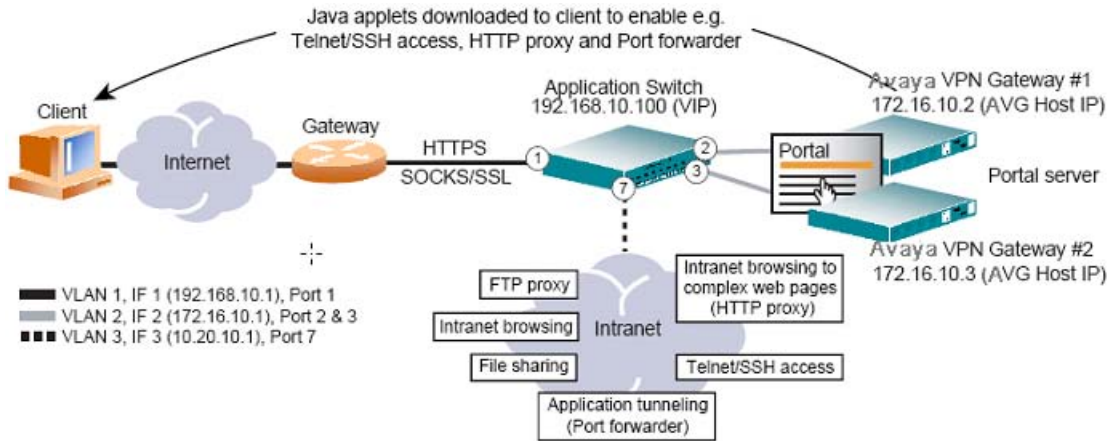


Figure 3: VPN in Clientless Mode with Application Switch

Configure the AVG

1. Disable standalone mode if it is currently enabled.

```
# /cfg/vpn 1/standalone

Current value: on

Standalone mode (on/off):off
```

2. Assign a virtual server IP (VIP) address to the portal server.

This step binds the portal server to the IP address of the virtual server that handles client connection requests to the Portal. When the AVG connects to a Application Switch, you must define the virtual server on the switch.

```
>> VPN 1#ips

Current value: <not set>

Enter server ips (comma separated):192.168.10.100
```

3. Apply the changes.

```
>> VPN 1#apply
```

Configure the Application Switch

Create the Necessary VLANs

In this configuration, three VLANs are present: VLAN 1 for the Application switch that connects to the Internet, VLAN 2 for the AVG devices, and VLAN 3 for the intranet. Because VLAN 1 is the default, only VLAN 2 and VLAN 3 requires additional configuration.

1. Configure VLAN 2 to include Application Switch Application Switch ports leading to the AVG devices.

```
# /cfg/vlan 2

>> VLAN 2#add 2

Port 2 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]:Y

>> VLAN 2#add 3

Port 3 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]:Y

>> VLAN 2#ena
```

2. Configure VLAN 3 to include the Application Switch port leading to the intranet.

```
# /cfg/vlan 3

>> VLAN 3#add 7

Port 7 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]:Y
```

3. Disable Spanning Tree Protocol (STP) for the AVG ports 2 and 3.

```
# /cfg/stp/port 2

>> Spanning Tree Port 2#off

>> Spanning Tree Port 2#../port 3

>> Spanning Tree Port 3#off
```

Configure One IP Interface for Each VLAN

You can reverse the order of the first two commands (**addr** and **mask**) in the following example. By entering the mask first, the Application Switch automatically calculates the correct

broadcast address. The calculated broadcast address appears immediately after you provide the IP address of the interface, and is applied with the other settings when you run the **apply** command.

1. Configure an IP interface for client traffic on the Application Switch with VLAN 1.

```
# /cfg/ip/if 1
>> IP Interface 1#addr 192.168.10.1
>> IP Interface 1#mask 255.255.255.0
>> IP Interface 1#broad 192.168.10.255
>> IP Interface 1#vlan 1
>> IP Interface 1#ena
```

2. Configure an IP interface for AVG traffic with VLAN 2.

```
# /cfg/ip/if 2
>> IP Interface 2#addr 172.16.10.1
>> IP Interface 2#mask 255.255.0.0
>> IP Interface 2#broad 172.16.255.255
>> IP Interface 2#vlan 2
>> IP Interface 2#ena
```

3. Configure an IP interface for intranet traffic with VLAN 3.

```
# /cfg/ip/if 3
>> IP Interface 3#addr 10.20.10.1
>> IP Interface 3#mask 255.255.255.0
>> IP Interface 3#broad 10.20.10.255
>> IP Interface 3#vlan 3
>> IP Interface 3#ena
```

4. Apply the changes.

```
# apply
```

Make sure you configure the VPN Gateways to use the IP address of IP interface 2 on VLAN 2 as the default gateway. For more information about gateway configuration, see the **gateway** command under "System Configuration" in the *Command Reference*.

Configure the AVG Load Balancing Parameters

Set and enable the IP addresses of the VPN Gateways, and create a group in the switch for load balancing.

1. Define each VPN Gateway as a real server and specify the real server IP address.

The real server IP (RIP) address that you specify is the IP address assigned to each VPN Gateway during the initial setup. To view the real IP address of each VPN Gateway in the cluster, you can use the **/info/isdlist** command.

```
# /cfg/slb/real 1
>> Real server 1#rip 172.16.10.2
>> Real server 1#ena
>> Real server 1#../real 2
>> Real server 2#rip 172.16.10.3
>> Real server 2#ena
```

2. Create a real server group and add the real servers (the VPN Gateways) to the group.

```
# /cfg/slb/group 1
>> Real server group 1#add 1
>> Real server group 1#add 2
```

3. Set the load balancing metric and health check type for real server group 1.

```
# /cfg/slb/group 1
>> Real server group 1#metric hash
>> Real server group 1#health sslh
```

4. Set and enable the IP address for Virtual Server 1, enable service on port 443, and assign server group 1 (the VPN Gateways) to this service.

The reason that you configure a virtual server is to ensure that the Application Switch responds to the ARP request for the virtual IP address (VIP). You cannot

use server load balancing with AVG because the Portal IP address must be preserved as the destination IP address in the TCP packets. Instead, use a redirect filter (see [Configure Redirect Filters](#) on page 49).

```
# /cfg/slb/virt 1

>> Virtual Server 1#vip 192.168.10.100

>> Virtual Server 1#ena

>> Virtual Server 1#service https

>> Virtual Server 1 https Service#group 1
```

5. Enable client processing on port 1 leading to the Internet.

```
# /cfg/slb/port 1

>> SLB Port 1#client ena
```

6. Turn on Layer 4 processing.

```
# /cfg/slb/on
```

7. Apply the changes.

```
# apply
```

Configure Redirect Filters

1. Create a filter to redirect client HTTPS traffic intended for port 443 on the Virtual Server IP (VIP) address.

When this filter is added to the switch port leading to the Internet, incoming HTTPS traffic destined for the virtual server IP address is redirected to the VPN Gateways in real server group 1.

```
# /cfg/slb/filt 100

>> Filter 100#dip 192.168.10.100

>> Filter 100#dmask 255.255.255.255

>> Filter 100#proto tcp

>> Filter 100#dport https

>> Filter 100#action redir
```

```
>> Filter 100#group 1
>> Filter 100#rport https
>> Filter 100#ena
```

2. Create a default filter to allow all other traffic.

```
# /cfg/slb/filt 224
>> Filter 224#sip any
>> Filter 224#dip any
>> Filter 224#proto any
>> Filter 224#action allow
>> Filter 224#ena
```

3. Add the filters to the client port leading to the Internet.

This step adds the HTTPS redirect filter and the default allow filter to the client port leading to the Internet.

```
# /cfg/slb/port 1
>> SLB Port 1#add 100
>> SLB Port 1#add 224
>> SLB Port 1#filt ena
```

4. Apply and save the Application Switch Application Switch configuration changes.

```
# apply
# save
```

Chapter 5: The Portal from an End-User Perspective

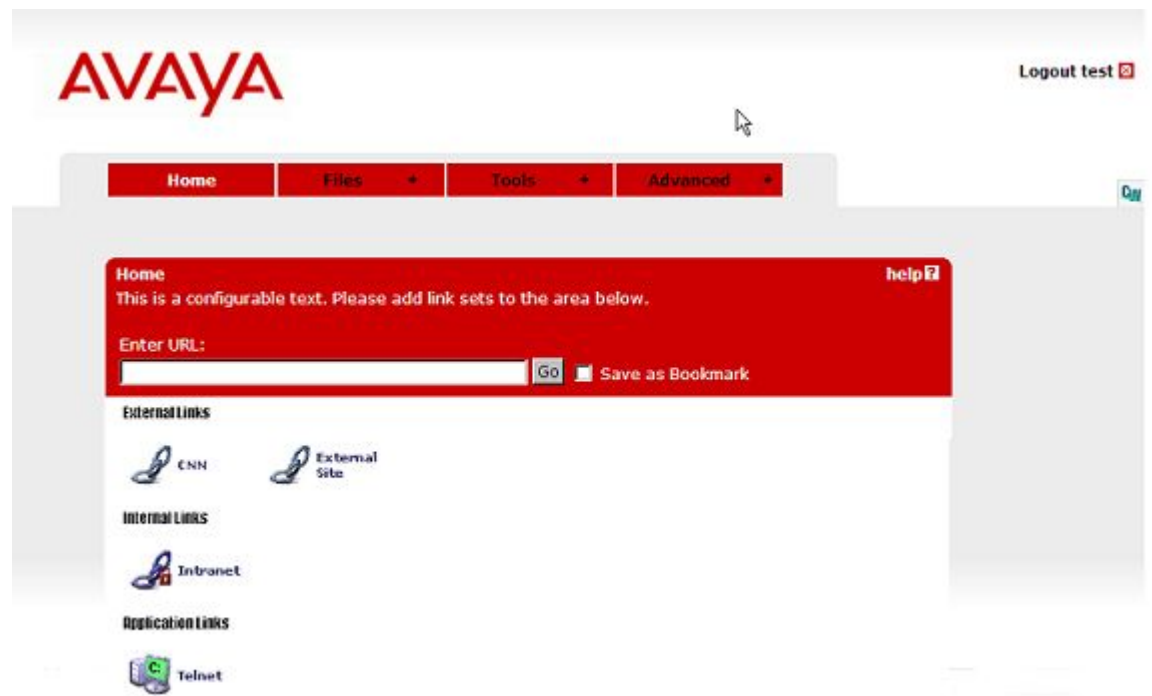
This chapter describes the Portal from an end-user perspective. It includes step-by-step instructions to access intranet resources in clientless mode, for example, through the Portal. For instructions to change the Portal look and feel, see [Customize the Portal](#) on page 249.

Accessing the Portal Web Page

In clientless mode, no VPN client need to be installed on the remote user's machine. Instead, the remote user accesses intranet resources through a secure SSL connection through the Portal.

In the available web browser, enter the domain address (for example, <https://vpn.example.com>) or IP address (for example, <https://10.1.82.146>) to the AVG cluster.

The Portal page:



The Login page's look and feel can be customized with respect to language, logo, colors and static text (see [Customize the Portal](#) on page 249).

1. To log in, enter the user name and password in the Username and Password fields, respectively.

The user's credentials are checked against a previously configured user record in the AVG local authentication database or in an external authentication database (for example, RADIUS, LDAP, SiteMinder, NTLM, RSA SecurID, or RSA ClearTrust).

*** Note:**

If a secondary authentication method is configured, an extra password field appears. The first field (Passcode) is used to authenticate to the primary authentication scheme and the second field (Password) is used to authenticate to the secondary authentication scheme. This feature primarily supports single-sign on to backend servers if the first authentication method is token-based or uses client certificate authentication. For more information, see the `/cfg/vpn #/aaa/auth #/adv/secondauth` command in the *Command Reference*.

*** Note:**

The RSA SecureID New Pin Mode is not supported as Secondary authentication.

Configuring authentication methods is described in [Authentication Methods](#) on page 117.

2. To direct the remote user to a specific authentication method (if several authentication methods are configured for the AVG), the corresponding option can be selected in the Login Service list box.

To configure a suitable display name for the authentication method and to make it appear in the Login Service list box, use the `/cfg/vpn #/aaa/auth #/display` command (see [Authentication Methods](#) on page 117).

*** Note:**

If no display name is configured for any of the authentication methods, the Login Service list box does not appear.

3. Click **Login**.

The Portal web page is displayed.

The Portal Web Page

After the user is successfully authenticated, the Portal web page appears.






The Portal web page consists of various tabs from which the remote user can access intranet resources. The access rules associated with the logged-on user groups determine which resources are available. See [Groups, Access Rules and Profiles](#) on page 157.

You can customize the Portal's look and feel with respect to language, logo, company name, colors and static text (see [Customize the Portal](#) on page 249).

Java Applet/ActiveX Control Icons

The icons to the right of the Portal tabs indicate whether certain Java applets and ActiveX controls are active. The following table shows the Java Applet/ActiveX Control Icons.

Table 1: Java Applet/ActiveX Control Icons

	Tunnel Guard running and checks succeeded.
	Tunnel Guard running and checks failed.
	Citrix Metaframe support is enabled.
	The Avaya IE cache wiper is running.
	The Net Direct agent is enabled on the VPN Gateway.

Tunnel Guard

Tunnel Guard is a Java applet that verifies whether components (for example, executables, DLLs and configuration files) are installed and active on the remote user's machine. For instructions on configuring Tunnel Guard, see [Configure Tunnel Guard](#) on page 269.

Citrix Metaframe Support

If Citrix Metaframe support is enabled, a Java applet starts at logon. This applet is not visible to the user and provides seamless support for securing Citrix client traffic through the VPN Gateway. The Citrix Metaframe support feature can be used with the Citrix Program Neighborhood as well as Citrix Nfuse, Citrix Web Interface and Citrix Presentation Server application portals through the

internal

or

external

Portal link types. For instructions about how to configure Portal links, see [Group Links](#) on page 203. Citrix Metaframe support is disabled by default, that is, the `/cfg/vpn #/portal/citrix` command is

`off`

.

IE Cache Wiper

The IE cache wiper is an ActiveX control that clears the cache (visited URLs and cached HTML documents) after a Portal session that runs Internet Explorer. The IE cache wiper is enabled by default. The command used to enable/disable the IE cache wiper is `/cfg/vpn #/portal/wiper`.

The Net Direct Agent

The Net Direct agent is an ActiveX control similar to the SSL VPN client, only it does not require manual installation. The Net Direct agent is temporarily downloaded to the remote user's machine and removed when the user exits the session. For instructions to configure the VPN Gateway for use with the Net Direct agent, see [Net Direct](#) on page 87.

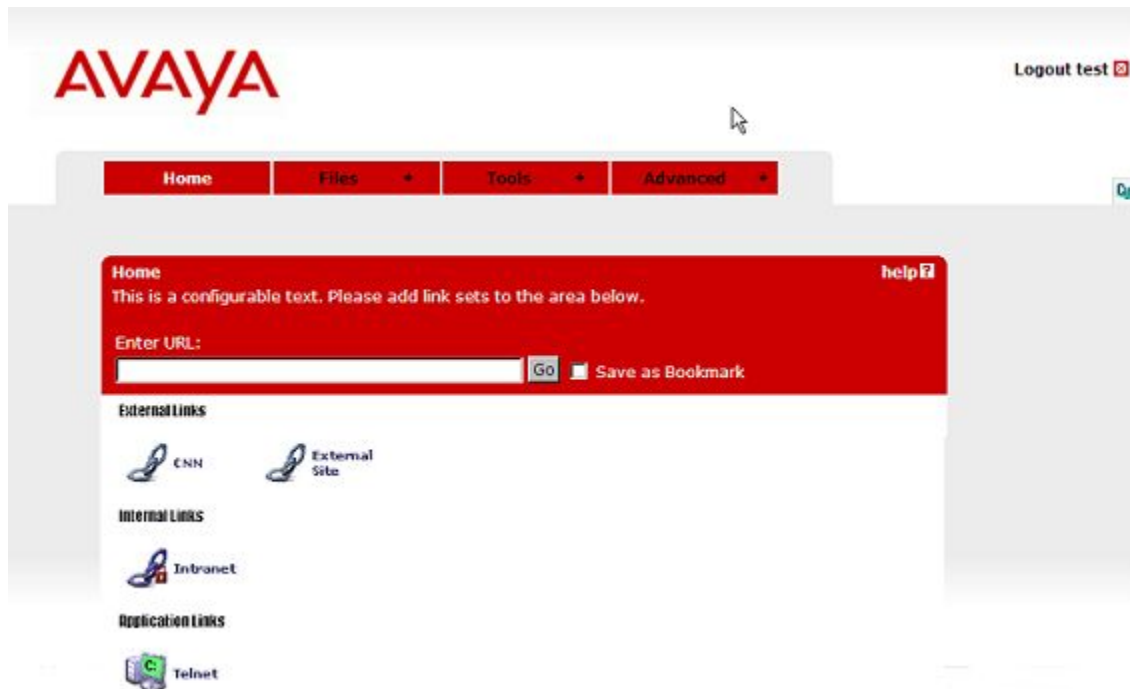
General Capabilities

In clientless mode, the following services are enabled:

- Intranet web browsing.
- Access to SMB (Windows file shares) and FTP file servers.
- Intranet mail access through external web-based solutions, for example, Outlook Web Access.
- Telnet and SSH access to intranet servers through terminal Java applet.
- Handling plugins, Flash and Java applets using HTTP proxy Java applet.
- Secure access to FTP file servers using native FTP client (FTP proxy).
- Port forwarding (application tunneling for third-party applications using a well-defined set of ports) through SOCKS encapsulated in SSL.

The Home Tab

The Home tab is the default Portal tab.



The **Enter URL** field (configurable) provides access to any web server through a secure SSL connection. The user should enter the address (with or without http://) and click **Go**. The client browser sends the request to the VPN Gateway as for example, `http://inside.example.com`. A new browser window appears, but now the request is rewritten with the AVG rewrite prefix (boldface) added, e.g. `https://vpn.example.com/http/inside.example.com`. This way, traffic is secured by the VPN Gateway.

Visited URLs can be saved as bookmarks by selecting the **Save as Bookmark** check box and then clicking **Go** (For more information see [The Tools tab, Edit Bookmarks](#) on page 60).

Links are defined within the context of a particular user access group, which means that all remote users who are members in that group have access to the links you define.

Examples of links are:

- Secure link (through VPN Gateway) or direct link to web page
- Secure automatic logon link to password-protected web page
- Link to FTP or SMB file server
- Application tunnel link (port forwarder) through SOCKS encapsulated in SSL
- HTTP Proxy link (ensures display of web pages linked through plugins, for example, Flash)
- Link to Telnet or SSH terminal servers
- Net Direct link (downloads the Net Direct client)

See [Group Links](#) on page 203 for instructions to configure Portal links.

The Files Tab

The Files tab to access a remote SMB (Windows file share) or FTP file server.

To access the file server, perform the following steps:

1. Enter the host name or IP address of the file server in the Host field and select the desired file server type, that is, SMB (Windows file share) or FTP.
2. To display additional options (see following step), select the More options check box.
3. To limit the view to a specific user's home share folder, enter the user's name in the **[Share]** field (optional). This field is ignored for FTP servers.

To browse to a specific share folder, combine this field with the **[Path]** field (see following step).

4. To limit the view to a specific workgroup, enter the workgroup's name in the **[Workgroup]** field (optional). This field is ignored for FTP servers.
5. To specify a path to a specific folder, enter the desired path in the **[Path]** field. This field is dependent on what is entered in the **[Share]** field.

For example, to browse to the folder `/temp/mystuff` under the share folder `john`, enter `john` in the **[Share]** field and `/temp/mystuff` in the **[Path]** field.

6. To make the file server accessible through a Bookmark (selectable from the Home tab), select **Save as Bookmark**.

For a more detailed explanation of the **Save as Bookmark** option, see [The Tools tab, Edit Bookmarks](#) on page 60.

7. Click **Open**.

Files and folders in the specified folder are displayed by file type icon, file name, size, and date.

*** Note:**

If single sign-on is not allowed (for security reasons), an error message will be displayed. The user can still access the requested file server by entering the Portal password once again in the **Password** field and clicking **Open**.

Domains for which single sign-on should be allowed can be added using the `/cfg/vpn #/aaa/ssodomains/add` command.

- To open a folder, click the folder name or icon.
- To open/download a file from the file server to your computer, click the file name or icon.
- To step up one level in the folder hierarchy, click **Up**.
- To create a new folder on the file server, click **New Folder**. Then enter a folder name in the **Folder name** field. Finally click **Create**.
- To upload a file from your computer to the file server, click **Upload**. Locate the desired file in the window displayed. To upload the file to the current folder, click **Start Upload**.
- To delete a file or folder, select the corresponding check box and click **Delete**.
- To view files and folders as icons, select **icons** instead of **detail** in the list box to the right of the **Delete** option.
- To limit the view to files of a specific format, enter the desired file extension (for example, `.txt`) after the * (asterisk) in the **Filter** field and press ENTER.
- To exit the file server session, select the session in the **File sessions** area and click **Close Session**.
- To add a new file server session, click **New Session**.

To simplify access, a link to the desired file server can be defined on the **Home** tab.

The Tools Tab, System Information

To view information about the current version, client information (for example, login name and browser) and so on, select **System Info** on the **Tools** tab. The summarized information

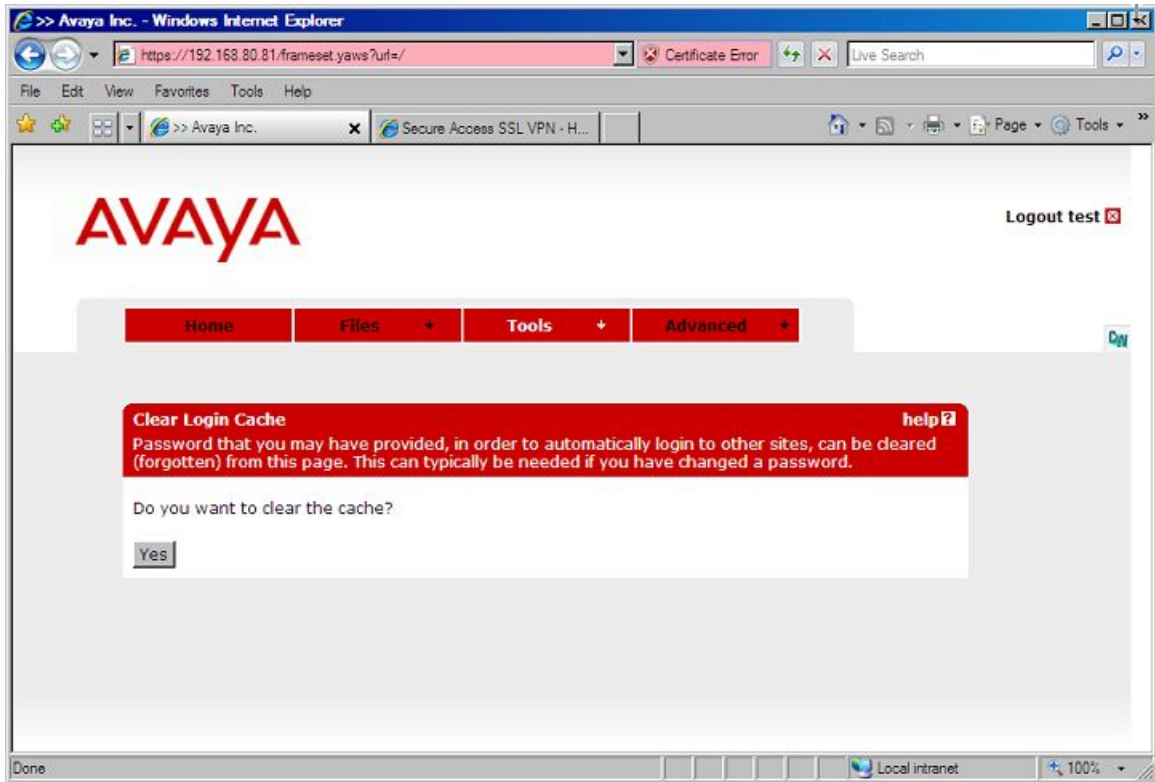
displayed on the System Information form provides an easy way for the user to obtain the relevant system data, for example, when in contact with Support or Helpdesk personnel.



The System information form also includes an option to perform a bandwidth test. The result is displayed in Mb/s.

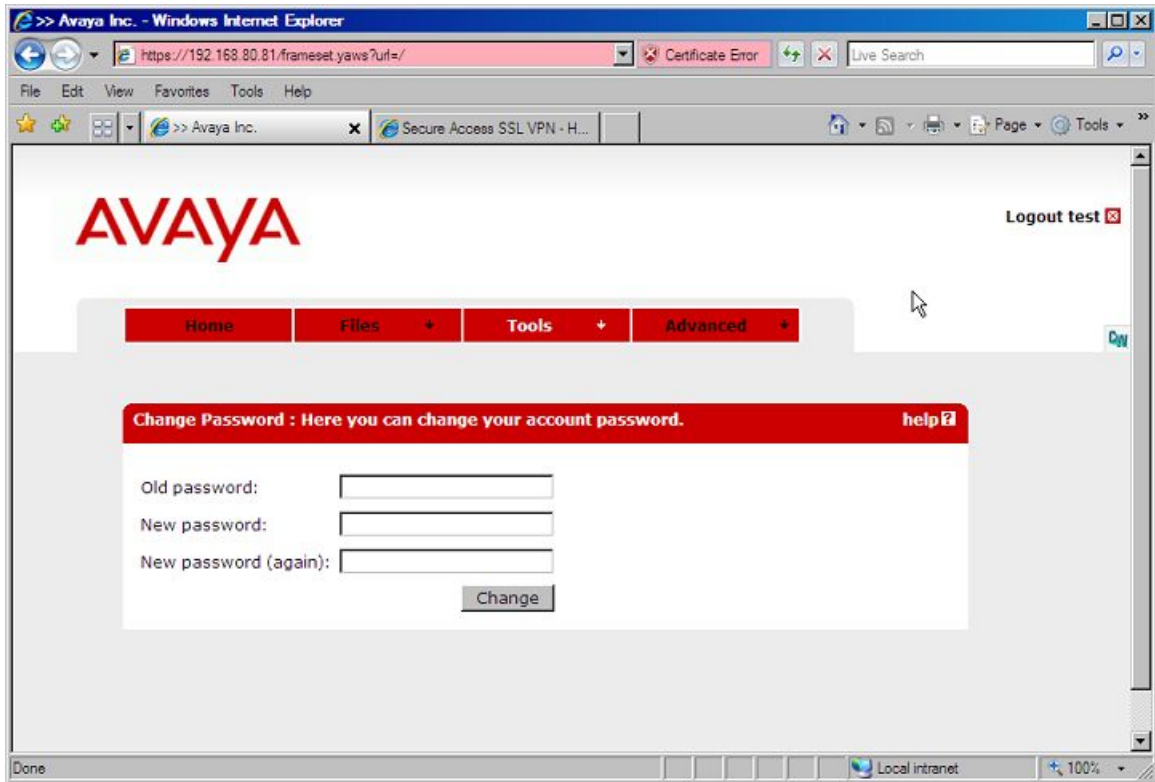
The Tools tab, Clear Login Cache

By selecting **Clear Login Cache** on the **Tools** submenu, the remote user has the option to clear the AVG system's cache from any kind of login information supplied during a Portal session.



The Tools tab, Change User Password

The **Change User Password** option on the **Tools** submenu lets the remote users to change their Portal password.

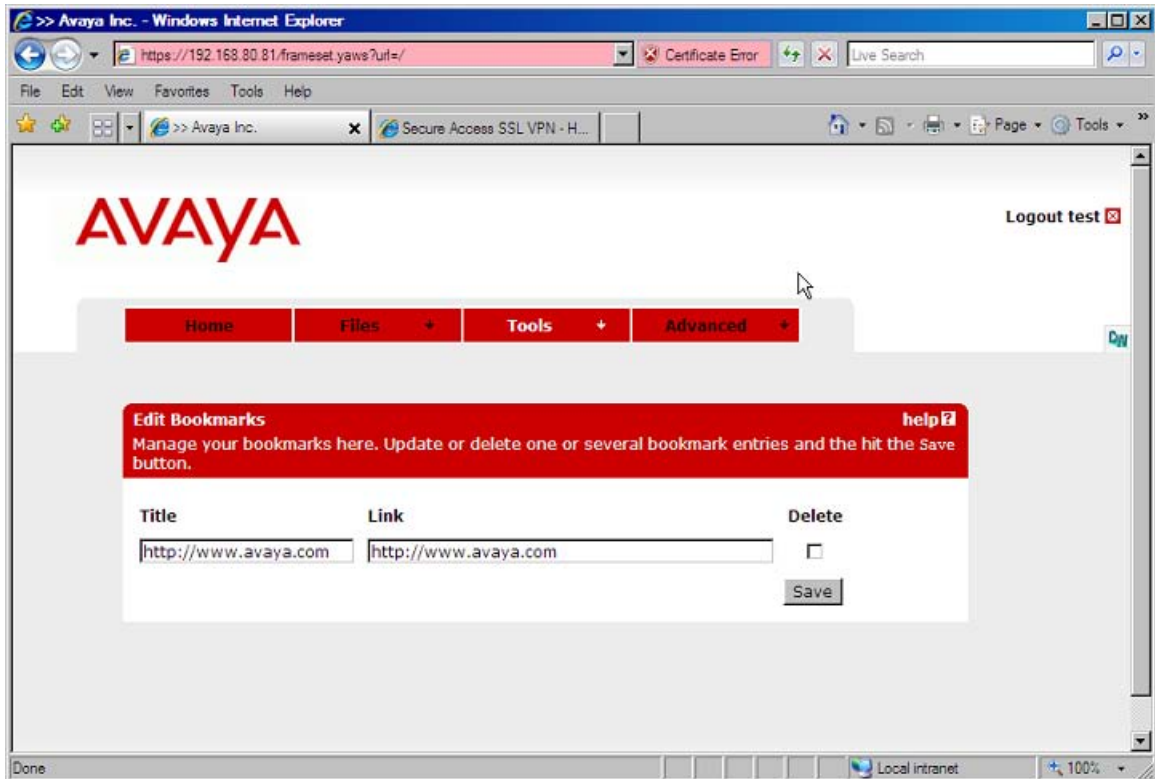


*** Note:**

This only applies if the user has logged in through the local database authentication method, that is, their password stored in the VPN Gateway's local database.

The Tools tab, Edit Bookmarks

The Tools tab also includes an option to edit previously saved bookmarks. URLs entered on the **Home** tab as well as file server information entered on the **Files** tab can be saved as bookmarks.



Saving bookmarks from one session to another is only supported for users stored in an LDAP/Active Directory database. User preferences (such as bookmarks and login information supplied to other web servers during the Portal session) are saved to an attribute in Active Directory called `isdUserPrefs`.

To enable the User Preferences feature, you should enable the CLI command `/cfg/vpn #/aaa/auth #/ldap/enauserpre`. You should also add the `isdUserPrefs` attribute to Active Directory (see Appendix H in the *User's Guide* for instructions).

Saved bookmarks can later be selected in the **Go to** list box on the Portal's Home tab.

The Tools Tab, Change Language

You can select the language themselves. The portal will automatically try to select the language for the user based on the default language set in the browser. The user will also be able to switch languages manually.

The Full Access Page

The **Full Access** page (select **Full Access** on the **Access** tab) provides a way for the users to launch their VPN client (if any) from within the Portal. Because the user has already logged in to the Portal, no further login to the VPN is required.

A VPN client connection enables the user to request resources as if working from within the intranet, that is, no (further) Portal interaction is required. Supported VPN clients are the Avaya IPsec VPN client (formerly the Contivity VPN client), the Avaya SSL VPN client and the Net Direct client.

The **Access** tab is not displayed on the Portal by default, nor is VPN client access enabled by default. Follow the instructions in [Transparent Mode](#) on page 355 and [Net Direct](#) on page 87 respectively to enable access to the VPN from the **Access** tab, using the IPsec/SSL VPN clients and/or the Net Direct client.

To start a VPN client from the Access tab, the user should do the following:

1. Click the **Yes** button.

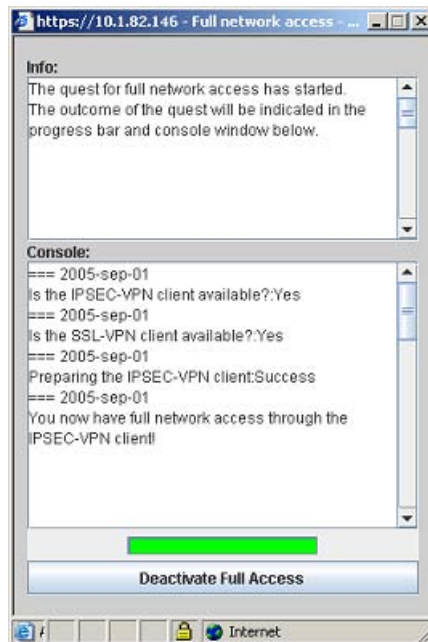
A Java applet is downloaded to the user's local machine. The Java applet checks if the IPsec VPN client is installed and able to connect to an Avaya VPN Router or to the IPsec VPN client. If so, the IPsec VPN client is silently activated on the remote user's machine.

If the IPsec VPN client is not installed on the remote user's machine or is unable to connect, the Java applet checks if the SSL VPN client is installed and able to connect to the VPN Gateway. If so, the SSL VPN client is silently activated on the remote user's machine.

If the SSL VPN client is not installed on the remote user's machine or is unable to connect, the Java applet goes on to check if the Net Direct client is enabled on the VPN Gateway and if it is able to connect. If so, the Net Direct client is silently activated on the remote user's machine.

When the user is successfully authenticated, a secure tunnel is set up between the user's local machine and the VPN Router/VPN Gateway.

The following figure is an example of the Java applet window when a connection to the AVG is successfully established with the IPsec VPN client:



2. Start a client application and request the desired intranet resource.

The user's group membership determines their access rights.

3. When you are finished with the session, close the connection by clicking the **Deactivate Full Access** button in the Java applet window.

The Java applet window is closed and the VPN client connection is terminated.

If neither of the VPN clients are installed or able to connect, intranet resources can only be accessed in clientless mode, that is, by requesting resources from the other Portal tabs.

The Advanced Tab, Telnet/SSH Access

The Telnet/SSH Access feature lets the user run a Telnet or SSH session to a specified server on the intranet. The session runs in a Java terminal emulation applet window. To simplify access, a link to the desired server can also be defined on the **Home** tab.

To enable display of applications with graphical user interfaces, SSH version 2 supports X11 forwarding.

Telnet/SSH Access [help](#)

From this page you can access Telnet or SSH servers on the Intranet. You can only access servers as defined by your security level.

Note: Your browser must support Java. If not download SUN's J2SE JRE from www.java.com.

If you do not know any Telnet or SSH servers on the Intranet you should either contact your system administrator or use the links on the [Home](#) page.

If you already sit behind a Proxy just specify it as the chaining Proxy below. If not you can safely ignore this setting.

A new window will be opened if you hit the ENTER key (or the Open... button). You can open multiple windows to access several servers in parallel.

Host:

Port: ☒ Telnet ☐ SSHv1 ☐ SSHv2

[Log File Path]: (Leave empty to skip)

[Keymap URL]: (Leave empty to skip)

[Proxy Host]: (Leave empty to skip)

[Proxy Port]: (Leave empty to skip)

To start a session, the user should do the following:

1. Enter the server's host name or IP address in the **Host** field.
2. Select the desired protocol (Telnet, SSHv1 or SSHv2).
3. In the **[Log File Path]** field (optional), enter the path to the folder where the log file should be saved.
4. If the user has a nonstandard keyboard, the **[Keymap URL]** field can be used to point to a keyboard mapping file located for example, on an intranet file server.

Keystrokes to be sent to the remote server automatically translates to the proper keys. Syntax example `http://inside.example.com/keyCodes.at386`.

Documentation describing the configuration file properties is in Appendix F, "Definition of Key Codes" in the *User's Guide*.

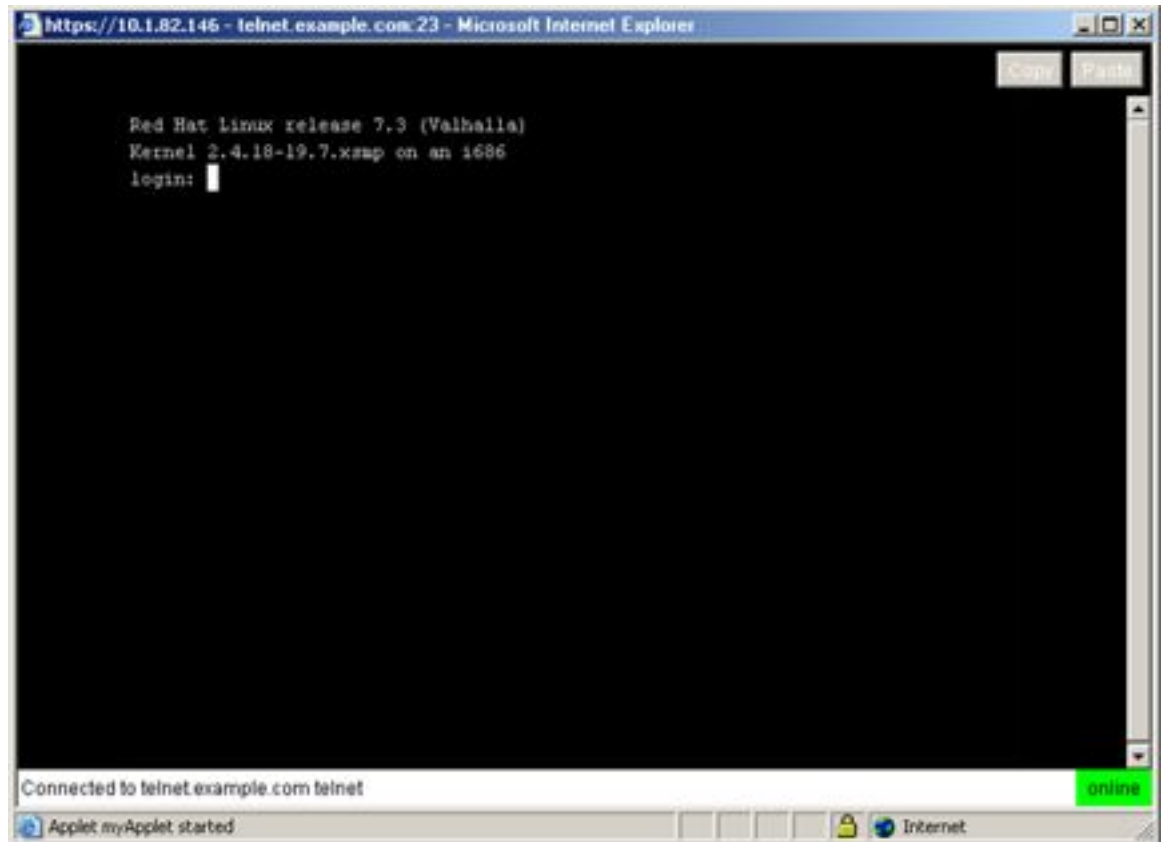
5. In the **[Proxy Host]** and **[Proxy Port]** fields, enter the IP address and port number of an intermediate Proxy server (if any).

Users work from a location requiring traffic to pass through an intermediate Proxy server on the intranet should enter the IP address (or domain name) and port of that proxy server. All applet traffic is tunneled to the AVG through the Proxy server. The Proxy server requires CONNECT support.

Users should be informed if this step is required. If the Proxy Host and Proxy Port fields are left blank, all applet traffic will be tunneled directly to the AVG.

6. Click **Open**.

The following is an example of Java applet window when a Telnet session is starts:



7. Click in the window to make it active before you log on to the terminal session.

Click the **Close** button top right.

The Advanced Tab, HTTP Proxy

You can access intranet web pages in a secure mode from **Home** tab. However, a web page may contain plugins (for example, a Flash movie) which can include embedded links to other web pages. If a user executes such an embedded link, the HTTP request may not reach the VPN Gateway and the URL will not be displayed.

To ensure display of all URLs—also ones that are embedded in plugins—the HTTP Proxy feature lets the user download a Java applet to the client. The client browser's proxy settings should then be changed to direct all HTTP requests to this Java applet. The Java applet in its turn routes each request through a secure SSL tunnel to the AVG 's proxy server, where it is unpacked and redirected to its proper destination.



To start a HTTP Proxy session, the user should proceed as follows:

1. In the **[HTTP Proxy Host]** and **[HTTP Proxy Port]** fields, enter the IP address and port number of an intermediate HTTP Proxy server (if any).

Users who are working from a location requiring traffic to pass through an intermediate HTTP Proxy server should enter the IP address (or domain name) and port of that proxy server. All applet traffic will thus be tunneled to the VPN Gateway through the HTTP proxy server. The HTTP Proxy server should have CONNECT support.

Users should be informed if this step is required. If the HTTP Proxy host and port fields are blank, all applet traffic will be tunneled directly to the VPN Gateway.

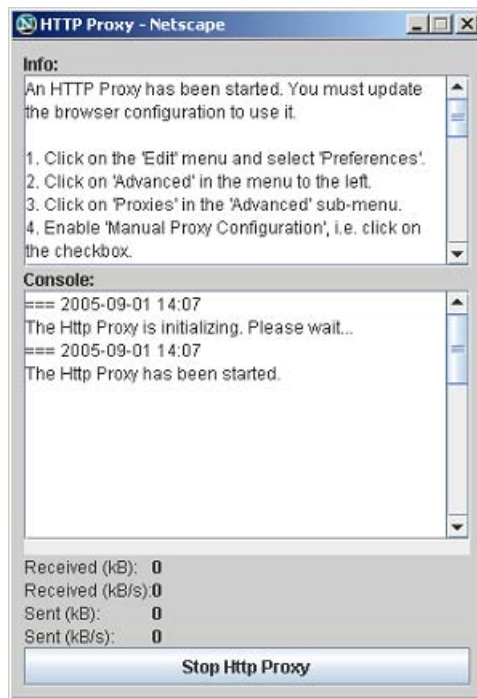
2. If Internet Explorer is used as the client browser, you can select the check box Reconfigure Internet Explorer to use the HTTP Proxy.

With this check box selected, you need not change the browser's proxy settings manually, that is, Step 4 can be ignored. Also, when you exit the HTTP Proxy session, the browser's original proxy settings are automatically restored.

3. Click **Open**.

The user is asked to install a signed applet (certified by Avaya). The Java applet window appears to confirm that an HTTP Proxy applet is started.

4. Reconfigure the browser proxy settings (not required for Internet Explorer).



You can manually reconfigure the browser proxy settings, unless Internet Explorer is used as client browser.

Instructions (related to the type of browser used) are displayed in the

Info

part of the Java applet window. The example to the left shows how to change Netscape proxy settings.

After you change the proxy settings, you open a new browser window and surf the intranet in encrypted mode through the AVG's HTTP Proxy. The Java applet window and the Portal session must be active.

To quit the HTTP Proxy session, you can click **Stop Http Proxy** in the Java applet window. If the browser is reconfigured manually, you can also reset the browser settings back to the original settings.

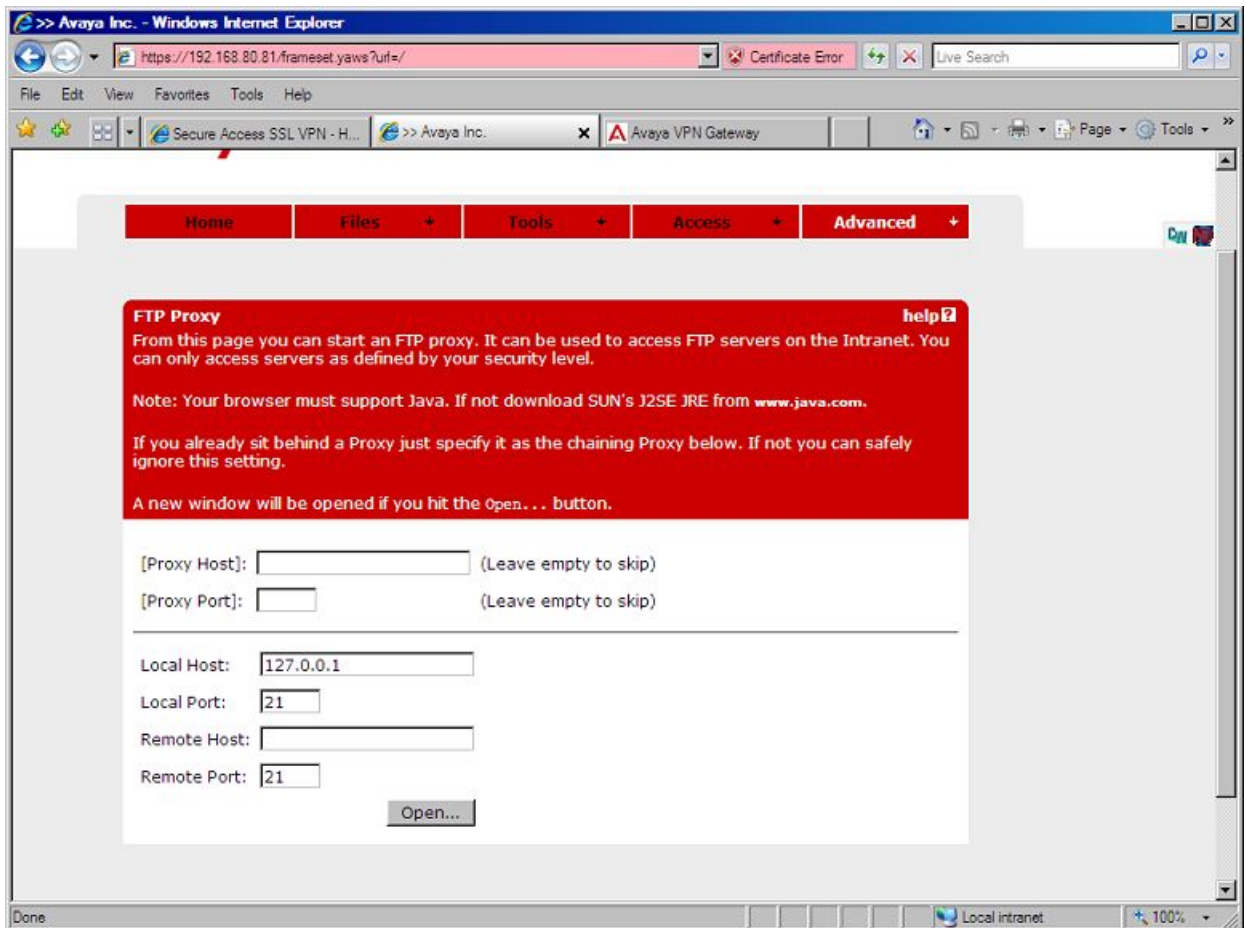
*** Note:**

Outlook Port forwarder links (if configured) or Outlook Port forwarder Portal sessions (Advanced tab) does not work if a proxy server configures in the client browser.

The Advanced Tab, FTP Proxy

The FTP Proxy feature lets the remote user access a remote FTP server through a native FTP client (installed on the remote user's machine).

When the FTP Proxy starts, a Java applet is downloaded to the client. The Java applet routes each request through a secure SSL tunnel to the AVG's proxy server, where it is relayed to the specified FTP server.



To start a FTP Proxy session, the user should proceed as follows:

1. In the **[Proxy Host]** and **[Proxy Port]** fields, enter the IP address and port number of an intermediate HTTP Proxy server (if any).

Users who works from a location requiring traffic to pass through an intermediate HTTP Proxy server enters the IP address (or domain name) and port of that proxy server. All applet traffic is tunneled to the VPN Gateway through the HTTP proxy server. The HTTP Proxy server has CONNECT support.

Users should be informed if this step is required. If the Proxy host and port fields are left blank, all applet traffic will be tunneled directly to the VPN Gateway.

2. In the **Local Host** field, enter an IP address in the 127.x.y.z range (for example, 127.0.0.1).

3. In the **Local Port** field, enter a free "local" port number.

Port numbers above 5000 are usually free to use. Avaya recommends that you use the application-specific port number for FTP, so you can use port 21.

4. In the **Remote Host** field, enter the host name or IP address to the remote FTP server.
5. In the **Remote Port** field, enter the application-specific port number (for example, 21 for an FTP session).
6. Click **Open**.

You can install a signed applet (certified by Avaya). The Java applet window appears to confirm that an FTP Proxy applet started.

7. You can now start native FTP client.

To access the remote FTP server you need to connect to the local host IP address.

8. To quit the FTP Proxy, you should click **Stop FTP Proxy** in the Java applet window.

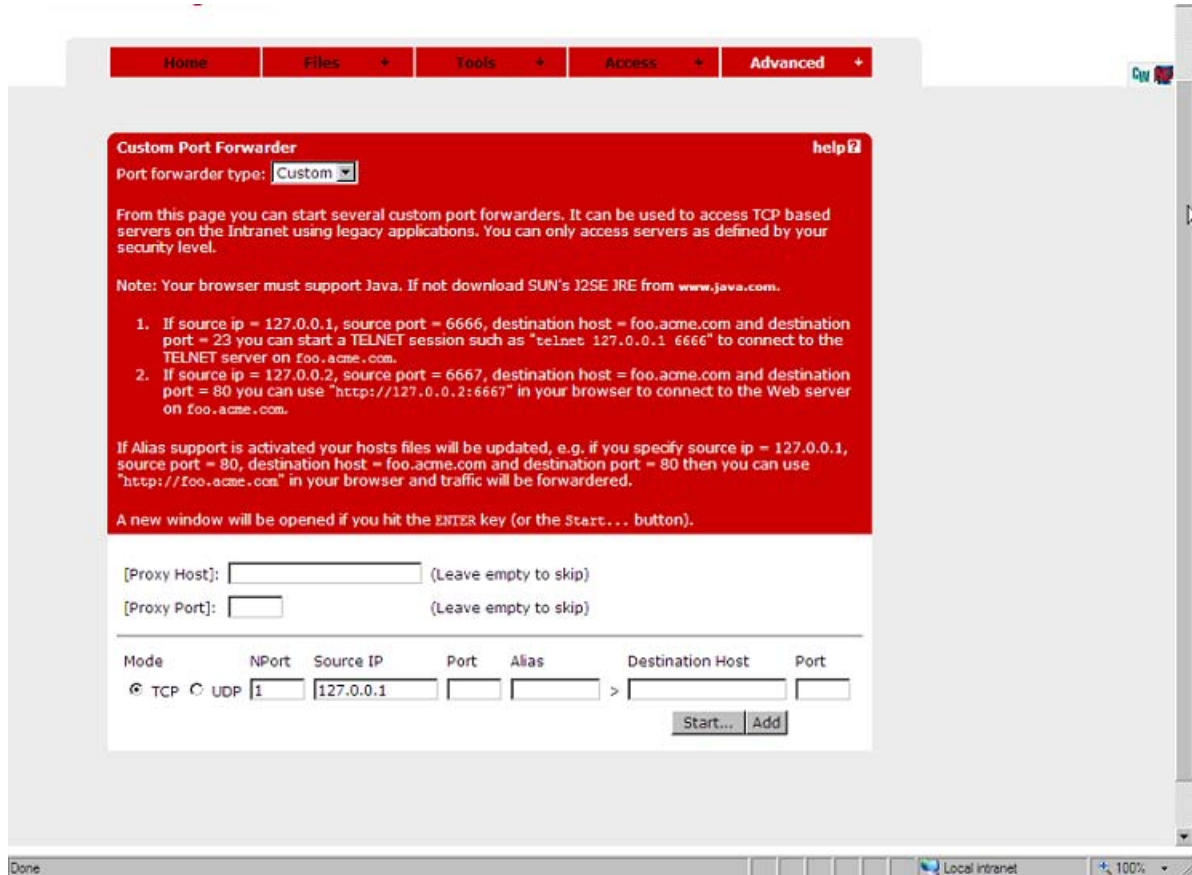
The Advanced Tab, Port Forwarders

Using the Port Forwarders tab, you can set up a secure SSL connection to an intranet application server and run a TCP- or UDP-based client application. Download a Java applet instructed to listen to a port number on the user's computer. The applet then forwards all incoming traffic to the application server. The Port Forwarder tab includes the following options:

- Custom
- Outlook

Custom Port Forwarder

The Custom Port Forwarder lets you start an optional TCP- or UDP-based application (for example, native Telnet or Outlook Express). To start a custom port forwarder, you should keep the **Custom** option in the **Port forwarder type** box.



Example of accessing to Outlook Express

In the following example, you can access the intranets POP3 and SMTP mail servers using Outlook Express.

1. In the **[Proxy Host]** and **[Proxy Port]** fields, enter the IP address and port number of an intermediate Proxy server (if any).

Users who are working from a location requiring traffic to pass through an intermediate Proxy server should enter the IP address (or domain name) and port of that Proxy server. All applet traffic will thus be tunneled to the VPN Gateway through the Proxy server. The Proxy server should have CONNECT support.

Users should be informed if this step is required. If the Proxy Host and Proxy Port fields remain blank, all applet traffic is tunneled directly to the VPN Gateway (unless Internet Explorer is configured to use a Proxy server).

2. Under **Mode**, select the desired packet transfer protocol, that is, TCP or UDP.
3. In the **Source IP** field, enter an IP address in the 127.x.y.z range (e.g 127.0.0.1).
4. In the **Port** field, enter a free "local" port number, for example, 5025.

Port numbers just above 5000 are usually free to use. The application-specific port number can also be used, e.g 25 for SMTP.

5. Usage of the **[Host Alias]** field (optional) is explained on the next page.
6. In the **Destination Host** field, enter the domain name (or IP address) of the intranet server you wish to connect to, for example, `pop3.example.com`.
7. In the **Port** field, enter the application-specific port number (e.g. 110 for a POP3 session).
8. Click **Add** to display a second row of input fields for the next tunnel.

To setup a connection to the SMTP server, enter a new IP address in the 127.x.y.z range in the Source IP field, for example,

`127.0.0.2.`

Then enter a new port number in the **Port** field (for example,

`5026`

). Finally enter the IP address or domain name to the SMTP server in the **Destination Host** field and the port to use in the **Port field**, in this case

`25`

.

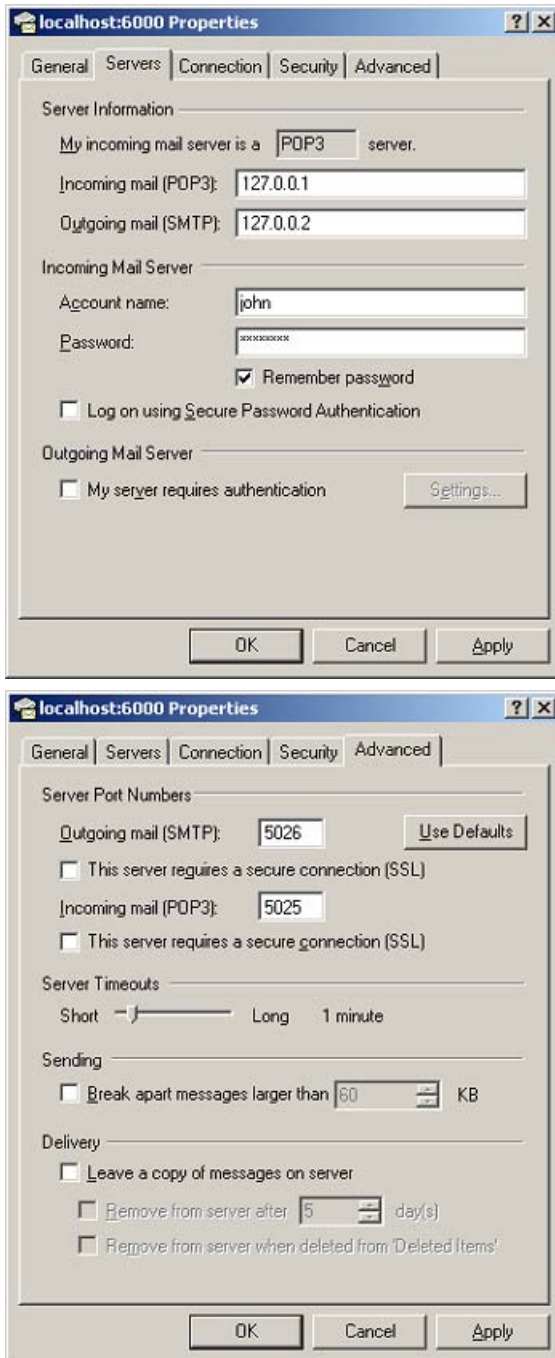
Up to 16 tunnels can be created for one port forwarder.

9. Click **Start**.

The user will be asked to install a signed applet for this session. By accepting, a Java applet window appears to confirm the information specified for the Port Forwarders.

Example of configuring Client Application

After you establish two connections, one to the POP3 server and one to the SMTP server. In the client application, in this case Outlook Express, specify that incoming or outgoing mail is delivered or collected by hosts 127.0.0.1 and 127.0.0.2, respectively.



The port numbers to use are entered in the "local" **Port** field for the POP3 and SMTP servers respectively; that is,

5025

and

5026

, respectively. By entering the application-specific port numbers in the "local" **Port** field, that is,

110

(for POP3) and

25

(for SMTP), existing port number settings in the mail client can be kept.

If the destination host is specified in the **Alias** field, and application-specific port numbers are used as "local" port numbers, no modifications to the client application are required.

 **Note:**

Use of host aliases is possible only if the user has administrator privileges on their client or has write access enabled for hosts and lmhosts files. Hosts and lmhosts files are located in %windir%\hosts on Windows 98 and ME and in %windir%\system32\drivers\etc\hosts on NT, XP, and Windows 2000.

If you expect the connection to include more than 15 minutes of inactivity, increase the TCP connection idle timeout value, using the `/cfg/vpn #/server/tcp/keep` command.

To quit the Port Forwarder, click **Stop Port Forwarder** in the Java applet window.

Telnet Port Forwarder

To establish a secure Telnet session using the Custom Port Forwarder, proceed as described in the preceding sections, enter only the host address to the Telnet server in the **Destination Host** field (for example, `telnet.example.com`) and port number

23

in the "remote" **Port** field instead. You can then start the Telnet client and connect to for example,

`127.0.0.1 5025`

. If the destination host is specified in the **Alias** field, you can instead connect to the actual destination host and the local port number in the Telnet client, for example,

`telnet.example.com 5025`

. If a short name is specified in the **Alias** field (for example,

`telnet`

), you can connect to

`telnet 5025`

in the Telnet client.

HTTP Port Forwarder

To establish a secure HTTP session using the Custom Port Forwarder, proceed as described in the preceding sections, only enter the host address to the Web server in the **Destination Host** field and port number

80

in the "remote" **Port** field instead. You can then start the browser and type for example,

127.0.0.1:5025

in the Address field. If the destination host is specified in the **Alias** field, the user can instead type the actual URL and the local port number in the browsers **Address** field, for example,

www.example.com:5025

. If a short name is specified in the **Alias** field (for example,

web

), you can connect to

web:5025

instead.

Port Forwarder Links

Define Custom Port Forwarder links to simplify access on the Portal **Home** tab by the AVG operator. A Custom Port forwarder link can be defined to automatically start the application (see [Group Links](#) on page 203).

Native Outlook Port Forwarder

You can start a native Outlook session to a specified Exchange server on the intranet using Outlook Port Forwarder. To start the Outlook Port Forwarder, you should select **Outlook** in the **Port forwarder type** list box. This displays a different set of input fields, as shown in the following figure.

! Important:

The following prerequisites must be fulfilled for the Outlook Port Forwarder to work:

- You should configure the Exchange servers domain name using the `/cfg/vpn # adv/dns/search` command. Using the preceding example, enter `example.com` following

the **search** command. If you use several Exchange servers, you should configure all the Exchange servers domain names in the DNS search list.

- You must have administrator's rights on your computer or have write access enabled for hosts and lmhosts files. Hosts and lmhosts files are in %windir%\hosts on Windows 98 and ME and in %windir%\system32\drivers\etc\hosts on NT, XP and Windows 2000.
- The Outlook Port forwarder is meant to be used by clients connecting to the AVG from outside the intranet. If the client has direct connectivity to the intranet, the port forwarder fails. If the client has access to intranet, DNS servers, communication fails as well.
- Your Outlook account must be hosted on the Exchange servers specified in the Port forwarder.
- The user's client machine must be of the Hybrid or Unknown node type. Enter `ipconfig/all` at the DOS prompt to check the node type.

To change the node type to Hybrid (if needed), go to the registry editor folder HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters. If not already present, add a new DWORD Value called NodeType. Double-click NodeType and enter 8 in the Value Data field. Click OK and restart the computer.

- If you configure the proxy server, the Outlook Port forwarder does not work. This also means that a HTTP Proxy link or HTTP Proxy portal session (Advanced tab) cannot be active at the same time as the Outlook Port forwarder.
- If a firewall exists between the VPN Gateway and the Exchange server, the firewall settings must allow traffic to the required Exchange server ports.

 **Note:**

These may vary with your environment. More information is at support.microsoft.com, for example, Knowledge Base Articles 280132, 270836, 155831, 176466, 148732, 155831, 298369, 194952, 256976, 302914, 180795, and 176466.

- When a user clicks an embedded link in an e-mail message, the web site associated with the link must appear in a new instance of Internet Explorer. In Internet Explorer, go to the **Tools** menu and select **Internet Options**. Under the **Advanced** tab, go to **Browsing** and deselect the **Reuse windows for launching shortcuts** option.
- If you expect the connection to include more than 15 minutes of inactivity, increase the TCP connection idle timeout value by using the `/cfg/vpn #/server/tcp/keep` command.

The following information should be supplied by the user on the Port Forwarder tab:

1. Select the **Start Outlook client** check box if Microsoft Outlook should start automatically when the Port Forwarder start.
2. In the **Source IP** field, enter an IP address in the 127.x.y.z range (for example, 127.0.0.1).

3. In the Exchange server (FQDN) field, enter the fully qualified domain name (FQDN) of the Microsoft Exchange Server, for example, `exchange.example.com`.
4. Click **Add** to enter information for yet another Outlook Port forwarder (if required).

Services provided (mail, calendar, address book) may be distributed between different Exchange servers. If this is the case, you can create several Outlook port forwarders where the relevant Exchange servers can be specified.

 **Note:**

If several port forwarders are required each port forwarder must have a unique source IP address. System automatically suggests a new source IP address if you choose to add another port forwarder.

5. Click **Start**.

Install a signed applet for this session.

6. Click **Yes**.

A Java applet window appears to confirm the information specified for the Port forwarders. Read the instructions, warnings, and validation messages carefully provided in the Java applet window. If the Port forwarder is not configured to start the Outlook client automatically, the user need to wait until the applet is fully initialized before manually starting the Outlook client.

7. Start the Outlook client (if not started automatically).
8. To quit the session, exit the Outlook client, then click the **Stop Port Forwarder** button in the Java applet window.

 **Note:**

You must not close the Java applet window as the last browser window, in which case the hosts files may not be cleaned up properly.

Port Forwarder API

The AVG software provides an API for developing a custom application that automatically logs in the user to the desired VPN and executes a previously configured Port forwarder link on the Portal's Home tab. This way, a remote user does not have to browse to the Portal and click the Port forwarder link to set up the required application tunnel.

Briefly, this is how to use the Port forwarder API.

1. Configure a Port forwarder link.

Instructions to create Port forwarder links see, [Group Links](#) on page 203.

2. Develop a Java application or applet that uses the Port forwarder API.

You can download the Port Forwarder API from the Portal through the URL `https://vpn.example.com/nortel_cacheable/portforwarder.zip`, where `vpn.example.com` is the DNS name of your Portal.

API programming instructions and examples are in Appendix I in the *User's Guide*.

The Download Tab

To download the Secure Portable Office (SPO) software images, elect Download tab. By clicking the links, SPO client downloads ISO image, U3P package, and MSI files.

*** Note:**

The Download tab will be available in the portal only when the SPO access is enabled.

Logging out from the Portal

To logout from the Portal, the user should click the **Logout** prompt or the exit button.

Idle Timeout

If the remote user is idle longer than the time specified as default session idle time for the VPN (using the `/cfg/vpn #/aaa/idlettl` command), the user will be logged out automatically.

*** Note:**

Session idle time can also be specified on group level (using the `/cfg/vpn #/aaa/group #/idlettl` command). Upon user login, the best idle time of the user's different groups and the default idle time for the VPN will be selected.

Maximum Session Length

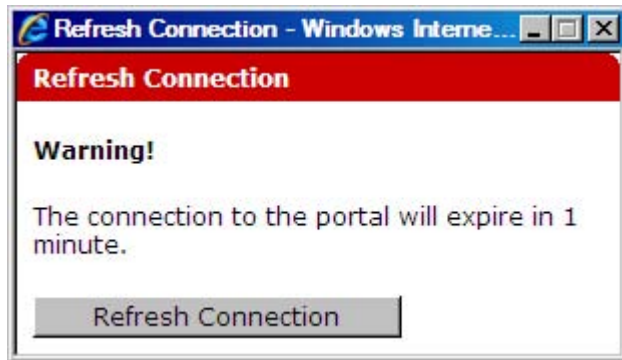
The user is automatically logged out after the time specified as maximum session length for the VPN (using the `/cfg/vpn #/aaa/sessionttl` command), regardless of the user being idle or not.

*** Note:**

Maximum session length can also be specified on group level (using the `/cfg/vpn #/aaa/group #/sessionttl` command). Upon user login, the best maximum session

length value for the user's different groups and the default maximum session length value for the VPN will be selected.

One minute before the user is automatically logged out, a message is displayed. The message warns the user about the upcoming logout and offers to refresh the Portal connection.



Internet Explorer Cache Wiper

When using Internet Explorer as browser, any HTML pages that have been accessed through the Portal will be cleared from the cache provided the IE cache wiper has been downloaded. The user has the option to download the IE cache wiper when logging in to the Portal, if the `/cfg/vpn #/portal/wiper` command is enabled (enabled by default). The IE cache wiper also clears the browser history from entries accumulated during the Portal session. All previously recorded entries will remain.

If desired, the IE cache wiper can be enabled or disabled on group level instead of VPN level. Set `/cfg/vpn #/portal/wiper` to

`group`

, then enable or disable `/cfg/vpn #/aaa/group # /wiper.`

Chapter 6: Bandwidth Management

This chapter provides procedures to configure Bandwidth Management (BWM) for Avaya VPN Gateway device.

Bandwidth Management enables administrators to allocate a portion of the available bandwidth for specific users or groups. The bandwidth policies take lower and upper bound. The lower bound (soft limit) is guaranteed and the upper bound (hard limit) is available according to the requirement. The BWM provides bandwidth policy management for the user traffic and IPsec Passthrough.

The following topics are covered in this chapter:

- [User traffic](#) on page 79
- [IPsec Passthrough](#) on page 79
- [Hard and soft limit](#) on page 80
- [Configure BWM](#) on page 80
- [Configure IPsec Passthrough](#) on page 81

User traffic

The user traffic is classified based on the group the user is placed. Based on the user source IP address, a filter is added to mark the traffic coming from the user to a particular queue. After adding the source IP address, the incoming packets are marked based on the traffic control filter and then queued according to the configuration. You can configure bandwidth management policy for user groups and extended groups. For more information about configuring bandwidth policy for user group, see [Configuring bandwidth policy](#) on page 181 and for extended group, see [Configuring bandwidth policy](#) on page 201.

IPsec Passthrough

The BWM Internet Protocol Security (IPsec) Passthrough handles the IPsec Branch Office (BO) tunnel traffic on a different bandwidth policy and bandwidth rate. The IPsec BO tunnel traffic is classified in a separate queue and subsequently handled with a different priority based on the specified configuration. For more information about the configuration, see [Configure IPsec Passthrough](#) on page 81.

Hard and soft limit

The hard limit is the upper boundary for the policy. A bandwidth class is never allowed to transmit above the hard limit. The traffic bursts between the soft limit and the hard limit. The hard limit ranges from 2000 to 400000 kilobits (kb). The default value is 2000 kb. To ensure a specific amount of throughput on a port, hard limit must be equal to or greater than the soft limit.

The soft limit is the desired or minimum guaranteed rate for a bandwidth policy. When the output bandwidth is available, a bandwidth class is allowed to send data at this rate. Exceptional condition is not reported when the data rate does not exceed the limit. The soft limit ranges from 2000 to 400000 kb and the default value is 2000 kb.

Configure BWM

You can configure BWM for user traffic and IPsec Passthrough. To configure BWM, see the following:

- [Enabling BWM](#) on page 80
- [Configuring BWM policy](#) on page 80

Enabling BWM

Perform the following procedure to enable BWM:

Enable BWM.

<pre>>>Main#cfg/bwm</pre>	(Displays BWM menu)
<pre>>> Bandwidth Management#ena</pre>	(Enable BWM)

Configuring BWM policy

You can configure a single BWM policy for multiple groups and extended profiles. All the groups and extended profiles do not share the same BWM policy, but each of them are assigned a separate bandwidth queue with the same rate as the bandwidth policy and the bandwidth is allocated accordingly.

The configured bandwidth policies are not effective for negligible time when a bandwidth policy is added, updated, or deleted. The traffic flow is normal and the user does not see any effect.

Perform the following procedure for configuring BWM policy:

1. Configure BWM policy.

```
>> Bandwidth Management#bwmpolicy
```

Enter BWM policy number or name: (1-255)1 (Specify BWM policy number or name. For example, 1)

Creating Bandwidth Management Policy 1 (The BWM policy 1 is created)

Policy name: (Specify policy name)

Enter the Soft limit (2000-400000): (Specify soft limit)

Enter the Hard limit (2000-400000): (Specify hard limit)

2. Apply the changes.

```
>> Bandwidth Management# apply (Apply changes)
```

Configure IPsec Passthrough

To configure IPsec Passthrough, see the following:

- [Enabling IPsec Passthrough](#) on page 82
- [Configuring bandwidth policy](#) on page 82
- [Configuring IPsec servers](#) on page 83

After configuring IPsec Passthrough servers, you can list, insert, or move the IPsec servers. For more information about configuration, see the following:

- [Listing the IPsec servers](#) on page 83
- [Inserting the IPsec servers](#) on page 84
- [Moving the IPsec servers](#) on page 84

Enabling IPsec Passthrough

Perform the following procedure for configuring IPsec Passthrough:

1. Enable BWM.
2. Configure a BWM policy.
3. Enable IPsec passthrough.

>> Bandwidth Management# ipsecpass	(Displays IPsec Passthrough menu)
>> IPsec Passthrough# ena	(Enable IPsec Passthrough)

Configuring bandwidth policy

Perform the following procedure to configure bandwidth policy for IPsec Passthrough traffic:

1. Enable BWM.
2. Configure BWM policy.

>> Bandwidth Management#bwmpolicy	
Enter BWM policy number or name: (1-255)2	(Specify BWM policy number or name. For example, 2)
Creating Bandwidth Management Policy 2	(The BWM policy 2 is created)
Policy name:	(Specify policy name)
Enter the Soft limit (2000-400000):	(Specify soft limit)
Enter the Hard limit (2000-400000):	(Specify hard limit)

3. Specify the bandwidth policy name.

Choose any one bandwidth policy configured using command **/cfg/bwm/bwmpolicy #**.

>> IPsec Passthrough# bwpolicy	(Specify Bandwidth policy)
--------------------------------	----------------------------

Current value:	(Displays the current bandwidth policy name)
Enter BW Policy name:	(Specify the configured bandwidth policy name)

4. Apply the changes.

Configuring IPsec servers

Perform the following procedure to configure or add the IPsec servers:

1. Enable BWM and configure a bandwidth policy.
2. Enable IPsec Passthrough and configure bandwidth policy.
3. Add the IPsec server.

>> IPsec Passthrough# servers	(IPsec server menu appears.)
>> IPsec Passthrough# add	(Adds the IPsec server)
IP address to add:	(Specify the IPsec server IP address)

Listing the IPsec servers

Perform the following procedure to list the IPsec servers:

1. Enable BWM and configure a bandwidth policy.
2. Enable IPsec Passthrough and configure bandwidth policy.
3. List the configured IPsec servers.

>> IPsec Passthrough#	(IPsec server menu appears)
servers	
>> IPsec Passthrough# list	(Lists the configured IPsec servers)
old:	
1:10.12.134.23	
Pending:	
1:10.12.134.24	
2:10.12.134.25	

Inserting the IPsec servers

Perform the following procedure to insert a IPsec server:

1. Enable BWM and configure a bandwidth policy.
2. Enable IPsec Passthrough and configure bandwidth policy.
3. Insert the configured IPsec servers.

<pre>>> IPsec Passthrough# servers</pre>	(IPsec server menu appears)
<pre>>> IPsec Passthrough# insert</pre>	(Inserts the IPsec server)
<pre>Index to insert at: 1</pre>	(Specify the index to insert the IPsec server)
<pre>IP address to add: 10.12.134.26</pre>	(Specify the IPsec server IP address)
<pre>>> IPsec Passthrough# list</pre>	(List the IPsec servers)
<pre>old: 1:10.12.134.23 Pending: 1:10.12.134.26 2:10.12.134.24 3:10.12.134.25</pre>	

Moving the IPsec servers

Perform the following procedure to move a IPsec server:

1. Enable BWM and configure a bandwidth policy.
2. Enable IPsec Passthrough and configure bandwidth policy.
3. Move the configured IPsec server.

<pre>>> IPsec Passthrough# servers</pre>	(IPsec server menu appears)
<pre>>> IPsec Passthrough# move</pre>	(Moves the IPsec server)

```
Index number to move: 1          (Specify the index number to
                                  move)
Destination index:3              (Specify the destination index)

>> IPsec Passthrough# list      (List the IPsec servers)

old:
1:10.12.134.23
Pending:
1:10.12.134.25
2:10.12.134.24
3:10.12.134.26
```


Chapter 7: Net Direct

This chapter provides procedures to use Net Direct for Avaya VPN Gateway device.

The following topics are covered in this chapter:

- [About the Net Direct Client](#) on page 87
- [Server Configuration](#) on page 90
- [Net Direct from a User Perspective](#) on page 106
- [Start Net Direct Outside Portal](#) on page 114

About the Net Direct Client

You can temporarily download Net Direct which is a VPN client to the client PC from the Web Portal. When the user exits Net Direct or the VPN session, the client is automatically uninstalled. Combined with Tunnel Guard and extended profiles, the Net Direct client offers a simple and secure access method.

Net Direct includes a network driver that captures network traffic and tunnels it through SSL to the Avaya VPN Gateway (AVG). The AVG then decrypts the traffic and forwards it to the requested destination. You can configure which network destinations are tunneled.

The Net Direct client is packet-based, whereas the SSL VPN client (see [Transparent Mode](#) on page 355) uses system calls. Because the Net Direct client thus operates on a low network level, it supports additional applications, for example, Microsoft Outlook and the ability to map network drives.

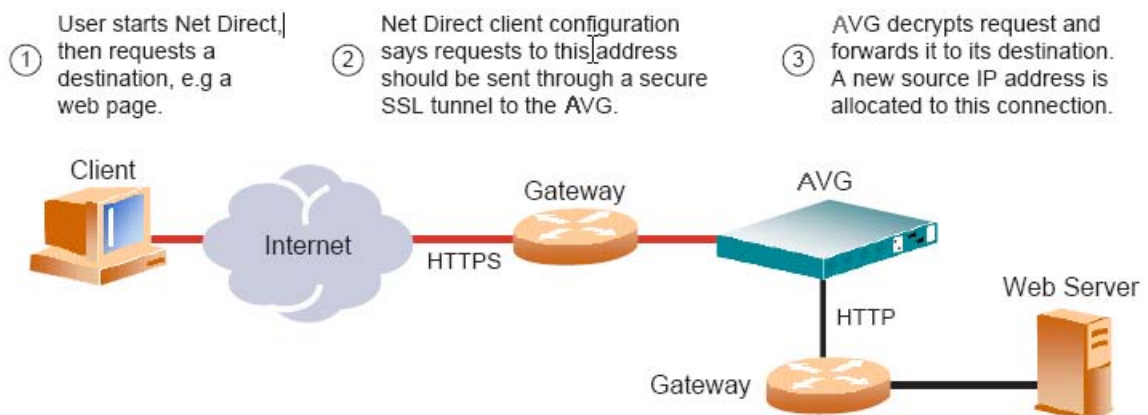


Figure 4: Net Direct Client Connection

Supported Operating Systems

Net Direct is supported on the Windows, Linux and Mac OS X (for PowerPC) operating systems.

On Windows, the end user must be administrator on PC (or know the administrator password) to be able to download or install the Net Direct client. The Windows administrator user name and password can however be stored on the AVG each group level. For remote users who are members of a group and for which a valid Windows administrator user name and password are stored, downloading and installing Net Direct is seamless. See [Configure Windows Administrator User Name/Password](#) on page 102.

You need to be the member of the admin group to download and install Net Direct on Mac OS X. If the user is not a member of the admin group or enters the wrong password when prompted, they can log in with the root password as an alternative. This requires that the user account is authorized to perform the command `su root`.

Downloading and installing Net Direct on Linux requires the user to be root user or ensure that the user account is authorized to perform the command `su root`. If the user is not running as root when attempting to download Net Direct, a window appears prompting the user for the root password.

For more information see to the Release Notes, for example, supported browsers and Java versions, limitations.

Net Direct Modes

The Net Direct client is available in three versions, or modes:

- Downloadable client
- Cached client (Windows only)
- Installed client (Windows only)

Downloadable Client

By clicking a link on the Web Portal, the Net Direct client is downloaded, installed, and started on the remote user's PC. While Net Direct runs in the background, the remote user can access intranet resources through their native applications – without the need to manually install VPN client software. When the user exits Net Direct or the Portal, the client is automatically uninstalled.

Cached Client

To cut down on network traffic and start-up time, a cached version of Net Direct is available as a configurable option. If caching is enabled, Net Direct leaves some components from the first installation on the client device when the user exits Net Direct or the Portal session. These components will only be retrieved from the server anew when they become outdated. How to enable caching is described on [2](#) on page 98.

Installed Client

The Net Direct client is also available as a setup.exe that you install permanently on the system of remote user.. No Portal login is then required. The user logs in through the user interface provided by the installable Net Direct client. Just like the downloadable and cached versions, the behavior of the installable version of Net Direct is completely controlled by the server settings made for the VPN Gateway (see the following sections).

Installable Net Direct supports installable Tunnel Guard.

Installing the installed client requires administrator privileges. For instructions about how to create a Portal link for downloading the installed version of Net Direct, see [Configure Link for Downloading Installed Version](#) on page 103

When connecting to the AVG, the system checks the version of the installed Net Direct client. If a more recent version is available, the user will have to option to go to a web page where the new version of the client can be downloaded.

Mobility

If the connection is lost during a Net Direct user session, the Net Direct device still remains in UP state because client enters into the roaming mode and will preserve the session till the roaming time expires. You can configure the following Net Direct parameters on per VPN per Group:

- roaming mode
- roaming time
- list of networks on which roaming is allowed

During roaming time, it can roam through any physical interface which is in the configured roaming networks. This allows user to maintain the VPN session in cases like:

- A Wifi User roaming from one access point area to another access point or a subnet
- A user migrating from 802.3 Ethernet environment to Wifi
- Temporary lose of connectivity to the server, due to an intermediate router or switch failure

- A Wifi user temporarily losing connectivity
- This feature is supported on Windows, Linux and MAC. It is also supported on portal version of Net Direct as well as NDIC.

Server Configuration

To enable use of the Net Direct client, follow the basic instructions in [Clientless Mode](#) on page 35 on how to set up a VPN. Then continue with the following steps.

Create IP Pool

The IP pool comes into play when the remote user tries to access a host using Net Direct. A new IP address has to be assigned as source IP for the unencrypted connection between the VPN Gateway and the destination host. Optionally, specific network attributes for this connection can also be defined.

Several IP pools can be configured, each with a unique ID number and unique properties. By mapping the desired IP pool to a user group, you can create different methods for IP address and network attributes assignment for different user groups. One of the configured IP pools should be selected as the default IP pool. Groups for which no IP pool is assigned (IP pool number=0) will use the default IP pool.

The IP pools are used to assign IP addresses for IPsec access (using the Avaya IPsec VPN client) as well (see [Transparent Mode](#) on page 355). If you have already configured an IP pool for use with the IPsec VPN client, this pool can also be used for the Net Direct client.

 **Note:**

If no IP pool is configured when you attempt to configure the Net Direct link, a wizard will prompt you for the required information for a local IP pool when you configure the link.

Create an IP pool and specify how network attributes should be assigned to the client.

Network attributes (including IP address) can be assigned either locally (from the AVG), from an external RADIUS server or from an external DHCP server.

When you configure an IP pool for the first time, you will enter a wizard. Depending on the choice you make for pool mechanism (that is,

`local, radius`

or

`dhcp`

), different questions will be displayed in the wizard.

```
>> Main#/cfg/vpn 1/ippool

Enter Pool number or name (1-10): 1

Creating Pool 1
Select one of local, radius, dhcp:<select the desired pool
mechanism here>

Set the pool name:<enter a name for the IP pool here>
```

The pool mechanism setting is equivalent to the **type** command in the Pool menu.

You can associate an IP pool with a particular host in a clustered environment. For more information, see [Configure host IP pool](#) on page 330.

Configure IP Address Range and Local Network Attributes

If you set the pool mechanism to

local

, you should configure the desired IP address range. You can also configure network attributes to be retrieved from the AVG when the client connects.

If you set the pool mechanism to

radius

or

dhcp

, continue with the relevant section (see the following pages) instead.

1. Configure an IP address range.

```
Set the lower ip for the pool range:10.1.82.140

Set the upper ip for the pool range:10.1.82.150
```

2. If needed, change the default proxy ARP setting.

```
Set proxyarp (on/off/all) [on]:
```

- on

: Means that the VPN Gateway that handed out the IP address for a specific client connection will respond to ARP requests on behalf of the Net Direct client for return traffic. The VPN Gateway then acts as a router and forwards IP packets to the client through the existing tunnel. Proxy ARP is used on all

interfaces for the relevant VPN except the traffic interface. This is the default setting.

- `off`

. Return traffic will not reach its destination unless specific routes are configured.

- `all`

. Same as

`on`

but proxy ARP is used on all interfaces.

3. Configure network attributes (optional).

The Net Direct client normally works fine without adding specific network attributes. You can however specify the desired attributes on the Network attributes menu if needed.

```
>> Pool 1#netattr
```

- `netmask:`

Sets the network mask for the client. The network mask should cover the IP address range specified in step 1. The default network mask is

`255.255.255.0.`

- `primary/secondary NBNS server:`

Sets the IP address of a primary NBNS server (NetBIOS Name Server). Used if the Net Direct client should use a specific NBNS server to have computer names resolved into IP addresses. NBNS servers provide WINS (Windows Internet Naming Service) which is part of the Windows NT server environment.

- `primary/secondary DNS server:`

Sets the IP address of a primary DNS server. Use this command if the Net Direct client should use a specific DNS server to have domain names resolved into IP addresses. If no (primary or secondary) DNS server is specified here, the DNS server specified for the VPN to which the remote user belongs will be used. The command to use is `/cfg/vpn #/adv/dns/servers`. (This option is only possible if a Secure Services Partitioning license is loaded). If only a default DNS server is specified (using the `/cfg/sys/dns/servers` command), this will be used.

- `name of client DNS domain:`

Lets you specify the name of the domain used while a Net Direct tunnel is connected. It ensures that domain lookup operations point to the correct

domain. This is particularly important for clients that use Microsoft Outlook or Exchange, to ensure that the mail server is mapped to the correct domain.

4. Enable the IP Pool.

```
>> Pool 1#ena
```

5. Apply the changes.
6. The next step is to make the IP pool the default IP pool for the VPN and/or map the IP pool to a group.

If you have several IP pools you might want to select another IP pool as the default IP pool. Continue with the section [Create a Default IP Pool](#) on page 96.

Configure RADIUS IP Pool

If you set the pool mechanism to

radius

(as described in the section [Create IP Pool](#) on page 90), you should configure the AVG to retrieve network attributes from a RADIUS server.

How to configure a RADIUS server is described in the section [RADIUS Authentication](#) on page 119 in [Authentication Methods](#) on page 117

To configure the VPN Gateway to retrieve network settings (including client IP address) through RADIUS attributes from an external RADIUS server, use the `/cfg/vpn #/aaa/auth # /radius/netattr` command. A minimum requirement is to configure retrieval of client IP address and primary DNS server. You can retrieve a number of network attributes, for example, primary/secondary DNS server, primary/secondary NBNS server and so on.

To configure the VPN Gateway to retrieve the filter attributes from the external RADIUS server, use the `/cfg/vpn #/aaa/auth #/radius/filtattr` command.

The following instructions assume that you continue with the IP pool wizard after having chosen

radius

as the pool mechanism.

1. If needed, change the default proxy ARP setting.

```
Set proxyarp (on/off/all) [on]:
```

- on:

Means that the VPN Gateway that handed out the IP address (from the IP pool) for a specific client connection will respond to ARP requests on behalf of the Net Direct client for return traffic. The VPN Gateway then acts as a router and

forwards IP packets to the client through the existing tunnel. Proxy ARP is used on all interfaces for the relevant VPN except the traffic interface. This is the default setting.

- `off.`

Return traffic will not reach its destination unless specific routes are configured.

- `all.`

Same as

`on`

but proxy ARP is used on all interfaces.

2. Enable the IP Pool.

```
>> Pool 1#ena
```

3. Configure fallback network attributes (optional).

```
>> Pool 1#netattr
```

For IP pools of the

`radius`

and

`dhcp`

types, network attributes can be configured on the AVG as fallback values if the RADIUS or DHCP server does not return a specific setting for a network attribute. This is done in the same way as for IP pools of the

`local`

type (see step 3 for instructions).

4. Apply the changes.
5. The next step is to make the IP pool the default IP pool for the VPN and/or map the IP pool to a group.

If you have several IP pools you might want to select another IP pool as the default IP pool. Continue with the section [Create a Default IP Pool](#) on page 96

Configure DHCP IP Pool

If you set the pool mechanism to

dhcp

(as described in the section [Create IP Pool](#) on page 90), you should configure the VPN Gateway to retrieve network attributes from a DHCP server.

The following instructions assume that you continue with the IP pool wizard after having chosen

dhcp

as the pool mechanism.

1. Configure the external DHCP server IP address.

```
Entering: DHCP menu
Entering: DHCP servers menu
DHCP server IP address: 10.1.82.100
Leaving: DHCP servers menu
```

2. If needed, change the default proxy ARP setting.

```
Set proxyarp (on/off/all) [on]:
```

- on:

Means that the VPN Gateway that handed out the IP address (from the IP pool) for a specific client connection will respond to ARP requests on behalf of the Net Direct client for return traffic. The VPN Gateway then acts as a router and forwards IP packets to the client through the existing tunnel. Proxy ARP is used on all interfaces for the relevant VPN except the traffic interface. This is the default setting.

- off.

Return traffic will not be able to reach its destination unless specific routes are configured.

- all.

Same as

on

but proxy ARP is used on all interfaces.

3. Enable the IP Pool.

```
>> Pool 1#ena
```

4. Configure fallback network attributes (optional).

```
>> Pool 1#netattr
```

For IP pools of the

radius

and

dhcp

types, network attributes can be configured on the AVG as fallback values if the RADIUS or DHCP server does not return a specific setting for a network attribute. This is done in the same way as for IP pools of the

local

type .

5. Apply the changes.

The next step is to make the IP pool the default IP pool for the VPN and/or map the IP pool to a group. Continue with the next section.

Create a Default IP Pool

One of the configured IP pools should be selected as the default IP pool for the VPN. Groups for which no IP pool is assigned (IP pool number=0) will use the default IP pool.

1. Configure an existing IP pool as the default IP pool.

```
>> Main#cfg/vpn 1/aaa/defippool

Current value: 0
IP pool number:1
```

2. Apply the changes.

Map the IP Pool to User Group (Optional)

As mentioned on [Create IP Pool](#) on page 90, several IP pools with different mechanisms (that is,

local, radius

or

dhcp

) can be configured. By mapping the IP pools to different user groups you can provide different ways of assigning IP address and network attributes depending on the user's group membership.

One of the configured IP pools should be selected as the default IP pool for the VPN. Groups for which no IP pool is assigned (IP pool number=0) will use the default IP pool. How to create a default IP pool is described in the next section.

This is how to map an IP pool to a user group:

1. Map the IP pool to the desired user group.

```
>> Main#cfg/vpn 1/aaa/group 1/ippool

Current value: 0
IP pool number:1
```

2. Map the next IP pool to another group in the same way.
3. Apply the changes.

Enable Net Direct

To enable Net Direct on the VPN Portal, proceed as follows:

1. Configure the VPN Gateway to enable Net Direct client access.

You can enable Net Direct globally, that is, for the whole VPN, or per user group.

- **on:**

Net Direct client access is enabled for all users in the current VPN. For the user to be able to download the Net Direct client, a Net Direct link must also be created on the Portal's Home tab. When set to

on

, all other Net Direct-related commands become visible.

- **group:**

Lets you delegate to group level whether or not Net Direct client access should be allowed. On group level, use the `/cfg/vpn #/aaa/group #/netdirect` command to grant or deny Net Direct client access for the desired group.

- **off:**

Net Direct client access is disabled.

```
>> Main#cfg/vpn 1/sslclient

>> SSL VPN Client#netdirect

Current value: off
Allow Net Direct vpn clients (on/group/off):on
```

When Net Direct is enabled, the SSL VPN client menu is expanded.

All items except

`tdiclient, lspclient, oldclients`

and

`xmlconfig`

can be used to configure the behaviour of the Net Direct client.

*** Note:**

The Net Direct configuration made on the SSL VPN client menu applies to all Net Direct modes of installation, that is, both the downloadable, cacheable and installed client.

The default values for the `udpports`, `rekeytref`, `rekeytime`, `idlecheck` and `clampmss` commands are usually fine for use with Net Direct so you do not normally have to change these settings. See the *Command Reference* for more information about these commands.

2. Verify that the setting for caching of Net Direct components is the desired one (only for Net Direct on Windows).

This step lets you specify whether or not caching of Net Direct components on the client machine should be allowed.

- **on:**

Leaves Net Direct components in the client machine's cache after the remote user has downloaded the Net Direct client from the Portal the first time. The next time the user clicks the Net Direct link, Net Direct will be installed and launched much quicker. When cached components are outdated, these will be fetched automatically from the Portal.

- **off:**

All Net Direct components are removed from the client machine when the remote user exits the Portal session.

```
>> SSL VPN Client#caching

Current value: on
Allow caching of Netdirect on client PCs:
```

3. Specify allowed operating systems.

This command lets you filter out untrusted operating systems (OSs) in the remote user's client PC environment. If the OS is not present in the list specified with this command, the Net Direct client is not allowed to connect to the VPN Gateway.

Press **TAB** to view available options, then enter a comma separated of allowed OSs, for example,

```
winxp
,
win2k.
```

```
>> SSL VPN Client#oslist

Current value: all
Enter list of allowed OSs for netdirect:
all          unknown      vista winxp    win2k        generic_win
mac          linux
Enter list of allowed OSs for netdirect:
```

- **all:**

All Net Direct client connections are allowed, irrespective of what OS the client runs on.

- **unknown:**

Net Direct clients running on an OS that cannot be identified (for example, new OS versions) are allowed to connect.

- **vista:**

Net Direct clients running on Vista are allowed to connect.

- **winxp:**

Net Direct clients running on Windows XP are allowed to connect.

- **win2k:**

Net Direct clients running on Windows 2000 are allowed to connect.

- **generic_win:**

Net Direct clients running on any other Windows version are allowed to connect.

- **mac:**

Net Direct clients running on Mac OS X are allowed to connect.

- **linux:**

Net Direct clients running on Linux are allowed to connect.

4. Set the desired split tunneling mode (optional).

This step lets you set the desired split tunnel mode. Split tunneling allows network traffic to travel either through a tunnel to the VPN Gateway or directly to the Internet.

- **disabled.**

Tunnels all network traffic through the Net Direct client to the AVG.

- `enabled`.

Tunnels traffic to specified networks (see the `splitnets` command in the next step) to the VPN Gateway. All other network traffic goes through the computer's normal network interface.

- `enabled_inverse`.

Does not tunnel traffic to specified networks (see the `splitnets` command in the next step), that is, traffic goes through the computer's normal network interface. All other network traffic is tunneled through the Net Direct client to the VPN Gateway.

- `enabled_inverse_local`.

Does not tunnel traffic to directly connected networks or to specified networks (see the `splitnets` command in the next step). This will for example, allow the remote user to print locally, even while tunneled to the VPN Gateway. All other network traffic is tunneled through the Net Direct client to the VPN Gateway. This is the default setting.

*** Note:**

The Mac OS X modes `enabled_inverse` and `disabled` do not tunnel the local net. The `enabled_inverse` mode is not supported on the Linux operating system. If the user is running Net Direct on Linux or Mac OS X and the split tunneling mode is not supported, the `enabled_inverse_local` mode is used as fallback.

```
>> SSL VPN Client#splittun

Current value: enabled_inverse_local
Enter one of disabled, enabled, enabled_inverse, or
enabled_inverse_local:
```

5. If **`enabled`**, **`enabled_inverse`** or **`enabled_inverse_local`** was selected in the previous step, specify the network addresses to be tunneled (or not tunneled if any of the inverse modes have been selected).

You can add several entries to the split networks list. Simply enter the `add` command once again after the first network address has been configured.

```
>> SSL VPN Client#splitnets/add

Enter network IP number: 10.1.82.100<example>

Enter netmask: 255.255.255.0<example>
```

6. Apply the changes.

Configure Net Direct Link

Start by selecting the VPN whose Portal web page should be provided with a Net Direct link. Then create a linkset (or use an existing linkset) to include the Net Direct link. The linkset text (optional) defines a heading for links included in the linkset.

1. Create a new linkset or use an existing linkset.

```
# /cfg/vpn 1/linkset 2

Creating Linkset 2

Linkset name:NetDirect<reference this name in the desired user
group>

Linkset text (HTML syntax, eg <b>A heading</b>):Network access

Autorun Linkset (true/false) [false]:<press ENTER>
```

2. Configure a Net Direct link to be displayed on the Portal's Home tab.

```
>> Linkset 2#link

Enter Link number or name (1-256):1

Creating Link 1
Enter link text:NetDirect

Enter type of link (hit TAB to see possible values)
[internal]:netdirect

Entering: NetDirect settings menu
Netdirect link has been created.
Leaving: NetDirect settings menu
```

If Net Direct has not been enabled (see [Enable Net Direct](#) on page 97) you will be prompted for the required information as you create the Net Direct link.

3. Reference the linkset in the desired user group.

If you have not yet created user access groups, you can reference the linkset in the desired group later. For instructions about how to create groups with access rules, see [Groups, Access Rules and Profiles](#) on page 157.

If you added the link to an existing linkset, this linkset may already be mapped to a group.

```
>> Link 1#/cfg/vpn 1/aaa/group

Enter group number or name: (1-1023)1
```

```
>> Group 1#linkset

>> Linksets#add<press TAB following the command to view
available linksets>

Linkset name:NetDirect<note that linkset names are case
sensitive>
```

4. Apply the changes.

Configure Windows Administrator User Name/Password

To be able to download and install the Windows Net Direct client, users have to be administrators on their PCs. For users that are not administrators, you can store the Windows administrator user name and password. The credentials are stored on group level.

This solution is suitable for larger companies, where the administrator account is identical for all or several of the employees' PCs. For successful installation of Net Direct, the administrator credentials entered here must match those of the administrator account on the group members' PCs.

* Note:

By supplying the Windows administrator user name and password as described in the following sections, the security in your Windows environment may be impaired. Carefully consider the risks before proceeding with this option.

1. Find the desired group and specify the Windows administrator user name.

```
>> Main#cfg/vpn 1/aaa/group 1/ndwauser

Current value: " "

Enter windows admin user name:john
```

2. Specify the Windows administrator password.

```
>> Main#cfg/vpn 1/aaa/group 1/ndwapasswo

Current value: " "

Enter windows admin password:password
```

3. Apply the changes.

When a user who belongs to this group logs in to the Portal and tries to download the Net Direct client on a PC that requires administrator privileges when installing new software, installation will be successful.

Tip! Another way of solving the administrator requirement issue is to enable caching of Net Direct components. With caching on, Net Direct need only be installed by an administrator the first time the client is downloaded through the Net Direct link on the Portal's Home tab. After that, the user can download, install and run Net Direct whenever they want. For instructions about how to enable caching, see [2](#) on page 98.

Configure Link for Downloading Installed Version

Follow these steps to create a portal linkset with a link for downloading the installed version of Net Direct.

Start by selecting the VPN whose Portal web page should be provided with a Net Direct link. Then create a linkset (or use an existing linkset) to include the Net Direct link. The linkset text (optional) defines a heading for links included in the linkset.

1. Create a new linkset or use an existing linkset.

```
# /cfg/vpn 1/linkset 2

Creating Linkset 2
Linkset name:Installed_ND<reference this name in the desired
user group>

Linkset text (HTML syntax, eg <b>A heading</b>):<press ENTER to
skip>

Autorun Linkset (true/false) [false]:<press ENTER>
```

2. Configure a Net Direct link to be displayed on the Portal's Home tab.

```
>> Linkset 2#link

Enter Link number or name (1-256):1

Creating Link 1
Enter link text:Download NetDirect installation package

Enter type of link (hit TAB to see possible values)
[internal]:external

Entering: External settings menu
Enter method (http/https):https

Enter host (eg www.company.com):vpn.example.com

Enter path (eg /):/nortel_cacheable/NetDirect_Setup.zip

Leaving: External settings menu
```

3. Reference the linkset in the desired user group.

If you have not yet created user access groups, you can reference the linkset in the desired group later. For instructions about how to create groups with access rules, see [Groups, Access Rules and Profiles](#) on page 157.

If you added the link to an existing linkset, this linkset may already be mapped to a group.

```
>> Link 1#/cfg/vpn 1/aaa/group

Enter group number or name: (1-1023)1

>> Group 1#linkset

>> Linksets#add<press TAB following the command to view
available linksets>

Linkset name:Installed_ND<note that linkset names are case
sensitive>
```

4. Apply the changes.

```
>> Linksets#apply

Changes applied successfully.
```

License Text and Banner

To display a window for the user to accept or reject a license agreement, a custom text can be pasted or entered in the CLI. A text can also be added to display a banner message to the user when Net Direct is successfully downloaded and installed.

* Note:

By suppressing presentation of the Avaya Software License Agreement you agree to accept the terms of the agreement on behalf of the users receiving the client software from you. If you do not wish to accept the license terms on behalf of the users, then do not suppress presentation of the agreement.

1. Enter or paste the desired license text.

This step lets you enter or paste a custom license text to be displayed in Net Direct's License agreement screen. The screen is displayed when Net Direct is started. The license text screen is not displayed for the installed Net Direct client.

* Note:

A license text from Avaya is supplied by default. By entering a new license text, you will replace the default license text. If desired, you can copy and save the

default license text before replacing it. To print the default license text in the CLI (for copying), enter

```
cur ndlicense.
```

If you do not want the License agreement screen to be displayed at all, simply type three periods (...) and press ENTER. This will remove the default license text or any previously entered or pasted custom license text.

```
>> Main#cfg/vpn 1/sslclient/ndlicense

Write or paste the text, press Enter to create a new line, and
then
type"..."

(without the quotation marks) to terminate.

Software License Agreement. Read the license agreement
carefully before accepting or rejecting the
terms. ...

>> SSL VPN Client#
```

Having entered/pasted the text, press ENTER and type three periods (...). Finally press ENTER once again.

2. Enter or paste the desired banner text.

The banner text screen will be displayed for the downloadable client as well as for the installed Net Direct client.

```
>> Main#cfg/vpn 1/sslclient/ndbanner

Write or paste the text, press Enter to create a new line, and
then
type"..."

(without the quotation marks) to terminate.

Welcome! You now have secure access to the intranet
through NetDirect. Do not leave your computer
unattended while connected! ...

>> SSL VPN Client#
```

Having entered/pasted the text, press ENTER and type three periods (...). Finally press ENTER once again.

3. Apply the changes.

To view the result of the configuration done in this example, see the section [Net Direct from a User Perspective](#) on page 106.

Enable Full Access

If not already active, the Net Direct client can be started from the Portal's **Full Access** page (select **Full Access** on the **Access** tab). This however requires that the Full Access feature is enabled.

For more information about starting the SSL VPN client from the **Full Access** page, see [The Portal from an End-User Perspective](#) on page 51.

1. Follow the instructions for enabling Net Direct client access previously in this chapter.
2. Enable the Full Access feature for the desired VPN.

```
>> Main#cfg/vpn 1/portal
>> Portal#faccess
>> Full Access#ena
```

3. Apply the changes.

```
>> Full Access#apply
Changes applied successfully
```

Net Direct from a User Perspective

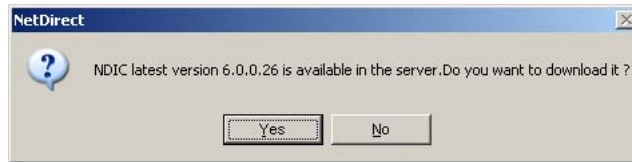
As mentioned previously, the Net Direct client can be downloaded temporarily from the Portal, to be used during a remote user's VPN session, or be installed permanently on the client machine.

Downloadable Version (Windows)

The downloadable version of Net Direct requires that a Net Direct link has been configured by the administrator (see [Server Configuration](#) on page 90). Consider the following instructions as directed to the user.

1. Log in to the Portal.
2. Click the Net Direct link.

If the installed Net Direct client (see [Installed Version \(Windows\)](#) on page 109) is already installed on the user's PC, the following message is displayed:



The installed version takes preference over the downloadable and cached versions.

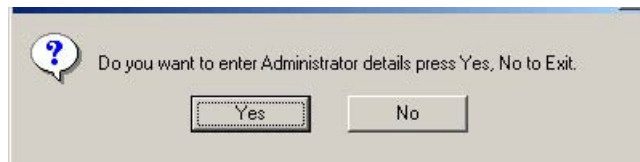
Click **Yes** to start the installed version of the Net Direct client. The Net Direct client window is displayed.

If RIP Listener is activated on the client machine, a message is displayed. It warns the user that the connection can be interrupted if the client computer's routing tables are changed due to an RIP message. RIP Listener is a Windows component that can be disabled if required. For more information about RIP Listener, see Windows Help and Support Center.

3. Click **OK**.

If the user has administrator privileges (which is required to install the Net Direct client), or if the Windows administrator password is stored in the CLI for the group in which the user is member (see [Configure Windows Administrator User Name/Password](#) on page 102), a progress bar is displayed while the Net Direct client is being downloaded.

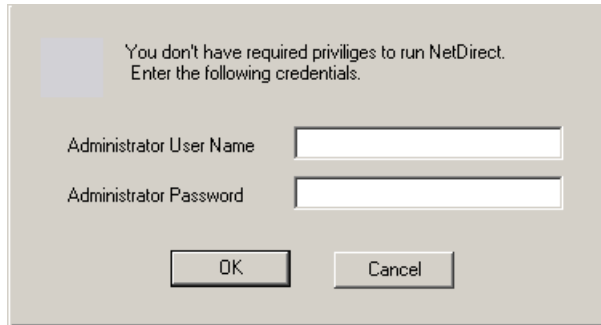
If the user does not have administrator privileges on the PC, the following message is displayed:



4. Click **Yes** if you have access to the Windows administrator user name and password for the PC.

If you click **No**, the process of downloading Net Direct will be cancelled.

The following window is displayed:



5. Enter the Windows administrator user name and password and click **OK**.

If Net Direct has been configured to display a license agreement window (see [License Text and Banner](#) on page 104), the **License Agreement screen** is displayed.

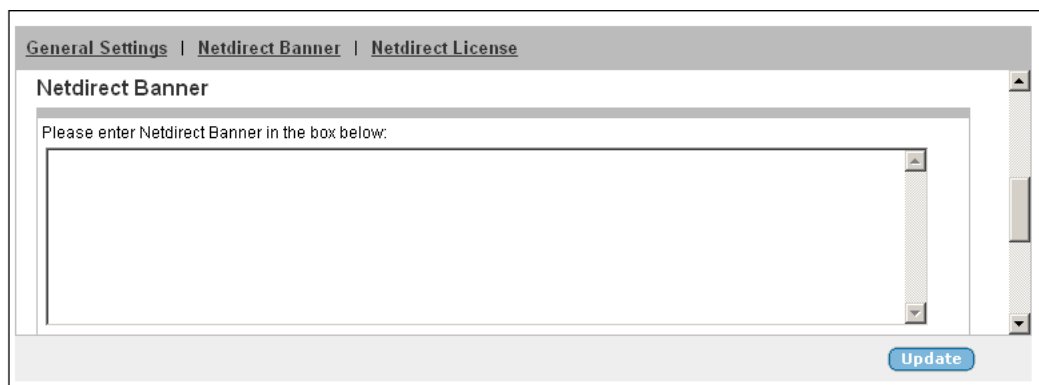
6. If you accept the license terms, click I Agree to continue with the installation.

A progress bar is displayed while the Net Direct client is being downloaded.

*** Note:**

The Net Direct client will not be started if the installable Avaya SSL VPN client or the Avaya IPsec VPN client (formerly the Contivity VPN client) is already running on the remote user's machine.

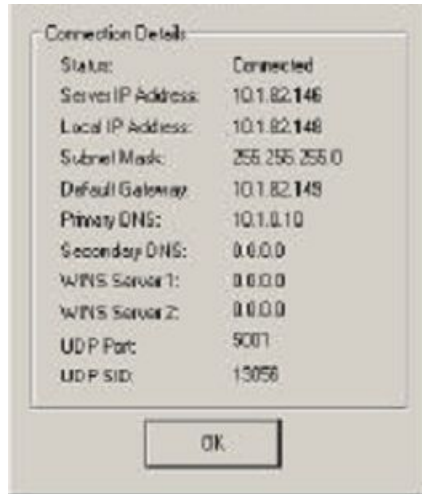
If Net Direct has been configured to display a banner message window (see [License Text and Banner](#) on page 104), this is displayed.



7. Click **OK**.

When the Net Direct client is fully installed and has connected to the VPN server (that is, the VPN Gateway), this is confirmed with an icon being displayed on the system tray.

By right-clicking the system tray icon and selecting **Status**, connection details are displayed:



8. The user can now start the desired TCP- or UDP-based native application to connect to an application server on the intranet.

Because the remote user has already authenticated to the Portal, no further login is required.

9. To exit the session, right-click the Net Direct icon on the system tray and select **Exit**.

When the user logs out from the Portal, reloads the page or closes the browser window, the Net Direct client will exit and be removed from the user's machine.

If errors should occur, the **NetDirectError.log** file is created on the client machine under

- C:\Documents and Settings\\Local Settings\Temp for Windows XP.
- C:\Users\\AppData\Local\Temp for Windows 7 and Windows Vista.

Installed Version (Windows)

As an alternative to the downloadable, session-based version of Net Direct, a Net Direct client installation package can be downloaded from the Portal for the user to install Net Direct permanently on the client machine. This however requires that a download link has been configured by the administrator (see [Configure Link for Downloading Installed Version](#) on page 103). Consider the following instructions as directed to the user.

1. Log in to the Portal.
 2. Click the download link.
- A file download window is displayed.

3. Save the setup.zip file to your desktop.
4. Unzip the file.
5. Run the setup.exe installation package and restart your computer.

This will install the Net Direct client permanently on your machine.

6. Start Net Direct.

Double-click the Net Direct Client icon on your desktop or select Net Direct from the Start menu.

If RIP Listener is activated on the client machine, a message is displayed. It warns the user that the connection can be interrupted if the client computer's routing tables are changed due to an RIP message. RIP Listener is a Windows component that can be disabled if required. For more information about RIP Listener, see Windows Help and Support Center.

7. Click **OK**.

The Net Direct client window is displayed.

8. In the Connection field, enter a name for the connection, for example, VPN 1.

To select a previously saved connection, select the desired entry in the **Connection** list box. All fields except the Password field will be completed.

9. In the User Name and Password fields, enter the credentials given to you for login to the VPN.

10. In the Destination field, enter the IP address or DNS name to the VPN.

IP address (if used) is the same as the Portal IP address. If DNS name is used,

`https://`

need not be entered.

Click **Advanced** to view some additional settings:

- **Port.** Used if another port number than the default SSL port of 443 is used.
- **Login Service.** Lets you select a specific authentication server to log in to (if configured).
- **Save Settings.** Saves the login and destination details (except password). The information is presented as default values the next time you start Net Direct or, if several connections have been defined, selectable in the **Connection** list box.

The "Client DNS Registration" feature will enable NDIC to register the tunnel IP address with the corporate DNS server (2) so that when anybody does a name lookup for the domain name of the laptop, the DNS server responds with the tunnel IP assigned to the laptop.

An alternative way of supplying and saving login details is to select **Connection Wizard** on the **File** menu and follow the steps.

11. Click **Connect**.

When Net Direct has connected to the VPN server, the Net Direct client window is minimized and the Net Direct icon is displayed on the system tray.

If Net Direct has been configured to display a banner message window (see [License Text and Banner](#) on page 104), the **Netdirect Banner** is displayed.

12. Click **OK**.

Three different statuses can be indicated by the Net Direct icon on the system tray.

By right-clicking the system tray icon and selecting **Status**, connection details are displayed:



13. The user can now start the desired TCP- or UDP-based native application to connect to an application server on the intranet.

Because the remote user has already authenticated to the Portal, no further login is required.

14. To exit the session, right-click the Net Direct icon on the system tray and select **Exit**.

When the user logs out from the Portal, reloads the page or closes the browser window, the Net Direct client will exit.

If errors should occur, the **NetDirectError.log** file is created on the client machine under

- C:\Documents and Settings\\Local Settings\Temp for Windows XP

- C:\Users\<user>\AppData\Local\Temp for Windows 7 and Windows Vista.

When connecting to the AVG, the system checks the version of the Net Direct client. If a more recent version is available, the user will have to option to go to a web page where the later version of the client can be downloaded.

Downloadable Version (Mac OS X and iMac)

Only the downloadable version of Net Direct is available for Mac OS X and iMac. The downloadable version of Net Direct requires that a Net Direct link has been configured by the administrator (see [Server Configuration](#) on page 90). Consider the following instructions as directed to the user.

1. Start Safari and log in to the Portal.
2. Click the Net Direct link.

Because you have to be a member of the admin group (or know the root password) to download Net Direct, you are prompted for your password.



3. Enter your password and click **OK**.

If the password is accepted, a Java applet window will be displayed (see next page).

If you are not a member of the admin group, click OK without entering anything in the field. You will then be prompted for the root password in a second login window. If you enter the wrong password in the preceding dialog, you will automatically be redirected to the root password dialog.



4. Enter the root password and click **OK**.

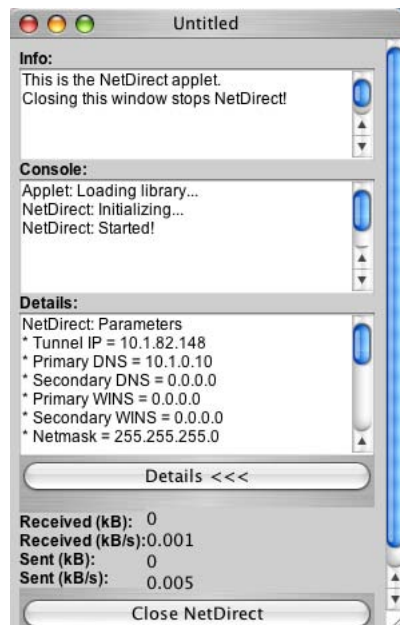
If the password is accepted, a Java applet window will be displayed (see following steps).

If you do not know the root password, Net Direct cannot be downloaded.

When the Net Direct client is fully installed and has connected to the VPN server (that is, the VPN Gateway), this is confirmed in the Java applet window.



Click the Details button to display connection details:



5. The user can now start the desired TCP- or UDP-based native application to connect to an application server on the intranet.

Because the remote user has already authenticated to the Portal, no further login is required.

6. To exit the session, click the Close Net Direct button in the Java applet window.

When the user logs out from the Portal, reloads the page or closes the browser window, the Net Direct client will exit and be removed from the user's machine.

If errors should occur, the **NetDirectError.log** file is created under `/tmp` on the client machine. This is the same path as for Linux.

Start Net Direct Outside Portal

The VPN Gateway can be configured to redirect the remote user to another web page (for example, corporate Portal), thus by-passing the AVG Portal altogether. This section describes the steps involved to be able to start the Net Direct client from the internal page.

For automatic login to the internal page, see the next section.

1. Configure automatic redirection.

```
>> Main#cfg/vpn #/portal/redirect

Current value: " "

Enter URL to redirect to:https://<var:portal>/http/
inside.example.com
```

2. On the web server to which the user should be redirected, insert the following script:

```

<%@ Language=VBScript %>
<HTML>
<HEAD>
<TITLE>NetDirect</TITLE>
</HEAD>
<BODY>
<OBJECT id=NetDirectOCX style="LEFT: 0px; TOP: 0px"
codeBase="https://YourAVGAddress/avaya_cacheable/NetDirect.cab#VERSION=6,0,1"
height=0 width=0
classid=clsid:7fa319fb-ffb9-4089-87eb-63179244e6e6><PARAM
NAME="_Version" VALUE="65536"><PARAM NAME="_ExtentX"
VALUE="26"><PARAM NAME="_ExtentY" VALUE="26"><PARAM
NAME="_StockProps" VALUE="0"></OBJECT>
Hello <%= Request.QueryString("user") %> : <%=
Request.QueryString("password") %>.
You want to access <%= Request.QueryString("portal") %>!
<%
If Request.QueryString("UserStatus") = "New" Then
Response.Write "If you have any problems with the site call the helpdesk!"
End If
Dim portal
portal = Request.QueryString("portal")
Response.Write "<SCRIPT LANGUAGE=JavaScript>
NetDirectOCX.StartDownload('/avaya_cacheable/
NetClient.zip', '443', '', '', '' & Request.QueryString
("portal") & '', '' & Request.QueryString
("user") & '', '' & Request.QueryString("password") & '', '', '', '');</SCRIPT>"
%>
</BODY>
</HTML>

```

Make sure that the correct version of the Net Direct client is specified. In the OBJECT tag in the preceding example, version 7.0.1 will be downloaded from the VPN Gateway.

Note that the sample html code on the previous page is not production code. Error handling adapted to your application should also be added.

Also note that newlines inserted into the script may damage the script.

Start Net Direct Outside Portal with Auto-Login

This example shows how to automatically log in the remote user to the internal site.

1. Configure automatic redirection.

```

>> Main#cfg/vpn #/portal/redirect

Current value: ""

Enter URL to redirect to:http:// <var:portal> /http/
InternalWebServer/NetDirect.asp? portal= <var:portal>
&user= <var:user> &password= <var:password>

```

Continued on next page.

2. On the web server to which the user should be redirected, insert the following script:

```
<%@ Language=VBScript%>
<HTML>
<HEAD>
<TITLE>NetDirect</TITLE>
</HEAD>
<BODY>
<OBJECT id=NetDirectOCX style="LEFT: 0px; TOP: 0px"
codeBase="https://YourAVGAddress/nortel_cacheable/
NetDirect.cab#VERSION=6,0,1"
height=0 width=0
classid=clsid:7fa319fb-ffb9-4089-87eb-63179244e6e6><PARAM
NAME="_Version" VALUE="65536"><PARAM NAME="_ExtentX"
VALUE="26"><PARAM NAME="_ExtentY" VALUE="26"><PARAM
NAME="_StockProps" VALUE="0"></OBJECT>
Hello <%= Request.QueryString("user") %> : <%=
Request.QueryString("password")%>.
You want to access <%= Request.QueryString("portal") %>! <%
If Request.QueryString("UserStatus") = "New" Then
Response.Write "If you have any problems with the site call the
helpdesk!"
End If
Dim portal
portal = Request.QueryString("portal")
Response.Write "<SCRIPT LANGUAGE=JavaScript>
NetDirectOCX.StartDownload('/nortel_cacheable/
NetClient.zip', '443', '', '', '' & Request.QueryString
("portal") & '', '' & Request.QueryString
("user") & '', '' & Request.QueryString("password") & '', '', '',
'');</SCRIPT>"
%>
</BODY>
</HTML>
```

Make sure that the correct version of the Net Direct client is specified. In the OBJECT tag in the preceding example, version

7.0.1

will be downloaded from the VPN Gateway.

Note that the sample html code is not production code. Error handling adapted to your application should also be added.

Also note that newlines inserted into the script may damage the script.

Chapter 8: Authentication Methods

This chapter describes how to select an authentication method for the VPN (Portal), and how to configure the settings of a particular method. After having configured the desired authentication methods, you should also specify in which order the authentication methods should be applied when a user logs in to the Portal.

External Database Authentication

The following external database authentication methods are supported:

- RADIUS
- LDAP
- NTLM
- SiteMinder
- RSA SecurID
- RSA ClearTrust

When a remote user wants to access a resource provided in the VPN, the Avaya VPN Gateway (AVG) authenticates the user by sending a query to an external RADIUS, LDAP, NTLM domain, Netegrity SiteMinder, RSA SecurID or RSA ClearTrust server. This makes it possible to use existing authentication databases within the intranet. The VPN Gateway includes username and password in the query and requires the name of one or more access groups in return. The name of the LDAP and RADIUS access group attribute is configurable.

You can configure more than one authentication method within any given VPN.

The authentication subsystem caches responses given to queries sent to the external databases. The TTL for the cache is the same as the idle timeout. The cache significantly relieves the burden put on the external databases.

Local Database Authentication

The VPN Gateway can also act as an authentication database itself. It can store thousands of user authentication entries each defining a user name, password, and the relevant access groups. This local authentication method can be useful if no external authentication databases exist, for testing purposes or if speedy deployment is needed. The local database authentication method can actually be used as a fallback to external database queries. If for

example a query to an LDAP server fails the VPN Gateway can query its own database. This comes handy if a client is to gain access to corporate resources for only a limited time.

Local database authentication is described on [Local Database Authentication](#) on page 147.

Client Certificate Authentication

With client certificate authentication enabled on the VPN Gateway, no Portal login is required for remote SSL users having a valid client certificate installed on their computers. When the Portal login has accepted the certificate, the user is directed straight to the Portal's Home tab.

With a signed client certificate imported to the remote user's Windows machine, users with the Avaya IPsec VPN client (formerly Contivity VPN client) or the users with NDIC can authenticate to the VPN through client certificate authentication once the client certificate has been selected in the IPsec VPN client.

Client certificate authentication is described on [Client Certificate Authentication](#) on page 149.

Login Service List Box

To support redirection to a specific authentication server, for example, for token login or for redirection to a specific Windows domain, the authentication method can be assigned a display name. This name (for example,

`SafeWord`

) will be selectable in the Login Service list box on the Portal login page and in the Avaya SSL VPN client login window, directing the user straight to the proper server for authentication. If the user selects

`default`

in the Login Service list box, authentication is carried out according to the configured authentication order.

Secondary and Two Factor authentication

When assigning authentication servers, you have the option to specify a second authentication server to use after the first one succeeds. With this option you enable both SSL Secondary authentication and IPsec Two Factor authentication.

The secondary authentication method is a feature primarily designed to support single-sign on to backend servers in cases where the first authentication method is token-based or uses client certificate authentication. You can use only RSA, SecurID, RADIUS and client certificate authentication mechanisms for a secondary authentication server. In IPsec Two Factor authentication the client provides both the username and password to the requesting server while in SSL Secondary authentication the client needs to provide only the password. Configuring a new certificate authentication server automatically supports IPsec Two Factor authentication. IPsec Two Factor authentication supports only certificate authentication as primary servers and local, RADIUS or LDAP as secondary servers.

*** Note:**

- To ensure SSL Secondary authentication works concurrently with IPsec Two Factor authentication, add the user ID from the certificate to the second authentication server
- To ensure that IPsec Two Factor authentication works concurrently with SSL Secondary authentication, manually add the user ID from the certificate when configuring a primary IPsec Two Factor authentication server

You can enable both SSL Secondary authentication and IPsec Two Factor authentication by selecting a secondary server from the **Secondary Authentication Server** list found in the VPN Gateways, <VPN Gateway name>, Authentication, <Authentication server name>, **Advanced** tab whenever you are adding or editing authentication servers.

RADIUS Authentication

The RADIUS authentication method lets you configure user authentication through an existing intranet RADIUS server. The RADIUS method supports Challenge/Response as well as token login methods such as SecurID, SafeWord and ActivCard.

1. Create a new VPN, or configure an existing VPN.

If you have already created a VPN to which you want to add RADIUS authentication, type the desired VPN number. To create a new VPN, type a VPN number not currently in use.

```
#/cfg/vpn

Enter vpn number (1-256):1
```

2. Create an authentication ID for RADIUS authentication.

Each time you create a new authentication ID, you will enter a wizard that prompts you for the required information. After the wizard is completed you will enter the regular menu for the current object.

```
>> VPN 1# aaa/auth
```

```
Enter auth id: (1-63)1
Creating Authentication 1
```

3. Select the authentication method, that is, **radius** .

This wizard step corresponds to entering **type** on the Authentication menu and selecting the desired authentication method.

```
Select one of radius, ldap, ntlm, siteminder, cleartrust, cert,
rsa or local:radius
```

4. Specify a name for the authentication method.

A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used. For more information about client filters, see [Groups, Access Rules and Profiles](#) on page 157.

This wizard step corresponds to entering **name** on the Authentication menu.

```
Auth name:radius
```

5. Specify the RADIUS server's IP address and port.

Port number 1812 is the default number but it can be changed if the RADIUS server uses another port number for the specified service.

```
IP Address to add:10.30.10.1 <example RADIUS server IP address>
Port (default is 1812):<press Enter for default port>
```

6. Enter a unique shared secret (password).

The shared secret is used to authenticate the VPN Gateway to the RADIUS server. Contact your RADIUS server administrator to obtain the shared secret.

```
Enter shared secret:<shared secret>
```

7. Specify the Vendor-ID for the group attribute.

This attribute is set to

```
1872 (alteon)
```

by default. It should correspond to the Vendor-Id used by your RADIUS server to send group names to the client. If your RADIUS server uses another Vendor-Id, you can change this value. Contact your RADIUS server administrator for more information. If you want to use a standard RADIUS attribute other than vendor-specific, set Vendor-Id to 0 and Vendor-Type to the desired attribute number (for example, 25 for class).

```
Enter vendor id for group attribute [alteon]:
```

8. Specify the Vendor-Type value for the group attribute.

The vendor type value is set to

```
1 (alteon-xnet-group)
```

by default. If your RADIUS server uses another Vendor-Type number, you can change this value. Contact your RADIUS server administrator for more information. Used in combination with the Vendor-Id number, the Vendor-Type number identifies the group in which users who should be allowed access to the VPN through RADIUS authentication are members. The group name(s) to which the vendor specific attribute points must be defined in the VPN, complete with one or more access rules (see [Groups, Access Rules and Profiles](#) on page 157 on [Authentication Methods](#) on page 117 for more information).

```
Enter vendor type for group attribute [1]:
```

9. Specify the Vendor-ID for the VPN ID attribute.

This attribute is set to

```
1872 (alteon)
```

by default. When a user authenticates to a specific VPN (as configured on the AVG), the AVG sends the VPN ID to the RADIUS server. The RADIUS server in its turn can make use of the VPN ID to return user information (for example, from a VPN-specific user database). The Vendor-Id should correspond to the Vendor-Id used by your RADIUS server. If your RADIUS server uses another Vendor-Id, you can change this value. Contact your RADIUS server administrator for more information.

```
Enter vendor id for VPN ID attribute [alteon]:
```

10. Specify the Vendor-Type value for the VPN ID attribute.

The vendor type value is set to 3 by default. If your RADIUS server uses another Vendor-Type number, you can change this value. Contact your RADIUS server administrator for more information. Used in combination with the Vendor-Id, the Vendor-Type number identifies the VPN to which the remote user has logged in.

```
Enter vendor type for VPN ID attribute [3]:
Leaving: RADIUS settings menu
```

When the preceding information is supplied, the Authentication menu is displayed. The

```
radius
```

option has been added, because the current authentication type is now set to

radius

.

[Authentication 1 Menu]	
type	- Set authentication mechanism
name	- Set auth name
display	- Set auth display name
domain	- Set windows domain for backend single sign-on
radius	- RADIUS settings menu
adv	- Advanced settings menu
del	- Remove Authentication

The RADIUS server IP address, port and shared secret settings can be edited under

radius /servers

. This is also where additional RADIUS servers can be added for redundancy.

Commands to edit the Vendor-Id and Vendor-Type attributes (for group names and VPN ID), RADIUS server timeout, idle timeout, session timeout and RADIUS macros are found under

radius

.

For Net Direct and IPsec user tunnels, network attributes (including client IP address) can be retrieved from a RADIUS server. If this is desired, set the **/cfg/vpn #/ippool #/type** command to

radius

. Then specify the required Vendor-Id and Vendor-Type values to retrieve network attributes from the RADIUS server, using the **netattr** command (found under

radius

in the preceding menu).

For a full explanation of all RADIUS authentication commands, see the *Command Reference*.

11. To direct the user to this specific authentication method, set the desired display name (optional).

The display name appears in the Login service list box on the Portal login page, in the SSL VPN client's login window and in the installed Net Direct client's login window. This is a way of quickly directing the remote user to the proper authentication server, if the VPN uses different authentication methods. If the user selects

default

in the list box, authentication is carried out according to the configured authentication order.

```
>> Authentication 1#display

Current value: " "

Auth display name:SafeID
```

12. Specify the authentication fallback order.

This step sets the preferred order for which configured authentication methods are applied when a remote user logs in to the Portal. Even if you have defined only one authentication method, this authentication ID should be specified.

When using more than one authentication method, specify the authentication ID that represents the method by which the main bulk of users are authenticated as the first number for best performance.

```
>> Authentication 1#../authorder

Current value:

Enter auth order (comma separated):1
```

13. Apply your configuration changes.

```
>> AAA#apply

Changes applied successfully.
```

LDAP Authentication

The LDAP authentication method lets you configure authentication towards an existing intranet LDAP server. The LDAP method also supports some advanced Active Directory features (for example, bookmarks and password expiry check) that are currently not supported by the NTLM authentication scheme.

1. Create a new VPN, or configure an existing VPN.

If you have already created a VPN (=Portal) to which you want to add LDAP authentication, type the desired VPN number. To create a new VPN, type a VPN number not currently in use.

```
#/cfg/vpn

Enter vpn number (1-256):1
```

2. Create an authentication ID for LDAP authentication.

Each time you create a new authentication ID, you will enter a wizard that prompts you for the required information. After the wizard is completed you will enter the regular menu for the current object.

```
>> VPN 1#aaa/auth

Enter auth id: (1-63)1

Creating Authentication 1
```

3. Select the authentication method, that is, **ldap**.

This wizard step corresponds to entering **type** on the Authentication menu and selecting the desired authentication method.

```
Select one of radius, ldap, ntlm, siteminder, cleartrust, cert,
rsa or local:ldap
```

4. Specify a name for the authentication method.

A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used. For more information about client filters, see [Groups, Access Rules and Profiles](#) on page 157.

This wizard step corresponds to entering **name** on the Authentication menu.

```
Auth name:AD Entering: LDAP settings menu Entering:
LDAP servers menu
```

5. Specify the LDAP vendor.

This step lets you specify the authentication server that can be accessed using LDAP.

```
Select the LDAP server vendor (microsoft/sun/novell/other):
[microsoft]
```

6. Specify the LDAP server IP address.

This step adds an LDAP server that is queried to perform authentication of a remote user prior to accessing resources on the Portal.

```
IP Address to add:192.168.10.85 <example LDAP server IP
address> Leaving: LDAP servers menu
```

7. Specify the search base entry.

This step assigns the DN (Distinguished Name) that points to the entry that is one level up from where all user entries are found.

```
Search Base Entry: Administrator DN
(cn=Administrator,cn=Users,dc=bluetail,dc=com):Administrator
DN [cn=Administrator,cn=Users,dc=bluetail,dc=com]
<example of searchbase syntax>
```

If user entries are located in several different places in the LDAP Dictionary Information Tree (DIT) or if the user's Portal login name is not identical with the user record identifier (RDN), a DN pointing to an entry from where the entire DIT can be searched should be assigned. This however requires the VPN Gateway to authenticate itself to the LDAP server, using the values specified for

```
isdBindDN
```

and

```
isdBindPassword
```

(see following steps). Also see example on [Search the LDAP Dictionary Information Tree \(DIT\)](#) on page 128.

8. Specify the LDAP group attribute name.

This step defines the LDAP attribute that contains the group names of which a particular user is a member. The group names in the LDAP attribute must be defined for the VPN on the VPN Gateway, complete with one or more access rules. If you specify more than one group attribute name, separate the names using comma (,).

```
Group attribute name (default is memberOf):<group attribute name>
```

9. Specify the LDAP user attribute name.

This step defines the LDAP attribute that contains the user names. The default user attribute name is uid.

```
User attribute name (default is sAMAccountName):<user attribute
name>
```

10. Specify the `isdBindDN` entry and Password (optional).

This step lets you point out an LDAP entry (distinguished name) to which the VPN Gateway should authenticate. Normally, this step can be skipped. It is only required if the VPN Gateway should authenticate to the LDAP server, for example, to be able to search the Dictionary Information tree (DIT). See example on [Search the LDAP Dictionary Information Tree \(DIT\)](#) on page 128.

```
Administrator DN: cn=Administrator,cn=Users,dc=bluetail,dc=com
Password: ldap
```

11. Specify if LDAPS should be used for traffic between the VPN Gateway and the LDAP server.

By setting this command to **true**, LDAP requests between the VPN Gateway and the LDAP server are made using a secure SSL connection, that is, LDAPS. The default value is **false**, which will be kept on pressing ENTER.

```
Enable LDAPS (true/false):
Leaving: LDAP settings menu
```

When the preceding information is supplied, the Authentication menu is displayed. The

```
ldap
```

option has been added to the menu, because the current authentication type is now set to

```
ldap
```

```
.
```

```
[Authentication 2 Menu]

type      - Set authentication mechanism
name      - Set auth name
display   Set auth display name
domain    - Set windows domain for backend single sign-on
ldap      - LDAP settings menu
adv       - Advanced settings menu
```

```
del - Remove Authentication
```

If needed, the IP address and port settings can be edited under

```
ldap/servers
```

. This is also where additional LDAP servers can be added for redundancy. Other LDAP commands, for example, to edit the search base entry, group and user attributes, LDAP server timeout and so on are found under

```
ldap
```

.

For a full explanation of available LDAP commands, see the *Command Reference*.

12. Set the desired display name for this authentication method (optional).

The display name appears in the Login service list box on the Portal login page, in the SSL VPN client's login window and in the installed Net Direct client's login window. This is a way of quickly directing the remote user to the proper authentication server, if the VPN uses different authentication methods. If the user selects

```
default
```

in the list box, authentication is carried out according to the configured authentication order.

```
>> Authentication 2#display

Current value: " "

Auth display name:LDAP<example display name>
```

13. Specify the authentication fallback order.

This step sets the preferred order for which the defined authentication methods are applied when a remote user logs in to the Portal. Even if you have defined only one authentication method, the authentication ID should be specified. To view which authentication ID number that corresponds to a currently configured authentication method, use the `/cfg/vpn #/cur` command.

When using more than one authentication method, specify the authentication ID that represents the method by which the main bulk of users are authenticated as the first number for best performance.

```
>> Authentication 1#../authorder

Current value: 1

Enter auth order (comma separated):
```

```
1,2
```

14. Apply your configuration changes.

```
>> AAA#apply
Changes applied successfully.
```

Search the LDAP Dictionary Information Tree (DIT)

Searching the LDAP Dictionary Information Tree (DIT) is necessary if

- user entries are located in several different places in the DIT
- if the user's Portal login name is not identical with the user record identifier (RDN) on the LDAP server.

The following example shows the adjustments that have to be made to the LDAP configuration if the user's Portal login name is not identical with the user record identifier (RDN) on the LDAP server.

1. Set the LDAP searchbase entry.

This step assigns a DN pointing to a position in the DIT from where all user records can be found.

```
>> Authentication 2#ldap
>> LDAP#searchbase
Current value:<not set>
Search Base Entry:ou=people,dc=foo,dc=com
(example of searchbase syntax)
```

2. Set the LDAP user attribute name.

In this example, the user's portal login name is not identical with the user record identifier (RDN). To find the user record in the LDAP Dictionary Information Tree (DIT), a combination of the user's login name and a user attribute is used when searching the tree.

In Active Directory, the

sAMAccountName

attribute contains the value that corresponds to the user's login name. Thus, if the user's login name is

```
bill
, the user record is found because it matches the
sAMAccountName
attribute value for the user whose record identifier (RDN) is
cn=bill smith
.
```

```
>> LDAP#userattr
Current value: uid
Attribute name:sAMAccountName
(example of user attribute)
```

3. Point out an LDAP entry to be used for AVG authentication.

To be able to search the DIT, the VPN Gateway must authenticate itself towards the LDAP server.

```
>> LDAP#isdbinddn
Current value: " "
DN:
(distinguished name)
```

4. Set a password for AVG authentication.

This step sets the password to be used when the VPN Gateway authenticates itself to the LDAP entry pointed out with the isdbinddn command.

```
>> LDAP#isdbindpas
Current value: " "
Enter password:
(password)
```

5. Apply your configuration changes.

```
>> LDAP#apply
Changes applied successfully.
```

NTLM Authentication

The NTLM authentication method lets you configure authentication towards a Windows server, Samba or Novell server. The NTLM method works with Active Directory, but if more advanced AD features like bookmarks and password expiry checks are desired, you should use the LDAP authentication method instead (see [LDAP Authentication](#) on page 123).

1. Create a new VPN, or configure an existing VPN.

If you have already created a VPN (=Portal) to which you want to add NTLM authentication, type the desired VPN number. To create a new VPN, type a VPN number not currently in use.

```
# /cfg/vpn  
  
Enter vpn number (1-256): 1
```

2. Create an authentication ID for NTLM authentication.

Each time you create a new authentication ID, you will enter a wizard that prompts you for the required information. After the wizard is completed you will enter the regular menu for the current object.

```
>> VPN 1#aaa/auth  
  
Enter auth id:3  
  
Creating Authentication 3
```

3. Set the authentication method to NTLM.

This wizard step corresponds to entering **type** on the Authentication menu and selecting the desired authentication method.

```
Select one of radius, ldap, ntlm, siteminder, cleartrust, cert,  
rsa  
or local:ntlm
```

4. Set the desired name for this authentication method.

A name is required. If the authentication method should later be referenced in a client filter, it is the method's name that should be referenced. For more information about client filters, see [Groups, Access Rules and Profiles](#) on page 157.

This wizard step corresponds to entering **name** on the Authentication menu.

```
Auth name:ntlm
```

5. Configure the NTLM server settings.

This step adds an NTLM server that is queried to perform user authentication.

```
IP Address to add:10.30.10.3 <example NTLM server IP address>
```

When the preceding information is supplied, the Authentication menu is displayed. The ntlm option has been added to the menu, because the current authentication type is now set to ntlm .

[Authentication 3 Menu]	
type	- Set authentication mechanism.
name	- Set auth name.
domain	- Set windows domain for backend single sign-on.
ntlm	- NTLM settings menu.
adv	- Advanced settings menu.
ena	- Enable Authentication.
del	- Remove Authentication.

If needed, the IP address can be edited under **ntlm/servers**. This is also where additional NTLM servers can be added for redundancy. Other NTLM commands are found under

```
ntlm
```

```
.
```

For a full explanation of available NTLM commands, see the *Command Reference*.

6. If you have multiple NTLM domains, set the desired display name (optional).

Set the display name to the Windows domain name of the NTLM server. The name appears in the Login Service list box on the Portal login page, in the SSL VPN client's login window and in the installed Net Direct client's login window. If the user selects this name from the list box, the authentication method associated with the name will automatically be used. If the user selects

```
default
```

instead, authentication will be carried out according to the configured authentication order.

```
>> Authentication 3#display

Current value: " "

Auth display name:<e.g. Windows domain name>
```

7. Specify the authentication fallback order.

This step sets the preferred order for which the defined authentication methods are applied when a remote user logs in to the Portal. Even if you have defined only one authentication method, the authentication ID representing that method should be specified. To view which authentication ID number that corresponds to a currently configured authentication method, use the `/cfg/vpn #/cur` command.

When using more than one authentication method, specify the authentication ID that represents the method by which the main bulk of users are authenticated as the first number for best performance.

```
>> Authentication 3#../authorder

Current value: 1,2
Enter auth order (comma separated):1,2,3
```

8. Apply your configuration changes.

```
>> AAA#apply

Changes applied successfully.
```

Netegrity SiteMinder Authentication

To configure the AVG to use a Netegrity SiteMinder server for user authentication is fairly easy. On the other hand, a great deal of configuration is required on the SiteMinder side. The VPN Gateway acts as a client, or agent, to the SiteMinder server. Therefore, the VPN Gateway should be configured as an agent in SiteMinder.

* Note:

SiteMinder authentication cannot be configured for VPNs that are bound to a specific interface using the `/cfg/vpn #/adv/interface` command. Binding VPNs to interfaces are typically used in a Secure Service Partitioning configuration (also see [Secure Service Partitioning](#) on page 313). An exception to the above is when common authentication is enabled for the VPN, using the `/cfg/vpn #/adv/cauth` command.

1. Create a new VPN, or configure an existing VPN.

If you have already created a VPN (Portal) to which you want to add SiteMinder authentication, type the desired VPN number. To create a new VPN, type a VPN number not currently in use.

```
# /cfg/vpn

Enter vpn number (1-256):1
```

2. Create an authentication ID for SiteMinder authentication.

Each time you create a new authentication ID, you will automatically enter a wizard that prompts you for the required information. After the wizard is completed you will enter the regular menu for the current object.

```
>> VPN 1#aaa/auth

Enter auth id:4

Creating Authentication 4
```

3. Select the desired authentication mechanism, that is, siteminder.

This step is equivalent to enter **type** on the

Authentication

menu and select the desired authentication method.

```
Select one of radius, ldap, ntlm, siteminder, cleartrust, cert,
rsa
or local:siteminder
```

4. Set the desired name for this authentication method.

A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used as the reference. For more information about client filters, see [Groups, Access Rules and Profiles](#) on page 157. This wizard step corresponds to entering **name** on the Authentication menu.

```
Auth name:siteminder
```

5. Configure the SiteMinder server settings

This step adds a SiteMinder server that is queried to perform user authentication.

```
IP Address to add:47.133.63.28 <example of IP address>
```

6. Confirm the suggested port numbers for authentication, authorization and accounting.

```
Authentication Port (default is 44442):<press ENTER to accept>
Authorization Port (default is 44443):<press ENTER to accept>
Accounting Port (default is 44441):<press ENTER to accept>
```

7. Enter a unique shared secret (password) that the VPN Gateway is used to authenticate itself to the SiteMinder server.

Apart from the shared secret, the VPN Gateway also uses its agent name (default agent name is

Avaya Agent

) and a group attribute (default group attribute is

64

). These three values MUST be the same as those defined for Agent and Agent Type in the SiteMinder Policy Server configuration. See the Technical Configuration Guide *Using Netegrity SiteMinder with Avaya VPN Gateway*.

```
Shared secret:secret
```

8. Specify whether or not SSO (single sign-on) should be allowed.

If set to `true`, the VPN Gateway is configured to automatically log in a remote user to the VPN if the user has a valid `SMSESSION` cookie from some other SiteMinder-enabled site. This works as long as the VPN (e.g. `vpn.example.com`) and the other SiteMinder-enabled site (e.g. `a.example.com`) are on the same DNS domain. The SiteMinder session will however be invalidated when the user logs out from the Portal, if `/cfg/vpn #/server /portal/wipecookie` is set to

on

(default value).

If the remote user logs in to `vpn.example.com` without a valid `SMSESSION` cookie, the VPN Gateway sets the `SMSESSION` cookie as a domain cookie. This way the user can auto-log in to `a.example.com`. The SiteMinder session will however be invalidated if the user logs out from the Portal.

*** Note:**

If `sso` is set to `true` but no display name or authentication order is configured for the SiteMinder authentication method on the VPN Gateway, it is not possible to log in to the VPN without a valid `SMSESSION` cookie.

Also see the **display** command in step 10 and the **authorder** command in step 11.

The default value is

```
false
```

```
.
```

```
Allow sso (true/false):true
```

9. Enter the desired domain scope.

This setting determines the value of the domain cookie when

```
sso
```

(see preceding step) is set to

```
true
```

```
.
```

- Scope

```
= 0:
```

The most specific domain name will be calculated from the host name. If the Portal's host name is

```
a.b.c.d.e
```

, the domain cookie's value will be

```
.b.c.d.e
```

```
.
```

- Scope

```
= 3:
```

If the Portal's host name is

```
a.b.c.d.e
```

, the domain cookie's value will be

```
.c.d.e
```

```
.
```

- Scope

```
= 2:
```

If the Portal's host name is

```
a.b.c.d.e
```

, the domain cookie's value will be

.d.e

.

The scope must be either

0

or greater than or equal to

2

.

The default value is

0

.

```
domain scope (integer > 1) :
```

When the preceding information is supplied, the Authentication menu is displayed. The

```
siteminder
```

option has been added to the menu, because the current authentication type is now set to

```
siteminder
```

.

```
Authentication 1 Menu
  type      - Set authentication mechanism
  name      - Set auth name
  display   - Set auth display name
  domain    - Set windows domain for backend single sign-on
  siteminder - Netegrity SiteMinder settings menu
  adv       - Advanced settings menu
  del       - Remove Authentication
```

If needed, the IP address can be edited under

```
siteminder/servers
```

. This is also where additional SiteMinder servers can be added for redundancy. Other SiteMinder commands (for example, for changing agent name, shared secret or group attribute and for configuring single-sign on) are found under `siteminder` .

For a full explanation of available SiteMinder commands, see the *comnet:Command Reference*.

10. Set the desired display name (optional).

The display name will appear in the Login service list box on the Portal login page, in the SSL VPN client's login window and in the installed Net Direct client's login window. This is a way of quickly directing the remote user to the proper

authentication server, if the VPN uses different authentication methods. If the user selects `default` in the list box, authentication will be carried out according to the configured authentication order .

```
>> Authentication 4#display

Current value: " "

Auth display name:(enter a name that is comprehensible to the end
user)
```

11. Specify the authentication fallback order.

This step sets the preferred order for which the defined authentication methods are applied when a remote user logs in to the Portal. Even if you have defined only one authentication method, the authentication ID representing that method should be specified.

```
>> Authentication 4#../authorder

Current value: 1,2,3
Enter auth order (comma separated):1,2,3,4
```

12. Apply your configuration changes.

RSA ClearTrust Authentication

Besides installing the ClearTrust components (see the ClearTrust documentation) on the desired machines in your network, you should also configure the VPN Gateway to act as a ClearTrust web server agent and point out configured ClearTrust dispatcher(s) or authorization server(s).

The VPN Gateway sets a ClearTrust single-sign-on cookie in the client browser. This means that the user does not have to log in once again if requesting a password-protected web page on a ClearTrust-aware backend server. The cookie is automatically validated against the ClearTrust authorization server.

This manual assumes that you are familiar with ClearTrust or have access to ClearTrust documentation. The following instructions describe the configuration required on the VPN Gateway.

1. Create a new VPN, or configure an existing VPN.

If you have already created a VPN (Portal) to which you want to add RSA ClearTrust authentication, type the desired VPN number. To create a new VPN, type a VPN number not currently in use.

```
# /cfg/vpn
```

```
Enter vpn number (1-256):1
```

2. Create an authentication ID for ClearTrust authentication.

Each time you create a new authentication ID, you will automatically enter a wizard that prompts you for the required information. After the wizard is completed you will enter the regular menu for the current object.

```
>> VPN 1# aaa/auth

Enter auth id:5

Creating Authentication 5
```

3. Select the desired authentication mechanism, that is, **cleartrust**.

This step is equivalent to enter **type** on the **Authentication** menu and select the desired authentication method.

```
Select one of radius, ldap, ntlm, siteminder, cleartrust, cert,
rsa
or local:cleartrust
```

4. Set the desired name for this authentication method.

A name is mandatory. If the current authentication method should later be referenced in a client filter, this name should be used as the reference. For more information about client filters, see [Groups, Access Rules and Profiles](#) on page 157. This wizard step corresponds to entering **name** on the **Authentication** menu.

```
Auth name:cleartrust
```

5. Configure the ClearTrust dispatcher settings

*** Note:**

The RSA SecurID New Pin mode is not supported when using Secondary Authentication service.

This step lets you point out one or several dispatchers that have previously been installed in the RSA ClearTrust setup. The dispatcher is a ClearTrust component responsible for providing information to the RSA ClearTrust web server agents about the availability of the authorization servers. It enables the agents to choose a new authorization server at start-up or if there is a failure. See the ClearTrust documentation for more information about the Dispatcher component.

```
Entering: RSA ClearTrust settings menu
Entering: ClearTrust dispatchers menu
Hostname to add:dispatcher.example.com
```

6. Confirm the suggested port number for authentication.

If your ClearTrust dispatcher uses another port number you can change the default value of 5608.

```
Authentication Port (default is 5608):<press ENTER to accept>
```

7. Specify whether or not SSO (single sign-on) should be allowed.

If set to `true`, the VPN Gateway is configured to automatically log in a remote user to the VPN if the user has a valid CTSESSION cookie from some other ClearTrust-enabled site. This works as long as the VPN (e.g. `vpn.example.com`) and the other ClearTrust-enabled site (e.g. `a.example.com`) are on the same DNS domain.

The ClearTrust session will however be invalidated when the user logs out from the Portal, if `/cfg/vpn #/server/portal/wipecookie` is set to

on

(default value).

If the remote user logs in to `vpn.example.com` without a valid CTSESSION cookie, the VPN Gateway will set the session cookie as a domain cookie. This way the user can auto-log in to `a.example.com`. The ClearTrust session will however be invalidated if the user logs out from the Portal.

*** Note:**

If

`sso`

is set to

`true`

but no display name or authentication order is configured for the ClearTrust authentication method on the VPN Gateway, it will not be possible to log in to the VPN without a valid CTSESSION cookie.

Also see the `display` command in step 10 and the `authorder` command in step 11.

The default value is `false`.

```
Leaving: ClearTrust dispatchers menu
Allow sso (true/false):true
```

8. Enter the desired domain scope.

This setting determines the value of the domain cookie when

SSO

(see preceding step) is set to

true

.

- Scope

= 0:

The most specific domain name will be calculated from the host name. If the Portal's host name is

a.b.c.d.e

, the domain cookie's value will be

.b.c.d.e

.

- Scope

= 3:

If the Portal's host name is

a.b.c.d.e

, the domain cookie's value will be

.c.d.e

.

- Scope

= 2:

If the Portal's host name is

a.b.c.d.e

, the domain cookie's value will be

.d.e

.

The scope must be either

0

or greater than or equal to

2

.

The default value is

0

.

```
domain scope (integer > 1):
```

When the preceding information is supplied, the Authentication menu is displayed. The

```
cleartrust
```

option has been added to the menu, because the current authentication type is now set to

```
cleartrust
```

.

```
[Authentication 5 Menu]
```

```
type          - Set authentication mechanism.
```

```
name          - Set auth name.
```

```
domain        - Set windows domain for backend single sign-on.
```

```
cleartrust    - RSA ClearTrust settings menu.
```

```
adv           - Advanced settings menu.
```

```
ena           - Enable Authentication.
```

```
del           - Remove Authentication.
```

9. Add one or more ClearTrust authorization servers.

Instead of letting the dispatcher (see step 5) manage communication with the ClearTrust authorization server(s) you can have the web server agent (that is, the AVG) communicate directly with the authorization server(s). Note that if a dispatcher is configured on the AVG, any authorization servers configured on the AVG will be ignored.

If your ClearTrust authorization server uses another port number you can change the default value of 5608.

```
>> Authentication 5#cleartrust/servers/add

Hostname to add:auth.example.com

Authentication Port (default is 5608):<press ENTER to accept>
```

If needed, additional ClearTrust authorization servers can be added for redundancy. Other ClearTrust commands, for example, for changing connection mode (standard or distributed), authentication type (basic, NT or SecurID) and connection mode (clear-text or anonymous SSL) are found under

```
cleartrust
```

```
.
```

For a full explanation of available ClearTrust commands, see the *comnet:Command Reference*.

10. Set the desired display name (optional).

The display name will appear in the Login service list box on the Portal login page, in the SSL VPN client's login window and in the installed Net Direct client's login window. This is a way of quickly directing the remote user to the proper authentication server, if the VPN uses different authentication methods. If the user selects

```
default
```

in the list box, authentication will be carried out according to the configured authentication order (see following step 11).

```
>> Authentication 5#display

Current value: " "

Auth display name:

(enter a name that is comprehensible to the end user)
```

11. Specify the authentication fallback order.

This step sets the preferred order for which the defined authentication methods are applied when a remote user logs in to the Portal. Even if you have defined only one authentication method, the authentication ID representing that method should be specified.

```
>> Authentication 5#../authorder

Current value: 1,2,3,4
Enter auth order (comma separated):1,2,3,4,5
```

12. Apply your configuration changes.

RSA SecurID Authentication

The RSA SecurID authentication method lets you configure user authentication through an existing RSA SecurID server.

Configure the RSA Server Settings

This description explains how to configure an RSA server under the system's global settings. If a Secure Service Partitioning license is loaded, it is also possible to configure the RSA server for a specific VPN, using the `/cfg/vpn #/adv/rsa` command.

1. Configure the RSA server settings.

This step adds an RSA server that will be queried to perform user authentication.

```
>> RSA#/cfg/sys/rsa

Enter RSA Server number or name: (1-255)1

Creating RSA Servers 1

RSA server symbolic name:rsaserver <example symbolic name>
```

2. Import the `sdconf.rec` file.

This step lets you import a copy of the `sdconf.rec` file from a TFTP/FTP/SCP/SFTP server. The `sdconf.rec` file is a configuration file that contains critical RSA ACE/Server information. Contact your RSA ACE/Server administrator to obtain the file and make it available on the desired TFTP/FTP/SCP/SFTP server.

```
>> RSA Servers 1#import

Select protocol (tftp/ftp/scp/sftp) [tftp]:ftp

Enter hostname or IP address of server:

Enter filename on server:sdconf.rec

FTP User (anonymous):user

Password:password
```

Configure the RSA Authentication Method

1. Create a new VPN, or configure an existing VPN.

If you have already created a VPN to which you want to add RSA SecurID authentication, type the desired VPN number. To create a new VPN, type a VPN number not currently in use.

```
#/cfg/vpn  
  
Enter vpn number (1-256):1
```

2. Create an authentication ID for RSA authentication.

Each time you create a new authentication ID, you will enter a wizard that prompts you for the required information. After the wizard is completed you will enter the regular menu for the current object.

```
>> VPN 1#aaa/auth  
  
Enter auth id:6  
  
Creating Authentication 6
```

3. Set the authentication method to RSA.

This wizard step corresponds to entering **type** on the Authentication menu and selecting the desired authentication method.

```
Select one of radius, ldap, ntlm, siteminder, cleartrust, cert,  
rsa or local:rsa
```

4. Set the desired name for this authentication method.

A name is required. If the authentication method should later be referenced in a client filter, it is the method's name that should be referenced. For more information about client filters, see [Groups, Access Rules and Profiles](#) on page 157.

This wizard step corresponds to entering **name** on the Authentication menu.

```
Auth name:rsa
```

When the preceding information is supplied, the Authentication menu is displayed. The

```
rsa
```

option has been added to the menu, because the current authentication type is now set to

```
rsa
```

```
.
```

[Authentication 6 Menu]	
type	- Set authentication mechanism.
name	- Set auth name.
domain	- Set windows domain for backend single sign-on.
rsa	- RSA SecureID menu.
adv	- Advanced settings menu.
ena	- Enable Authentication.
del	- Remove Authentication.

For a full explanation of available commands, see the *Command Reference*.

5. Reference the RSA server symbolic name.

This name identifies the RSA server we created in the previous section.

```
>> Authentication 6#rsa/rsaname
Current value: " "
RSA server symbolic name:rsaserver
```

6. Configure the RSA server group name.

This step sets the user access group (as defined on the VPN Gateway) to which authenticated users will be assigned. The access rules pertaining to this group will determine the user's access rights.

```
>> RSA#rsagroup
Current value: " "
```

```
Group name:rsagroup1 <example group name>
```

7. Set the desired display name (optional).

The display name will appear in the Login service list box on the Portal login page, in the SSL VPN client's login window and in the installed Net Direct client's login window. This is a way of quickly directing the remote user to the proper authentication server, if the VPN uses different authentication methods. If the user selects

default

in the list box, authentication will be carried out according to the configured authentication order.

```
>> RSA#../display

Current value: " "

Auth display name:<e.g. SecurID>
```

8. Specify the authentication fallback order.

This step sets the preferred order for which the defined authentication methods are applied when a remote user logs in to the Portal. Even if you have defined only one authentication method, the authentication ID representing that method should be specified. To view which authentication ID number that corresponds to a currently configured authentication method, use the `/cfg/vpn #/cur` command.

When using more than one authentication method, specify the authentication ID that represents the method by which the main bulk of users are authenticated as the first number for best performance.

```
>> Authentication 6#../authorder

Current value: 1,2,3,4,5

Enter auth order (comma separated):1,2,3,4,5,6
```

9. Apply your configuration changes.

```
>> AAA#apply

Changes applied successfully.
```

Local Database Authentication

The AVG device can act as an authentication database itself. It can store thousands of user authentication entries each defining a user name, password, and the relevant access groups. The local authentication method can be useful if no external authentication databases exist, for testing purposes or if speedy deployment is needed.

If you ran the VPN quick setup wizard during the initial setup procedure, local database authentication has already been created as authentication ID 1.

1. Create a new VPN, or configure an existing VPN.

If you have already created a VPN (Portal) to which you want to add Local database authentication, type the desired VPN number. To create a new VPN, type a VPN number not currently in use.

```
# /cfg/vpn  
  
Enter vpn number (1-256):1
```

2. Create an authentication ID for local database authentication.

Each time you create a new authentication ID, you will automatically enter a wizard that prompts you for the required information. After the wizard is completed you will enter the regular menu for the current object.

```
>> VPN 1#aaa/auth  
  
Enter auth id:7  
  
Creating Authentication 7
```

3. Set the authentication method to Local Database.

This step is equivalent to enter **type** on the

Authentication

menu and select the desired authentication method.

```
Select one of radius, ldap, ntlm, siteminder, cleartrust, cert,  
rsa or local, http:local
```

4. Set the desired name for this authentication method.

A name is required. If the authentication method should later be referenced in a client filter, it is the method's name that should be referenced. For more information about client filters, see [Groups, Access Rules and Profiles](#) on page 157.

This wizard step corresponds to entering **name** on the Authentication menu.

```
Auth name:local
```

5. Add users to the local database.

This step adds a user to the local authentication database. You need to provide the user name and password for the user, as well as the group(s) of which the user is a member. The user name must be unique.

The group name you specify when adding a user must exist in the current VPN configuration, along with one or more access rules. To view available group names, press TAB.

```
Enter user name:john
Enter passwd:<John's VPN password>
Enter group names (comma separated):staff,engineering
```

When the preceding information is supplied, the Authentication menu is displayed. The

```
local
```

option has been added to the menu, because the authentication type is now set to

```
local
```

```
.
```

```
[Authentication 7 Menu]

type      - Set authentication mechanism.

name      - Set auth name.

domain    - Set windows domain for backend single sign-on.

local     - local database menu.

adv       - Advanced settings menu.

ena       - Enable Authentication.

del       - Remove Authentication.
```

To add more users to the Local database, use the `local/add` command. To add users by importing a populated database, use the `local/import` command.

For a full explanation of available Local database commands, see the *Command Reference*.

6. Specify the authentication fallback order.

This step sets the preferred order for which the defined authentication methods are applied when a remote user logs in to the Portal. Even if you have defined only one authentication method, the authentication ID representing that method should be specified.

If you use Local Database for authentication in combination with other methods within the VPN, specify the number representing the Local Database method first because that is performed extremely fast regardless of the number of users in the database.

```
>> Authentication 7#../authorder  
  
Current value: 1,2,3,4,5,6  
Enter auth order (comma separated):7,1,2,3,4,5,6
```

7. Apply your configuration changes.

```
>> AAA#apply  
  
Changes applied successfully.
```

Client Certificate Authentication

With client certificate authentication enabled, login to the VPN is not required for remote users with a valid client certificate installed on their computers. When the VPN accepted the certificate, the user is granted access to the VPN. Client certificate authentication is also considered more secure.

To enable client certificate authentication, the following steps need to be completed:

- Generate unique client certificates
- Configure client certificate authentication
- Configure the virtual SSL server

Generate Unique Client Certificates

Each user should be provided with a unique client certificate, generated from a CA certificate. The certificates can be generated by an external certificate management tool or by using the

commands available on the VPN Gateway. The CA certificate must however be installed on the VPN Gateway.

For general instructions on AVG certificate management (for example, how to add certificates to the VPN Gateway and how to use the VPN Gateway to generate client certificates), see the "Certificates and Client Authentication" chapter in the *Users Guide*.

To authenticate a user with a client certificate, the VPN Gateway extracts user name and group membership information from the client certificate's subject part. No password information is required. Before you generate the client certificate, you should determine which entries in the subject part that should be used for extracting this information. The AVG provides the following command to print a certificate's subject entries:

```
# /cfg/cert 1/subject

Certificate subject:
C/countryName (2.5.4.6)           = US
ST/stateOrProvinceName (2.5.4.8)  = California
L/localityName (2.5.4.7)         = Testing
O/organizationName (2.5.4.10)    = Test Inc. 11:06:34
2005-12-08
OU/organizationalUnitName (2.5.4.11) = test dept
CN/commonName (2.5.4.3)         = www.example.com
emailAddress/emailAddress (1.2.840.113549.1.9.1) = tester@example.com
```

The left column shows available entries. The right column shows the values specified for the CA certificate. When generating the client certificate you will be prompted for new values for the same entries.

You can for example use the

```
CN/commonName
```

entry to extract user name. Then, as you generate a client certificate for a specific user, enter the user name of that user when prompted for Common Name. Make a note of the OID (object identifier), in this case 2.5.4.3. The OID should later be configured with the **userid** command (see step 5 on page 153).

To map the user to access groups (as defined on the VPN Gateway), choose one or several entries to use for extraction of group names. Then, as you generate a client certificate for the user, enter the group name when prompted for the entry you have decided to use for group name. Make a note of the OID(s). They should later be configured with the **groupoid** command (see step 5 on page 153).

*** Note:**

The iauto link (described in [Example 5: Automatic Login Link Secured by the AVG](#) on page 220) can be used together with client certificate authentication, but only if the backend server does not require a password. Only the user and domain credentials will be passed to the backend server when client certificate authentication is used.

Mapping Group Names to CA Certificate

Instead of extracting group names from the user's client certificate, they can be retrieved from the CA certificates that were used to generate the client certificates. The trick is to use several different CA certificates, where each CA certificate represents a user access group. One CA certificate could for example, represent the engineering group and another the accounting group.

To generate client certificates for a specific group, simply use the CA certificate you have in mind for this group. No modifications need to be made to the CA certificates. Then map the CA certificate to the group, using the `cacerts` command (see step 5 on page 153).

* Note:

The CA certificate that was used to generate the client certificates must be installed on the VPN Gateway. For instructions about how to add certificates to the VPN Gateway, see the "Certificates and Client Authentication" chapter in the *Users Guide*.

This method can be combined with the method described in the previous section. The group names retrieved from the CA certificate will be appended to those extracted from the client certificate. Note that all group names have to be defined on the VPN Gateway with access rules. See [Groups, Access Rules and Profiles](#) on page 157.

If a default group is specified (`/cfg/vpn #/aaa/defgroup`), this group name will be assigned to the user if no other group has been configured.

Configure Client Certificate Authentication

1. Create a new VPN, or configure an existing VPN.

If you have already created a VPN to which you want to add client certificate authentication, type the desired VPN number. To create a new VPN, type a VPN number not currently in use.

```
# /cfg/vpn

Enter vpn number (1-256):1
```

2. Create an authentication ID for client certificate authentication.

Each time you create a new authentication ID, you will automatically enter a wizard that prompts you for the required information. After the wizard is completed you will enter the regular menu for the current object.

```
>> VPN 1#aaa/auth
```

```
Enter auth id:2
Creating Authentication 2
```

3. Set the authentication type to **cert**, that is, Client Certificate.

This step is equivalent to using the **type** command on the Authentication menu and selecting the desired authentication method.

```
Select one of radius, ldap, ntlm, siteminder, cleartrust, cert,
rsa or local:cert
```

4. Set the desired name for this authentication method.

A name for the authentication method is required. If the authentication method should later be referenced in a client filter, it is the method's name that should be referenced. For more information about client filters, see [Groups, Access Rules and Profiles](#) on page 157.

This step is equivalent to using the **name** command on the Authentication menu.

```
Auth name:clicert
```

When the preceding information is supplied, the Authentication menu is displayed. The

```
cert
```

option has been added to the menu, because the current authentication type is now set to (Client Certificate).

```
[Authentication 2 Menu]
```

```
type      - Set authentication mechanism.
```

```
name      - Set auth name.
```

```
domain    - Set windows domain for backend single sign-on.
```

```
cert      - Client Certificate settings menu.
```

```
adv       - Advanced settings menu.
```

```
ena       - Enable Authentication.
```

dis	- Disable Authentication.
del	- Remove Authentication.

5. Enter the Cert menu and specify the user OID.

Valid values for general names are commonName, emailAddress, givenName, initials, surname, and title.

```
>> Authentication 2#cert/useroid/subject/name
Current value: commonName
User OID within 'subject':
```

6. Enter the GroupOIDs menu and specify the group OIDs.

Follow this step if you are extracting group names from the client certificates.

```
>> Cert#groupoids/add
Enter group OID within 'subject':2.5.4.7 <equivalent to
localityName>
```

7. Map your group names to the proper CA certificate.

Follow this step if you are retrieving group names from the CA certificates that were used for generating the client certificates.

Example: If you have chosen to generate client certificates for the engineering group from CA certificate 1, map the engineering group to this certificate.

```
>> GroupOIDs#../cacerts/add
Enter certificate number:1
Enter group name:engineering
```

8. Enable client certificate authentication.

As opposed to the other authentication methods, client certificate authentication should not be included in the authentication order. The method can instead be enabled/disabled from the Authentication menu.

```
>> GroupOIDs# ../../
>> Authentication 2#ena
```

*** Note:**

The Portal will accept client certificates for authentication provided that only one authentication ID of the

`cert`

type has been configured and enabled.

9. Apply your configuration changes.

```
>> Authentication 2#apply
```

Configure the Portal Server

The portal server should have the relevant CA certificates installed and be configured to request client certificates.

1. Install the CA certificate(s) used to generate the client certificates on the VPN Gateway.

A certificate can be pasted or imported to the VPN Gateway. For a full description, see the "Adding Certificates to the AVG " section in the "Certificates and Client Authentication" chapter in the *Users Guide*.

2. Specify the CA certificate(s) used to generate the client certificates as CA certificate(s) for the portal server.

This step is also mentioned in the "Generating Client Certificates" section in the "Certificates and Client Authentication" chapter in the *Users Guide*.

```
>> Main#cfg/vpn 1/server/ssl/cacerts

Current value: " "

Enter certificate numbers (separated by comma):1
```

3. Configure the portal server to request client certificates.

To be able to use the Portal applets (that is, the features available on the Portal's Advanced tab) this parameter should be set to **optional**.

Optional means that the remote user will be prompted for a client certificate upon accessing the VPN (Portal). If the user does not have a client certificate or chooses not to use it for authentication, the Portal login page is displayed instead.

```
>> SSL Settings#verify
```

```
Current value: none  
Certificate verification (none/optional):optional
```

4. Apply your configuration changes.

```
>> SSL Settings#apply  
Changes applied successfully.
```

If no other authentication method besides client certificate authentication is configured, your configuration will be more secure. Even though the Portal login page is displayed if a user cancels client certificate authentication, it is not possible to log in. This means that it is not possible to be logged in to the VPN without a client certificate.

Client Certificate Authentication Combined with Other Method

If another authentication method (for example, RADIUS) is configured in parallel with the client certificate method, it is possible to authenticate with both methods. For users authenticating through their client certificate – and for users who have a valid client certificate but logs in through the other method – requesting intranet resources in the VPN will be extremely safe. Users without a valid client certificate will have to log in by means of the other authentication method.

To ensure that sensitive information or servers can only be accessed by remote users with a client certificate installed, you can create an extended profile that will grant these users more generous access rights. Users authenticating with any other authentication method will then be provided with the base profile's access rules, which can be more limited. For more information about extended profiles, see [Groups, Access Rules and Profiles](#) on page 157.

Configuring IPsec Two Factor authentication

Perform the following steps to configure IPsec Two Factor authentication:

1. Configure client certificate authentication (see [Configure Client Certificate Authentication](#) on page 151).
2. Select the configured authentication method from the Authentication menu (cfg/vpn x/aaa/auth).

```
>> AAA#auth  
Enter auth id:(1-63)
```

```
local(1) ldap(4) ldaps(2) radius(3) cert(5) rsa(6)
```

The certificate menu displays.

*** Note:**

In this example the certificate authentication method configured is cert (5)

3. Enter the advanced settings menu to choose the secondary authentication method.

```
[Authentication 5 Menu]

type- Set authentication mechanism
name - Set auth name
domain - Set Windows domain for backen single sign-on
cert - Client Certificate settings menu
adv - Advanced settings menu
ena - Enable Authentication
dis -Disable Authentication
del - Remove Authentication
```

4. Type **secondauth** command to choose the secondary authentication server.

```
>> Authentication 5# adv

[Advanced Menu]
groupauth - Set Authentication server list for group information
secondauth - Set Secondary authentication server
validatedn - Set Validate Cert-DN before Cleartrust server
revcertdn - Revert Cert-DN before Cleartrust validation
cac - Common Access Card Support
```

5. Choose the second authentication mechanism from the displayed list.

```
>> Advanced# secondauth

Current value: ""
Enter auth server:
local(1) ldap(4) ldaps(2) radius(3) cert(5) rsa(6)

Enter auth server: _
```

Chapter 9: Groups, Access Rules and Profiles

This chapter describes the authorization part of the AAA subsystem, that is, how to configure access rules and profiles for specific user groups.

When the remote user is authenticated and user's group(s) have been returned from the external authentication database (for example, RADIUS), the Access rules will map these group names to group names defined on the Avaya VPN Gateway. If local database authentication is used, the user's user name and password should be configured in the user's local database. This is also where the user is mapped to one or more groups.

For more information about selecting authentication databases and methods, see [Authentication Methods](#) on page 117.

Group Parameters

All the group's members will share the limitations and capabilities that you assign to the group. The most important parameters form the group's access rules, that is, the rules that control which hosts and subnets the group member should be authorized to (or not authorized to).

The following parameters can be configured for a group:

- Linksets
- User type
- Access rules
- Default group
- Extended profiles
- Number of login sessions
- Idle timeout/Max session length
- IP pool
- Tunnel Guard rules
- IPsec tunnel access
- IE cache wiper (enable/disable)
- Citrix MetaFrame support (enable/disable)
- NetDirect (enable/disable)

- Windows admin user name/password
- SPO access
- SPO Application Index
- Bandwidth policy

Linksets

Each user group can be provided with one or several linksets. The linkset itself contains one or several links. The links appear on the Portal's **Home** tab for the user to access intranet or Internet web sites, mail servers or web applications. When a group member is logged in to the Portal, all linksets mapped to the user's group will be displayed on the **Home** tab.

Make sure the links defined for the group are not contradicted by the access rules (see following sections) specified for the group.

For instructions about how to create linksets and links, see [Group Links](#) on page 203.

User Type

The user type determines which Portal tabs will be displayed for the user. Note that the user type distinction has no effect on access rules or vice versa.

The following user types are available:

- Novice. Displays the Home tab.
- Medium. Also displays the Files tab (and the Access tab if enabled).
- Advanced. Displays all tabs, that is, also the Advanced tab.

For a full explanation of the Portal, see [The Portal from an End-User Perspective](#) on page 51.

Access Rules

To be able to configure an access rule, you first have to create one or several network, service and application specific definitions. A network definition identifies hosts and/or subnets to which the user should be authorized (or unauthorized). A service definition identifies ports and/or protocols to which the user should be authorized (or unauthorized). An application specific definition identifies a path to a subfolder and/or file to which the user should be authorized (or unauthorized). The access rule is configured by referencing the desired network, service and application specific definitions in the access rule.

When the user requests a resource (for example, an intranet web server), the access rules associated with the user's group are applied in order until a match is found. The system first checks Access rule 1, then Access rule 2 and so on.

If a match is found between the requested resource and the network/service/path referenced in the access rule, the action specified for the access rule is performed (accept or reject). The remaining access rules (with higher numbers) will be ignored. This means that the order in which the access rules are defined could be important. If no match is found in any access rule, the user's request is rejected.

Default Group

If a user group returned from the authentication database cannot be matched against any group configured on the VPN Gateway, the user is automatically mapped to the default group (if configured). First, create a group with limited access rights. Then use the `/cfg/vpn # /aaa/defaultgroup` command to make this group the default group.

Extended Profiles

Extended profiles can be created to provide better or fewer access rights to a remote user depending on:

- authentication method (for example, RADIUS)
- access method (SSL, IPsec, Net Direct, or SPO)
- source network (for example, a branch office)
- if a client certificate is used
- if the client PC has passed/failed the Tunnel Guard checks
- if the user has installed the Internet Explorer cache wiper.

For instructions about how to configure extended profiles, see [Working with Extended Profiles](#) on page 182.

Number of Login Sessions

You can also define the maximum number of simultaneous Portal/VPN sessions allowed for members of a group.

Example: If the value is set to 2, two simultaneous VPN sessions (that is, from two different computers) are allowed for a specific user.

The default value is 0 = unlimited number of sessions.

Idle Timeout

The idle timeout for a remote user's VPN session can be configured as a default value for the whole VPN using the `/cfg/vpn #/aaa/idlettl` command. It can also be configured on group level (see step 2) or, if desired, on extended profile level.

Example: If the value is set to 20m (20 minutes), the remote user is automatically logged out from the Portal session (or the VPN client session) following 20 minutes of inactivity.

Maximum Session Length

Like the idle timeout, the maximum length of a remote user's VPN session can be configured as a default value for the whole VPN using the `/cfg/vpn #/aaa/sessionttl` command. It can also be configured on group level (see step 2) or, if desired, on extended profile level.

Example: If the value is set to 1h (1 hour), the remote user is automatically logged out from the Portal session (or the VPN client session) after 1 hour, irrespective of the user being idle or not.

IP Pool

To enable Net Direct and Avaya IPsec VPN client connections, an IP pool has to be configured, using the `/cfg/vpn #/ippool` command. By mapping the IP pools to different user groups you can provide different ways of assigning IP address and network attributes depending on the user's group membership.

One of the configured IP pools should be selected as the default IP pool. Groups for which no IP pool is assigned (IP pool number=0) will use the default IP pool.

For more information about IP pools, see [Net Direct](#) on page 87 and [Transparent Mode](#) on page 355.

Tunnel Guard rules

By mapping a Tunnel Guard SRS rule to a group, all group members will be subject to a Tunnel Guard check upon login. The SRS rule determines which software should be present (or not present) on the client machine for the user to be granted access to the VPN.

For more information about Tunnel Guard, along with configuration instructions, see [Configure Tunnel Guard](#) on page 269.

IPsec Tunnel Access

For a group member to be able to log in to the VPN with the Avaya IPsec VPN client (formerly Contivity VPN client), the group should be mapped to a previously created user tunnel profile. If group login is used, a shared secret should also be configured for the current group.

For more information about IPsec access with the Avaya IPsec VPN client, along with configuration instructions, see [Transparent Mode](#) on page 355.

IE Cache Wiper

Whether or not remote users should be able to install the IE cache wiper can be configured per VPN or per group. To delegate this setting to a per group level, set the `/cfg/vpn #/portal/wiper` command to

```
group
```

. Then enable or disable the feature using the `wiper` command for the desired user groups. When the IE cache wiper is enabled, the user – if running Internet Explorer – will have the option to download an ActiveX component (the IE cache wiper). The IE cache wiper removes the Portal address from the browser's visited URLs list when the Portal session is over. In addition, HTML pages cached during the session are cleared from the cache memory.

Citrix Metaframe Support

Whether or not remote users should be able to install the Java applet supporting Citrix Metaframe web links can be configured per VPN or per group. To delegate this setting to a per group level, set the `/cfg/vpn #/portal/citrix` command to

```
group
```

. Then enable or disable the feature using the `citrix` command for the desired user groups.

When enabled, a Java applet is started when users belonging to the current group logs in to the Portal. The applet enables support for Citrix Metaframe web links on the Portal. The link is created by specifying the URL to the Citrix Metaframe server with the

```
internal
```

link type.

When disabled, links to Citrix Metaframe servers are only supported if created by means of the

```
custom
```

port forwarder link type. If Citrix Metaframe links are not used,

`off`

is the recommended setting, because this saves the AVG from starting the Java applet.

Net Direct Access

Whether or not remote users should be able to download the Net Direct client can be configured per VPN or per group. To delegate this setting to a per group level, set the `/cfg /vpn #/sslclient/netdirect` command to

`group`

. Then enable or disable the feature with the `netdirect` command for the desired user groups.

For more information about the Net Direct client, along with configuration instructions, see [Net Direct](#) on page 87.

Windows Administrator User Name/Password

You can also configure a common Windows administrator user name/password combination for members of the current group. To be able to install the Net Direct client (downloadable from the Portal), users has to be administrator users on their PCs.

Multiple Groups

If a user belongs to several groups, the system starts by checking Group 1 (as defined on the VPN Gateway) to see if that group name matches any of the group names returned from the authentication database. It then continues with Group 2 and so on until all matches are found. A list of matching groups, reflecting the CLI order, is then maintained by the system during the user's login session.

When the user requests a resource, the access rules associated with Group 1 in this session-based list are checked in sequential order until a match is found. If a match is found, the remaining groups will be ignored. If no match is found, the access rules associated with Group 2 are checked and so on.

Following is a list of parameters and how they are treated when a user belongs to several groups:

- Linksets: All linksets configured for the user's different groups will be displayed on the Portal's **Home** tab.
- User type. The best user type assigned to the user's different groups will be applied. This means that if the user belongs to one group configured with the novice user type and another with the advanced user type, all of the Portal's tabs will be displayed.
- Tunnel Guard SRS rules. The groups are checked in CLI configuration order. The first found SRS rule in any of the user's groups is used.
- IE cache wiper and Citrix support. IE cache wiper and Citrix Metaframe support will be enabled if it is enabled for any of the groups.
- Idle timeout and maximum session length: The highest value among the user's groups and the default value will be selected at login.

ID or Name?

In general, when you are creating new items in the CLI (new groups, new network definitions, new client filters, new extended profiles and so on) you will always start by entering a wizard. The wizard prompts you for an ID, a numerical value, of the item you wish to create. Having specified the item's ID, you are prompted for the item's name.

The next time you wish to access the item, for example, to edit a parameter, you can use either the numerical ID or the name. To view the names of existing items, press TAB.

SPO Access

The SPO client provides VPN access from portable storage such as USB compliant flash memory and CD ROM.

The SPO client provides enhanced mobility, portability, and security compared to traditional VPN access methods. The SPO client can be deployed and managed from the AVG server thus simplifying SPO client maintenance and updates.

Enter the command

```
cfg/ vpn #/ aaa/ group/ spoaccess
```

and set spoaccess to

```
on
```

to enable the SPO access for a group.

You need to configure the

```
spowindex
```

under Groups to specify the applications that are accessible by users in that group application software. For information on these configuration steps see [Specifying the Secure Portable Office Software Index](#) on page 178.

Bandwidth policy

Bandwidth Management (BWM) enables administrators to allocate a portion of the available bandwidth for specific users or groups. The bandwidth policies take lower and upper bound. The lower bound (soft limit) is guaranteed and the upper bound (hard limit) is available according to the requirement. The BWM provides bandwidth policy management for user traffic and IPsec Passthrough. or more information about configuring bandwidth policy for user group, see [Configuring bandwidth policy](#) on page 181 and for extended group, see [Configuring bandwidth policy](#) on page 201.

AAA Configuration Order

From top to bottom, the following steps are required for a fully operational AAA system:

- Configure the desired authentication mechanism(s). This could be an external authentication mechanism (for example, RADIUS), the VPN Gateway's local database or client certificate authentication. The steps are described in [Authentication Methods](#) on page 117.
- Configure network definitions. A network definition identifies hosts and subnets to which the user should be authorized (or unauthorized). The network definition should later be referenced in an access rule. The steps are described further on in this chapter.
- Configure service definitions. A service definition identifies ports and/or protocols to which the user should be authorized (or unauthorized). The service definition should later be referenced in an access rule. The steps are described further on in this chapter.
- Configure application specific definitions. An application specific definition identifies the path to which the user should be authorized (or unauthorized). The application specific definition should later be referenced in an access rule. The steps are described further on in this chapter.
- Configure groups. If external database authentication is used, user records are typically configured on the external authentication server along with one or several group names. The corresponding (or relevant) group names should also be configured on the local database authentication sever. If local database authentication is used, both users and groups should be configured on the VPN Gateway (see Configure users). The steps are described further on in this chapter.
- Configure access rules for the group. This is done by referencing previously created network, service and application specific definitions and setting the action to accept or reject. The steps are described further on in this chapter.

- Configure linksets with links. Linksets are displayed on the Portal's Home tab for the logged in group member. Linkset and link configuration is described in [Group Links](#) on page 203.
- Configure users. If local database authentication is used, the user should be configured on the VPN Gateway. This is also where to map the user to one or several previously defined groups. The steps are described in [Authentication Methods](#) on page 117.

Extended Profiles

If extended profiles should be applied to groups, a couple of more steps are involved. See [Working with Extended Profiles](#) on page 182 for configuration examples.

Network, Service and Path Configuration

To be able to reference a network, service or path (application specific definition) when defining the access rules for a group, you have to first configure the desired network, service and path definitions. The definitions exemplified in this section will later be referenced in access rules in the group configuration examples on [Group Configuration](#) on page 172.

Create Network Definitions

Access to Outlook Web Access Server

This example describes how to create a network definition identifying an Outlook Web Access server on the intranet.

1. Specify a network name.

Enter the AAA menu of the desired VPN, select

```
network
```

and specify a network number not currently in use. To view previously created networks, press TAB following the **network** command.

```
# /cfg/vpn 1/aaa/network<press TAB to view existing networks>
Enter network number or name: (1-1023)1
```

```
Creating Network 1
Network name:OWa
```

2. Define a subnet identifying the Outlook Web Access server.

Each subnet is identified by an index number. After having entered the index number of the current subnet, enter the desired network address and netmask.

When creating a subnet, enter either the host name or the network address/netmask. Note that the network mask can be entered in number of bits, for example, 32 instead of 255.255.255.255.

*** Note:**

When creating network definitions to be used in IPsec or Net Direct connections, specify the network using a network address and mask. Host names will be ignored.

```
>> Network 1#subnet

Enter subnet number: (1-1023)1

Creating Network Subnet 1
Enter host name:<press ENTER to skip>

Enter network address:192.168.128.10

Enter network netmask:32
```

Access to Intranet Web Server

This example describes how to create a network definition identifying a web server on the intranet. The steps are the same as in the previous example, except for the network name and host IP address.

1. Specify a network name.

Specify a network number not currently in use, for example, 2 to create Network 2.

```
# /cfg/vpn 1/aaa/network 2

Creating Network 2
Network name:webserver
```

2. Define a subnet identifying the intranet web server.

```
>> Network 2#subnet
```

```

Enter subnet number: (1-1023)1

Creating Network Subnet 1
Enter host name:<press ENTER to skip>

Enter network address:192.168.201.10

Enter network netmask:32

```

Access to Intranet File Server

This example describes how to create a network definition identifying an intranet file server.

1. Specify a network name.

Specify a network number not currently in use, for example, 3 to create Network 3.

```

# /cfg/vpn 1/aaa/network 3

Creating Network 3
Network name:fileserver

```

2. Define a subnet identifying the intranet file server.

```

>> Network 3#subnet

Enter subnet number: (1-1023)1

Creating Network Subnet 1
Enter host name:<press ENTER to skip>

Enter network address:192.168.202.1

Enter network netmask:32

```

3. Apply the changes.

```

>> Network Subnet 1#apply

Changes applied successfully.

```

Access Allowed to Specific Subnet

This example describes how to create a network definition identifying a specific subdomain in a company's intranet to which the group members should be authorized. The subdomain is called **sales.example.com**.

1. Specify a network name.

Specify a network number not currently in use, e.g 4 to create Network 4.

```
# /cfg/vpn 1/aaa/network 4

Creating Network 4
Network name:sales
```

2. Define the subnet to include in the current network definition.

When creating a subnet, enter either the host name or the network address/netmask. To specify all hosts within a subdomain, you can use an asterisk (*) as a wildcard.

```
>> Network 4#subnet

Enter subnet number: (1-1023)1

Creating Network Subnet 1
Enter host name:*.sales.example.com

Enter network address:<press ENTER to skip>

Enter network netmask:<press ENTER to skip>
```

3. Apply the changes.

```
>> Network Subnet 1#apply

Changes applied successfully.
```

 **Note:**

It is fully possible to create a network definition consisting of several subnet definitions.

Access Denied to Specific Subnet

This example describes how to create a network definition identifying a specific subdomain in the company intranet to which the group members should be unauthorized. The subdomain is called **secret.example.com**.

1. Specify a network name.

Specify a network number not currently in use, for example, 5 to create Network 5. To view previously created networks, press TAB following the **network** command.

```
# /cfg/vpn 1/aaa/network 5

Creating Network 5
Network name:secret
```

2. Define the subnet to include in the current network definition.

When creating a subnet, enter either the host name or the network address/netmask. To specify all hosts within a subdomain, you can use an asterisk (*) as a wildcard.

```
>> Network 5#subnet

Enter subnet number: (1-1023)1

Creating Network Subnet 1
Enter host name: *.secret.example.com

Enter network address:<press ENTER to skip>

Enter network netmask:<press ENTER to skip>
```

3. Apply the changes.

```
>> Network Subnet 1#apply

Changes applied successfully.
```

We will later reference these network definitions in different access rules in the group configuration examples starting on [Group Configuration](#) on page 172.

Create Service Definition

Note:

By running the Quick AAA Setup wizard using the `/cfg/vpn #/aaa/quick` command you can create 10 default service definitions, each identifying one or several common application protocols.

Access to FTP and SMB Protocols

This example describes how to create a service definition allowing access to the FTP and SMB application protocols.

1. Specify a service name and allowed port numbers.

Enter the AAA menu of the desired VPN and select

```
service
```

. Then specify a index number not currently in use. To view previously created service definitions, press TAB following the **service** command.

```
# /cfg/vpn 1/aaa/service (press TAB to view existing services)

Enter service number or name: (1-1023)1

Creating Service 1
Service name:ftp/smb

Enter service protocol (list of tcp,udp,icmp):tcp

Enter service ports:20,21,139

>> Service 1#
```

2. Apply the changes.

```
>> Service 1#apply

Changes applied successfully.
```

We will later reference this service definition in an access rule in the group configuration examples starting on [Group Configuration](#) on page 172.

Create Path (Appspec) Definition

Access to Subfolder on Web Server

This example describes how to create an Appspec definition identifying a path to a subfolder. We will later reference this Appspec definition in an access rule where the

```
webserver
```

network definition we created in the example on [Access to Intranet Web Server](#) on page 166 will also be referenced.

The path to define in this example is

```
/public
```

. When the remote user tries to access the web server identified in the

```
webserver
```

network definition, the following URL will create a match:

192.168.201.10/public.

The path setting is checked for the following protocols: HTTP, HTTPS, FTP and SMB (Windows file share). The syntax for entering the path is shown following sections:

- For SMB, write the path as /WORKGROUP/FILESHARE/FILE PATH, e.g. /**AVAYA/homes/public**. This will give access to the

public

directory in the

homes

share in the

AVAYA

workgroup/domain.

- For FTP, write the path as ABSOLUTE FILE PATH, e.g. /**home/share/public/**. This will give access to the

/home/share/public

directory. Note that all paths are absolute from the root.

- For web servers (HTTP or HTTPS), write the path as SERVER PATH, e.g. /**intranet**. This will give access to the

/intranet

path on the web server.

1. Specify a name for the Appspec definition and enter the desired path.

Enter the AAA menu of the desired VPN and select

appspec

. Then specify an appspec index number not currently in use. To view previously created appspec definitions, press TAB following the **appspec** command.

```
# /cfg/vpn 1/aaa/appspec (press TAB to view existing entries)
```

```
Enter appspec number or name: (1-1023)1
```

```
Creating AppSpecific 1
```

```
AppSpec name:public
```

```
Enter path:/public
```

2. Apply the changes.

```
>> AppSpecific 1#apply
```

Changes applied successfully.

We will reference this appspec definition in an access rule in the group configuration examples starting on [Group Configuration](#) on page 172.

Group Configuration

This section describes how to configure a group on the VPN Gateway and gives three examples of how to define access rules for this specific group.

Example 1: Access to Specific Services on Specific Intranet Hosts

By defining the access rules described in this example, the group members will be able to access only the following intranet resources:

- Read mail through Outlook Web Access
- Browse a specific intranet web server
- Browse files on a specific file server through SMB or FTP

Define Group 1 With Access Rules

1. Specify a group name. and select user type.

Enter the AAA menu for the desired VPN and select

```
group
```

. Then specify a group number not currently in use. To view previously created groups, press TAB following the **group** command.

When an external database is used for authentication (for example, RADIUS), the group name assigned in the AVG configuration (that is, in this step) is matched against group names retrieved from the external authentication database.

```
# /cfg/vpn 1/aaa/group (press TAB to view existing groups)

Enter group number or name: (1-1023)1

Creating Group 1
Group name:staff
```

2. Specify the other group parameters.

Some additional prompts are displayed in the group configuration wizard. See [Group Parameters](#) on page 157 for explanations.

```
Enter number of sessions (0 is unlimited):<press ENTER to accept>

Enter user type (advanced/medium/novice):advanced

TTL for idle sessions (max 31d):<press ENTER to use VPN's idle
timeout>

Max TTL for sessions (max 31d or infinity):<press ENTER to use
VPN's session timeout>

Allow vpn admin (true/false):<displayed in Secure Service
Partitioning configs>

Use ActiveX to clear cache (on/off):<displayed if delegated to
group level>

Citrix support (on/off):<displayed if delegated to group level>

Allow Netdirect vpn clients (on/off):<displayed if delegated to
group level>
```

3. Define Access rule 1.

This step lets you reference the network definition we created in the example on [Access to Outlook Web Access Server](#) on page 165, i.e

owa

. It consists of a subnet definition identifying an Outlook Web Access server. You are also making use of the default service definition

http

, corresponding to TCP port number 80.

Pressing ENTER at the application specific name prompt will insert an asterisk (*), meaning that there are no restrictions to paths in the specified domain.

```
>> Group 1#access

Enter access rule number: (1-1023)1

Creating Access rule 1
Enter network name:OWa

Enter service name:http

Enter application specific name:*

(meaning all paths)

Enter action (accept/reject):accept
```

*** Note:**

The default value for action is

```
reject
```

(obtained by pressing ENTER).

4. Define Access rule 2.

This step lets you reference the network definition we created in the example on [Access to Intranet Web Server](#) on page 166, i.e

```
webserver
```

. It consists of a subnet definition identifying an intranet web server. You are also making use of the predefined service definition

```
http
```

, corresponding to TCP port number 80.

Reference the application specific name we created in the example on page [Access to Subfolder on Web Server](#) on page 170. This means that group members are only allowed access to the

```
/public
```

subfolder on the web server identified by the

```
webserver
```

network definition.

```
>> Group 1#access

Enter access rule number: (1-1023)2

Creating Access rule 2
Enter network name:webserver

Enter service name:http

Enter application specific name:public

Enter action (accept/reject):accept
```

5. Define Access rule 3.

This step lets you reference the network definition we created in the example on [Access to Intranet File Server](#) on page 167, i.e

```
fileserver
```

. It consists of a subnet definition identifying an FTP and SMB file server. You are also making use of the service definition we created in the example on [Access to FTP and SMB Protocols](#) on page 169, that is,

```
ftp/smb
```

, corresponding to TCP port numbers 20, 21 and 139.

```
>> Group 1#access

Enter access rule number: (1-1023)3

Creating Access rule 3
Enter network name:fileserver

Enter service name:ftp/smb

Enter application specific name:*
(meaning all paths)

Enter action (accept/reject):accept
```

6. Apply the changes.

```
>> Access rule 3#apply

Changes applied successfully.
```

Example 2: Access Allowed to All Services on Hosts in a Specific Subdomain

By defining the access rules described in this example, group members will be able to access all available applications within the

```
sales.example.com
```

sub domain.

Access Allowed to Specific Subnet

1. Specify the group for which the access rule should be applied, then enter the access menu.

This step lets you reference the network definition we created in the example on [Access Allowed to Specific Subnet](#) on page 167, i.e

```
sales
```

. By entering an asterisk (*) as the service and application specific references, all port numbers, protocols and paths are implied.

```
# /cfg/vpn 1/aaa/group 1

>> Group 1#access

Enter access rule number: (1-1023)1

Creating Access rule 1
Enter network name:sales

Enter service name:*

(meaning any TCP or UDP traffic)

Enter application specific name:*

(meaning all paths)

Enter action (accept/reject):accept
```

2. Apply the changes.

```
>> Access rule 1#apply

Changes applied successfully.
```

Example 3: Access Allowed to the Complete Intranet, Except for Hosts in a Specific Subdomain

By defining the access rules described in this example, group members will be able to access all intranet resources except for all hosts in the **secret.example.com** sub domain, regardless of the protocol used.

* Note:

Remember that when a match is found for a requested resource, the action specified for the matching resource in an access rule is performed (

```
accept
```

```
or
```

```
reject
```

), and access rules with a higher number are ignored. Therefore, it is extremely important that the access rule that rejects access to all hosts within the **secret.example.com** subdomain in this example is defined as access rule number 1.

Access Rule 1: Access Denied to Specific Subdomain

1. Specify the group for which the access rule should be applied, then enter the access menu.

This step lets you reference the network definition we created in the example on [Access Denied to Specific Subnet](#) on page 168, that is,

```
secret
```

. By entering an asterisk (*) as the service and application specific references, all port numbers, protocols and paths are implied.

Set the action to

```
reject
```

```
# /cfg/vpn 1/aaa/group 1

>> Group 1#access

Enter access rule number: (1-1023)1

Creating Access rule 1
Enter network name:secret

Enter service name:*

(meaning any TCP or UDP traffic)

Enter application specific name:*

(meaning all paths)

Enter action (accept/reject):reject
```

2. Apply the changes.

```
>> Access rule 1#apply

Changes applied successfully.
```

Access Rule 2: Access Allowed to All Hosts

1. Specify the group for which the access rule should be applied, then enter the access menu.

By entering an asterisk (*) as the network, service and applications specific references (or by pressing ENTER), all hosts (irrespective of domain) and all port numbers, protocols and paths are implied.

```
# /cfg/vpn 1/aaa/group 1

>> Group 1#access

Enter access rule number: (1-1023)2

Creating Access rule 2 Enter network name:*

(meaning all hosts)

Enter service name:*

(meaning any TCP or UDP traffic)

Enter application specific name:*

(meaning all paths)

Enter action (accept/reject):accept
```

2. Apply the changes.

```
>> Access rule 2#apply

Changes applied successfully.
```

Specifying the Secure Portable Office Software Index

Software index is the Secure Potable Office (SPO) application index. This is the position in which the SPO client resides. Every group has a defined software index. This group of users will not have access to any other software index other than this particular software index. You can add, delete, insert, and move the software index.

List all the SPO software index

This section explains how to view the list of SPO software indices.

1. Specify the group for which the SPO software index needs to be inserted.

```
/cfg/ vpn #/aaa/group1/sposwindex
```

```
[SPOSoftIndex Menu]
list      - List all values
del       - Delete a value by number
add       - Add a new value
insert    - Insert a new value
move      - Move a value by number
```

2. Enter the following command to view the list of SPO software indices.

```
>> SPOSoftIndex# list
1: Putty
2: "SPO Client MSI"
3: "SPO Client U3P"
```

Add a software index

This section explains how to add the software index.

1. Specify the group for which you want to add a software index.

```
/cfg/ vpn #/aaa/group1/sposwindex
```

2. Enter the following command to add a software index.

```
SPOSoftindex# add
```

```
Software name: SPO Client
```

The new software is added to the list.

Old:

```
1. Putty
```

```
2: SPO U3P
```

Pending:

```
1. Putty
```

```
2: SPO U3P
```

```
3: SPO Client
```

Delete a software index

This section explains how to delete a software index.

1. Specify the group for which you want to delete a software index.

```
/cfg/ vpn #/aaa/group1/sposwindex
```

2. Enter the following command to delete a software index.

```
SPOSoftindex# del
```

```
Software name: SPO Client
```

The new software is deleted from the list.

Old:

- 1. Putty
- 2: SPO U3P
- 3: SPO Client

Pending:

- 1. Putty
- 2: SPO U3P

Insert a new software index

This section shows the steps to insert a new software index.

1. Specify the group for which the SPO software index needs to be inserted.

```
/cfg/ vpn #/aaa/group1/sposwindex
```

[SpoSoftIndex Menu]	
list	- List all values
del	- Delete a value by number
add	- Add a new value
insert	- Insert a new value
move	- Move a value by number

2. Enter the following menu to insert the SPO software index.

```
SPOSoftindex# insert
```

3. Specify the index and the software name that you want to insert in the specified index.

```
Index to insert at: 3
```

```
Software name: SPO Client U3P
```

Old:

- 1: Putty
- 2: SPO Client MSI

Pending:

- 1: Putty
- 2: SPO Client MSI
- 3: SPO Client U3P

Move a software index

This section shows the steps to move a new software index from one position to other.

1. Specify the group for which the SPO software index needs to be moved.

```
/cfg/ vpn #/aaa/group1/sposwindex
```

[SposwIndex Menu]	
list	- List all values
del	- Delete a value by number
add	- Add a new value
insert	- Insert a new value
move	- Move a value by number

2. Enter the following menu to insert the SPO software index.

```
SPOSoftindex# move
```

3. Specify the index and the software name that you want to move in the specified index.

```
Index number to move: 1
```

```
Destination index: 3
```

```
Software name: SPO Client U3P
```

```
Old:
```

```
1: Putty
```

```
2: SPO Client MSI
```

```
3: SPO Client U3P
```

```
Pending:
```

```
1: SPO Client U3P
```

```
2: SPO Client MSI
```

```
3: Putty
```

Configuring bandwidth policy

You cannot restrict a user if the policies are not configured for a group or extended profile under which a user falls. When a user is part of more than one group or extended profile, and for each of them if a bandwidth policy is configured, then the bandwidth policy chosen for this user is the one with the best rate (soft limit).

Perform the following procedure to configure bandwidth policy for a group:

1. Specify the group to insert bandwidth policy management name.

```
/cfg/vpn #/aaa/group #/bwpolicy
```

2. Specify the bandwidth policy management name.

Choose any one bandwidth policy configured using command `/cfg/bwm/bwmpolicy #`.

```
Current value: ""  
Enter BW Policy name:
```

Working with Extended Profiles

Specifying access rules on Group level (as described in the previous sections in this chapter) is sufficient to have a working AAA system. However, if security considerations in your company require a more fine-grained authorization control, one or more extended profiles can be added to a user group.

In short, extended profiles are used to give the remote user better or fewer access rights depending on how the user's accesses the VPN.

Base Profiles and Extended Profiles

All the data that can be defined for a group on Group level (access rules, linksets, user type and so on.) can also be defined for an extended profile. Data defined on Group level, that is, directly under the Group menu, adhere to the group's base profile. Data defined on the Extended profile menu adhere to the group's extended profile.

When is the Extended Profile Applied?

The client filter referenced in the extended profile determines when the extended profile's access rules should be applied.

The client filter identifies

- the source network (for example, a branch office)
- the authentication method (for example, RADIUS)
- the access method (for example, SSL, IPsec, Net Direct, or SPO)
- if a client certificate is installed on the remote user's machine
- whether or not the Tunnel Guard checks have failed
- if the IE cache wiper is installed on the remote user's machine.

When the user is authenticated, the system starts by checking Extended profile 1 to see if a match can be found between the client filter's condition and the security status of the user.

If no match is found in Extended profile 1, the system goes on to check Extended profile 2 for a matching client filter and so on. When a match is found, that particular extended profile's data (that is, access rules, links and so on) will be applied. Data defined for the base profile will be appended to the extended profile's data. If no match is in any of the extended profiles, only the base profile's data will be applied.

Linksets

The linksets to be displayed on the Portal for the logged in group member can be determined by the user's source network or authentication method. For example, if an extended profile references a source network that is considered secure, this profile could provide another set of links than the base profile. The base profile's linksets are however appended to the extended profile's linksets.

Access Rules

The access rules that apply during the currently logged in group member's session are also determined by the extended profile. For example, the access rules defined for an extended profile that references a secure authentication method could be more generous. Like with linksets, the base profile's access rules are appended to those of the extended profile.

The extended profile's access rules are executed prior to those of the base profile. This means that if a matching extended profile is found (for example, the profile's client filter matches the user's source network), and a match is found in any of the profile's access rules (for example, the access rule's network definition matches the user's requested network), the action specified for the access rule (for example, accept) will be performed. The base profile may contain an access rule with the same network definition, but this access rule will be ignored.

User Type

Where user type is concerned, the best user type assigned to the user group's extended profile and base profile will be applied. This means that if the extended profile has the novice user type assigned to it and the base profile uses the advanced user type, the advanced user type will be applied, that is, all of the Portal's tabs will be displayed for the logged in user.

Multiple Groups

If a user belongs to several groups, the system starts by checking Group 1 (as defined on the VPN Gateway) to see if that group name matches any of the group names returned from the authentication database. It then continues with Group 2 and so on until all matches are found.

A list of matching groups, reflecting the CLI order, is then maintained by the system during the user's login session.

Where profiles are concerned, each group is treated separately by the system. The extended profile(s) associated with Group 1 are first checked in sequential order to see if a match can be found between the user's security level (for example, source network) and the client filter referenced in the extended profile. If a match is found, the extended profile's access rules and links will be applied and the base profile's data will be appended.

The system continues to check Group 2 for extended profiles in the same way. If no match is found in an extended profile, the base profile will be used. The system then checks Group 3. If a match is found in an extended profile, this profile's access rules and links will be applied and the base profile's access rules and links will be appended. This means that several extended and base profiles may be active at the same time for the logged in user.

Using the preceding example, the following access rules could be valid during a session for a logged in user that belongs to Group 1, Group 2 and Group 3:

Table 2: Valid Access Rules for a User that Belongs to Multiple Groups

Group 1	Group 2	Group 3
Extended profile 1 (no match)	Extended profile 1 (no match)	Extended profile 1 (match)
Extended profile 2 (match)	Extended profile 2 (no match)	
Base profile	Base profile	Base profile
Result: The access rules of Extended profile 2 and the base profile will be valid for the user's current session.	Result: Only the base profile's access rules will be valid for the user's current session.	Result: The access rules of Extended profile 1 and the base profile will be valid for the user's current session.

When the user requests a resource, for example, an intranet host, the system will first check the access rules that are valid for Group 1. The extended profile's access rules are checked prior to the base profile's access rules.

If no match is found between the user's request and the network, services and so on specified in Group 1's access rules, the system goes on to check Group 2, that is, only the base profile's access rules in this example. If a match is found in any of Group 2's access rules, the access rules pertaining to Group 3 will be ignored. If no match is found in Group 2, the system goes on to check the access rules valid for Group 3.

To avoid the complexity of overlapping access rules when multiple access groups are configured, we recommend that each individual group's access rules cover separate areas.

Client filters

This section describes the procedure to add a new client filter for SPO client users:

1. Enter the following command to access the filters.

```
>> Main#/cfg/vpn VPN-1/aaa/filter 4
```

```
Creating Client Filter 4
```

```
Filter name : spo
```

```
[Client Filter 4 Menu]
```

```
name - Set filter name
```

```
cert - Client certificate present
```

```
iewiper - IE cache wiper present
```

```
tg - TunnelGuard checks passed
```

```
methods - Set access methods
```

```
authserver - Set authentication servers
```

```
clientnet - Set client network reference
```

```
comment - Set comment
```

```
del - Remove client filter
```

2. Enter the method as SPO.

```
>> Client Filter 4#
```

```
Usage: methods <ssl|ipsec|netdirect|spo>
```

```
ssl      ipsec      netdirect  spo
```

3. Apply the changes.

```
>> Client Filter 4# apply
Changes applied successfully.
```

Example 1: Define the Staff Group

In this example, we will create a group called

```
staff
```

. The base profile should contain a link to an Outlook Web Access server and an access rule that allows access to that OWA server. Access to the OWA server should be allowed, regardless whether the user requests the server from an Internet café or from a secure network.

We will also add an extended profile to the

```
staff
```

group. The extended profile references a client filter which, in its turn, references a client network. The client network consists of a subnet identifying a secure network, that is, a branch office. When a group member connects to the SSL VPN from the branch office network over the internet, that group member should have more generous access rights.

Define the Base Profile

1. Specify the group name and user type.

```
>> Main#cfg/vpn 1/aaa/group 1

Creating Group 1
Group name:staff

Enter number of sessions (0 is unlimited):<press ENTER to accept>

Enter user type (advanced/medium/novice):<press ENTER to select
advanced>

Enter windows admin password:<press ENTER to skip>
```

2. Specify the access rule pertaining to the base profile.

This step lets you reference the network definition we created in the example on [Access to Outlook Web Access Server](#) on page 165, i.e

```
owa
```

. It consists of a subnet definition identifying an Outlook Web Access server. You are also making use of the default service definition

http

, corresponding to TCP port number 80.

*** Note:**

To create 10 default service definitions, run the Quick AAA Setup wizard, using the `/cfg/vpn #/aaa/quick` command. If you ran the VPN Quick Setup wizard during the Initial Setup procedure, these service definitions have already been created.

```
>> Group 1#access

Enter access rule number: (1-1023)1

Creating Access rule 1

Enter network name:OWa

Enter service name:http

Enter application specific name:* <meaning all paths>

Enter action (accept/reject):accept
```

3. Create a linkset containing a link to the OWA server.

The linkset and the link will be displayed on the Portal's Home tab.

For a full reference to all available link options, see [Group Links](#) on page 203.

```
>> Group 1#/cfg/vpn 1/linkset

Enter Linkset number or name (1-1024):1

Creating Linkset 1
Linkset name:OWa

Linkset text [Enter to skip]:<press ENTER>

Autorun Linkset (true/false) [false]:<press ENTER>
```

4. Create a link and enter a link text to be displayed on the Portal's Home tab.

```
>> Linkset 1#link

Enter Link number or name (1-256):1
```

```
Creating Link 1
Enter link text:E-mail
```

5. Select link type.

```
Enter type of link (hit TAB to see possible values)
[internal]:internal

Entering: Internal settings menu
```

6. Enter the link properties.

```
Enter method (http/https):http

Enter host (eg inside.company.com):owa.example.com

Enter path (eg /):/

Leaving: Internal settings menu
```

7. Map the linkset to the staff group.

```
>> Link 1#/cfg/vpn 1/aaa/group 1/linkset/add

linkset name:Owa
```

8. Apply the changes.

```
>> Linksets#apply

Changes applied successfully.
```

Create a Network Identifying the Branch Office Network

To be able to reference the client network in the client filter, you should first create the network definition identifying the branch office network.

1. Specify the network name.

```
>> Main#cfg/vpn 1/aaa/network

Enter network number or name: (1-1023) 1
Creating Network 1
Network name:branchoffice
```

2. Create the subnet(s) to be included in the network definition.

When creating a subnet, enter either the host name or the network address/netmask. To specify all hosts within a subdomain, you can use an asterisk (*) as a wildcard.

```
>> Network 1# subnet
Enter subnet number: (1-1023)1

Creating Network Subnet 1
Enter host name: *.denver.example.com

Enter network address:<press ENTER to skip>

Enter network netmask:<press ENTER to skip>
```

Define a Client Filter Referencing the Client Network

To be able to reference the client filter in the extended profile, you have to first define the client filter.

1. Specify the client filter's name.

```
>> Main#cfg/vpn 1/aaa/filter

Enter client filter number or name: (1-63)1

Creating Client Filter 1
Filter name:branchoffice
```

2. Reference the previously created network.

```
>> Client Filter 1#clientnet

Current value: *
Enter client network name:branchoffice
```

3. Apply the changes.

Define the Extended Profile

Now it is time to define the extended profile. The extended profile is triggered when the group member accesses the Portal from the network referenced in the extended profile's client filter.

Because the user is connecting from a secure network, more generous access rules can be presented to the user.

1. Create the extended profile and reference the previously created client filter.

```
>> Main#cfg/vpn 1/aaa/group 1/extend

Enter profile number or filter reference name: (1-63)1

Creating Extended Profile 1
Enter client filter name:branchoffice

Enter user type (advanced/medium/novice):advanced
```

2. Specify Access rule 1.

This access rule allows access to all networks and protocols.

```
>> Extended Profile 1#access

Enter access rule number: (1-1023)1

Creating Access rule 1
Enter network name:*

<meaning all hosts on all networks>

Enter service name:*

<meaning all ports and protocols>

Enter application specific name:*

<meaning all paths>

Enter action (accept/reject):accept
```

* Note:

Leaving an extended profile without access rules is not the same as denying all traffic. If no access rule at all is specified for the extended profile, the base profile's access rules will be applied.

3. Create a linkset including a link to an FTP file server on the intranet.

This linkset will be displayed on the Portal's Home tab. The linkset defined for the base profile will be appended to this linkset, that is, both linksets will be displayed for group members accessing the Portal from the branch office network.

For a full reference to all available linkset and link options, see [Group Links](#) on page 203.

```
>> Group 1#/cfg/vpn 1/linkset

Enter Linkset number or name (1-1024):2
```

```

Creating Linkset 2
Linkset name:ftp

Linkset text [Enter to skip]:<press ENTER>

Autorun Linkset (true/false) [false]:<press ENTER>

```

4. Create a link and enter a link text to be displayed on the Portal's Home tab.

```

>> Linkset 1#link

Enter Link number or name (1-256):1

Creating Link 1
Enter link text:FTP file server

```

5. Select link type and enter the link properties.

```

Enter type
of link
(hit TAB to
see
possible
values)
[internal]:

<TAB>

smb      ftp      proxy      ftpproxy  telnet
netdrive wts      outlook    netdirect  terminal
external internal  iauto

Enter type
of link
(hit TAB to
see
possible
values)
[internal]:
ftp

Entering      : FTP
               settings menu

Enter FTP
host

:ftp.exam
ple.com

```

```
Enter
initial
path on
host (/!
for home
directory)

:

/!

Leaving      : FTP
               settings menu
```

6. Map the linkset to the extended profile we created for the **staff** group.

```
>> Link 1#/cfg/vpn 1/aaa/group 1/extend 1/linkset/add
linkset name:ftp
```

7. Apply the changes.

```
>> Linksets#apply
Changes applied successfully.
```

Result

Bill is a member of the

staff

group. This is what will happen depending on how Bill accesses the Portal:

- From an Internet café: The extended profile will not be triggered. This is because the client filter referenced in the extended profile points to the branch office network, not the Internet café's network. Only the linkset mapped to the base profile, that is, directly under the Group menu, will be displayed on the Portal's Home tab. If Bill tries to access the Outlook Web Access server, either by clicking the link or by entering the address in the **Home** tab's URL field, access will be allowed. A match will be found between the requested resource and the network referenced in Access rule 1. If Bill tries to request any other resource, no match will be found in the access rule and access will be denied.
- From the branch office network: The extended profile will be triggered. This is because a match is found between Bill's source network and the client network referenced in the extended profile's client filter. Both linksets will be displayed, because the base profile's linksets are always appended to those of the extended profile. The access rule defined for the extended profile will be applied, which means Bill is granted access to all hosts

and protocols on the intranet and the internet. The base profile's access rule will be appended but has no real effect in this example.

Example 2: Define the Engineer Group

In this example, we will create a group called

`engineer`

. The base profile should contain a link to an intranet web server and an access rule that allows access to all hosts in the

`sales.example.com`

subdomain.

Members of the

`engineer`

group exist in the VPN Gateway's local database as well as in a RADIUS authentication server's database. Thus, group members can authenticate to the Portal using local database authentication or RADIUS authentication. The latter is used for token login and is considered more secure.

For users logging in to the Portal using local database authentication, only the base profile's links and access rules should be applied. The Advanced tab should not be visible on the Portal. For users logging in to the Portal using RADIUS authentication, links and access rules defined for the extended profile should be applied. The extended profile should contain an extra set of links, an access rule that allows access to all hosts and a user type allowing display of all of the Portal's tabs.

Define the Base Profile

This example describes how to configure the engineer group with the required links and access rules.

1. Define the **engineer** group.

This step lets you specify the group's name and user type. By setting the user type to **medium**, the Advanced tab will not be visible on the Portal for the logged in group member.

```
#/cfg/vpn 1/aaa/group 2

Creating Group 2
Group name:engineer

Enter number of sessions (0 is unlimited):<press ENTER to accept>
```

```
Enter user type (advanced/medium/novice):medium
Enter windows admin password:<press ENTER to skip>
```

2. Specify the access rules pertaining to the group's base profile.

In this example we can make use of the network definition we created in the example on [Access Allowed to Specific Subnet](#) on page 167, that is,

```
sales
```

. To allow all services and paths (that is, application specific name), press ENTER when prompted.

```
>> Group 2#access 1
Creating Access rule 1
Enter network name: sales
Enter service name:*
Enter application specific name:*
Enter action (accept/reject):accept
```

3. Create a linkset including a link to the intranet web server.

For a full reference to all available link options, see [Group Links](#) on page 203.

```
>> Group 2#/cfg/vpn 1/linkset
Enter Linkset number or name (1-1024):3
Creating Linkset 2
Linkset name:intranet
Linkset text [Enter to skip]:<press ENTER>
Autorun Linkset (true/false) [false]:<press ENTER>
```

4. Create a link and enter a link text to be displayed on the Portal's Home tab.

```
>> Linkset 1#link
Enter Link number or name (1-256):1
Creating Link 1
Enter link text:Link to web server
```

5. Select link type and enter the link properties.

```

Enter type of link (hit TAB to see possible values)
[internal]:

<TAB>

smb      ftp      proxy     ftpproxy   custom mail
telnet   netdrive  wts       outlook    netdirect
terminal external  internal  iauto

Enter type of link (hit TAB to see possible values)
[internal]:
internal

Entering
: Internal settings menu

Enter
method   :http
(http/
https)

Enter host (eg inside.company.com)

:
inside.example.com

Enter path (eg /)

:
/

Leaving
: Internal settings menu

```

6. Map the linkset to the engineer group.

```

>> Link 1#/cfg/vpn 1/aaa/group 2/linkset/add
linkset name:intranet

```

7. Apply the changes.

```
>> Linksets#apply
Changes applied successfully.
```

Define Client Filter for Token Login

Before you create the extended profile you should define the client filter. The client filter should later be referenced in the extended profile. The extended profile in its turn should be triggered when a group member authenticates through the RADIUS server.

1. Set the client filter's name and specify which authentication server it refers to.

```
# /cfg/vpn 1/aaa/filter 1

Enter client filter number or name: (1-63)1

Creating Client Filter 1
Filter name:radius
```

2. Set the authentication server name.

This step lets you specify the authentication server used. The authentication server should be referenced by the name that was assigned to the authentication method, using the `/cfg /vpn 1/aaa/auth #/name` command.

For instructions about how to configure an authentication method, see [Authentication Methods](#) on page 117.

```
>> Client Filter 1#authserver

Current value: *
Authentication server names (separated by comma):radius
```

3. Apply the changes.

This client filter should now be referenced in the extended profile. The access rules specified in this profile determine the access rights for group member's authenticating by means of token authentication.

Create Extended Profile for Token Login

To grant members of the

engineer

group better access rights when using token login, we should add an extended profile to the group. The extended profile should be triggered when a group member authenticates through

token login, supplied by the RADIUS server. Reference the client filter we created in the example in the previous section.

1. Specify the group for which you wish to create the extended profile. Then create the extended profile and reference the client filter's name.

The base profile's user type is

```
medium
```

. To provide better access rights for users using token login, specify advanced as user type.

```
# /cfg/vpn 1/aaa/group 2

>> Group 2#extend

Enter profile number or filter reference name: (1-63)1

Creating Extended Profile 1
Enter client filter name:radius

Enter user type (advanced/medium/novice):advanced
```

2. Specify the access rules pertaining to the extended profile.

This step lets you specify the group member's access rights when the user authenticates through token login. The group members should be granted access to hosts on all networks. All services should be available.

```
>> Extended Profile 1#access

Enter access rule number: (1-1023)1

Creating Access rule 1
Enter network name:*

(meaning all hosts)

Enter service name:*

(meaning any TCP, UDP or ICMP traffic)

Enter application specific name:*

(meaning any path)

Enter action (accept/reject):accept
```

3. Create and map linksets to the extended profile.

Linksets mapped to the extended profile will be displayed when the user authenticates through token login. Linksets mapped to the base profile will be appended to those of the extended profile.

For a full reference to all available link options, see [Group Links](#) on page 203.

4. Apply the changes.

```
>> Extended Profile 1#apply  
Changes applied successfully.
```

Result

Lisa is a member of the

`engineer`

group. This is what will happen depending on how Lisa authenticates to the Portal.

- Local database authentication. The extended profile will not be triggered, because Lisa authenticated to the Portal through local database authentication. Only the base profile will be used in Lisa's session. The linkset mapped to the base profile will be displayed on the Portal's Home tab. If Lisa tries to access a host within the

`sales.example.com`

sub domain, for example, by entering the address in the **Home** tab's URL field, access will be allowed. A match will be found between the requested resource and the network referenced in Access rule 1. If Lisa tries to request any other host, access will be denied.

- RADIUS authentication. The extended profile will be triggered, because Lisa authenticated to the Portal through RADIUS database authentication. Any linksets mapped to the extended profile will be displayed on the Portal's Home tab. The base profile's linkset will also be displayed, because the base profile's linksets and access rules are always appended to the extended profile. The access rule defined for the extended profile will be applied, which means Lisa is granted access to all hosts and protocols on the intranet and the internet.

 **Note:**

If a match for the requested resource cannot be found in any of the access rules defined for the extended profile, the access rules of the base profile will be applied in sequential order.

Extended Profile for Users with Client Certificate

The two previous examples describe how to create extended profiles for remote users connecting from a secure network and through a secure authentication method.

In the same way, an extended profile could be created for users with a valid client certificate installed. Because client certificate authentication is considered more secure, the extended profile could provide more generous access rules.

1. Configure a group with access rules.

These access rules are configured directly under the Group level and constitutes the base profile. The access rules should apply to users without a client certificate.

2. Create a new client filter.

```
# /cfg/vpn 1/aaa/filter

Enter client filter number or name: (1-63)1

Creating Client Filter 1
Filter name:clientcert
```

3. Set the cert option to true.

```
>> Client Filter 1#cert

Current value: ignore
Client certificate present (true/false/ignore):true
```

4. Create an extended profile for users with a client certificate.

Reference the client filter you have just created.

```
# /cfg/vpn 1/aaa/group 2/extend

Enter profile number or filter reference name: (1-63)1

Creating Extended Profile 1
Enter client filter name:clientcert

Enter user type (advanced/medium/novice):advanced
```

5. Specify the access rules pertaining to the extended profile.

These access rules are configured for the Extended profile and should apply to users with a valid client certificate installed.

6. Apply the changes.

Extended Profile for Users with IE Cache Wiper

To make sure that sensitive information is not left in the computer's cache memory after a Portal session, a user group can be configured to reject access to certain intranet resources if the remote user is not running the IE cache wiper. On the other hand, an extended profile (with

more generous access rules) could be created for those who actually run the IE cache wiper.

When a user logs in to the Portal from a computer for the first time, they are asked whether or not to install the IE cache wiper. For users running Internet Explorer, the IE cache wiper clears cached HTML documents after a Portal session. In addition, the Portal address is removed from the visited URLs list.

1. Configure a group with access rules.

These access rules are configured directly under the Group level and constitutes the base profile. The access rules should apply to users without the IE cache wiper running.

2. Create a new client filter.

```
# /cfg/vpn 1/aaa/filter

Enter client filter number or name: (1-63)1

Creating Client Filter 1
Filter name:cachewiper
```

3. Set the iewiper option to true.

```
>> Client Filter 1#iewiper

Current value: ignore
IE cache wiper present (true/false/ignore):true
```

4. Create an extended profile for users with the IE cache wiper installed.

Reference the client filter you have just created.

```
# /cfg/vpn 1/aaa/group 2/extend

Enter profile number or filter reference name: (1-63)1

Creating Extended Profile 1
Enter client filter name:cachewiper

Enter user type (advanced/medium/novice):advanced
```

5. Specify the access rules pertaining to the extended profile.

These access rules are configured for the Extended profile and should apply to users with the IE cache wiper running.

6. Apply the changes.

Configuring bandwidth policy

Perform the following procedure to configure bandwidth policy for an extended group:

1. Specify the extended group to insert bandwidth policy management name.

```
/cfg/vpn #/aaa/group #/extend #
```

2. Select bandwidth policy.

```
>> Extended Profile 1#  
bwpolicy
```

3. Specify the bandwidth policy management name.

Choose any one bandwidth policy configured using command **/cfg/bwm/bwmpolicy #**.

```
Current value: ""  
Enter BW Policy name:
```

Extended profiles for users with NAP

Perform the following procedure to configure extended profiles for users with Network Access Protection (NAP):

1. Configure a group with access rules.

These access rules are configured directly under the Group level and constitutes the base profile. The filter is created to check if NAP checks are passed.

2. Create a new client filter.

```
# /cfg/vpn 1/aaa/filter  
  
Enter client filter number or name: (1-63)1  
  
Creating Client Filter 1  
Filter name:nap
```

3. Set the NAP option to true.

```
>> Client Filter 1#nap  
  
Current value: ignore  
NAP passed (true/false/unsupported/ignore):true
```

4. Create an extended profile for users with the IE cache wiper installed.

Reference the client filter you have just created.

```
# /cfg/vpn 1/aaa/group 2/extend

Enter profile number or filter reference name: (1-63)1

Creating Extended Profile 1
Enter client filter name:nap

Enter user type (advanced/medium/normal/novice):advanced
```

5. Specify the access rules pertaining to the extended profile.

These access rules are configured for the extended profile and applies to the users running NAP.

6. Apply the changes.

Chapter 10: Group Links

This chapter describes how to configure various types of hypertext links that appear on the Portal's Home tab.

Link Types

The following link types are available:

- WTS and Citrix . Gives the user access to setting up WTS and Citrix. ([WTS and Citrix Setup](#) on page 205)
- SMB. Gives the user access to folders on an SMB (Windows file share) file server ([Example 1: Link to SMB \(Samba\) File Server](#) on page 208).
- FTP. Gives the user access to folders on an FTP file server ([Example 2: Link to FTP File Server](#) on page 210).
- External. Link (direct) to web page. Suitable for external web sites ([Example 3: Direct Link to Web Page](#) on page 216).
- Internal. Link (secured) to web page. Suitable for internal web pages ([Example 4: Secured Link to Web Page](#) on page 218).
- Iauto. Automatic login link (secured) to password-protected web page ([Example 5: Automatic Login Link Secured by the AVG](#) on page 220).
- Terminal. Link to terminal server through Java applet for Telnet or SSH connections ([Example 6: Link to Terminal Server](#) on page 225).
- HTTP proxy. Link for accessing web pages through the AVG 's HTTP Proxy server ([Example 9: HTTP Proxy Link](#) on page 242).
- FTP proxy. Application tunnel link to a specified FTP server ([Example 10: FTP Proxy Link](#) on page 245).
- Custom. Application tunnel link to a custom application server ([Example 7a: Custom Port Forwarder Link](#) on page 227).
- Telnet. Application tunnel link to terminal server for Telnet connections.
- Mail. Application tunnel link to mail server (for example, Outlook Express).
- Netdrive. Application tunnel link for mapping a network drive to an SMB (Windows file share) file server.
- WTS. Application tunnel link (port forwarding) to Windows Terminal Server.
 - [Example 7b: Windows Terminal Server Port Forwarder Link with Automatic Portal Login](#) on page 233

- [Example 7c: Windows Terminal Server Port Forwarder Link with Automatic Backend Server Login](#) on page 235
- Outlook. Application tunnel link to Microsoft Exchange server ([Example 8: Outlook Port Forwarder Link](#) on page 238).
- NetDirect. Portal link used to automatically download and start the Net Direct agent, that is, the downloadable version of the SSL VPN client ([Configure Net Direct Link](#) on page 101).
- Citrix. Application tunnel link to Citrix. ([Example 5a: Automatic Login Link to Citrix Metaframe Server](#) on page 223)
- Vdesktop. Application to access secure Web-based applications and services.

Linksets

Each user group can be provided with one or several linksets. The linkset itself contains one or several links. The linksets and included links appear on the Portal's **Home** tab for the user to access intranet or Internet web sites, mail servers, file servers or web applications. When a group member is logged in, all linksets mapped to the user's group will be displayed.

The purpose of creating linksets is that when the linkset is created, it can be mapped to several user groups. Thus, links that should be common to several user groups can easily be assigned to the desired groups, without the need to create the links over and over again for each group. For group-specific links, simply create a linkset that is exclusive for that group.

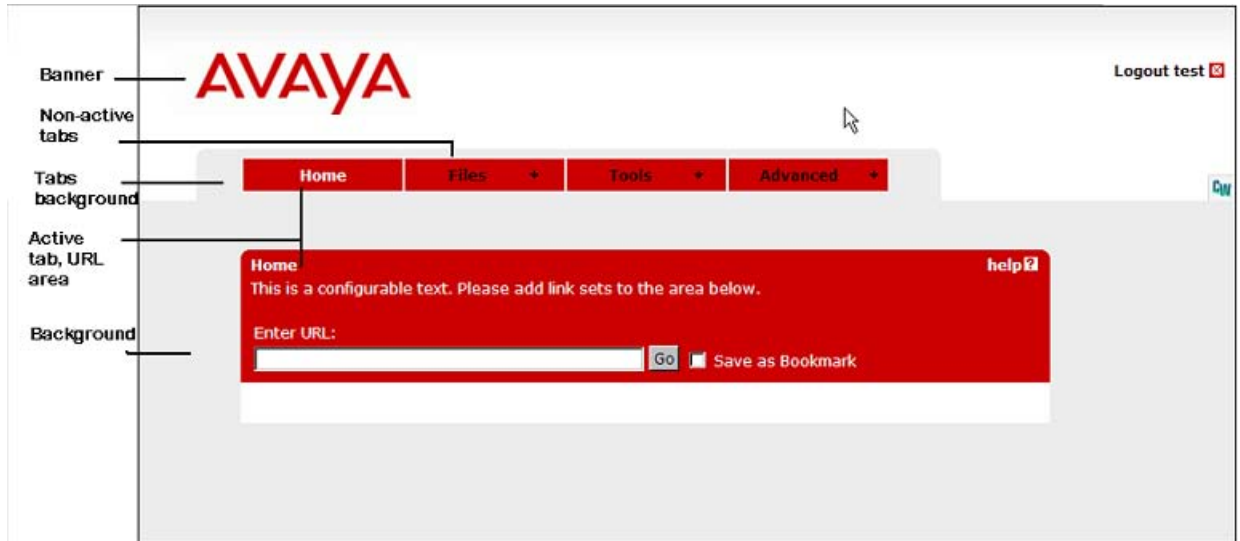
Make sure that access to the resource provided through the link is not contradicted by any access rules that apply to the group(s) in which the remote user is a member.

Linkset Name

The linkset name (set with the **name** command) is used to map the linkset to the desired user access group.

Linkset Text

Optionally, using the **text** command, the linkset can be provided with a heading that is displayed on the Portal's Home tab. Using HTML tags, the heading can be formatted as desired.



Autorun Support

With autorun support enabled, all links in the linkset will be executed automatically as soon as the remote user is logged in to the Portal. The links will not be visible on the Portal's Home tab.

Configuration Examples

This section includes examples of how to create linksets with different link types and shows how to map the linksets to groups.

WTS and Citrix Setup

The VPN Gateway hosts the ActiveX and Java versions of the Citrix and WTS clients. It allows the user to install them on demand. Users will no longer need to have the client already installed. When the built-in client is enabled, the following additional parameters can be configured.

- Screen resolution
- Color depth
- Enable local drive mapping
- Enable local printer mapping
- Application to start after logon

- Enable single sign-on
- Enable Java version as the default client
- KeyMap URL
- Hide port forwarder window
- Enable clipboard redirection

1. Create a new linkset.

```
Enter type of link (hit TAB to see possible values) [internal]:
wts
```

```
Entering: WTS settings menu
```

2. Specify the Desktop Connection settings.

```
Local host ip address [127.0.0.2]:
```

```
Local port [3390]:
```

```
Remote Desktop Connection host: 172.16.2.1
```

```
Remote Desktop Connection port [3389]:
```

```
Host mapping [Enter to skip]:
```

```
Application path []:
```

```
Working Directory []:
```

*** Note:**

Mac OS X uses 127.0.0.1 by default. To use loopback address other than 127.0.0.1, Mac user must configure the loopback alias manually.

3. Configure the Desktop parameters.

```
Screen size : (Full Screen/
800x600/1024x768/1152x864/1280x720/1280x768/1280x800/1280x960/12
80x1024/1360x768/1600x900/1600x1200/1680x1050/1920x1080)
[800x600]:
```

```

Color depth : (8 bit/15 bit/16 bit/24 bit/32 bit (True Color))
[16 bit]:

Map local drives : (on/off) [off]:

Connect local printers : (on/off) [off]:

Enable single sign on : (on/off) [off]:

Enable JavaRDP as default client : (on/off) [off]:

KeyMap URL []:

Hide port forwarder window : (on/off) [on]:

Paste text to show up in the Applet window, press Enter to create
a new line, and then type "..." (without the quotation marks) to
terminate.

If you *only* enter "..." a default text will be generated:

```

Create a Linkset for File Server Access

1. Specify the VPN for which you like to create a linkset.

In this example we will create a specific linkset for file server access. The linkset should include two links, one for access to an SMB (Windows file share) file server and one for access to an FTP server.

The linkset name should later be used to map the linkset to a group.

The linkset text (optional) will display a heading just above the links that are included in the linkset. Any HTML source can be used to format the heading, for example,

```
<b>Heading</b>
```

for a boldface heading. In the following example, the FONT tag has been used to format the heading with the Impact typeface.

```

# /cfg/vpn 1/linkset

Enter Linkset number or name (1-1024):1

Creating Linkset 1
Linkset name:files

```

```
Linkset text (HTML syntax, eg <b>A heading</b>):<FONT
FACE="Impact">File server access</FONT>

Autorun Linkset (true/false) [false]:<press ENTER>
```

2. Apply the changes.

```
>> Linkset 1#apply

Changes applied successfully.
```

Example 1: Link to SMB (Samba) File Server

As one of the links in the linkset we have just created, create a direct link to the home share folder of the currently logged on user. This link type should be used for SMB (Windows file share) file servers.

1. Create a new link for the current linkset.

```
>> Linkset 1#link

Enter Link number (1-256):1

Creating Link 1
```

2. Enter the link text to be displayed next to the link on the Portal's Home tab.

```
Enter link text:Link to home share folder
```

3. Enter the desired link type, that is, SMB.

To view available link types, press TAB following the prompt.

```
Enter type of link (hit TAB to see possible
values) [internal]:

<TAB>

smb      ftp      proxy    ftpproxy  custom    mail
telnet   netdrive wts      citrix    outlook   netdirec
t
terminal external internal iauto     vdesktop
```

```
Enter type of link (hit TAB to see possible
values) [internal]:
smb
```

```
Entering
: SMB settings menu
```

4. Specify the file server host.

The file server host can be entered as an IP address or a host name.

```
Enter SMB host:smb.example.com
```

5. Specify the Windows workgroup (optional).

If needed, a Windows workgroup can be specified. To skip this option, press ENTER.

```
Enter Workgroup on SMB host:<Windows workgroup name (press ENTER
to skip)>
```

6. Specify the name of the shared network folder.

In this example we will create a link to the currently logged in user's home share folder. This can be achieved by including the `<var:user>` macro. The macro expands to the remote user's user name as provided on the Portal login page.

To provide access to a folder on a lower level in the file structure, simply add a forward slash (/) and the folder name, for example, **home share/<var:user>/manuals/drafts**. Folder names are not case sensitive and spaces can be used in folder names.

Note:

When configuring an SMB (Windows file share) link to be displayed on a PDA Portal, specifying a shared network folder is required.

```
Enter name of shared network folder on host:home share/
<var:user>
```

7. Select whether or not you want to add the domain as a single-sign-on domain (if applicable).

For security reasons, automatic login to the SMB file server (using the Portal login credentials) is only possible if the SMB server's domain name or IP address is specified as a single sign-on domain, using the `/cfg/vpn #/aaa/ssodomains/add` command or by answering **yes** in this step.

If not, an error message will be displayed to the user, saying that Single Sign-on is not allowed. The folder specified in the link will however be shown if the user enters

password in the **Password** field and clicks the **Open** button on the Portal's **Files** tab.

*** Note:**

Single sign-on is always possible if the user name and password is specified in the link. Enter the link specification after the

Enter SMB host

: prompt (see step 4), e.g.: user:password@smb.example.com.

```
Domain not covered by ssodomain. Add? (yes/no) [yes]:
Leaving: SMB settings menu
```

8. View the resulting HREF and link text.

```
>> Link 1#cur

Link 1:
HREF =    [<smb>/xnet/smb/smb.example.com//home%20share/
<var:user>]
Link text =    [Link to home share folder]
Link type = <not set> [smb]
```

9. Apply the changes.

Example 2: Link to FTP File Server

This example shows how to create a direct link to an FTP file server.

1. Create a new link for the current linkset.

```
>> Linkset 1#link

Enter Link number (1-256):2

Creating Link 2
```

2. Define the link text to appear on the Portal's Home tab.

```
Enter link text:Link to FTP file server
```

3. Enter the desired link type, that is, FTP.

To view available link types, press TAB following the prompt.

```
Enter type of link (hit TAB to see possible
values) [internal]:
```

```
<TAB>
```

```
smb      ftp      proxy    ftpproxy  custom    mail
telnet   netdrive  wts      citrix    outlook   netdirec
t
terminal external  internal iauto     vdesktop
```

```
Enter type of link (hit TAB to see possible
values) [internal]:
ftp
```

```
Entering
: FTP settings menu
```

4. Specify the file server host.

The file server host can be entered as an IP address or a host name.

```
Enter FTP host:192.168.128.3
<FTP host by IP address or host name>
```

5. Specify the shared network directory.

By specifying an initial path, a specific directory can be listed right away when the user clicks the link. In this example, the initial path `/!` is specified. For FTP servers, this translates into the currently logged in user's home directory.

Like with the SMB link, macros can be used. To provide access to a folder or file on a lower level in the file structure, the initial path syntax could be as follows: `/home/share/<var:user>/Manuals/drafts/`. Note that directory names are case sensitive for FTP file servers. Spaces can however be used in directory names.

```
Enter initial path on host (/! for home directory):/!
```

6. Select whether or not you want to add the domain as a single-sign-on domain (if applicable).

For security reasons, automatic login to the FTP file server (using the Portal login credentials) is only possible if the file server's domain name or IP address is specified as a single sign-on domain, using the `/cfg/vpn #/aaa/ssodomains/add` command or by answering `yes` in this step.

If not, an error message will be displayed to the user saying that Single Sign-on is not allowed. The directory specified in the link will however be shown after the user

has entered password in the **Password** field and clicked the **Open** button on the Portal's **Files** tab.

Single sign-on is always possible if the user name and password is specified in the link. Enter the link specification after the

Enter FTP host:

prompt (see step 4), e.g.: `user:password@ftp.example.com`. For anonymous mode, enter `ftp` or `anonymous` before the colon (:) and any text string after the colon.

```
Domain not covered by ssodomain. Add? (yes/no) [yes]:
Leaving: FTP settings menu
```

7. View the resulting HREF and link text.

```
>> Link 2#cur

Link 2:
HREF =    [<ftp>/xnet/ftp/192.168.128.3/!]
Link text =    [Link to FTP server]
Link type = <not set> [ftp]
```

8. Apply the changes.

```
>> Link 2#apply

Changes applied successfully.
```

Map the Linkset to a Group

Linkset 1 now includes two links, one link to an SMB file server and one link to an FTP file server. For a group member to be able to access the links, the linkset must be mapped to the desired groups.

1. Map Linkset 1 to the **staff** group.

This step assumes that we have previously created a group called **staff**.

```
>> Main#cfg/vpn 1/aaa/group

Enter group number or name: (1-1023)staff

>> Group 1#linkset

>> Linksets#add
```

```
linkset name:files
```

2. Apply the changes.

```
>> Linksets#apply
Changes applied successfully.
```

When a member of the **staff** group logs in to the Portal, Linkset 1 (including the two file server links) will be visible on the Home tab.

Set Net Direct as Prerequisite

To configure the AVG system, the external, internal, and custom links needs to be configured. For web-based applications, the internal and external link types require Net Direct as the prerequisite. For local applications, custom link type requires the Net Direct as the prerequisite. When Net Direct is set as prerequisite, the user can directly open the link by double clicking on the link. This avoids the user to open the Net direct before opening the link. By default the Net Direct option is disabled. In the following sections, procedures to enable Net Direct for these link types is shown.

Net Direct based custom link type

The following procedure explains the steps to enable the Net Direct for custom link:

1. Specify the linkset to include the link.

```
/cfg/vpn 1/linkset 1
```

Linkset 1 Menu

name	Set linkset name
text	Set linkset text
autorun	Set autorun support
link	Link menu
del	Remove linkset

2. Specify the link number.

```
Enter Link number <1-256>: 1
Creating Link 1
```

3. Define the link text to appear on the Portal's Home tab.

```
Enter Link text: MCS
```

4. Enter the desired link type.

```
Enter type of link (hit TAB to see possible values) [internal]:
custom
```

```
Entering: custom settings menu
```

5. Select the type of server as Net Direct.

```
Select type(Net Direct(ND)/PortForwarder(PF))[PF]:ND
```

6. Specify the path to the application to be started when the user clicks the link.

```
Application path []: usb:/spoclient/apps/mcs/mcs.exe
```

7. If desired, enter arguments to the application. This step identifies the command-line argument to be used by the application.

```
Application arguments []:
```

```
Leaving: custom settings menu
```

Net Direct-based internal link type

Follow these steps to enable the Net Direct.

1. Specify the linkset to include the link.

```
>> Linkset 3# link
```

```
Enter the link number (1-256): 2
```

```
Creating Link 2
```

2. Define the link text to appear on the Portal's Home tab.

```
Enter Link text: Web MCS
```

3. Enter the desired link type.

```
Enter type of link (hit TAB to see possible values) [internal]:  
internal
```

```
Entering: internal settings menu
```

4. By default Net Direct option is disabled for internal link. Enable the Net Direct option.

```
Enable NetDirect (on/off): on
```

5. Enter the protocol to access the application through web.

```
Enter method (http/https): https
```

6. Enter the address of the HTTP server.

```
Enter host (eg inside.company.com): 47.103.241.98
```

7. Specify the path to the application to be started when the user clicks the link.

```
enter path (eg/): /pca/pca?action=request&type=launchWebClient
```

```
Leaving: internal settings menu
```

Net Direct-based external link type

Follow these steps to enable the Net Direct.

1. Specify the linkset to include the link.

```
>> Linkset 3# link
```

```
Enter the link number (1-256): 3
```

```
Creating Link 3
```

2. Define the link text to appear on the Portal's Home tab.

```
Enter Link text: Web MCS - Direct
```

3. Enter the desired link type.

```
Enter type of link (hit TAB to see possible values) [internal]:  
external
```

```
Entering: External settings menu
```

4. By default Net Direct option is disabled for internal link. Enable the Net Direct option.

```
Enable NetDirect (on/off): on
```

5. Enter the protocol to access the application through web.

```
Enter method (http/https): https
```

6. Enter the address of the HTTP server.

```
Enter host (eg www.company.com): 47.103.241.98
```

7. Specify the path to the application to be started when the user clicks the link.

```
Enter path (eg/): /pca/pca?action=request&type=launchWebClient
```

```
Leaving: External settings menu
```

Other Link Types

The following sections provide examples on how to configure the other available link types. The instructions assume that you are familiar with creating linksets and mapping linksets to groups. If not, read the previous section, [Create a Linkset for File Server Access](#) on page 207.

Example 3: Direct Link to Web Page

This example shows how to create a link to a web page. As opposed to the internal link, the external link directs the HTTP request straight to the specified resource, that is, without adding the AVG rewrite prefix (compare to [Example 4: Secured Link to Web Page](#) on page 218).

1. Specify the VPN and the linkset where you want the link included.

```
# /cfg/vpn 1/linkset 1

>> Linkset 1#link

Enter Link number (1-256)3

Creating Link 3
```

2. Define the link text to appear on the Portal's Home tab.

```
Enter link text:Link to Avaya's public web site
```

3. Enter the desired link type.

Press TAB when prompted to see available link types.

```
Enter type of link (hit TAB to see possible
values) [internal]:

<TAB>

smb      ftp      proxy    ftpproxy  custom    mail
telnet   netdrive wts      citrix    outlook   netdirec
t
terminal external internal iauto     vdesktop

Enter type of link (hit TAB to see possible
values) [internal]:
external

Entering : external
settings menu
```

4. Specify the access protocol, fully qualified domain name, and path.

A path must always be specified. When a forward slash (/) is specified as the path, the document root of the web server is implied.

```
Enter method (http/https):http

Enter host (eg www.company.com):www.avaya.com

Enter path (eg /):/
```

```
Leaving: External settings menu
```

5. View the resulting HREF and link text.

```
>> Link 3#cur

Link 3:
HREF = [http://www.avaya.com/]
Link text = [Link to Avaya's public web site]
Link type = <not set> [external]
```

6. Apply the changes.

```
>> Link 3#apply

Changes applied successfully.
```

Example 4: Secured Link to Web Page

This example shows how to create a secure link to an internal web page on your intranet. The internal link directs the HTTP request, where the rewrite prefix (boldface) is added to the link.

Example: `https://vip.example.com/http/inside.example.com/`

1. Specify the VPN and the linkset where you want the link included.

```
# /cfg/vpn 1/linkset 1

>> Linkset 1#link

Enter Link number (1-256)4

Creating Link 4
```

2. Define the link text to appear on the Portal's Home tab.

```
Enter link text:Link to internal phone list
```

3. Enter the desired link type.

Press TAB when prompted to see available link types.

```
Enter type of link (hit TAB to see possible
values) [internal]:

<TAB>
```

smb	ftp	proxy	ftpproxy	custom	mail
telnet	netdrive	wtb	citrix	outlook	netdirect
terminal	external	internal	iauto	vdesktop	

Enter type of link (hit TAB to see possible values) [internal]:
internal

Entering : internal
settings menu

4. Specify the access protocol, domain name, and path.

A path must always be specified. When forward slash (/) is specified as the path, the document root of the web server is implied.

To create a link to the currently logged in user's home page (if any) on the intranet, you can use the `<var:user>` macro as an element in the specified path: Example: `/~<var:user>`

```
Enter method (http/https):http
Enter host (eg inside.company.com):inside.example.com
Enter path (eg /):/accounting/phonelist.html
Leaving: Internal settings menu
```

5. View the resulting HREF and link text.

```
>> Link 4#cur

Link 4:
HREF = [/http/inside.example.com/accounting/phonelist.html]
Link text = [Link to internal phone list]
Link type = <not set> [internal]
```

6. Apply the changes.

```
>> Link 4#apply

Changes applied successfully.
```

Example 5: Automatic Login Link Secured by the AVG

This example shows how to use the `iauto` link type to create an automatic login link to a password-protected web page. The HTTP request is directed to the AVG, where the rewrite prefix (boldface) is added to the link.

Example: `https://vip.example.com/https/inside.example.com/`

The

`iauto`

link supports form-based authentication as well as HTTP-based authentication, such as NTLM or basic (`www-authenticate`). The AVG automatically retrieves the URL to analyze which type of authentication method it uses.

For an example on how to use the `iauto` link together with a port forwarder, see [Example 7c: Windows Terminal Server Port Forwarder Link with Automatic Backend Server Login](#) on page 235.

1. Specify the VPN and the linkset where you want the link included.

```
# /cfg/vpn 1/linkset 1
>> Linkset 1#link
Enter Link number (1-256)5
Creating Link 5
```

2. Define the link text to appear on the Portal's Home tab.

```
Enter link text:Secure auto-logon link to web page
```

3. Enter the desired link type.

Press TAB when prompted to see available link types.

```
Enter type of link (hit TAB to see possible
values) [internal]:
```

<TAB>

smb	ftp	proxy	ftpproxy	custom	mail
telnet	netdrive	wt	citrix	outlook	netdirect

```

terminal      external      internal  iauto      vdesktop

Enter type of link (hit TAB to see possible
values) [internal]:
iauto

Entering
: iauto settings menu

```

4. Specify the URL to the password-protected web page.

Having entered the URL, the AVG automatically retrieves the URL to analyze which authentication type it uses.

Example 1: In this example, a web page using HTTP-based authentication was found.

```

Enter login URL (eg http://owa.foo.com/exchange/
<var:user>):http://inside.example.com/login/login.htm

Server uses web authentication.Link created.

```

A link to the web page has been created. When the user clicks the link on the Portal's Home tab, the AVG automatically attempts to authenticate to the web page using the credentials provided by the user on Portal login. If successful, the user is automatically logged in. If not, the AVG generates a temporary form for the user to log in with the required credentials.

If the web server requires a domain name along with user name, use the `/cfg/vpn # /linkset #/link #/iauto/mode` command to change the mode from

normal

to

add_domain

. Also see the **mode** command in the *Command Reference*.

Example 2. In this example, a web page using form-based authentication was found. The input fields found on the form are displayed in the CLI for you to specify what values to insert in the fields when the user clicks the

iauto

link.

```
>> Link 5#iauto
```

```

Enter login URL (eg http://owa.foo.com/exchange/
<var:user>):http://inside.example.com/login/login.asp

Found form with the following input fields:

user      password
Specify how they should be expanded for each user.
The macros <var:user>, <var:password> and <var:domain> can be used.

Enter value for key 'user': []<var:user>
Enter value for key 'password': []<var:password>

Link created.

```

In the preceding example, the

user

and

password

fields were found on the form. The names correspond to the

input name

value in the web page's source code.

Enter the values to be inserted in the fields. Macros, text strings or a combination of both can be used. By using the <var:us er> and <var:pas sword> macros as values (as in the preceding example), the macros will expand to the credentials provided by the remote user on the Portal login page. If these are the credentials that the target web page requires, the user is automatically logged in. If not, the web page's form is displayed instead.

The <var:domain> macro can be used if the form includes an input field for a Windows domain. In this case, the macro will expand to the domain name specified for the current authentication ID, using the `/cfg/vpn #/aaa/auth #/domain` command.

5. View the resulting settings (form-based example).

```

>> Link 5#cur

Link text      = [Secure auto-
                  logon link to web
                  page]

Link type      = <not set> [iauto]

```

Iauto menu:	
Authentication type	= auto
HTTP or HTTPS	= http
Internal host	= [www.example.com]
Path on internal server	= [/login/login.asp]
Use this as a proxy link	= off
Basic auth mode	= normal
IAuto Mapping: <var:user>	1: user
	2: password <var:password>

If needed, the values that you have specified can later be edited using the `/cfg/vpn # /linkset #/link #/iauto/mapping` command.

Link properties like method (http or https), host and path can be edited separately, using the commands on the IAuto menu. Use the `/cfg/vpn #/linkset #/link #/iauto` command.

For a full account of available `iauto` commands, see the *Command Reference*.

6. Apply the changes.

```
>> Link 5#apply
Changes applied successfully.
```

Example 5a: Automatic Login Link to Citrix Metaframe Server

This example shows how to configure a single sign-on link to Web Interface 2.0 and Web Interface 3.0 on a Citrix Metaframe server.

1. Specify the VPN and the linkset where you want the link included.

```
# /cfg/vpn 1/linkset 1

>> Linkset 1#link

Enter Link number (1-256)5

Creating Link 5
Enter link text:Single sign-on to Citrix Metaframe Server

Enter type of link (hit TAB to see possible values)
[internal]:iauto

Entering: Iauto settings menu
```

2. Enter the login URL.

Example 1. Single sign-on to Web Interface 2.0:

```
Enter login URL (eg http://
owa.foo.com/exchange/
<var:user>):

http://citrix.example.com/      default/login.asp?
Citrix/MetaFrameXP/           ClientDetection=On
```

Example 2. Single sign-on to Web Interface 3.0:

```
Enter login URL (eg http://
owa.foo.com/exchange/
<var:user>):

http://citrix.example.com/      default/login.aspx?
Citrix/MetaFrameXP/           ClientDetection=On
```

The AVG automatically retrieves the URL to analyze which authentication type it uses.

```
Found form with the following input fields:
state      LoginType  user      password  domain      Log In
Specify how they should be expanded for each user.
The macros <var:user>, <var:password> and <var:domain> can be
used.

Enter value for key 'state': [LOGIN]<press ENTER>

Enter value for key 'LoginType': [Explicit]<press ENTER>

Enter value for key 'user': []<var:user>

Enter value for key 'password': []<var:password>
```

```

Enter value for key 'domain': []<var:domain>

Enter value for key 'Log In': []<press ENTER>

Link created.
Leaving: Iauto settings menu

```

Enter the values to be inserted in the fields. Macros, text strings or a combination of both can be used. By using the <var:us er> and <var:pas sword> macros as values (as in the preceding example), the macros will expand to the credentials provided by the remote user on the Portal login page. If these are the credentials that the target web page requires, the user is automatically logged in. If not, the web page's form is displayed instead.

3. Apply the changes.

```

>> Link 5#apply

Changes applied successfully.

```

Example 6: Link to Terminal Server

This example shows how to create a link to a terminal server using Telnet or SSH. When the remote user clicks the link, a terminal window is opened in a new browser window by way of a Telnet/SSH terminal Java applet.

1. Specify the VPN and the linkset where you want the link included.

```

# /cfg/vpn 1/linkset 1

>> Linkset 1#link

Enter Link number (1-256)6

Creating Link 6

```

2. Define the link text to appear on the Portal's Home tab.

```

Enter link text:Terminal access

```

3. Enter the desired link type.

Press TAB when prompted to see available link types.

```

Enter type of link (hit TAB to see possible
values) [internal]:

```

```

<TAB>
smb      ftp      proxy    ftpproxy  custom  mail
telnet   netdrive  wts      citrix    outlook  netdirec
t
terminal external  internal iauto     vdesktop

Enter type of link (hit TAB to see possible
values) [internal]:

Entering
: terminal settings menu

```

4. Specify the remote host, the remote port, and the terminal access protocol.

Enter the IP address or host name of the Telnet or SSH server. TCP port 23 is the default port used for Telnet. If you want to use SSH, specify TCP port 22 as the remote port

```

Enter remote host:terminal.example.com

Enter remote port [23/22]:23

Enter protocol (ssh/sshv2/telnet) [telnet]:telnet

```

5. If a keymap URL is specified, the user's keyboard mappings can be configured through an external configuration file located on the specified web server.

This feature is designed for users with non-standard keyboards. Example: When prompted for a keymap URL, enter the URL, path (if any) and finally the name of the keyboard mapping file, e.g. `http://inside.example.com/keyCodes.at386`.

Documentation describing the configuration file properties is in Appendix F, "Definition of Key Codes " in the *User's Guide*.

```

Keymap URL [Enter to skip]:

```

6. Enter the address and port of an intermediate HTTP Proxy server (if any).

If users are working from a location requiring traffic to pass through an intermediate HTTP Proxy server on the intranet, enter the IP address (or domain name) and port of that proxy server. All applet traffic will thus be tunneled to the VPN Gateway

through the HTTP proxy server. The HTTP Proxy server should have CONNECT support.

Skipping the prompts means that all applet traffic will be tunneled directly to the AVG, unless Internet Explorer has been configured to use a proxy. In this case this proxy server will be used instead.

```
HTTP Proxy Host [Enter to skip]:
HTTP Proxy Port:
```

7. If an intermediate HTTP Proxy server is specified, enter the credentials to access this server (if required).

This step will not be displayed if the previous step was skipped.

```
HTTP Proxy Username [Enter to skip]:
HTTP Proxy Password:
Leaving: Terminal settings menu
```

8. View the resulting HREF and link text.

```
>> Link 6#cur

Link 6:
HREF = [<telnet>/terminalform.yaws?host=terminal.example.com
&telnet=true&ssh=false&port=23&ph=&pp=&phu=&php=]
Link text = [Terminal access]
Link type = <not set> [terminal]
```

9. Apply the changes.

When the remote user clicks the Telnet or SSH link on the Portal, a terminal window appears (in the SSH case, the user has to log in first). To be able to type anything in the terminal window, the user must first click on the window (anywhere) to activate it.

Example 7a: Custom Port Forwarder Link

By clicking a Port Forwarder link, the remote user is provided with one or more secure tunnels to an intranet application server. The purpose is to be able to run one or more UDP- or TCP-based client applications, for example, Telnet or Windows Terminal Server, towards a specified application server.

When the user clicks the link, a Java applet is downloaded. The Java applet is instructed to listen to a port number on the user's own computer (that is, 127.0.0.1 or any other IP address within the 127.x.y.z range). The applet then forwards all incoming traffic to an application server on the intranet.

Setting up a Port Forwarder link to be displayed on the Portal's Home tab (instead of letting the user set up a Port Forwarder on the Portal's Advanced tab) is a way of making application access simpler for the user. In addition, group members whose user type is set to

novice

or

medium

will not have access to the Advanced tab. A third advantage with the Port Forwarder link is that it can be set to launch the application automatically.

Using the Port Forwarder API (see page [PortForwarder API](#) on page 241), you can develop a custom application that automatically logs in the user to the VPN and executes the Port Forwarder link.

Note:

The

custom

link type (exemplified here) lets you configure a port forwarder link for an application of your own choice. Examples 7a, 7b, and 7c show ways of applying the custom port forwarder for two different applications, Telnet and Windows Terminal Server. Another way of configuring port forwarder links for these applications is to use the

telnet

and

wtS

link type wizards. The only difference is that some relevant parameters (like port numbers) are suggested automatically by the wizards. Other available port forwarder link type wizards are

netdrive, mail

and

outlook

.

The following example describes how to set up a custom port forwarder link to a Telnet server.

1. Specify the VPN and the linkset where you want the link included.

```
# /cfg/vpn 1/linkset 1
>> Linkset 1#link
```

```
Enter Link number (1-256)7
Creating Link 7
```

2. Define the link text to appear on the Portal's Home tab.

```
Enter link text:Link to Telnet server
```

3. Enter the desired link type.

Press TAB when prompted to see available link types.

```
Enter type of link (hit TAB to see possible values)
[internal]:
<TAB>
smb      ftp      proxy    ftpprox  custom    mail
y
telnet   netdrive wts      citrix   outlook   netdire
ct
terminal external internal iauto    vdeskto
p

Enter type of link (hit TAB to see possible values)
[internal]: custom

Entering : Custom port
settings menu
```

4. Specify the desired traffic mode.

```
Traffic mode (udp/tcp) [tcp]:
```

TCP is a connection-oriented protocol. It does not transfer any data until a connection between two hosts has been established. TCP guarantees that all data will be delivered to the receiving host in the same order as it is sent.

UDP is a connection-less protocol. No connection to a receiving host needs to be established before the data is transferred. UDP does not guarantee delivery but is lightweight and efficient.

5. Enter local host IP address and local port.

The SSL tunnel will be established between the specified TCP/UDP port on the user's local machine (local host IP=any IP address within the 127.x.y.z range) and the VPN Gateway.

When specifying the local port, use port numbers just above 5000 which are usually free to use or use the application-specific port number. On Windows machines any port number can be used.

```
Local host ip address [127.0.0.1]:<press ENTER to accept>
Local port [5001]:<press ENTER to accept>
```

6. Specify destination host (IP address or host name) and destination port.

The VPN Gateway relays data from the user's local machine to the specified target (destination host) and application-specific port (destination port).

```
Remote destination host:telnet.example.com
Remote destination port:23
<Telnet-specific port number>
```

7. Specify the desired host mapping (optional).

Host mapping can be specified for example, if the user should start the application manually. Example: If the host alias is

```
telnet
```

and the local port number

```
5001
```

, the user can start the Telnet client and use

```
telnet 5001
```

as host name/port to connect to the server specified as destination host.

*** Note:**

Usage of host aliases requires the alias to be mentioned in the Java applet window (see [11](#) on page 232). It also requires the user to have administrator privileges on the client computer or have write access enabled for the hosts and lmhosts files. Hosts and lmhosts files are located in %windir%\hosts on Windows 98 and ME and in %windir%\system32\drivers\etc\hosts on NT, XP and Windows 2000.

```
Host mapping [Enter to skip]:
```

8. Press ENTER to not create another port forwarder.

In this example, one connection is sufficient for the link we are configuring. However, one single Port forwarder link can be configured to set up multiple connections. For example, to configure an Outlook Express link, you have to configure the Port forwarder link to set up one connection to an SMTP server and another to a POP3 server.

```
Create yet another port forwarder? (yes/no) [no]:n
```

9. Specify the application to be started (optional).

This step defines the application to be started when the user clicks the link. Start by entering the name of the executable, (e.g. `cmd.exe` to open the Command window). By pressing ENTER to skip, no application will be started when the user clicks the link. The user can however be instructed to start the application manually (see [11](#) on page 232). If `browser` is entered as executable, the user's default browser will be started.

*** Note:**

The VPN Gateway must be able to find the executable either through the PATH variable or in the registry (on Windows clients), that is, HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths. To make sure the program is found, the complete path to the executable can also be entered after the

Application path

prompt. Generally, only graphical applications (that is, applications that open their own windows) can be started using the Port forwarder link. This example describes how to open the Command window (`cmd.exe`) to run the Telnet client. In the following example, the executable is entered without a path.

```
Application path []:cmd.exe
```

10. If desired, specify an argument to the application.

The argument identifies the command-line argument to be used by the application, e.g.

```
http://127.0.0.1:5025
```

if the executable is

```
browser
```

. Note that each application has its own set of arguments.

In this example, the argument to cmd.exe tells the application to start Telnet and connect to the local host IP address and port we specified in step 5.

```
Application arguments [!]/c start telnet 127.0.0.1 5001
```

11. Enter a custom text (for example, with user instructions) to be displayed in the Java applet window (optional).

The custom text (if entered or pasted) will be displayed in the Java applet window automatically displayed when the user clicks the link. The instructions can for example be used to explain the purpose of the port forwarder(s) or how to launch the application (for example, by using the specified host alias).

```
Paste text to show up in the Applet window, press Enter to create
a
new line, and then type "..." (without the quotation marks) to
terminate. If you *only* enter "..." a default ext will be
generated:
>...
```

If a custom text is entered or pasted, remember to press ENTER after the last line, followed by three periods (...). Finally press ENTER to view the next prompt.

If no custom text is desired, simply type the three periods and press ENTER to view the next prompt. This will result in a standard text being displayed in the Java applet window, with information about the host/ lmhost file mappings and the sockets that are opened for the port forwarder. Following is an example of a Java applet standard text:

```
Started port forwarder(s):
tcp:127.0.0.1:5001 -> telnet.example.com:23
Host alias mapping(s):
telnet -> 127.0.0.1
```

12. Enter the address and port of an intermediate HTTP Proxy server (if any).

If users are working from a location requiring traffic to pass through an intermediate HTTP Proxy server on the intranet, enter the IP address (or domain name) and port of that proxy server. All applet traffic will thus be tunneled to the VPN Gateway through the HTTP proxy server. The HTTP Proxy server should have CONNECT support.

Skipping the prompts means that all applet traffic will be tunneled directly to the AVG, unless Internet Explorer has been configured to use a proxy. In this case this proxy server will be used instead.

```
HTTP Proxy Host [Enter to skip]:
HTTP Proxy Port:
```

13. If an intermediate HTTP Proxy server is specified, enter the credentials to access this server (if required).

This step will not be displayed if the previous step was skipped.

```
HTTP Proxy Username [Enter to skip]:
HTTP Proxy Password:
Creating Tunnel 1
```

14. Apply the changes.

```
>> Link 7#apply

Changes applied successfully.
```

*** Note:**

If you expect the connection to include more than 15 minutes of inactivity, increase the TCP connection idle timeout value, using the `/cfg/vpn #/server/tcp/keep` command.

Example 7b: Windows Terminal Server Port Forwarder Link with Automatic Portal Login

This example describes a more advanced application of the Port Forwarder link. It shows how the `<var:portal>` macro can be included in the argument to have the browser connect to a terminal applet residing on an intranet web host used for Windows Terminal Server sessions. The terminal applet in its turn will be instructed to connect to the user's local machine to enable a secure SSL session.

For more information about macros, see the Variables section in the *Command Reference*.

*** Note:**

Instead of creating a custom port forwarder link to a Windows Terminal Server, we recommend using the

`wt`

link type. It automatically provides the relevant port numbers for the link in a wizard. This example just uses the WTS application to show the principles of configuring a custom port forwarder link.

1. Specify the VPN and the linkset where you want the link included.

```
# /cfg/vpn 1/linkset 1

>> Linkset 1#link

Enter Link number (1-256)7

Creating Link 7
```

2. Define the link text to appear on the Portal's Home tab.

```
Enter link text:Link to Windows Terminal Server
```

3. Enter the desired link type.

```
Enter type of link (hit TAB to see possible values)
[internal]:custom

Entering: Custom port forwarder settings menu
```

4. Specify local host IP and port, remote host and port, host mapping (if desired), application path and arguments, custom Java applet text (optional) and HTTP proxy server (if any).

In this example, a terminal applet on the Windows Terminal Server web page should be instructed to connect to source IP address 127.0.0.2 on port 3389, which is the application-specific port number for Windows Terminal Server sessions.

When the user clicks the link, a new browser window appears. For the browser to be able to access the terminal applet on the intranet host, the connection has to be made through the Portal. This is done by including the `<var:portal>` macro in the argument. The macro expands to the Portal's IP address.

For detailed descriptions of each prompt, see example 7a on [Example 7a: Custom Port Forwarder Link](#) on page 227.

```
Traffic mode (udp/tcp) [tcp]:<press ENTER to accept>

Local host IP address [127.0.0.1]:127.0.0.2

Local port [5005]:3389

Remote destination host:www.example.com

Remote destination port:3389

Host mapping [Enter to skip]:wts

Create yet another port forwarder? (yes/no) [no]:n

Application path []:browser
```

```

Application arguments []:https://<var:portal>/http/
www.example.com /TSWeb/connect_new_server.asp?
Server=127.0.0.2

Paste text to show up in the Applet window, press Enter to create
a
new line, and then type "..." (without the quotation marks) to
terminate. If you *only* enter "..." a default text will be
generated:
>...
HTTP Proxy Host [Enter to skip]:
Creating Tunnel 1
Leaving: Custom port forwarder settings menu

```

5. Apply the changes.

```

>> Link 7#apply

Changes applied successfully.

```

Example 7c: Windows Terminal Server Port Forwarder Link with Automatic Backend Server Login

This example describes an even more advanced scenario – almost identical to the one described in example 7b – but here the backend server requires user authentication. To enable the remote user to access the resource with one single click, the Port Forwarder and iauto links will have to be combined.

1. Create a dummy group.

The purpose of creating a dummy group is to hide the iauto link. We will later embed the iauto link in the port forwarder link. Because no user belongs to the dummy group, the iauto link will not be visible.

```

# /cfg/vpn 1/aaa/group 30

Creating Group 30

Group name:iauto_dummy

Enter number of sessions (0 is unlimited):<press ENTER>

Enter user type (advanced/medium/novice):<press ENTER>

```

2. Create the iauto link.

```

>> Group 30#/cfg/vpn 1/linkset 2

Creating Linkset 2

```

```

Linkset name:iauto

Linkset text (HTML syntax, eg <b>A heading</b>):<press ENTER>

Autorun Linkset (true/false) [false]:<press ENTER>

>> Linkset 2#link 1

Creating Link 1

Enter link text:iauto for port forwarder

Enter type of link (hit TAB to see possible values)
[internal]:iauto

Entering: Iauto settings menu

Enter login URL (e.g. http://owa.foo.com/exchange/
<var:user>):http://www.example.com/TSWeb/
connectauth.asp

Found form with the following input fields:

user      password
Specify how they should be expanded for each user.
The macros <var:user>, <var:password> and <var:domain> can be
used.

Enter value for key 'user': []<var:user>

Enter value for key 'password': []<var:password>

Link created.

Leaving: Iauto settings menu

```

3. Map the linkset we just created to group 30.

```

# /cfg/vpn 1/aaa/group 30/linkset/add iauto

>> Linksets#

```

4. Create the port forwarder link.

Specify the VPN and the linkset where you want the link included.

```

# /cfg/vpn 1/linkset 3

Creating Linkset 3

Linkset name:wts

Linkset text (HTML syntax, eg <b>A heading</b>):WTS links

Autorun Linkset (true/false) [false]:<press ENTER>

```

```
>> Linkset 3#link
Enter Link number (1-256)1
Creating Link 1
```

5. Enter the link text to be displayed on the Portal's Home tab.

```
Enter link text:WTS auto-logon link
```

6. Enter the desired link type.

```
Enter type of link (hit TAB to see possible values)
[internal]:custom
Entering: Custom port forwarder settings menu
```

7. Specify local host IP and port, remote host and port, host mapping (if desired), application path and arguments, custom Java applet text (optional), and HTTP proxy server (if any).

The only difference compared to example 7b, is that the iaauto link we created initially is included in the executable argument instead of the web server address.

The argument (see the following) includes the string

```
"link.yaws?t=iauto&a=1&b=2&c=1"
```

where a = xnet id (1), b = linkset id (2), c = link id (1). Xnet ID is equivalent to VPN ID.

The <var:portal> macro is still present because the connection to the intranet web server is made through the Portal. The macro expands to the Portal's IP address.

```
Traffic mode (udp/tcp) [tcp]:<press ENTER to accept>
Enter local host IP address [127.0.0.1]:127.0.0.2
Enter local port [5005]:3389
Remote destination host:www.example.com
Remote destination port:3389
Host mapping [Enter to skip]:wts
Create yet another port forwarder? (yes/no) [no]:n
Application path []:browser
```

```

Application arguments []:https://<var:portal>/link.yaws?
t=iauto&a=1&b=2&c=1

Paste text to show up in the Applet window, press Enter to create
a new line, and then type "..." (without the quotation marks) to
terminate. If you *only* enter "..." a default text will be
generated:
>...
HTTP Proxy Host [Enter to skip]:
Creating Tunnel 1
Leaving: Custom port forwarder settings menu

```

8. Map linkset 3 to group 1.

```

>> Link 1#/cfg/vpn 1/aaa/group 1/linkset

>> Linksets#add

linkset name:wts

```

9. Apply the changes.

```

>> Linksets#apply

Changes applied successfully.

```

Example 8: Outlook Port Forwarder Link

This example shows how to create a Port forwarder link to a Microsoft Exchange server on the intranet, enabling secure transfer of mail messages, calendar, address book entries and similar.

For the Outlook Port forwarder to work, the following prerequisites must be fulfilled:

- The Exchange server's domain name suffix must be configured using the `/cfg/vpn # /adv/dns/search` command. See step 8 on page 241.
- The user must have administrator's rights on their computer or have write access enabled for the hosts and lmhosts files. Hosts and lmhosts files are located in %windir%\hosts on Windows 98 and ME and in %windir%\system32\drivers\etc\hosts on NT, XP and Windows 2000.
- The user's client machine must be of the Hybrid or Unknown node type. The node type can be checked by entering `ipconfig /all` at the DOS prompt.

To change the node type to Hybrid (if needed), go to the registry editor folder HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters. If not already present, add a new DWORD Value called NodeType. Double-click NodeType and enter 8 in the Value Data field. Click OK and restart the computer.

- The Outlook Port forwarder link is meant to be used by clients connecting to the VPN Gateway from outside the intranet. If the client has direct connectivity to the intranet, the Port forwarder will fail. If the client has access to intranet DNS servers, communication will fail as well.
- To test DNS resolution, the VPN Gateway should be able to ping the Exchange server from the CLI, using the fully qualified name (FQDN).
- The user's Outlook account must be hosted on the Exchange server(s) specified in the Port forwarder.
- The Outlook Port forwarder link will not work if a proxy server is configured in the client browser. This also means that a HTTP Proxy link or HTTP Proxy portal session cannot be active at the same time as the Outlook Port forwarder.
- If you expect the connection to include more than 15 minutes of inactivity, increase the TCP connection idle timeout value, using the `/cfg/vpn #/server/tcp/keep` command.
- To ensure proper operation, specify the DNS name of the portal server, using the `/cfg/vpn #/server/dnsname` command.
- If a firewall exists between the VPN Gateway and the Exchange server, the firewall settings must allow traffic to the required Exchange server ports. Note that these may vary with your environment. More information can be found on <http://support.microsoft.com>, for example, Knowledge Base Articles 280132, 270836, 155831, 176466, 148732, 155831, 298369, 194952, 256976, 302914, 180795 and 176466.
- When a user clicks an embedded link in an e-mail message, the web site associated with the link must be displayed in a new instance of Internet Explorer. In Internet Explorer, go to the Tools menu and select Internet Options. Under the Advanced tab, go to Browsing and deselect the "Reuse windows for launching shortcuts" option.

This is how to create an Outlook port forwarder link to be displayed on the Portal:

1. Specify the VPN and the linkset where you want the link included.

```
# /cfg/vpn 1/linkset 1

>> Linkset 1#link

Enter Link number (1-256)8

Creating Link 8
```

2. Define the link text to appear on the Portal's Home tab.

```
Enter link text:Link to Outlook
```

3. Enter the desired link type.

```
Enter type of link (hit TAB to see possible values)
[internal]:out look

Entering: Custom port forwarder settings menu
```

4. Specify the desired local host IP address and the FQDN of the Exchange server.

The local host IP address should be set to 127.0.0.1 or any other IP address in the 127.x.y.z range. The Exchange server address must be entered as a fully qualified domain name (FQDN) and not as an IP address.

The services provided by the Exchange server (mail, calendar, address book and so on) may be distributed between different Exchange servers. If this is the case, you have the option to create several Outlook port forwarders where the relevant Exchange servers can be specified.

If several port forwarders are required, note that each port forwarder must have a unique source IP address. A new source IP address is automatically suggested by the system if you choose to add another port forwarder.

```
Specify the Exchange settings...

Local host IP address [127.0.0.1]:<press ENTER to accept>

Fully qualified host mapping:exchange1.example.com

Create yet another Outlook port forwarder? (yes/no) [no]:yes

Local host IP address [127.0.0.2]:<press ENTER to accept>

Fully qualified host mapping:exchange2.example2.com

Create yet another Outlook port forwarder? (yes/no) [no]:no
```

5. Specify the path to the application to be started when the user clicks the link.

```
Application path [outlook.exe]:<press ENTER to accept>
```

6. If desired, enter arguments to the Outlook client.

An example of an argument can be

```
/Profile myprofile.
```

For a reference to available Outlook arguments, see Microsoft Knowledge Base Article no 296192 available on <http://support.microsoft.com/?kbid=296192>.

```
Application arguments []:
```

7. Enter a custom text (for example, with user instructions) to be displayed in the Java applet window (optional).

For a more detailed description of this step, see example 7a on [Example 7a: Custom Port Forwarder Link](#) on page 227.

```
Paste text to show up in the Applet window, press Enter to create
a
new line, and then type "..." (without the quotation marks) to
terminate. If you *only* enter "..." a default text will be
generated:
> ...
Creating Tunnel 1
Creating Tunnel 2
Leaving: Custom port forwarder settings menu
```

8. Configure the Exchange servers' domain name suffixes as DNS search entries for the portal server.

This step is absolutely necessary for the Outlook Port forwarder to work. Using the Exchange servers exemplified in step 4 the following domain names can have to be entered.

```
# /cfg/vpn 1/adv/dns/search

Current value: ""
Enter search domains (separated by
comma):example.com,example2.com
```

9. Apply the changes.

```
>> DNS Settings#apply

Changes applied successfully.
```

PortForwarder API

The AVG software provides an API for developing a custom application that automatically logs in the user to the desired VPN and executes a previously configured Port forwarder link on the Portal's Home tab. This way, a remote user does not have to browse to the Portal and click the Port forwarder link to set up the required application tunnel(s).

Briefly, this is how to use the Port forwarder API.

1. Configure a Port forwarder link of the desired type.
2. Develop a Java application/applet that uses the Port forwarder API.

The Port Forwarder API can be downloaded from the Portal through the URL https://vpn.example.com/nortel_cacheable/portforwarder.zip,

where `vpn.example.com` is the DNS name of your Portal. API programming instructions and examples is in Appendix I in the *User's Guide*.

Example 9: HTTP Proxy Link

Like the

internal

link, the

proxy

link lets the user access a web page through a secure SSL connection. However, a web page may contain plugins (for example, a Flash movie) which, in their turn, may include embedded links to other web pages. If you click a, the HTTP request may not reach the VPN Gateway and the URL cannot be displayed.

To ensure display of all URLs—including those embedded in plugins—the HTTP Proxy feature lets you download a Java applet to the client. The client browser's proxy settings should be changed to direct all HTTP requests to this Java applet. The Java applet then turn routes each request through a secure SSL tunnel to the AVG proxy server, where it is unpacked and redirected to the proper destination.

For users with Internet Explorer, the link can be configured to change/clear the proxy settings automatically.

* Note:

Outlook Port forwarder links (if configured) or Outlook Port forwarder portal sessions (Advanced tab) will not work if a proxy server is configured in the client browser.

1. Specify the VPN and the linkset where you want the link included.

```
# /cfg/vpn 1/linkset 1

>> Linkset 1#link

Enter Link number (1-256)9

Creating Link 9
```

2. Define the link text to appear on the Portal's Home tab.

```
Enter link text:HTTP Proxy link
```

3. Enter the desired link type.

```
Enter type of link (hit TAB to see possible values)
[internal]:proxy

Entering: Proxy settings menu
```

4. Select whether or not to reconfigure the clients browser's proxy settings.

If you enter `yes` here, the user does not have to reconfigure the browser's proxy settings manually. They are automatically reconfigured to use 127.0.0.1 and 4567 as proxy server address and port. This is specified for both HTTP and HTTPS (Secure) traffic in IE's Proxy settings window. When the user exits the Java applet window, the proxy settings are automatically restored to the original settings.

Note that automatic updating and clearing of the proxy settings are only possible for Internet Explorer running on Windows.

If set to `no`, or if another browser than Internet Explorer is used (for example, Netscape), instructions on how to reconfigure the proxy settings manually is provided in the Java applet window displayed when the user clicks the HTTP Proxy link.

```
Update client proxy settings (only for Windows)? (yes/no)
[no]:yes
```

5. Select whether or not to open a new browser window.

```
Open a new browser window? (yes/no) [no]:
```

If you enter

`yes`

here, a new browser window will automatically be opened when the user clicks the HTTP Proxy link. If set to

`no`

, the user should open a new browser window to start browsing in HTTP Proxy mode.

6. If desired, specify the URL to be opened.

You will only be prompted for an URL if you chose to open a new browser window (see the previous step).

When you enter the URL, also specify the protocol, that is, `http` or `https` (see following example).

```
Open browser using initial URL, e.g. http://foo.bar.com [Enter to skip]:http://www.example.com
```

7. Enter the address and port of an intermediate HTTP Proxy server (if any).

If users who work from a location requiring traffic to pass through an intermediate HTTP Proxy server on the intranet, enter the IP address (or domain name) and port of that proxy server. All applet traffic will thus be tunneled to the VPN Gateway through the HTTP proxy server. The HTTP Proxy server should have CONNECT support.

Skipping the prompts means that all applet traffic is tunneled directly to the AVG, unless Internet Explorer has been configured to use a proxy. In this case this proxy server will be used instead.

```
HTTP Proxy Host [Enter to skip]:
HTTP Proxy Port:
```

8. If an intermediate HTTP Proxy server is specified, enter the credentials to access this server (if required).

This step will not be displayed if the previous step was skipped.

```
HTTP Proxy Username [Enter to skip]:
HTTP Proxy Password:
```

9. Apply the changes.

```
>> Link 9#apply

Changes applied successfully.
```

To access a web page in HTTP Proxy mode, the remote user should first click the link to download the HTTP Proxy applet, then reconfigure the browser's proxy settings (instructions are provided in the Java applet window). For users with Internet Explorer, the link can be configured to change/clear the proxy settings automatically.

Finally, the user should open a new browser window to start browsing in HTTP Proxy mode. As an alternative, the link can be configured to open a new browser window automatically.

To quit surfing in HTTP Proxy mode, the user should click the Stop Port Forwarder button in the Java applet window and manually restore the original browser settings. Note that this last step is not required if the link is set to configure/clear the browser's proxy settings automatically.

Example 10:FTP Proxy Link

To enable access to an FTP server through a native FTP client (installed on the remote user's machine), a Portal link can be created. When the user clicks the link, a Java applet is downloaded. The Java applet is instructed to listen to a port number on the user's own computer (that is, 127.0.0.1 or any other IP address within the 127.x.y.z range).

The Java applet forwards all incoming traffic to a specified remote FTP server. The FTP client (if specified) will be started automatically on the remote user's machine and connect to the local IP address on the client machine. The AVG will then act as an FTP Proxy and relay data from the FTP client to the remote FTP server.

1. Specify the VPN and the linkset where you want the link included.

```
# /cfg/vpn 1/linkset 1

>> Linkset 1#link

Enter Link number (1-256)9

Creating Link 10
```

2. Define the link text to appear on the Portal's Home tab.

```
Enter link text:FTP Proxy link
```

3. Enter the desired link type.

```
Enter type of link (hit TAB to see possible values)
[internal]:ftpproxy

Entering: FTP proxy settings menu
```

4. Enter local host IP address and local port.

The SSL tunnel will be established between the specified TCP port on the user's local machine (local host IP=any IP address within the 127.x.y.z range) and the VPN Gateway.

When specifying the local port, use port numbers just above 5000 which are usually free to use or use the application-specific port number for FTP file transfer, that is, 21. On Windows machines any port number can be used.

```
Local host ip address [127.0.0.1]:<press ENTER to accept>

Local port [21]:<press ENTER to accept>
```

5. Specify the FTP server (IP address or host name) and port.

The VPN Gateway relays data from the user's local machine to the specified target (remote FTP server) and application-specific port (remote FTP port).

```
Remote FTP server:ftp.example.com
Remote FTP port [21]:<press ENTER to accept>
```

6. Specify the application to be started (optional).

This step defines the application to be started when the user clicks the link. Enter the path to the FTP client, e.g. `c:\program files\application\app.exe`.

By default, `cmd /c start ftp` is suggested, which means that the FTP session will be run in the command window.

```
Application path [cmd /c start ftp]:<path to application>
```

If it is preferred that the user starts the application manually, you can clear the application path using the **app** command on the FTP proxy menu (**/cfg/vpn #/linkset #/link # /ftpproxy**).

7. Specify an argument to the application (optional).

This step identifies the command-line argument to be used by the application. Note that each FTP application has its own set of arguments. See the documentation for the FTP client to be started with the FTP Proxy link.

The default argument tells the application (see the previous step) to connect to the local host IP address and port we specified in.

```
Application arguments [127.0.0.1]:<application argument>
```

8. Enter a custom text (for example, with user instructions) to be displayed in the Java applet window (optional).

The custom text (if entered or pasted) will be displayed in the Java applet window automatically displayed when the user clicks the link. The instructions can for example be used to explain the purpose of the FTP Proxy or how to start the application.

```
Paste text to show up in the Applet window, press Enter to create
a
new line, and then type "..." (without the quotation marks) to
terminate. If you *only* enter "..." a default text will be
generated:
>...
```

If a custom text is entered or pasted, remember to press ENTER after the last line, followed by three periods (...). Finally press ENTER to view the next prompt.

If no custom text is desired, simply type the three periods and press ENTER to view the next prompt. This will result in a standard text being displayed in the Java applet window, with information about the host/ lmhost file mappings and the sockets that are opened for the FTP proxy. Following is an example of a Java applet standard text:

```
Started FTP proxy:
tcp;127.0.0.1:21 -> ftp.example.com:21
```

9. Enter the address and port of an intermediate HTTP Proxy server (if any).

If users are working from a location requiring traffic to pass through an intermediate HTTP Proxy server on the intranet, enter the IP address (or domain name) and port of that proxy server. All applet traffic will thus be tunneled to the VPN Gateway through the HTTP proxy server. The HTTP Proxy server should have CONNECT support.

Skipping the prompts means that all applet traffic will be tunneled directly to the AVG, unless Internet Explorer has been configured to use a proxy. In this case this proxy server will be used instead.

```
HTTP Proxy Host [Enter to skip]:
HTTP Proxy Port:
```

10. If an intermediate HTTP Proxy server is specified, enter the credentials to access this server (if required).

This step will not be displayed if the previous step was skipped.

```
HTTP Proxy Username [Enter to skip]:
HTTP Proxy Password:
```

11. Apply the changes.

```
>> Link 10#apply

Changes applied successfully.
```

Net Direct Link

Instructions on how to create the Net Direct link is in [Net Direct](#) on page 87.

Chapter 11: Customize the Portal

This chapter explains how to customize the Portal with respect to logo, company name, color, static link texts and language version.

Default Appearance

The default appearance of the Portal is displayed. The colors referred to as colors 1-4 below correspond to colors 1-4 in the CLI.



Colors are defined as hexadecimal codes. The default colors are:

- Non-active tabs = #58B2C9 (color 4)
- Tabs background = #D0E4E9 (color 2)
- Active tab, URL area and clean icons = #2088A2 (color 3)
- Background = #ACCDD5 (color 1)

Change Color Theme

Even though the Portal's individual colors can be changed (see next section), we recommend using color themes. Also consider how the applied colors fit with the colors of your company logo.

1. Select the desired color theme.

```
>> Main#cfg/vpn 1/portal/colors  
  
>> Portal Colors#theme  
  
Color theme (default/aqua/apple/jeans/cinnamon/candy):
```

2. Apply the changes.

```
>> Portal Colors#apply  
  
Changes applied successfully.
```

Change the Colors

To change individual colors on the Portal, proceed as follows:

1. Select the desired color.

In this example, the non-active tabs color will be changed to red.

For a reference to some common colors and their hexadecimal color codes, see [Common Colors](#) on page 250.

```
>> Portal Colors#color4  
  
Current value: #accdd5  
Color name (HTML syntax, eg #003399 for blue):#FF0000
```

2. Apply the changes.

```
>> Portal Colors#apply  
  
Changes applied successfully.
```

Common Colors

The following table lists a number of common web safe colors. For further reference, search the Internet for "web colors" and you will get access to sites with full reference to hexadecimal color codes.

Table 3: Common Colors with Hexadecimal Color Codes.

Color	Hexadecimal code
White	FFFFFF
Black	000000
Darkgray	A9A9A9
Lightgrey	D3D3D3
Red	FF0000
Green	008000
Blue	0000FF
Yellow	FFFF00
Orange	FFA500
Violet	EE82EE
Darkviolet	9400D3
Pink	FFC0CB
Brown	A52A2A
Beige	F5F5DC
Limegreen	32CD32
Lightgreen	90EE90
Darkblue	00008B
Navy	000080
Lightskyblue	87CEFA
Mediumblue	0000CD
Darkred	8B0000

Change the Banner Image

To substitute the Avaya banner image for your own company banner, make the desired image file (in .gif format) available on a TFTP, FTP, SCP or SFTP server. Then proceed as follows:

1. Specify the VPN for which you wish to change the logo, enter the Portal menu and type the import command.

Changing the logo will affect both the login and portal pages.

Note that the size of the banner must not exceed 16 MB. If the cluster consists of several VPNs, the total size of imported banners in the different VPNs must not exceed 16 MB.

```
>> Portal Colors#../  
  
>> Portal#import  
  
Select protocol (tftp/ftp/scp/sftp) [tftp]:ftp  
  
Enter hostname or IP address of server:192.168.128.1  
  
Enter filename on server: company.gif  
FTP User (anonymous):john  
  
Password:password  
  
received 8207 bytes
```

2. Apply the changes.

```
>> Portal #apply  
  
Changes applied successfully.
```

Change Company Name

The company name is shown as a tool tip when you move the mouse pointer over the logo and as the browser window name.

1. On the Portal menu, enter the companynam command and type the desired text.

```
>> Portal#  
  
companynam  
  
Current value: Avaya  
Company Name:Company Inc.
```

2. Apply the changes.

```
>> Portal #apply  
  
Changes applied successfully.
```

Change Icon Mode

The link icons can be either clean or fancy. Clean icons use a single color, as defined with the `color3` command. Fancy icons are multi-colored, shaded and animated. The default icon mode is

fancy

.

1. On the Portal menu, enter the `iconmode` command.

```
>> Portal#  
iconmode  
  
Current value: fancy  
Home tab icon mode (clean/fancy) [fancy]:clean
```

2. Apply the changes.

```
>> Portal #apply  
  
Changes applied successfully.
```

Change Number of Link Columns

1. On the Portal menu, choose `linkcols`. Then enter the desired number of columns.

```
>> Portal#linkcols  
  
Current value: 2  
Home tab columns [2]:4
```

2. Apply the changes.

```
>> Portal#apply  
  
Changes applied successfully.
```

If the number of link columns is set to 4, links 1 to 4 are placed on the first row, links 5-8 on the second row and so on. Additional links are added in sequential order from left to right on the next row. If for example link 2 is deleted, links 3-4 are adjusted

left to fill the blank space, link 5 is moved up to the first row and links 6-8 are adjusted left.

Change Link Area Width

1. On the Portal menu, choose linkwidth. Then enter the desired percentage.

```
>> Portal#linkwidth  
  
Current value: 100%  
Link Width (auto/0-100%) [auto]:75%
```

2. Apply the changes.

```
>> Portal#apply  
  
Changes applied successfully.
```

Hide Enter URL Field

The Enter URL field on the Home tab is configurable. It is displayed by default but you can hide it if desired.

1. On the Portal menu, choose linkurl.

```
>> Portal#linkurl  
  
Current value: on  
URL input field on link page (on/off) [on]:off
```

2. Apply the changes.

```
>> Portal#apply  
  
Changes applied successfully.
```

Change the Static Text

The static text is displayed on the Home tab in the URL area (see page [Default Appearance](#) on page 249).

1. On the Portal menu, choose `linktext`.

Add the desired text as a static text. Press ENTER to create a new line and type three periods "...". Finish by pressing ENTER once again.

```
>> Portal#linktext

Write or paste the text, press Enter to create a new line, and
then
type "..."(without the quotation marks) to terminate.

> Click the desired link below: > ...
```

2. Apply the changes.

```
>> Portal#apply

Changes applied successfully.
```

Change Static Text on Login Page

The static text displayed on the Portal Login Page can be changed as well. The default text is "This is a configurable text: ".

1. On the Portal menu, choose `logintext`.

Type or paste the desired text message. The text can be entered as an ordinary text string or as HTML code. Press ENTER to create a new line and type three periods "..." (without the quotation marks). Finish by pressing ENTER once again.

```
>> Portal#logintext

Write or paste the text, press Enter to create a new line, and
then
type "..."(without the quotation marks) to terminate.> Welcome
to the Company Inc. Security Portal. Please log in:
> ...
```

2. Apply the changes.

```
>> Portal#apply

Changes applied successfully.
```

Change Portal Language

The VPN Gateway software supports export of an English dictionary file whose entries can be translated to any language. After the translation, the file can be imported and set to replace the English language version on the Portal. Tab names, general text, button and field labels will thus display the imported file's language version.

1. Start by exporting the language definition file.

Specify the desired file transfer method and the IP address of the file server to which you want to export the language definition file. Also enter a name for the language definition file, e.g.

`template.po`

, and the ISO 639 language code (press ENTER to export the predefined language definition file in English).

```
>> Main#cfg/lang/export

Select TFTP or FTP (tftp/ftp) [tftp]:ftp

Enter hostname or IP address of server:192.168.128.1

Enter filename on server:template.po

Enter (ISO 639) Language Code (default is predefined language):
FTP User (anonymous):john

Password:password

sent 51895 byte
```

2. Translate the language definition file you have exported.

Open the language definition file with a text editor, for example, Notepad. Check that the

`charset`

parameter specified in the Content-Type entry is set according to the character encoding scheme you are using.

```
"Content-Type: text/plain; charset=iso-8859-1\n"
```

Next, translate the entries displayed under

`msgstr`

(message string). Do not translate the entries under

```
msgid
```

(message id). As you translate the file it may not be perfectly obvious where in the Portal your translation will turn up. If the text strings do not display where you expected (when the file is loaded to the Portal), simply edit the language definition file and reload it (see step3).

```
#: portal.erl:764
msgid ""
" page."
msgstr ""
"pagina

."
<example in Spanish>
```

There are very useful Open Source software tools for translating po files. You can find tools that run on Windows as well as Unix (search for **po files editor** in your web search engine). A translation tool is particularly useful when a new version of the AVG software is released. The new template file supplied with the software can be exported and merged with a previously translated language file, so that only new and changed text strings need to be translated.

3. Import the language definition file you have translated to the VPN Gateway.

Specify the desired file transfer method and the IP address of the file server from which you want to import the language definition file. Enter the name of the translated file and the ISO 639 language code corresponding to your new language version. The language code is saved to the configuration together with the imported language definition file.

Tip: To view valid language codes, use the **vlist** command. To limit the list to language codes starting with a specific letter, enter e.g.

```
vlist e.
```

```
>> Main#cfg/lang/import

Select TFTP or FTP (tftp/ftp) [tftp]: f
Enter hostname or IP address of server: 192.168.128.1
Enter filename on server:template.po

Enter (ISO 639) Language Code:esl

<for Spanish>

FTP User (anonymous):john

Password:password

received 54520 bytes
Language definition loaded.
```

4. Set the Portal to use the new language version.

Specify the ISO 639 language code corresponding to your new language version.

```
>> Main#cfg/vpn 1/portal/lang/setlang  
Current value: en  
<English, default language>  
Enter (ISO 639) Language Code [en]:esl  
<for Spanish>
```

5. Apply the changes.

```
>> Portal Language#apply  
Changes applied successfully.
```

Check the New Appearance

To check the new appearance of the Portal, connect to the Portal by entering the VPN's domain name in your browser. The default logo will be replaced on the Login Page as well as on the Portal.

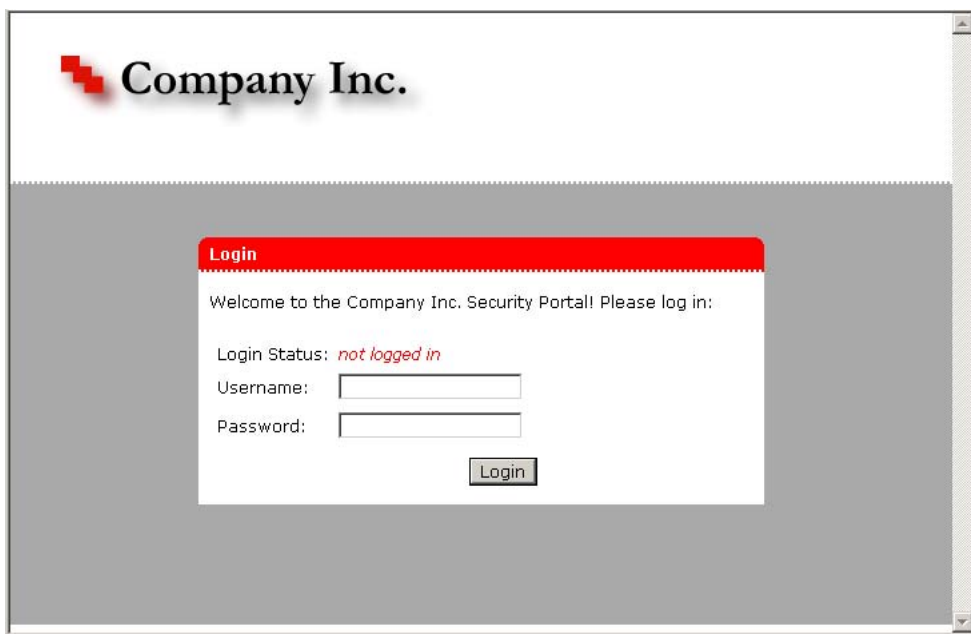


Figure 5: Login Page with New Logo, Colors and Static Text

After login, the Portal is displayed with a new logo, company name, static text and color.

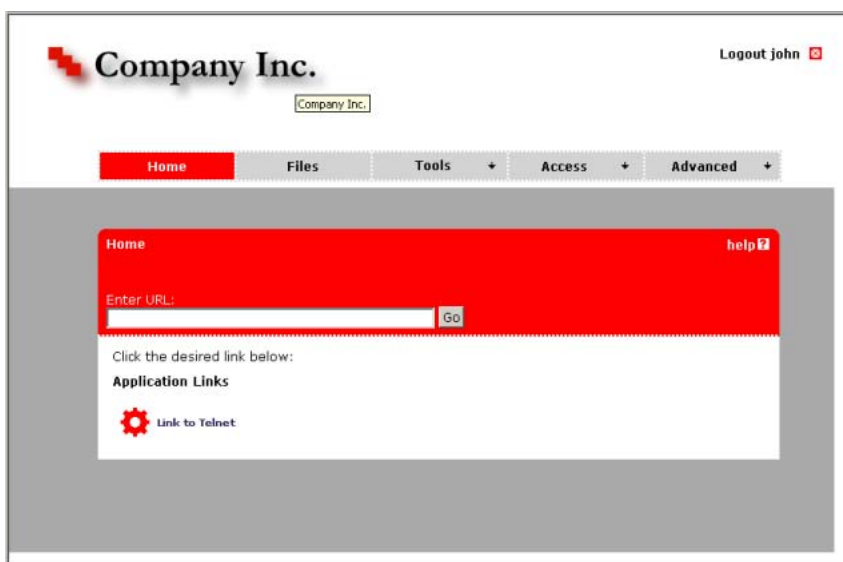


Figure 6: Portal with New Logo, Colors, Static Text and Company Name

Automatic Redirection to Internal Site

To automatically redirect a visitor to an internal site by passing the default portal altogether, proceed as follows:

1. On the Portal menu, choose `redirect`.

```
>> Portal#redirect

Current value: " "

Enter URL to redirect to:https:// <var:portal> /http/
<var:user> : <var:password> @inside.example.com/protected
```

2. Insert a logout link on the internal site.

For the visitor to be able to logout from the portal internal site, a logout link should be inserted on that page. This is what it might look like:

```
<a href=https://vpn.example.com/logout.yaws> Logout from portal </a>
```

To remove automatic redirection, enter the `redirect` command and press `ENTER` when prompted for the URL.

Automatic Redirection to Password-Protected Site

A visitor can be redirected to an internal password-protected site without a second login, provided the user name and password required on the intranet site is identical with the Portal's user name and password.

1. On the Portal menu, choose `redirect`.

```
>> Portal#redirect

Current value: " "

Enter URL to redirect to:https:// <var:portal> /http/
<var:user> : <var:password> @inside.example.com /protected
```

2. Insert a logout link on the internal site.

For the visitor to be able to logout from the portal from the internal site, a logout link should be inserted on that page. This is what it might look like:

```
<a href=https://vpn.example.com/logout.yaws> Logout from portal </a>
```

To remove automatic redirection, enter the `redirect` command and press `ENTER` when prompted for the URL.

Group-controlled Redirection to Internal Sites

Using the `<var:group>` macro, you may also redirect visitors to different internal sites, depending on their group membership.

1. On the Portal menu, choose linktext.

```
>> Portal#linktext

Write or paste the text, press Enter to create a new line, and
then
type "..."(without the quotation marks) to terminate.
><script> if ( " <var:group> " == "deptA")
{ location.replace ("https://vpn.example.com/http/
inside.example.com/deptA.html");} else if ( "
<var:group> " == "deptB") { location.replace ("https://
vpn.example.com/http/inside.example.com/
deptB.html"); } </script>

> ...
```

In the preceding example, deptA and deptB are group names.

2. Insert a logout link on the internal site.

For the visitor to be able to logout from the portal from the internal site, a logout link should be inserted on that page. This is what it might look like:

```
<a href=https://vpn.example.com/logout.yaws> Logout from portal </a>
```

*** Note:**

In the same way, the <var:user> macro can be used to control the action taken depending on which user is currently logged in.

3. Apply the changes.

```
>> Portal#apply

Changes applied successfully.
```

Upload Custom Content

The Custom Content feature is used to upload custom content (for example, Java applets, HTML pages, executables) to an area on the VPN Portal.

To access uploaded content, the user should specify the whole path to the content, e.g.

```
https://vpn.example.com/content/example.html.
```

You can also create a Portal link to the content, using the External Website link type (see [Group Links](#) on page 203). For a usage example, see Appendix I, "Using the Port Forwarder API" in the *User's Guide*.

*** Note:**

Content uploaded to the Custom Content area is accessible without the user having to log on to the Portal.

1. Create a zip file containing the content you wish to upload.

If the content you wish to import to the Portal requires caching on the remote user's machine when executed, create a directory called

`nortel_cacheable`

. Then store the content in this directory before zipping the files (sub-directories may exist). Note that file and directory names are case sensitive.

Examples of zip file contents:

- `noncacheable_content1.html`
- `subdir/noncacheable_content2.html`
- `avaya_cacheable/mycacheable_content1.html`
- `avaya_cacheable/subdir/mycacheable_content2.html`

Also see the `/cfg/vpn/server/http/allow*` commands in the Command Reference used to allow or deny caching of different file types.

*** Note:**

A previously imported zip file will be replaced with the new file. If you want to save existing Portal content, first export this content using the Export Custom Content button (see following step).

2. Upload the zip file to the Portal.

```
>> Main#cfg/vpn 1/portal/content

>> Portal Custom Content#import

Select protocol (tftp/ftp/scp/sftp) [tftp]:ftp

Enter hostname or IP address of server: www.example.com
Enter filename on server: example.zip
FTP User (anonymous): john
Password:
received 321 bytes
example.zip download succeeded.
```

3. Enable access to custom content.

```
>> Portal Custom Content#ena
```

This will make it possible for the remote user to access the custom content you have just uploaded.

4. Apply the changes.

Chapter 12: HTTP to HTTPS Redirection

This chapter describes how to configure the Avaya VPN Gateway (AVG) to automatically transform an HTTP client request into the required HTTPS request. By configuring such a redirect service on the VPN Gateway, the user can simply enter the fully qualified domain name in the web browser's address field, without having to specify (or knowing) the protocol required to establish a secure connection.

The redirect service is configured by adding an additional virtual HTTP server. When the virtual HTTP server on the VPN Gateway receives a request, it will redirect the browser to the virtual HTTPS server by sending an HTTP Location header to the browser.

This configuration example assumes that you have already set up a working HTTPS server for the Portal. If not, see [Clientless Mode](#) on page 35.

Configure HTTP to HTTPS Redirection

Log in as the administrator to the VPN Gateway.

1. Create a virtual HTTP server.

This step creates a new virtual HTTP server.

```
#
/cfg/ssl/server

Enter virtual server number: (1-256)
1

Creating Server 1

>> Server 1#

type

Current value: generic

Type (generic/http/socks):

http
```

2. Define a name for the virtual HTTP server.

This step lets you specify a name, by which you can identify the virtual HTTP server. To view the numbers and related names of all configured servers, use the **/info/servers** command. The name you specify is mainly intended for your own reference, and is not critical for the configuration itself. As the following example

suggests, the name can indicate the service for which the virtual server is created.

```
>> Server 1#
name
Current value:
" "
Enter new server name:
redirect service
```

3. Set listen TCP port for the HTTP server.

Each time you create a new virtual server, the listen port is automatically set to 443. For the HTTP to HTTPS redirect service in this example, the virtual HTTP server must be set to listen to port 80 (the default port used for HTTP).

```
>> Server 1#port
Current value: <not set> [443 (https)]
Enter listen port number:80
```

4. Assign the desired virtual server IP address to the HTTP server.

This is the address the client will connect to. It will typically be the same as the address of the portal HTTPS server.

```
>> Server 1#vips
Current value: " "
Enter server ips (comma separated):192.168.10.100
```

5. Disable SSL for the virtual HTTP server.

```
>> Server 1#ssl
>> SSL Settings#dis
```

6. Enable HTTPS to HTTP redirection.

```
>> SSL Settings#../http/httpsredir
```

```
Current value: off  
Perform http to https redirect (on/off):on
```

7. Apply the changes.

```
>> HTTP Settings#apply  
  
Changes applied successfully.
```

The remote user can now access the Portal either using http or https. If the user enters e.g.

`http://vpn.example.com`

in the browser, the request will be redirected to

`https://vpn.example.com.`

Chapter 13: Configure Tunnel Guard

This chapter describes how to configure the Avaya VPN Gateway (AVG) for use with Tunnel Guard. Tunnel Guard is an application that maintains checking that the required components (executables, DLLs, configuration files, and so on.) are installed and active on the remote user's machine.

*** Note:**

Tunnel Guard is also known as the Avaya Endpoint Access Control Agent. However, CLI configuration is performed under the Tunnel Guard context.

How is Tunnel Guard Activated?

For HTTPS connections, the Tunnel Guard applet is downloaded to the client machine and started as soon as the user has successfully logged in to the Portal.

For IPsec VPN client (formerly Contivity VPN client) connections, Tunnel Guard (if installed) is activated when the remote user logs in to the VPN.

*** Note:**

If Tunnel Guard is not installed on client machine, the IPsec or NDIC based users can bypass the Tunnel Guard checks using the command

```
/cfg/vpn #/aaa/tg/bypass
```

. In this case, user gets restricted access to the backend based on tg_failed rule.

Tunnel Guard SRS Rules

Which components to look for on the client machine is configurable through a certain specification, a Software Requirement Set (SRS) rule. The SRS rule in its turn should be mapped to one or more user groups, using the `/cfg/vpn #/aaa/group #/tgsrs` command. When Tunnel Guard is done checking the client machine, it reports the result to the server. If the SRS rule check succeeded (required components were present on the client machine), the user is permitted access to intranet resources as specified in the user group's access rules. If the check failed, the behaviour is configurable. Either the session/tunnel can be torn down or the user may be granted restricted access.

If needed, a specific Tunnel Guard SRS rule administrator can be created. The SRS rule administrator is only granted access to the Tunnel Guard Admin applet (accessible through the BBI). For instructions about how to create an administrator user in the CLI, see Chapter 5, "Managing Users and Groups" in the *User Guide*.

Configuration Using Wizard

This section describes how to use the Quick setup wizard to configure the VPN Gateway for use with Tunnel Guard. This is initially for testing purposes. You can later let this test setup evolve to a proper Tunnel Guard solution.

1. Specify the VPN for which you want to configure EAC Agent.

```
>>Main#/cfg/vpn 1/aaa/tg
```

2. Run the Tunnel Guard Wizard Quick Setup wizard.

```
>> TG#quick
```

```
In the event that the Tunnel Guard checks fails on a client,
the session can be teardown, or left in restricted mode
with limited access.
Which action do you want to use for Tunnel Guard
failure? (teardown/restricted) [restricted]:<press ENTER to
accept>
```

```
Do you want to create a tunnelguard test user? (yes/no) [yes]:
```

```
Enabling Tunnel Guard
Creating Client Filter 1
Name: tg_passed
Creating Client Filter 2
Name: tg_failed
Creating Linkset 2
Name: tg_passed
This Linkset just prints the TG result
Creating Linkset 3
Name: tg_failed
This Linkset just prints the TG result
Creating Group 2
Name: tunnelguard
Creating Extended Profile 1
Giving full access when tg passed
Creating Access rule 1
Creating Extended Profile 2
Giving no access when tg failed
Using SRS rule: srs-rule-test
Adding user 'tg' with password 'tg'
```

```
Use 'diff' to view pending changes, and 'apply' to commit
>> TG#
```

3. Apply the changes.

```
>> TG#apply

Changes applied successfully.
```

Apart from enabling Tunnel Guard, the wizard creates the following settings:

- Two client filters,

```
tg_passed
```

```
and
```

```
tg_failed
```

. The filters are used to trigger different extended profiles, depending on whether the Tunnel Guard checks failed or succeeded.

- Two linksets,

```
tg_passed
```

```
and
```

```
tg_failed
```

, for printing the result of the Tunnel Guard checks on the Portal's Home tab. The linkset texts read "The Tunnel Guard checks succeeded!" and "The Tunnel Guard checks failed." respectively. The latter linkset text also includes the variables `<var:tgFailureReason>` and `<var:tgFailureDetail>`, who expand to more detailed information about the failure (see [Tunnel Guard Checks Failed](#) on page 274).

- A test SRS rule called

```
srs-rule-test
```

. It checks if the

```
tg.txt
```

file is present in the

```
c:\tunnelguard
```

folder on the remote user's machine.

- A group called

```
tunnelguard
```

with two extended profiles. Extended profile 1 is triggered when the Tunnel Guard checks have succeeded. Its access rule gives access to all networks. Extended profile 2 is triggered when the Tunnel Guard checks have failed. It

has no access rules which means access is denied to all networks and services.

- A Tunnel Guard test user with user name and password

`tg`

is created and mapped to the

`tunnelguard`

group.

- The SRS rule

`srs-rule-test`

is mapped to the

`tunnelguard`

group.

- The

`tg_passed`

linkset is mapped to Extended profile 1. The

`tg_failed`

linkset is mapped to Extended profile 2.

Having run the wizard, you can test the behaviour of the Tunnel Guard feature right away. See the section [Test Tunnel Guard Using Wizard Settings](#) on page 272.

To create your own Tunnel Guard configuration, either edit the settings created by the wizard or create a completely new configuration based on the information given preceding sections. For instructions about how to create Tunnel Guard SRS rules, see [Configure SRS Rules](#) on page 275.

For more information about base profiles, extended profiles and client filters, see [Groups, Access Rules and Profiles](#) on page 157.

Test Tunnel Guard Using Wizard Settings

To test how Tunnel Guard behaves when configured with the wizard settings, proceed as follows:

1. In your browser, enter the IP address or domain name to the desired VPN.

The Portal login page is displayed.

2. Log in to the Portal using `tg` as user name and password.

The Tunnel Guard applet is downloaded to your machine. Because

`tg`

is a member of the

`tunnelguard`

group, and the SRS rule

`srs-rule-test`

is mapped to this group, the Tunnel Guard applet will now check if the file `tg.txt` is present in your `c:\tunnelguard` folder.



In this example, we have used the wizard to set

`restricted`

mode as fail action. This means that the tunnel is not torn down even if the Tunnel Guard checks fail. The result is displayed on the Portal page.

If

`teardown`

is set as fail action, the remote user will not get past the login page. A message is displayed telling the user that the Tunnel Guard checks have failed (also see [Restricted Mode vs. Teardown Mode](#) on page 275).

Tunnel Guard Checks Succeeded

The Tunnel Gurad checks succeeded message appears if the `tg.txt` file is present in the `c:\tunnelguard` folder.

To confirm that Tunnel Guard is running and that the checks have succeeded, the Tunnel Guard Success icon is displayed to the right of the Portal tabs (for an explanation of the other icons, see [The Portal from an End-User Perspective](#) on page 51).



The client filter called

`tg_passed`

triggered when the Tunnel Guard checks succeeded. This in its turn triggered Extended profile 1 in the

`tunnelguard`

group, because Extended profile 1 references the client filter

`tg_passed`

.

The linkset used in Extended profile 1 is a linkset called

`tg_passed`

. It has no links but prints the text "The Tunnel Guard checks succeeded!".

Extended profile 1 gives access to all networks and services.

Tunnel Guard Checks Failed

The Tunnel Guard checks failed message appears if the `tg.txt` file is not present in the `c:\tunnelguard` folder.

To confirm that Tunnel Guard is running but the checks have failed, the Tunnel Guard Failure icon is displayed to the right of the Portal tabs (for an explanation of the other icons, see [The Portal from an End-User Perspective](#) on page 51).



The client filter called

`tg_failed`

triggered when the Tunnel Guard checks failed. This in its turn triggered Extended profile 2 in the

`tunnelguard`

group, because Extended profile 2 references the client filter

`tg_failed`

.

The linkset used in Extended profile 2 is a linkset called

`tg_failed`

. It has no links but prints the text "The Tunnel Guard checks failed.". It also contains the `<var:tgFailureReason>` variable that prints the Tunnel Guard rule expression used (srs-test), along with a Tunnel Guard rule comment. In the preceding example, the comment is "This is a Test Rule". The linkset furthermore includes the `<var:tgFailureDetail>` variable that expands to the software definition comment specified for the current SRS rule, along with specific failure details generated by the Tunnel Guard applet.

Extended profile 2 denies access to all networks and services.

Restricted Mode vs. Teardown Mode

The previous example shows the result when EAC Agent operates in

`restricted`

mode. The user is logged in to the Portal but access is restricted.

If EAC Agent had been set to operate in

`teardown`

mode, the user cannot have been logged in to the Portal at all. Instead, the Login page displays the result of the Tunnel Guard check.

The Tunnel Guard rule expression and the Tunnel Guard rule comment are automatically displayed, that is, no variable has to be configured.

When the user clicks the **details** link, a message window appears.

This window provides more detailed information about the failed Tunnel Guard check, for example, a specification of missing files on the client machine. The text that reads "To be used for testing" in the preceding example is configurable.

If desired, the **details** link can be hidden by setting `/cfg/vpn #/aaa/tg/details` to

`off`

. This will also disable the `<var:tgFailureDetail>` variable.

Configure SRS Rules

To configure Tunnel Guard SRS rules, you must log in to the Browser-Based Management Interface (BBI). For instructions about how to Tunnel Guard Rules, see the "Configure Tunnel Guard" chapter in the *BBI Application Guide for VPN*.

Making API Calls

Tunnel Guard requires a Windows Platform DLL that implements at least one common entry point as described in the following section.

Windows

```
#include <windows.h>
/* return values */
#define STATUS_SUCCESS 0
#define STATUS_FAILURE -1
#define STATUS_REQUIRES_UPDATE 1
/* simple check */
int WINAPI CheckStatus(void);
```

This API can block until it returns one of the required statuses in 10 seconds or less. If an answer is not returned in a timely manner, it is assumed the personal firewall software is unavailable, and the call times out and returns an error message.

Configuration from Scratch

This section is an example of how to set up a working Tunnel Guard solution from scratch, that is, without using the wizard. It illustrates how to configure Tunnel Guard to check that the proper anti-virus program is installed on the remote user's machine and – if the Tunnel Guard checks fail – how to direct the remote users to a web site where they can update their virus program.

Enable Tunnel Guard

1. Enable Tunnel Guard.

```
>> Main#cfg/vpn 1/aaa/tg
>> TG#ena
```

2. Set the desired fail action.

By setting the action to

```
teardown
```

, the tunnel will be torn down if the Tunnel Guard checks fail. By setting the action to

```
restricted
```

, the remote user can be given limited access if the Tunnel Guard checks fail.

```
>> TG#action

Current value: teardown

Fail action (teardown/restricted):restricted
```

3. Set the desired time interval for SRS rule rechecks.

This step sets the time interval for SRS rule rechecks made by Tunnel Guard on the client machine. If a recheck fails (that is, the required file is no longer present or the required process is no longer running), the tunnel/session is terminated. Depending on access method, this means that the remote users is kicked out from the Portal or has their IPsec tunnel torn down.

```
>> TG#recheck

Current value: 15m
Enter recheck interval in seconds (60-86400):
```

The default recheck interval is 15m = 15 minutes.

4. Apply the changes.

IPsec Settings

The Tunnel Guard application is started (if enabled) when the remote user connects to the VPN with the IPsec VPN client (formerly the Contivity VPN client). Following are instructions on how to configure the AVG for use with the Tunnel Guard application.

1. Specify the interval between connection attempts.

This step lets you specify the interval between connection attempts from the Tunnel Guard server (on the VPN Gateway) to the Tunnel Guard client (on the client machine). This setting only applies to clients with the Tunnel Guard application installed – not Tunnel Guard applets downloaded from the Portal.

```
>> TG#ipsec/timeout

Current value: 2s
Enter Agent Query Timeout Interval in seconds (1-65535):
```

The default value is 2s = 2 seconds.

2. Specify the minimum version of the Tunnel Guard application (agent).

This step lets you enter the minimum version of the Tunnel Guard application. A VPN client with an older version of the Tunnel Guard application will not be able to connect to the VPN Gateway.

This setting only applies to clients with the Tunnel Guard application installed – not Tunnel Guard applets downloaded from the Portal. The default value is

0.0.0.0

, that is, all client versions are allowed.

```
>> IPSec settings#minver

Current value: 0.0.0.0
Enter Minimum Agent Version on the form N.N.N.N:
```

3. Apply the changes.

Configure Tunnel Guard SRS Rules

By configuring Tunnel Guard SRS rules you can specify what software components to look for on the remote user's machine. For instructions about how to configure Tunnel Guard SRS rules, see [Configure SRS Rules](#) on page 275.

Configure Linksets

Typically, linksets are configured to contain a set of links. In this example we will use the linksets used to communicate information to the remote user on the Portal.

1. Define a linkset to print the result of the Tunnel Guard checks when they succeed.

To create a heading for the linkset on the Portal, the linkset `text` command is used. In this example, the `text` command is simply used to print the result of the Tunnel Guard checks. No links will be configured for the linkset.

Specify a linkset number not currently in use, for example, 2.

```
>> TG#.../.../ linkset

Enter Linkset number or name (1-1024):2

Creating Linkset 2

Linkset name:tg_passed

Linkset text (HTML syntax, eg <b>A heading</b>):The Tunnel
Guard checks succeeded!
```

```
Autorun Linkset (true/false) [false]:<press ENTER>
```

2. Define a linkset to print the result of the Tunnel Guard checks when they fail.

This linkset should also contain a link to the web site where a new anti-virus program can be downloaded.

```
>> Linkset 2#../ linkset 3

Creating Linkset 3

Linkset name:tg_failed

Linkset text (HTML syntax, eg <b>A heading</b>):The Tunnel
Guard checks failed. Click the link below to download
new antivirus software.

Autorun Linkset (true/false) [false]:<press ENTER>
```

3. For the current linkset, define a link to direct the user to the anti-virus program download site.

```
>>
Linkset
3# link

Enter Link number or name (1-256): 1

Creating Link 1

Enter link text: Anti-virus program download site

Enter type of link (hit TAB to see possible values) [internal]:

smb ftp proxy custom mail
netdrive wts outlook netdirect telnet
internal iauto terminal external

Enter type of link (hit TAB to see possible values) [internal]:
```

```

internal
Entering

:Internal
settings
menu

Enter
host (eg
inside.co
mpany.com
)

:

antivir
us.exam
ple.com

Enter
path
(eg /)

:

/update

```

Configure a Network

1. Create a network definition identifying a web server on the intranet.

This is the web site where the remote user will be able to download the proper anti-virus program. Specify a network number not currently in use, for example, 2 to create Network 2.

```

>> Link 1#../../aaa/network 2

Creating Network 2

Network name:webserver

```

2. Define a subnet identifying the intranet web server.

When creating a subnet, enter either the host name or the network address/netmask. Note that the network mask can be entered in number of bits, for example, 32 instead of 255.255.255.255.

*** Note:**

When creating network definitions to be used in IPsec or Net Direct connections, specify the network using a network address and mask. Host names will be ignored.

```
>> Network 2#subnet
Enter subnet number: (1-1023)1
Creating Network Subnet 1
Enter host name:<press ENTER to skip>
Enter network address:192.168.201.10
Enter network netmask:32
```

Configure a Group

In this example we will choose the

novice

user type for the group. This will limit display to the **Home** and **Tools** tabs when the Tunnel Guard checks fail. In addition, no access rules will be created for the group's base profile, that is, the parameters specified directly on group level. This will deny access to all networks, services and paths. Instead, we will use extended profiles to specify the group's access rights, depending on whether the Tunnel Guard checks fail or succeed.

The reason for not specifying access rules on group level is that the access rules pertaining to the group's base profile are appended to those of the extended profile.

You can read more about groups, access rules and profiles in [Groups, Access Rules and Profiles](#) on page 157.

1. Create a user access group.

```
>> Network Subnet 1#../../group 2
Creating Group 2
Group name:staff
Enter number of sessions (0 is unlimited):<press ENTER>
Enter user type (advanced/medium/novice):novice
```

2. Map the Tunnel Guard SRS rule to the group.

```
>> Group 2#tgsrs

Current value: " "

Enter Tunnel Guard SRS rule name:<SRS rule name>
```

3. Add the desired users to the local database and map them to the group.

For instructions about how to configure different authentication methods (including local database authentication), see [Authentication Methods](#) on page 117.

```
>> Group 2#../auth 1/local/add

Enter user name:lisa

Enter passwd:<password>

Enter group names (comma separated):staff
```

Create Client Filters

Two client filters should be created. The first client filter should be triggered when the Tunnel Guard checks succeed. The other client filter should be triggered when the Tunnel Guard checks fail.

1. Create the first client filter.

This client filter should be triggered when the Tunnel Guard checks succeed.

```
>> Local database#../filter

Enter client filter number or name: (1-63)1

Creating Client Filter 1

Filter name:tg_passed
```

2. Configure the client filter to be triggered when the Tunnel Guard checks succeed.

```
>> Client Filter 1#tg

Current value: ignore

Tunnel Guard passed (true/false/ignore):true
```

3. Create a new client filter.

This client filter should be triggered when the Tunnel Guard checks succeed.

```
>> Client Filter 1#../filter

Enter client filter number or name: (1-63)2

Creating Client Filter 2

Filter name:tg_failed
```

4. Configure the client filter to be triggered when the Tunnel Guard checks fail.

```
>> Client Filter 2#tg

Current value: ignore

Tunnel Guard passed (true/false/ignore):false
```

Configure Extended Profiles

1. Create an extended profile to be triggered when the Tunnel Guard checks succeed.

As the client filter name, reference the

tg_passed

client filter.

```
>> Client Filter 2#../group 2/extend

Enter profile number or filter reference name (1-63):1

Creating Extended Profile 1

Enter client filter name:tg_passed

Enter user type (advanced/medium/novice):advanced
```

2. Create the desired access rules for the extended profile.

To allow access to all networks, services and paths (application specific name), press ENTER when prompted.

```
>> Extended Profile 1#access

Enter access rule number: (1-1023)1

Creating Access rule 1
```

```
Enter network name:<press ENTER>
Enter service name:<press ENTER>
Enter application specific name:<press ENTER>
Enter action (accept/reject):accept
```

3. Reference the linkset used to confirm that the Tunnel Guard checks succeeded.

```
>> Access Rule 1#../linkset/add
Linkset name:tg_passed
```

4. Create an extended profile to be triggered when the Tunnel Guard checks fail.

As the client filter name, reference the client filter we created in step [3](#) on page 282.

```
>> Linksets#../../extend
Enter profile number or filter reference name (1-63):2
Creating Extended Profile 2
Enter client filter name:tg_failed
Enter user type (advanced/medium/novice):novice
```

5. Create the desired access rules for the extended profile.

To limit access to the web site where to download the anti-virus program, reference the network definition we created in the section [Configure a Network](#) on page 280.

```
>> Extended
Profile
2#access

Enter access rule 1
number

(1-1023)

:

Creating
Access rule 1
```

Enter network name:	webserver			
Enter service name:	<press TAB to view available services>			
	pop3	fileshare	ssh	web
	smtp	https	email	http
	telnet	ftp	imap	smb
Enter service name:	web			
:				
Enter application specific name:	<press ENTER to allow all paths>			
Enter action (accept/reject):	accept			

6. Reference the linkset used to confirm that the Tunnel Guard checks failed.

This linkset also contains a link that directs the remote user to the anti-virus program download site.

```
>> Access rule 1#../linkset/add
Linkset name:tg_failed
```

For more instructions on how to create groups, access rules and profiles, see [Groups, Access Rules and Profiles](#) on page 157.

7. Apply the changes.

```
>> Linksets#apply
Changes applied successfully.
```

Test the Example Configuration

To test how Tunnel Guard behaves when configured as described in the previous example, proceed as follows:

1. In your browser, enter the IP address or domain name to the desired VPN.

The Portal login page is displayed.

2. Log in to the Portal using `lisa` as user name and password.

The Tunnel Guard applet is downloaded to your machine. Because

`lisa`

is a member of the

`staff`

group, and the SRS rule is mapped to this group, the Tunnel Guard applet will now check if the requested anti-virus program is present on Lisa's PC.



In this example, we have used the wizard to set

`restricted`

mode as fail action. This means that the tunnel is not torn down even if the Tunnel Guard checks fail. The result is displayed on the Portal page.

Tunnel Guard Checks Succeeded

If the requested anti-virus software is present on the client PC, you receive a Tunnel Guard checks succeeded message.

The client filter called

`tg_passed`

triggered when the Tunnel Guard checks succeeded. This in its turn triggered Extended profile 1 in the

`staff`

group, because Extended profile 1 references the client filter

tg_passed

.

The linkset used in Extended profile 1 is a linkset called

tg_passed

. It has no links but prints the text "The Tunnel Guard checks succeeded!".

Extended profile 1 gives access to all networks and services. It is configured with the user type

advanced

, which gives access to all tabs.

Tunnel Guard Checks Failed

If the Tunnel Guard checks failed, that is, the requested anti-virus software is not present on the client machine, you receive a Tunnel Guard check failed message and a link to download new antivirus software.

The client filter called

tg_failed

triggered when the Tunnel Guard checks failed. This in its turn triggered Extended profile 2 in the

staff

group, because Extended profile 2 references the client filter

tg_failed

.

The linkset used in Extended profile 2 is a linkset called

tg_failed

. It prints the text "The Tunnel Guard checks failed. Click the following link to download new anti-virus software". The linkset includes one link, directing the user to an anti-virus program download site.

Extended profile 2 only allows access to the download site. It is configured with the user type

novice

, which gives access to the **Home** and **Tools** tabs only.

Chapter 14: Network Access Protection

This chapter provides procedures to configure Network Access Protection (NAP) for the Avaya VPN Gateway device.

Network Access Protection is a Microsoft® technology which enforces system health requirements for clients trying to access private network. NAP provides a platform for validating the health state of the client that attempts to access the private network, and for limiting the client access to the network based on the health policy.

The NAP controls access to the network resources based on a client computer identity and compliance with corporate governance policy. The network administrator can define the network access based on who a client is, the groups to which the client belongs, and the degree to which the client is compliant with corporate governance policy.

The NAP provides policy enforcement components to ensure the computers connecting or communicating on a network meet the system health requirements. If a client cannot prove it is compliant with system health requirements (for example, the latest operating system and antivirus updates are not installed), its access to the network or communication on the network is limited to a restricted network containing server resources for remedying the compliance issues. After the updates are installed, the client requests access to the network again. If compliant, the client is granted unlimited access to the network.

The following sections are covered in this chapter:

- [NSG NAP architecture](#) on page 289
- [System Health Agent](#) on page 290
- [Configuring NAP](#) on page 290

NSG NAP architecture

The NSG NAP architecture allows you to deploy the NAP clients with or without the availability of Microsoft Network Policy Server (NPS) on the back-end network. If the Microsoft NPS is present, NAP checks with Microsoft NPS to make an access decision. If the Microsoft NPS is unavailable, you can still deploy clients with NAP support enabled, and later add a Microsoft NPS if desired. Microsoft Windows Server 2008 can act as a remote NPS.

The following are the prerequisites for NAP to work:

- Ensure that the TG is enabled in the server.
- Ensure that access rules are configured for the NAP and TG checks.
- Ensure that the AHA 5.2.2.0 or above is installed on client PC.

The NAP feature is tightly coupled with Tunnel Guard (TG) feature. AHA installs the System Health Agent (SHA) and Enforcement Client (EC) on the client PC to provide the NAP

functionality. NAP uses Tunnel Guard protocol for communicating between the SHA and the Policy server, and carrying Statements of Health (SoH) from different SHAs. Tunnel Guard rechecks configured in the recheck interval also facilitates NAP rechecks.

You can use the NAP feature with the following tunnel based clients:

- Avaya VPN client (AVC)
- Contivity (IPsec Client)
- Net Direct Installable Client (NDIC)
- L2TP Client

*** Note:**

The Portal mode does not support NAP.

System Health Agent

System Health Agents are client components that collect the system health reports of the client, and then send to the System Health Validator (SHV). The SHVs are Policy server (NSG or Remote NPS) components that validate the health statements received from SHA. SHV sends Statement of Health Response (SoHR) in response to the Statement of Health (SoH) received from the clients.

Configuring NAP

Perform the following procedure to configure NAP.

1. Set Policy Decision Point (PDP) to remote.

<code>>> Main#cfg/vpn 1/aaa/nap</code>	(Displays NAP menu)
<code>>> NAP#pdp</code>	(Select PDP)
<code>Current value: local</code>	(Displays current PDP value)
<code>Policy Decision Point (local/remote): remote</code>	(Specify the value as remote)

2. Add Remote Network Policy Server (NPS).

You can define the policies either in the AVG (local) or in a remote NPS. You can configure the Policy Decision Point in the NSG server. The Remote NPS uses the

RADIUS protocol, and you can specify the list of IP/Port and shared secret. The NPS should be in the private side.

>> NAP#servers	(Select Remote NPS)
>> Remote Network Policy Servers# add	(Add Remote NPS)
Server IP Address:	(Specify the server IP address)
Server Port [1812]:	(Displays the default server port. To change, specify the port number)
Shared secret:	(Specify the shared secret)
>> Remote Network Policy Servers# list	(View the added Remote NPS details)

3. Enable automatic remediation.

Automatically corrects the health compliance issues and provides necessary updates to allow a noncompliant computer to become compliant.

>> NAP# autoremed	(Select auto remediation from NAP menu)
Current value: false	(Displays current value)
Enable Auto Remediation[true/false]:true	(Enable auto remediation)

4. Enable probation settings.

Probation time is a grace time to allow clients to attain compliance before being restricted. The clients have full access to network until the probation time expires. The administrator can configure the probation mode, and specify the absolute date and time in the probation setting.

>> NAP# probation	(Select probation from NAP menu)
>> Probation Settings# ena	(Enable full access to the network during trial period)
>> Probation Settings# date	(Select date)
Current date: " "	(Displays current date)

Enter date (YYYY-MM-DD):	(Specify date for the trial period)
>> Probation Settings# time	(Select time)
Current time: " "	(Displays current time)
Enter time (24-hour, HH:MM:SS):	(Specify time for the trial period)

5. Configure Windows System Health Validator (WSHV).

By default, firewall, and automatic updates are enabled.

*** Note:**

Perform this procedure step only when PDP is local and SHV list contains WSHV.

>> NAP# wshv	(Select WSHV from NAP menu)
>> Windows System Health Validators# virus	(Displays Virus Menu)—Optional
>> Virus Protection# enabled	(Enable virus protection)
>> Virus Protection# uptodate	(Enable automatic updates)
>> Windows System Health Validators# spyware	(Display Spyware Menu)—Optional
>> Spyware Protection# enabled	(Enable Spyware)
>> Spyware Protection# uptodate	(Enable automatic updates)
>> Windows System Health Validators#secupdates	(Displays Security Updates Protection Menu)—Optional
>> Security Updates Protection#enabled true	(Enable Security Updates Protection)

6. Apply the changes.

You can configure extended profiles for users with NAP. For more information, see [Extended profiles for users with NAP](#) on page 201.

Chapter 15: WholeSecurity

Symantec WholeSecurity Confidence Online offers on-demand protection for all users logging into the network through remote access technologies (like SSL VPNs).

How Does it Work?

When the remote users connects to the VPN, they are automatically redirected to a WholeSecurity Confidence Online server on the intranet. The Confidence Online software is downloaded to the endpoint machine and performs a scan to identify any eavesdropping threats, including Trojan horses, remote controls, keystroke loggers and worms – before the user has actually logged on to the VPN.

If no threat is found, the VPN's login screen is displayed. If malicious code is detected, the offending process can be terminated, quarantined and reported.

Configuration

The configuration on the Avaya VPN Gateway (AVG) is limited to enabling WholeSecurity, specifying the URL to a WholeSecurity Confidence Online server and configuring a user access group that allows redirection to an intranet web site prior to logging in to the VPN.

The rest of the configuration is done using the WholeSecurity Confidence Online management interface. It includes specifying a deployment, which defines the type of scan to be performed and what action should be taken when the scan fails. For instructions, see the Confidence Online manual.

Requirements

The following requirements apply for a successful deployment:

- Fully qualified domain names (FQDNs) must be used to access the AVG and the WholeSecurity server. IP addresses do not work.
- The AVG should use a certificate that matches its FQDN. A certificate created by the wizard will not work.
- The client browser should trust the certification authority (CA) of the AVG certificate. If a private CA is used, that CA certificate should be added to the browser. The CA certificate

must be added to Internet Explorer (MSCAPI store) even when using Firefox/Mozilla. If a self-signed certificate is used, that certificate should be added to the browser as a "Trusted Root Certification Authority".

- The AVG and WholeSecurity servers should be in the same domain. For example, if the AVG is *vpn.example.com*, the WholeSecurity server should also reside in the *example.com* domain, e.g as *ws.example.com*.

Configure a Deployment in WholeSecurity

Before you start configuring the AVG, install the WholeSecurity Confidence Online software on a server on the intranet and configure a deployment. See the Confidence Online manual for instructions.

* Note:

The WholeSecurity server creates a virtual directory named `/integration` and by default, access is denied to all IP addresses. Because the AVG needs to access scripts in this directory to check the scan results, you must add the AVG 's interface IP address (not the Portal IP address) to the allowed list. This can be done using the IIS management console or equivalent.

Enable WholeSecurity on the AVG

This section and the next describe each step of the configuration required on the AVG. A quicker way of making the same settings is to run the WholeSecurity wizard (using the `/cfg/vpn #/aaa/wholesec/quick` command). Refer to the following sections for examples of information to be supplied in the wizard.

1. Specify the URL to the WholeSecurity Confidence Online server.

This step lets you enter a URL to the WholeSecurity Confidence Online server, according to the following format:

```
https://<confidence_online_server>/llclient /<deployment>/online.html.
```

For example, if the Confidence Online server is running at

```
ws.example.com
```

and the deployment is called

```
SSLVPN
```

, the resulting URL can be:

```
https://ws.example.com/llclient/SSLVPN/online.html
```

```
>> Main#cfg/vpn 1/aaa/wholesec

>> WholeSecurity#url

Current value: " "

WholeSecurity deployment URL:https://ws.example.com/
llclient/SSLVPN/online.html
```

2. Enable WholeSecurity.

```
>> WholeSecurity#ena
```

3. Specify a logout URL.

This is the page to which the user is directed when logging out from the VPN session. When WholeSecurity is enabled, the Login page will not be displayed on logout.

```
>> WholeSecurity#logouturl

Current value: " "

Redirect URL on logout:
```

4. Apply the changes.

Configure an Anonymous Group

For the remote user to be subject to a Confidence Online scan before actually logging in to the VPN, redirection to the Confidence Online server must take place as soon as the remote user points to the URL of the VPN. Normally, the remote user cannot be redirected to a site on the intranet without first logging in to the VPN. However, by creating an anonymous group, this will be allowed.

1. Start by creating a network definition corresponding to the WholeSecurity Confidence Online server.

```
>> Main#cfg/vpn 1/aaa/network

Enter network number or name: (1-1023)3

Creating Network 3
Network name:wholesecurity
```

2. Specify the properties of the subnet included in the network definition.

```
>> Network 1#subnet

Enter subnet number: (1-1023)1

Creating Network Subnet 1
Enter host name:ws.example.com

Enter network address:<press ENTER to skip>

Enter network netmask:<press ENTER to skip>
```

3. Configure the allowed paths on the WholeSecurity Confidence Online server.

By specifying an application specific (appspec) definition identifying specific paths, you can limit the user's access rights on the WholeSecurity Confidence Online server.

The first time you create an appspec definition you will enter a wizard. Start by specifying the name of the appspec definition, for example,

```
wholesecurity
```

. Continue with specifying the first path, that is, `/cgi-bin/rr.fcgi`. This is not an example; the path should be entered exactly like this.

```
>> Network Subnet 1#../../appspec

Enter appspec number or name: (1-1023) 1
Creating AppSpecific 1
AppSpec name:wholesecurity

Enter path:/cgi-bin/rr.fcgi
```

If you want to know more about groups, access rules, appspec definitions and so on, see [Groups, Access Rules and Profiles](#) on page 157.

4. Enter the next path.

This path identifies the deployment. In the following example, the deployment is called

```
SSLVPN
```

```
.
```

```
>> AppSpecific 1#paths/add

Enter path:/llclient/SSLVPN
```

5. Configure an anonymous group and set the user type to **novice** .

Because the anonymous group will only be used for accessing the Confidence Online server, the

novice

user type will be sufficient.

```
>> Network Subnet 1#../../group 3

Creating Group 3
Group name:wholesecurity

Enter number of sessions (0 is unlimited):<press ENTER to skip>

Enter user type (advanced/medium/novice):novice
```

6. Configure the access rules of the anonymous group.

By referencing the network definition we created in step 1, access will be granted to the Confidence Online server and nothing else.

By referencing the

https

service definition, access will be limited to the HTTPS protocol. Typically, the

https

service definition is available by default. If not, you can create this service definition (see [Groups, Access Rules and Profiles](#) on page 157).

By referencing the application specific definition we created in step 3, access will be granted to the specified paths on the Confidence Online server and nothing else.

```
>> Group 3#access

Enter access rule number: (1-1023)1

Creating Access rule 1
Enter network name:wholesecurity

Enter service name:https

Enter application specific name:wholesecurity

Enter action (accept/reject):accept
```

7. Make the group an anonymous group.

The final step is to make the group we just created an anonymous group.

```
>> Access rule 1#../../anongroup  
Current value: " "  
Enter group name:wholesecurity
```

As long as WholeSecurity is enabled and a Confidence Online server URL is specified, all requests for the VPN Portal will be redirected to the Confidence Online server. To limit access to just that server, all remote users are automatically placed in the anonymous group when pointing to the VPN Portal. The access rules of the anonymous group grants access to the Confidence Online server and nothing else.

When the Confidence Online scan has been successfully performed, the remote user is allowed to log in to the VPN using the ordinary login screen. The user is then assigned their regular groups, granting access to additional sites and services.

Chapter 16: Virtual Desktop

Symantec On-Demand Agent (SODA) provides a Virtual Desktop environment to secure Web-based applications and services. Files created while in the virtual desktop are encrypted as they are saved to a hard drive or removable media. Integrating Virtual Desktop with AVG will provide a secure environment for end users while accessing confidential information. Virtual Desktop is a Java application with a set of C dll's to do all sort of hooking to secure the virtual desktop environment.

The virtual desktop licenses are available in volumes of 50, 100, 250, 500, 1000, 2000, and 5000.

Starting vdesktop

Integrated Virtual Desktop will be started under the following scenarios:

- Pre-logon: Users can launch Virtual Desktop before logging on. An additional link will be displayed on the Login page to start Virtual Desktop.
- Always: User session is moved to virtual desktop, upon successful login. Current user session cookies are migrated to the virtual desktop session so that the user does not have to authenticate again. Portal session outside the virtual desktop will be closed.
- “Virtual Desktop” Tunnel Guard rule: Users will be forced to use the Virtual Desktop, if the tunnel guard check for host integrity fails (firewall, virus scanner and so on). The session outside the Virtual Desktop will be closed.
- Force: Users will be forced to always login from within the Virtual Desktop. On navigating to the portal login page, virtual desktop will be launched. Portal login page will be loaded inside Virtual Desktop. This is a per VPN setting.

Access vdesktop using CLI

Follow these steps to access vdesktop using CLI:

1. Access the vpn menu.

```
Main #cfg/vpn
```

2. Enter the vpn number for which you want to activate vdesktop.

```
Enter vpn number <1-1024> - 1
```

3. Enter the vpn name for which you want to activate vdesktop.

Enter vpn name

4. To access the vdesktop menu, enter the following command.

```
>> VPN 1 # vdesktop
```

[Virtual Desktop Menu]	
ena	- Enable Virtual Desktop
dis	- Disable Virtual Desktop
prelogon	- Set display virtual desktop link
always	- Set enforce user to always use virtual desktop after login.
force	- Set force virtual desktop before login
switch	- Set allow user to switch between normal and virtual desktop
secure	- Set secure mode
persist	- Set persistent mode
filesep	- Set file separation
remdisk	- Set removable disk support
print	- Set printing support
netshare	- Set network share
cryptlevel	- Set encryption level
timeout	- Set inactivity timeout
connctrl	Set Connection control
mcd	Malware detection menu

5. To enable the vdesktop feature, enter the following command.

```
>> Virtual Desktop# ena
Current value: off
Enable users to use virtual desktop (on/group/off):
```

6. To display virtual desktop link in login page, enter the following command.

```
>> Virtual Desktop# prelogin
Current value: off
enable virtual desktop before login <on/off>: on
```

7. To enforce the user to always use virtual desktop after login, enter the following command.

```
>> Virtual Desktop# always Current value: off enforce user to always use
virtual desktop after login<on/off>:on
```

8. To enforce the user to use the virtual desktop before login, enter the following command:

```
>> Virtual Desktop# force Current value: off enforce user to always use
virtual desktop before login <on/off>: on
```

9. To allow the user to switch between normal and virtual desktop, enter the following command.

```
>> Virtual Desktop# switch Current value: off allow user to switch between
normal and virtual desktop <on/off>: on
```

10. To allow the user to use only default browser, enter the following command.

```
>> Virtual Desktop# secure Current value: off force the user to use the
default browser alone in the virtual desktop.
```

11. To allow the user to enable persistent mode, enter the following command.

```
>> Virtual Desktop# persist Current value: off enable persistent mode in
virtual desktop.
```

12. To prevent the user from using files that are not on vdesktop, enter the following command.

```
>> Virtual Desktop# filesep Current value: off prevents user from using or
seeing the files that are on the normal desktop.
```

13. To allow the user to copy files, enter the following command.

```
>> Virtual Desktop# remdisk Current value: off permits users to copy the
files from virtual desktop to a removable disk.
```

14. To allow the user to print files, enter the following command

```
>> Virtual Desktop# print Current value: off permits users to print files
from virtual desktop.
```

15. To allow the user to map files, enter the following command

```
>> Virtual Desktop# netshare Current value: off permits users to save
files and map drives through windows smb.
```

16. To allow the user to set the encryption level, enter the following command

```
>> Virtual Desktop# cryptlevel Current value: 128 set encryption level for
virtual desktop:
```

Possible values are 40, 128,512, and 1024.

17. To allow the user to set the time out value, enter the following command

```
>> Virtual Desktop# cryptlevel Current value: 5 inactivity timeout for
virtual desktop in minutes:
```

18. To allow the connection control, enter the following command

```
>> Virtual Desktop# conncntrl
```

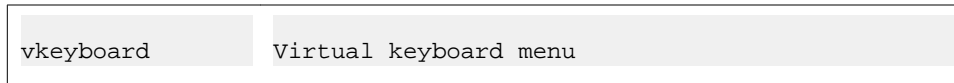
Connection control acts as a firewall allowing only portal traffic from virtual desktop.

19. To access the malware detection menu, enter the following command

```
>> Virtual Desktop# mcd
```

Malicious Code Detection (mcd) detects and protects against a variety of malicious software like key loggers, screen scrappers, and password grabblers using the havioral or signature-based signature based engines. You can use the following sub-menu to enable or disable the key logger and screen scrapper detection or account creation is the malware detection menu:

[MCD Menu]	
ena	- Enable virtual desktop
dis	- Disable virtual desktop
keylogger	- Set detect Key loggers
scrsscrap	- Set detect screen scrappers
acntcreate	- Set disable creation of local machine account



20. Apply the changes.

```
>>Virtual Desktop apply
```


Chapter 17: Secure Portable Office (SPO) Client

The SPO client provides VPN access from portable storage such as USB flash memory and CD ROM.

The SPO client provides enhanced mobility, portability, and security compared to traditional VPN access methods. You can deploy and manage the SPO client from the AVG server to simplify SPO client maintenance and updates.

Secure Portable Office Client Release 9.0, in virtual mode, supports the following software in Windows 32-bit and 64-bit platforms.

- Software released with Avaya Contact Center:
 - Microsoft Data Access 2.8
 - Jet Database Endine 4.0
 - Microsoft.Net Framework 3.5
 - Avaya Contact Center Express Desktop 5.0
 - Avaya One-X Agent 2.0
- Oracle Java Runtime Environment 1.7
- Avaya 2050 IP Softphone 4.2
- Avaya customized Ceedo 4.x
- Net Direct x64 bit support for Release 9.0
- Microsoft IE9
- Mozilla Firefox 7.x

For more information on Installation and configuration of SPO client parameters see, *Configuration-Secure Portable Office Client Guide* (NN46120-301).

Configuring SPO General Settings

The General Settings form allows you to change the settings for the SPO. The following procedure describes the steps to configure general settings.

1. Specify the VPN for which you want to configure the SPO client.

```
/cfg/vpn 1/spoclient
```

```

[SPO Client Menu]
  logoimport - Import logo banner image
  logfile    - Show installed logo file
  sysicon    - Import system tray icon image
  sysiconfil - Show installed sysicon file
  restorelog - Restores default Nortel logo
  restoresys - Restores default Nortel system tray icon
  bannertext - Set static banner text/licence/warning for users
  backupserv - Configure SPO Client backup servers
  software   - SPO Client Software Image Menu
  apps       - SPO Client Application Menu
  version    - Set SPO Client software version
  name       - Set SPO Client software name

```

2. Specify the SPO client software name.

You can enter up to 30 alphanumeric characters.

```

>> SPO Client# name
Current value: Nortel SPO CLIENT
Enter SPO Client name: SPO software

```

3. Specify the SPO client version name.

```

>> SPO Client# version
Current value: 7.1.1.0
Enter the software version [ 7.1.1.0 ]:

```

4. Enter the Banner/License Agreement or Warning text for SPO users.

```

>> SPO Client# bannertext
Write or paste the text, press Enter to create a new line, and then type "..."
<without the quotation marks> to terminate.
>

```

5. Specify the SPO logo file of the client.

```

>> SPO Client# logfile
Installed logo = logo.gif

```

6. Specify the system icon file for SPO client.

```

>> SPO Client# sysiconfile
Installed Sysicon = sysicon.ico

```

7. Apply the changes.

Importing logo

This section describes how to import the logo image for SPO client:

1. Enter the VPN number.

Enter vpn number <1-256>:1

2. Enter the SPO client menu.

VPN 1#spoclient

```
>> VPN 1# spoclient
-----
SPO Client Menu]
  logoimport - Import logo banner image
  logfile    - Show installed logo file
  sysicon    - Import system tray icon image
  sysiconfil - Show installed sysicon file
  restorelog - Restores default Nortel logo
  restoresys - Restores default Nortel system tray icon
  bannertext - Set static banner text/licence/warning for users
  backupserv - Configure SPO Client backup servers
  software   - SPO Client Software Image Menu
  apps       - SPO Client Application Menu
  version    - Set SPO Client software version
  name       - Set SPO Client software name
```

3. Enter the following command to import the logo.

```
spoclient# logoimport
```

4. Enter the protocol using which you want to transfer the logo.

```
Select protocol <tftp/ftp/scp/sftp>:tftp
```

5. Enter the IP address or hostname of the server.

```
Enter the IP address or hostname of the server:10.127.232.41
```

6. Enter the filename on the server.

The file should be in .gif or .jpeg format. The file size should be less than 5 KB.

```
Enter the filename on the server:spoclient.gif
```

Importing system tray icon

This section describes how to import system tray icon to a USB flash drive.

1. Enter the VPN number.

```
Enter vpn number <1-256>:1
```

2. Enter the SPO client menu.

```
VPN 1#spoclient
```

3. Enter the following command to import the system tray icon.

```
spoclient# sysicon
```

4. Enter the protocol using which you want to transfer the system tray icon.

```
Select protocol <tftp/ftp/scp/sftp>:tftp
```

5. Enter the IP address or hostname of the server.

```
Enter the IP address or hostname of the server:10.127.232.41
```

6. Enter the filename on the server.

The file size should be less than 5 KB in size and only in .ico format.

Enter the filename on the server:spoclient.ico

Adding a Backup Server

When the SPO client connects successfully to the server, it retrieves a list of all the backup servers. For subsequent connections of the SPO client, if there is any failure in the primary server the SPO client can use the backup server to connect. The following procedure explains the steps to add a backup server.

1. To specify the backup server for an SPO client, enter the following command.

```
/cfg/vpn 1/spoclient/backupserv
```

```
>> SPO Client# backupserv
-----
[Backup Server Menu]
  list      - List all values
  del       - Delete a value by number
  add       - Add a new value
```

2. Enter the following command to add the backup server.

```
/cfg/vpn 1/spoclient/backupserv/add
```

3. Specify a name, network IP or DNS name, port number, and description for the backup server.

```
>> Backup Server# add
Enter the name:secondary_server
Enter network IP address or DNS name: 10.127.232.51
Enter the Port number:5050
Enter the Description:The is the secondary server in the backup server list.
```

4. Apply the changes.

Importing a SPO client Software Image

This procedure explains the steps to import a SPO client software image:

1. To access the software image menu, enter the following command:

```
/cfg/vpn 1/spoclient/software
```

```
>> SPO Client# software

-----
[SPO Client Software Image Menu]
iso      - Add CDROM ISO image
u3p      - Add USB U3P image
msi      - Add generic Microsoft installer file
list     - List SPO Client software image directory
del      - Delete software image
```

2. Select the SPO client software image (iso, u3p, or msi) that you want to upload to the SPO client.

Only .iso, .u3p and .msi file types can be uploaded.

3. Import the files using one of the system protocols: ftp, tftp, scp, or sftp.

Select the protocol <tftp/ftp/scp/sftp>: ftp

4. Specify the IP address or host name of the server from where the file needs to be imported.

Enter hostname or IP address of the of server: ftp.client.net

5. Enter the image file name

Enter the image path:SPOClient.iso

Administering third-party applications

This section describes how to administer SPO client software updates and third-party applications.

1. Enter the VPN number.

Enter vpn number <1-256>:1

2. Enter the SPO client menu.

VPN 1# spoclient

3. Enter the following command to application menu for the third party software

spoclient# apps

4. Enter the index number or name.

```
Enter index number or name (1-50) : 1

Creating spo client Application 1

Application name : FtpClient

Application version : 1.0
```

```
SPO client Application [1] menu
```

```
name - Set application name
```

```
version - Set application version
```

```
software - Add SPO application
```

```
del - Delete application
```

5. Enter the software application name.

```
Application name:FtpClient
```

6. Enter software application version.

```
Application version: 1.0
```

7. Enter the software menu.

```
SPO client Application 1# software
```

8. Enter the appropriate protocol to transfer the software image.

```
Select protocol <tftp/ftp/scp/sftp>:tftp
```

9. Enter the IP address or hostname of the server.

```
Enter the IP address or hostname of the server:10.127.232.41
```

10. Enter the filename on the server.

```
Enter the filename on the server:FtpClient.zip
```

Only .u3p, .msi, .zip file formats are supported.

You can also view the list of uploaded files by entering the command `/cfg/vpn 1/ spoclient/software/list`

```
>> SPO Client Software Image# list
./:
total 29M k
 15M k   SPOClient.iso
  7.1M k SPOClient.msi
  7.1M k SPOClient.u3p
  4.0k k apps/
./apps:
total 18M k
 2.1M k   Miranda_Portable_0.7.3.paf.zip
 852k k   PuTTY_Portable.zip
  7.1M k   SPOClient.msi
  7.1M k   SPOClient.u3p
```

You can add a new client filter for SPO. For information on this see [Client filters](#) on page 185.

You need to configure the SPO client access under groups to specify the users belonging to that group that can access the SPO feature. For information on SPO access see [SPO Access](#) on page 163.

You need to configure the SPO client under Groups to specify the applications that are accessible by that group and to specify the index of the SPO for that group. You can also add, edit, and delete a software index for a SPO client. For information on these configuration steps see [Specifying the Secure Portable Office Software Index](#) on page 178.

Chapter 18: Secure Service Partitioning

The Avaya VPN Gateway (AVG) provides the ability to partition a cluster of VPN Gateways into separate VPNs. The idea is to give service providers (ISPs) the possibility to host multiple VPN customers on a shared Remote Access Services (RAS) platform.

The high-level capabilities include:

- Multiple domains. The ability to host up to 250 public termination points for end-customer SSL and IPsec VPNs.
- Secure VPN binding. Each VPN is bound to a private IP interface. VLAN tagging can be used when private IP address spaces overlap.
- Private network authentication. Existing authentication servers within the customer's private network can be used.
- Access control. Unique access rules can be specified for each user group in the various VPNs.
- Private network name resolution. If desired, private network DNS servers can be mapped to the VPN.
- Split administration. VPN management is enabled for each VPN customer through a web interface, without exposing global administration access.
- High availability. The Secure Service Partitioning (SSP) solution is compatible with the AVG cluster's high availability solutions.

This chapter describes the steps required to set up a basic SSP solution, in this case two AVG Portals, each of which is bound to a private network.

For an overview of all other steps required for a fully functional SSP solution, see " [Clientless Mode](#) on page 35 in the *Application Guide for VPN*.

802.1Q VLAN Tags

Access to private customer networks can be enabled through 802.1Q VLAN tags. The AVG platform will connect to a device that can direct traffic to the appropriate private side network based on 802.1Q tags. These private networks may actually be a member of a site-to-site VPN using MPLS, IPsec, L2 Optical Ethernet or any other VPN technology as long as the device connected to the AVG platform can direct traffic to/from these VPNs based on 802.1Q VLAN tags.

Where functionality is concerned, there is no difference between using VLAN tagged interfaces or physical interfaces. For small setups, it is fully possible to use the physical interfaces (that is, ports) to split two VPNs. It is likewise possible to VLAN tag only some of the interfaces.

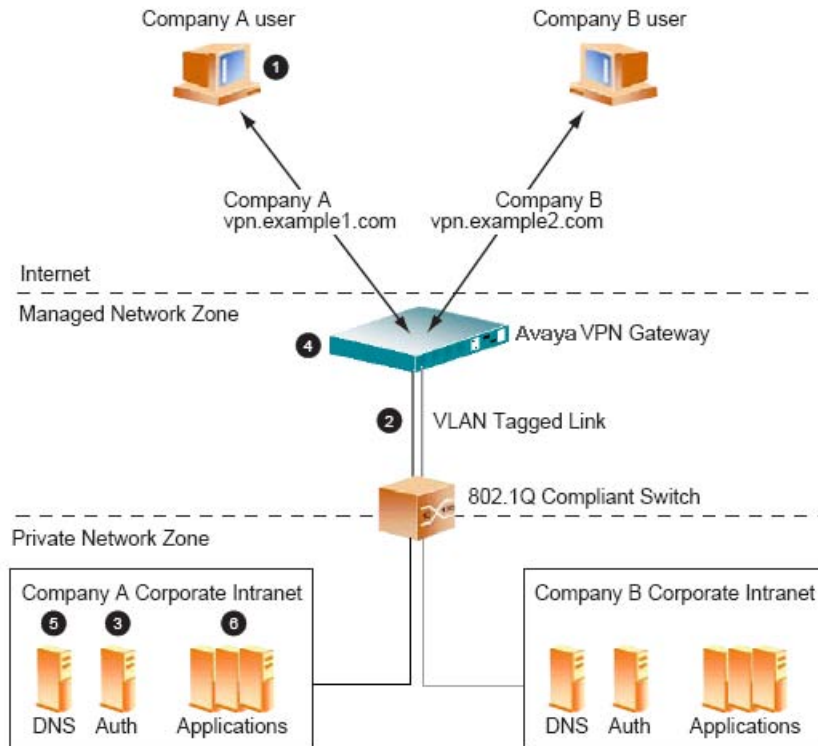
License Keys

To enable the Secure Service Partitioning feature in the AVG software, a license key must be obtained from Avaya. This also the case if you wish to enable SSL or IPsec access for more than 50 concurrent users. To obtain the license keys, you have to provide the MAC address of each VPN Gateway for which a license should be installed.

For instructions about how to obtain the MAC address and how to paste the license key, see [Licenses](#) on page 26 in [Customize the Portal](#) on page 249.

Connection Example

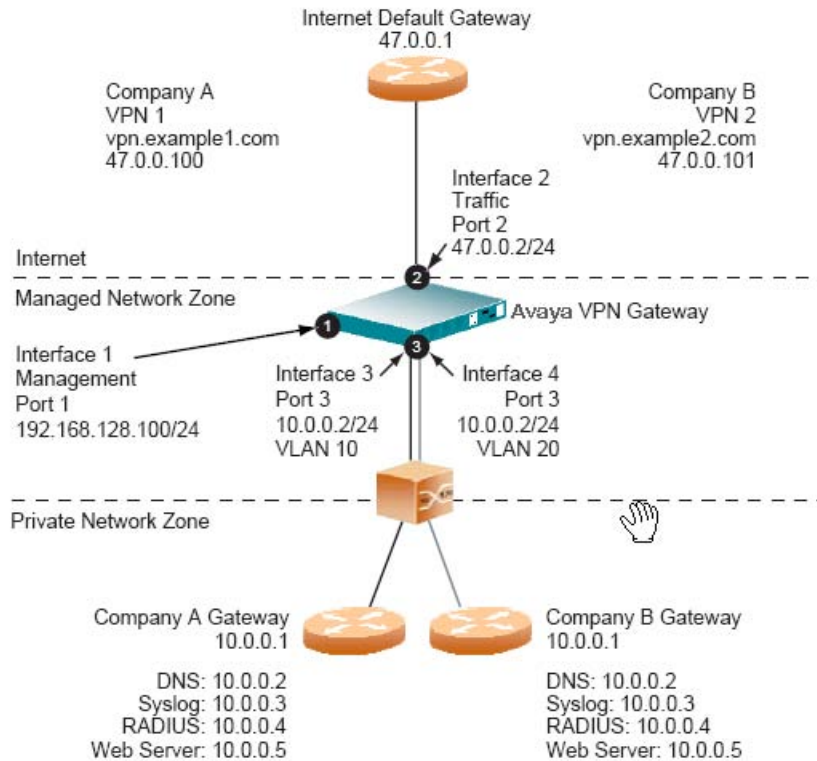
1. A user from Company A browses to <https://vpn.example1.com> from the Internet. This DNS domain name points to a virtual address on the AVG 's traffic interface. The appropriate SSL certificate is presented for the Company A Portal. A custom login screen is presented. The user provides appropriate login credentials which are validated using any of the supported authentication schemes such as RADIUS, LDAP, NTLM or RSA SecurID.
2. All connections from the Company A Portal are bound to a specific interface (may be VLAN-tagged) on the private/internal side.
3. In this example the authentication server is located inside Company A's corporate Intranet.
4. After validating the login credentials, the user is bound to a user-group based on the response from the authentication server. This group will determine access rules for the user and restrict access to certain resources within the private network. The custom Company A Portal is presented including only the application links applicable for this user.
5. As the user selects application links from the Portal, the AVG will query the private DNS server to resolve host names into IP addresses.
6. The user will access applications within the private network zone.



Configuration Example

In this example we will create two unique VPN Portal configurations on a single AVG platform. These two independent customer Portals will link to two respective private networks in a secure fashion such that the first Portal will not provide access to the second internal network and vice versa.

This example will use completely overlapping IP addresses to demonstrate support for this topology. Any customer network subnets can be used as appropriate.



Initial Setup

Before you can start configuring the VPNs you should perform an initial setup of the system. The initial setup procedure is described in the "Initial Setup" chapter in the *Users Guide*.

Configure the Interfaces

Four interfaces are required to configure the two VPNs.

Configure Interface 1

When you ran the initial setup, Interface 1 was created as the management interface, that is, on the private or internal side (not facing the Internet) of the VPN Gateway. If you need to view or edit the settings for Interface 1, follow these steps.

1. Verify that the management interface on the "private" or "internal" side of the VPN Gateway has the correct IP address and network mask.

```
>> Main#/cfg/sys/host 1/interface 1
```

```
>> Host Interface 1#ip

Current value: 192.168.128.100
Enter new IP address of the Interface:<enter new IP or press
ENTER if correct>

>>

Host Interface 1#netmask

Current value: 255.255.255.0
Enter the network mask:<enter new network mask or press ENTER if
correct>
```

2. Verify that this interface uses the desired physical port on the VPN Gateway.

During the initial setup you were prompted for a port number for the management interface. If you wish to use another port number, use the **del** command to delete the current port number and the **add** command to add the desired port number.

```
>> Host Interface 1#ports/list

1
```

3. Verify that the default gateway is assigned the correct IP address.

You had the option to configure a default gateway during the initial setup. This step shows how to add, edit or view the IP address of the default gateway. The default gateway must always reside on the traffic interface, that is, on the public or external side (facing the Internet).

```
>> Interface Ports#../../gateway

Current value: " "

Enter default gateway address:47.0.0.1
```

In the next step we will create the traffic interface.

Configure Interface 2

During the initial setup you may have created Interface 2 as well, if you chose to set up a two-armed configuration. This instruction assumes that Interface 2 has not yet been configured.

1. Configure Interface 2 with an IP address and network mask to be used by the traffic interface on the "public" or "external" side (facing the Internet) of the VPN Gateway.

Bind the interface to port 2 on the VPN Gateway.

```
>> Main#/cfg/sys/host 1/interface 2

Creating Host Interface 2
Enter new IP address of the Interface:47.0.0.2

Enter the network mask:24

<equals 255.255.255.0>

Enter VLAN tag id [0]:<press ENTER>

Entering: Interface ports menu
Port to add:2

Leaving: Interface ports menu
```

2. Apply the changes.

```
>> Host Interface 2#apply

Changes applies successfully.
```

Configure Interface 3

1. Configure Interface 3 with an IP address and network mask that matches the network required for the Company A's private network zone.

Bind the interface to port 3 on the VPN Gateway and set the VLAN tag ID to 10.

```
>> Main#/cfg/sys/host 1/interface 3

Creating Host Interface 3
Enter new IP address of the Interface:10.0.0.2

Enter the network mask:24

<equals 255.255.255.0>

Enter VLAN tag id [0]:10

Entering: Interface ports menu
Port to add:3

Leaving: Interface ports menu
```

2. Configure a default gateway address for Interface 3.

```
>> Host Interface 3#gateway
```

```
Current value:
Enter default gateway address:10.0.0.1
```

You also have the option to configure static routes for the backend (private side) traffic, using the **/cfg/host #/interface #/routes** command.

3. Apply the changes.

```
>> Host Interface 3#apply

Changes applied successfully.
```

Configure Interface 4

1. Configure Interface 4 with an IP address and network mask that matches the network required for Company B's private network zone.

Bind the interface to the port 3 on the VPN Gateway and set the VLAN tag ID to 20.

```
>> Main#/cfg/sys/host 1/interface 4

Creating Host Interface 4
Enter new IP address of the Interface:10.0.0.2

Enter the network mask:24
<equals 255.255.255.0>

Enter VLAN tag id [0]:20

Entering: Interface ports menu
Port to add:3

Leaving: Interface ports menu
```

2. Configure a default gateway address for Interface 4.

```
>> Host Interface 4#gateway

Current value:
Enter default gateway address:10.0.0.1
```

You also have the option to configure static routes for the backend (private side) traffic, using the **/cfg/host #/interface #/routes** command.

3. Apply the changes.

```
>> Host Interface 4#apply

Changes applied successfully.
```

If required, configure new interfaces for additional customer private networks. Use unique VLAN tag IDs for each interface.

Configure VPN 1

In this example, two VPNs should be configured, one for Company A (VPN 1) and one for Company B (VPN 2).

* Note:

If you ran the Quick VPN setup wizard during the initial setup, VPN 1 has already been created. You can either edit the settings for VPN 1 to adapt it to the requirements of your customer or keep it as a test VPN for your own testing. This configuration example assumes that you have not yet created a VPN.

Configure the VPN

1. Create a VPN and enter the Portal IP address.

A portal server is automatically created along with the VPN. The portal server is connected to the Portal IP address(es) and listens to TCP port 443 (https). The Portal IP address is used by the remote user to access the VPN Portal.

```
# /cfg/vpn 1

Creating VPN 1
VPN name:<optional>

Enter server ips (comma separated):47.0.0.100
```

2. Enable standalone mode.

This step sets the portal server to standalone mode, which is required if the VPN Gateway is not connected to an Application Switch.

```
>> VPN 1#standalone

Current value: off
Standalone mode (on/off):on
```

3. Specify the certificate to be used by the portal server.

You are prompted to type the index number of an existing certificate. To view all certificates currently added to the AVG cluster by index number and name, use

the `/info/certs` command. For more information about how to import a certificate to the AVG, see the "Certificates and Client Authentication" chapter in the *Users Guide*.

```
>> VPN 1#server/ssl/cert

Current value: unset
Enter certificate number: (1-1500)1
```

*** Note:**

If the certificate you specify is a chained certificate, you need to first add the CA certificates up to and including the root CA certificate, and then specify the CA certificate chain of the server certificate. For more information about how to construct the server certificate chain, see the `cachain` command under "SSL Server SSL Configuration" in the *Command Reference*.

4. Assign a Fully Qualified Domain Name (FQDN) to the portal server.

The domain name you specify should be registered in DNS to resolve to the virtual server IP address you specified in the previous step. The FQDN for the portal server corresponds to the URL that remote users will type in the address field of their web browser to access the Portal login page when the VPN is fully deployed.

```
>> SSL Settings#../dnsname

Current value: " "

Enter fully qualified DNS name of VIP:vpn.example1.com
```

5. Apply your changes.

```
>> Server#apply

Changes applied successfully
```

Bind VPN 1 to Interface 3 and Configure the DNS Settings

By binding VPN 1 to Interface 3, this interface will be the target for all private traffic for Company A.

1. Bind VPN 1 to Interface 3.

```
>> Server#../adv

>> Advanced#interface
```

```
Current value: 0
Enter backend interface number (0 = default interface):3
```

2. Configure the VPN to use a common authentication server (optional).

This step lets you enable common authentication for several VPNs, even if the VPNs are bound to specific interfaces. This ability can be used in cases when the ISP wishes to share the same set of authentication servers for several end-customers.

- **on:**

Sets the AVG to use the default routing for authentication services.

- **off:**

Authentication requests will be routed through the referenced backend interface (see the **interface** preceding command) to an authentication server on the end-customer's private network.

```
>> Advanced#cauth
Current value: off
Common auth servers (on/off):
```

3. Configure the VPN to use a common accounting server (optional).

This step lets you enable common RADIUS accounting for several VPNs, even if the VPNs are bound to specific interfaces. This ability can be used when the ISP wishes to share the same set of accounting servers for several end-customers.

- **on:**

Sets the AVG to use the default routing for accounting services.

- **off:**

Accounting information will be routed through the referenced backend interface (see the **interface** preceding command) to a RADIUS accounting server on the end-customer's private network.

```
>> Advanced#cradacct
Current value: off
Common accounting servers (on/off):
```

4. Configure the DNS settings for the portal server.

This step specifies a DNS search domain. The search domain(s) you specify is automatically appended to the host names a remote user types in the various address fields on the Portal (provided a match is found).

```
>> Advanced#dns/search

Current value: " "

Enter search domains (separated by
comma):example1.com,support.example.com
```

5. Configure the DNS server.

This step configures the system to use Company A's private DNS server.

```
>> DNS Settings#servers/add

IP Address to add:10.0.0.2
```

6. Apply your changes.

```
>> DNS Servers#apply

Changes applied successfully
```

Create IP Pool

The IP pool comes into play when the remote user tries to access a host using Net Direct or the Avaya IPsec VPN client (formerly the Contivity VPN client). A new IP address has to be assigned as source IP for the unencrypted connection between the VPN Gateway and the destination host. Optionally, specific network attributes for this connection can also be defined.

As the ISP administrator, you can configure several IP pools, each with a unique ID number and unique properties. By mapping the desired IP pool to a user group, the end-customer can then establish different methods for IP address and network attributes assignment for different user groups.

One of the configured IP pools should be selected as the default IP pool for a VPN. Groups for which no IP pool is assigned (IP pool number=0) will use the default IP pool.

For more information about the Net Direct client and the IPsec VPN client, see [Net Direct](#) on page 87 and [Transparent Mode](#) on page 355, respectively.

Create the IP pool.

Network attributes (including IP address) can be assigned either locally (from the AVG), from an external RADIUS server or from an external DHCP server.

When you configure an IP pool for the first time, you will enter a wizard. Depending on the choice you make for pool mechanism (that is,

local, radius

or

dhcp

), different questions will be displayed in the wizard.

```
>> Main#/cfg/vpn 1/ippool

Enter Pool number or name (1-1023):1

Creating Pool 1
Select one of local, radius, dhcp:

<select the desired pool mechanism here>
```

The pool mechanism setting is equivalent to the **type** command in the Pool menu.

You can associate an IP pool with a particular host in a clustered environment. For more information, see [Configure host IP pool](#) on page 330.

Configure IP Address Range and Local Network Attributes

If you set the pool mechanism to

local

, you should configure the desired IP address range. You can also configure network attributes to be retrieved from the AVG when the client connects.

If you set the pool mechanism to

radius

or

dhcp

, continue with the relevant section (see the following pages) instead.

1. Configure an IP address range.

```
Set the lower ip for the pool range:10.1.82.140

Set the upper ip for the pool range:10.1.82.150
```

2. If needed, change the default proxy ARP setting.

```
Set proxyarp (on/off/all) [on]:
```

- **on:**

Means that the VPN Gateway that handed out the IP address (from the IP pool) for a specific client connection will respond to ARP requests on behalf of the Net Direct/IPsec VPN client for return traffic. The VPN Gateway then acts as a router and forwards IP packets to the client through the existing tunnel. Proxy ARP is used on all interfaces for the relevant VPN except the traffic interface. This is the default setting.

- **off.**

Return traffic will not be able to reach its destination unless specific routes are configured.

- **all.**

Same as

on

but proxy ARP is used on all interfaces.

3. Configure network attributes (optional).

The Net Direct client normally works fine without adding specific network attributes. You can however specify the desired attributes on the Network attributes menu if needed.

```
>> Pool 1#netattr
```

- **netmask:**

Sets the network mask for the client. The network mask should cover the IP address range specified in step 1. The default network mask is

255.255.255.0.

- **primary/secondary NBNS server:**

Sets the IP address of a primary NBNS server (NetBIOS Name Server). Used if the Net Direct or IPsec VPN client should use a specific NBNS server to have computer names resolved into IP addresses. NBNS servers provide WINS (Windows Internet Naming Service) which is part of the Microsoft Windows NT server environment.

- **primary/secondary DNS server:**

Sets the IP address of a primary DNS server. Use this command if the IPsec VPN client should use a specific DNS server to have domain names resolved into IP addresses. If no (primary or secondary) DNS server is specified here, the DNS server specified for the VPN to which the remote user belongs will be used. The command to use is **/cfg/vpn #/adv/dns/servers**. If only a default DNS server is specified (using the **/cfg/sys/dns/servers** command), this will be used.

- name of client DNS domain:

Lets you specify the name of the domain used while a Net Direct or IPsec user tunnel is connected. It ensures that domain lookup operations point to the correct domain. This is particularly important for clients that use Microsoft Outlook or Exchange, to ensure that the mail server is mapped to the correct domain.

4. Enable the IP Pool.

```
>> Pool 1#ena
```

5. Apply the changes.
6. The next step is to map the IP pool to a group, or make it the default IP pool for the VPN.

Continue with the section [Map the IP Pool to User Group \(Optional\)](#) on page 96.

Configure RADIUS IP Pool

If you set the pool mechanism to

radius

(as described in the section [Create IP Pool](#) on page 323), you (or the end-customer) should configure the VPN Gateway to retrieve network attributes from a RADIUS server.

How to configure a RADIUS server is described in the "Authentication Methods" chapter in the *VPN Administrator's Guide* and in [Authentication Methods](#) on page 117 in this guide.

To configure the VPN Gateway to retrieve network settings (including client IP address) through RADIUS attributes from an external RADIUS server, use the `/cfg/vpn #/aaa/auth # /radius/netattr` command. A minimum requirement is to configure retrieval of client IP address and primary DNS server. You can retrieve a number of network attributes, for example, primary/secondary DNS server, primary/secondary NBNS server and so on.

The following instructions assume that you continue with the IP pool wizard after having chosen

radius

as the pool mechanism.

1. If needed, change the default proxy ARP setting.

```
Set proxyarp (on/off/all) [on]:
```

- on:

Means that the VPN Gateway that handed out the IP address (from the IP pool) for a specific client connection will respond to ARP requests on behalf of the

Net Direct/IPsec VPN client for return traffic. The VPN Gateway then acts as a router and forwards IP packets to the client through the existing tunnel. Proxy ARP is used on all interfaces for the relevant VPN except the traffic interface. This is the default setting.

- `off`.

Return traffic will not be able to reach its destination unless specific routes are configured.

- `all`.

Same as

`on`

but proxy ARP is used on all interfaces.

2. Enable the IP Pool.

```
>> Pool 1#ena
```

3. Configure fallback network attributes (optional).

```
>> Pool 1#netattr
```

For IP pools of the

`radius`

and

`dhcp`

types, network attributes can be configured on the AVG as fallback values if the RADIUS or DHCP server does not return a specific setting for a network attribute. This is done in the same way as for IP pools of the

`local`

type (see [VPNs](#) on page 19 on [VPNs](#) on page 19 for instructions).

4. Apply the changes.
5. The next step is to map the IP pool to a group, or make it the default IP pool for the VPN.

Continue with the section [Map the IP Pool to User Group \(Optional\)](#) on page 96.

Configure DHCP IP Pool

If you set the pool mechanism to

dhcp

(as described in the section [Create IP Pool](#) on page 323), you should configure the VPN Gateway to retrieve network attributes from a DHCP server.

The following instructions assume that you continue with the IP pool wizard after having chosen

dhcp

as the pool mechanism.

1. Configure the external DHCP server IP address.

```
Entering: DHCP menu
Entering: DHCP servers menu
DHCP server IP address:10.1.82.100

Leaving: DHCP servers menu
```

2. If needed, change the default proxy ARP setting.

```
Set proxyarp (on/off/all) [on]:
```

- on:

Means that the VPN Gateway that handed out the IP address (from the IP pool) for a specific client connection will respond to ARP requests on behalf of the Net Direct/IPsec VPN client for return traffic. The VPN Gateway then acts as a router and forwards IP packets to the client through the existing tunnel. Proxy ARP is used on all interfaces for the relevant VPN except the traffic interface. This is the default setting.

- off.

Return traffic will not be able to reach its destination unless specific routes are configured.

- all.

Same as

on

but proxy ARP is used on all interfaces.

3. Enable the IP Pool.

```
>> Pool 1#ena
```

4. Configure fallback network attributes (optional).

```
>> Pool 1#netattr
```

For IP pools of the

radius

and

dhcp

types, network attributes can be configured on the AVG as fallback values if the RADIUS or DHCP server does not return a specific setting for a network attribute. This is done in the same way as for IP pools of the

local

type (see [3](#) on page 330 on step 3 for instructions).

5. Apply the changes.
6. The next step is to map the IP pool to a group, or make it the default IP pool for the VPN.

Continue with the next section.

Map the IP Pool to User Group

As mentioned on [Create IP Pool](#) on page 323, several IP pools with different mechanisms (that is,

local, radius

or

dhcp

) can be configured. By mapping the IP pools to different user groups you (or the end-customer) can provide different ways of assigning IP address and network attributes depending on the user's group membership.

One of the configured IP pools should be selected as the default IP pool for the VPN. Groups for which no IP pool is assigned (IP pool number=0) will use the default IP pool. How to create a default IP pool is described in the next section.

This is how to map an IP pool to a user group:

1. Map the IP pool to the desired user group.

```
>> Main#cfg/vpn 1/aaa/group 1/ippool
```

```
Current value: 0
IP pool number:1
```

2. Map the next IP pool to another group in the same way.
3. Apply the changes.

Create a Default IP Pool

One of the configured IP pools should be selected as the default IP pool for the VPN. Groups for which no IP pool is assigned (IP pool number=0) will use the default IP pool.

1. Configure an existing IP pool as the default IP pool.

```
>> Main#cfg/vpn 1/aaa/defippool

Current value: 0
IP pool number:1
```

2. Apply the changes.

Configure host IP pool

Perform the following procedure to associate an IP pool with a particular host in a clustered environment:

1. Enable hippool command on the VPN menu.

```
>> Main# cfg/vpn #/hostippool

Enable Host IP Pool feature (true/false): true
```

(The hippool command appears in the VPN menu)

2. Define the host IP pool.

```
>>vpn 1# hippool

Enter Pool number or name: 1

Creating Host IP pool 1

Set the pool name:test
```

(Specify the host IP pool number or name. For example, 1)

Creates host IP pool

(Specify the host IP pool name)

Set proxyarp [on off all] [on]:on	(Enable proxyarp)
-----------------------------------	-------------------

3. Enable the host IP pool.

>>Host IP Pool 1# ena	(Enable host IP pool)
-----------------------	-----------------------

4. Create the host.

>>Host IP Pool 1# host	(Select host)
Enter the Host number: 1	(Specify the host number)
Enter Host IP address:	(Specify the host address)
Set the lower ip for the pool range:	(Specify the Lower IP address for the pool range)
Set the upper ip for the pool range:	(Specify the upper IP address for the pool range)

5. Configure network attributes (optional).

>> Host 1# netattr	(Network Attributes menu appears)
--------------------	-----------------------------------

6. Apply changes.

Enable IPsec

To enable access to the VPN through IPsec user tunnels (that is, for remote users with the Avaya IPsec VPN client installed) or IPsec branch office tunnels, proceed as follows:

1. Enable IPsec.

>> Main#/cfg/vpn 1/ipsec
>> IPsec#ena

2. Apply the changes.

IPsec User Tunnel Configuration

When IPsec has been enabled for the VPN, the end-customer can configure the IPsec user tunnel(s) through the VPN Administrator web user interface. If the end-customer wishes to use local client IP address assignment instead of retrieving network attributes (including client IP

address) from a RADIUS server, the IP pool must also be configured before the end-customer can continue with the configuration.

IPsec user tunnel configuration is described in the section [Avaya IPsec VPN Client](#) on page 368 in [Transparent Mode](#) on page 355 in this *Application Guide* and in the same section in the "Transparent Mode" chapter in the *VPN Administrator's Guide*.

IPsec Branch Office Tunnel Configuration

When IPsec has been enabled for the VPN, the end-customer can configure the IPsec branch office tunnel(s) through the VPN Administrator web user interface.

IPsec branch office tunnel configuration is described in [Branch Office Tunnels](#) on page 337 in this *Application Guide* and in the "Branch Office Tunnels" chapter in the *VPN Administrator's Guide*.

License Allocation

By default, the SSL and IPsec user licenses you have loaded to the AVG cluster are shared by all VPNs. Using the license allocation feature, you can however dedicate the desired number of concurrent users to different VPNs. For example, an SSL user license valid for 2000 concurrent users can be distributed as desired amongst configured VPNs. Also see the section [License Pool \(SSL and IPsec Users\)](#) on page 28 in [Customize the Portal](#) on page 249.

1. Allocate the desired number of concurrent SSL users to VPN 1.

```
# /cfg/vpn 1/adv/license

>> License allocation#SSL

Current value: 0
Enter number of SSL licenses:50
```

2. Allocate the desired number of concurrent IPsec users to VPN 1.

```
>> License allocation#ipsec

Current value: 0
Enter number of IPsec licenses:50
```

3. Apply your changes.

Enable Access to Web Interface through HTTP or HTTPS

For VPN Administrators to be able to access the web user interface, access through HTTP or HTTPS should be enabled.

1. Enable access to the AVG cluster through HTTP.

In this example we will enable access to the web user interface through HTTP.

```
>> Main#/cfg/sys/adm/http
>> HTTP#ena
```

2. Apply your changes..

```
>> HTTP#apply
Changes applied successfully.
```

VPN Administration

For end-customers to be able to manage their VPNs through the web user interface, VPN administration must be enabled globally for the VPN.

1. Enable VPN administration globally for the VPN.

```
# /cfg/vpn 1/adv/vpnadmin
Current value: false
Allow VPN admin (true/false):true
```

2. Apply the changes.

Configure VPN Administrator Access Group

The next step is to enable VPN administration for the desired user access group.

The VPN Administrator group configured in this example has full access to all networks and services. If you wish to configure less generous access rights (for example, to limit access to a specific network), you should first configure the desired network definition. This network name can then be referenced when prompted for a network name in the access rule. For instructions, see [Groups, Access Rules and Profiles](#) on page 157.

1. Configure a user access group.

```
# /cfg/vpn 1/aaa
>> AAA#group
Enter group number or name: (1-1023)1
```

```

Creating Group 1
Group name:vpn_admin

Enter number of sessions (0 is unlimited):<press ENTER>

Enter user type (advanced/medium/novice):advanced

Allow vpn admin (true/false):true

```

2. Configure access rules.

The asterisks (*) imply that access to all networks, protocols and paths is allowed.

```

>> Group 1#access

Enter access rule number: (1-1023)1

Creating Access rule 1
Enter network name:*

Enter service name:*

Enter application specific name:*

Enter action (accept/reject):accept

```

3. Apply the changes.

```

>> Access rule 1#apply

Changes applied successfully.

```

Configure VPN Administrator User

The following steps show how to configure a user in the user's local database and map this user to the VPN Administrator group configured in the previous example. This instruction assumes that you have already configured a local database. If not, see the section [Local Database Authentication](#) on page 147 in [Authentication Methods](#) on page 117.

1. In the System tree view, under Authentication, select Auth Servers

```

# /cfg/vpn 1/aaa/auth 1/local

>> Local database#add

Enter user name:john

Enter passwd:<password>

```

```
Enter group names (comma separated):<press TAB to view configured groups>

    trusted      vpn_admin
Enter group names (comma separated):vpn_admin
```

2. Apply the changes.

Configure VPN 2

To configure VPN 2, simply follow the steps in the section [Configure VPN 1](#) on page 320 but substitute the values with values that are appropriate for VPN 2.

Update DNS Server

The local DNS servers should be updated with the domain names used for the VPNs, and be configured to perform reverse DNS lookups.

Remaining Configuration

when you have configured the basics for a VPN, you can delegate per domain configuration to members of the VPN Admin group within the VPN. This allows the end-customer in a managed VPN service to configure authentication methods, user access groups, access rules, linksets, Tunnel Guard checks, WholeSecurity scans and much more.

The end-customers can also customize their Portals, for example, change the color theme, banner and static texts. Note that the total size of imported banners in the different VPNs must not exceed 16 MB.

End-user instructions on how to manage their own VPNs through the web user interface is in the *VPN Administrator's Guide*.

Chapter 19: Branch Office Tunnels

In addition to IPsec-based user tunnels, where the remote user connects to the Avaya VPN Gateway (AVG) through an IPsec VPN client, the AVG also provides the ability to configure and establish IPsec-based branch office tunnels. Several peer-to-peer branch office tunnels can be configured for each virtual private network (VPN). Tunnels get automatically established whenever they are configured or when the system starts. Like user tunnels, branch office tunnels make use of a previously configured IKE profile. The IKE profile includes the preferred encryption settings for the tunnel.

Clustering Branch Office Tunnels

Branch office tunnels can co-exist with the clustering capabilities of the AVG. When there are more than one VPN Gateway in the cluster, and if several Portal IP addresses have been defined for a VPN, these IP addresses are evenly distributed among the AVGs on the public side of the cluster.

User clients, such as the Avaya IPsec VPN client (formerly Contivity), Net Direct and browsers, typically connect to the cluster by using a name registered in DNS. Round robin DNS is then used to spread out client requests evenly to the different cluster members. This is not applicable to branch office tunnels. Instead, one Portal IP address is configured (out of the list of IP addresses defined for the VPN) to be the endpoint for the tunnel. This IP address will always be brought up on one of the AVGs in the cluster. The branch office tunnel will be established from the AVG that currently owns the Portal IP address.

If a cluster member (AVG) fails, all Portal IP addresses will migrate to surviving cluster members. Because branch office tunnels are associated to a Portal IP address, any existing tunnels are likewise moved to the surviving AVG(s).

Scalability and Load Balancing

To achieve higher capacity, more AVGs can be added to the cluster. If there are two AVGs and both machines terminate a number of BO tunnels as well as regular IPsec/Net Direct/SSL, traffic capacity will increase by simply adding an AVG to the cluster.

Connection Example

Refer to [Figure 7: Branch Office Tunnel](#) on page 339.

1. A user working at the Headquarters (HQ) wishes to access a web server located at the Branch Office (BO). The user browses to `http://accounting.denver.example.com` which corresponds to the IP address 10.1.2.10. The request is routed to the VPN Gateway.
2. The VPN Gateway finds a match between the user's source IP (10.0.1.19) and a local network specified in the BO tunnel profile configuration. The VPN Gateway also finds a match between the user's destination IP (10.1.2.10) and a remote network specified in the BO tunnel profile configuration.
3. The double match in step 2 means that the packets will be routed through the BO tunnel to the BO tunnel's endpoint. If Nailed Up tunnel mode is used, the packets will enter the tunnel instantly. If On Demand mode is used, there will be a slight delay before the tunnel gets established. The BO tunnel's endpoint is the branch office's public IP address (for example, the Portal IP address of a VPN). This IP address should be specified as the remote IP address in the BO configuration on the HQ's VPN Gateway.
4. To authenticate to the BO endpoint, the HQ endpoint sends a shared secret (which has to be specified in the BO configuration at both endpoints). As an alternative, a string can be extracted from an X509 certificate and be matched against a string in the endpoints' BO configuration (see [Configuration Example](#) on page 339).
5. The VPN Gateway (or corresponding device) at the BO endpoint routes the packets to their destination, that is, 10.1.2.10.
6. For return traffic, the VPN Gateway at the BO endpoint recognizes 10.1.2.10 as belonging to a local network that is allowed to send traffic through the BO tunnel. The destination IP address (10.0.1.19) is recognized as belonging to a remote network in the BO configuration on the BO's VPN Gateway, so the packets are routed back through the BO tunnel.

As we can see from the preceding example, the BO configuration on the HQ's VPN Gateway should be mirrored in the BO configuration on the BO's VPN Gateway (or corresponding device). Networks specified as remote networks on one endpoint should be defined as local networks on the other endpoint and vice versa.

When a request is initiated from the branch office, the preceding steps are exactly the same, only reversed.

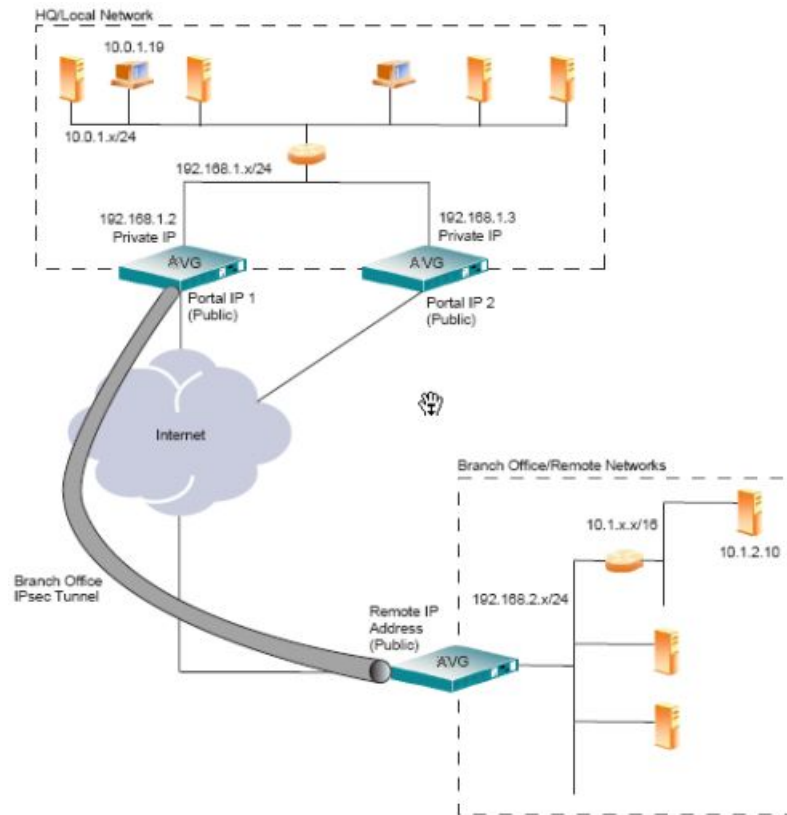


Figure 7: Branch Office Tunnel

The preceding configuration shows two VPN Gateways in a cluster. If the AVG that currently owns the BO tunnel fails, the tunnel migrates to the other AVG. For the networks on the private side to be aware of the tunnel shift and thus send the packets to the right AVG, the AVG will announce the branch office networks on the private side through RIPv2 messages.

Configuration Example

In this example we will create a branch office tunnel similar to that in the connection example in the previous section.

Initial Setup

Before you can start configuring the branch office tunnel you should perform an initial setup of the system. The initial setup procedure is described in the "Initial Setup" chapter in the *Users Guide*.

Basic VPN Setup

If the VPN Gateway should be used to configure a basic VPN, see [Clientless Mode](#) on page 35.

Secure Service Partitioning

If the VPN Gateway should be used to perform secure service partitioning, that is, host VPNs for different end-customers, go to [Secure Service Partitioning](#) on page 313. For instructions about how to configure interfaces for the different VPNs, configure the VPNs and bind the interfaces to the VPNs.

Configure Branch Office Tunnel

Branch office tunnels use IPsec for secure transfer of packets. To enable the IKE daemon (IPsec server) on the VPN Gateway, proceed as follows:

Enable IPsec

1. Enable IPsec.

```
>> Main#/cfg/vpn 1/ipsec  
  
>>IPsec# ena
```

2. Apply the changes.

Create Access Group

The purpose of creating an access group to be used by the branch office tunnel profile is to accomplish a more fine-grained access control to the remote networks at the branch office. The group's access rules are applied when the response packets arrive at the local VPN Gateway.

For instructions about how to create access groups, see [Groups, Access Rules and Profiles](#) on page 157.

Create IKE Profile and Branch Office Tunnel Profile

In a secure service partitioning configuration, the IKE profile can also be configured by the end-customer (with VPN administration rights) through the web user interface.

1. Create an IKE profile.

This step creates an IKE profile. If needed, several different IKE profiles can be created with different settings for encryption. The default settings for the IKE profile are usually fine for use with branch office tunnels. The NAT traversal options are however not applicable for branch office tunnels. For detailed information about available commands on the IKE profile menu, see the *Command Reference*.

```
>>IPsec# ikeprof

Enter IKE profile number (1-64):1

Creating IKE Profile 1
Enter name of IKE profile:ike profile 1
```

2. Create a branch office tunnel profile.

This step creates a branch office tunnel profile. The profile defines different criteria for the IPsec tunnel, for example, local and remote endpoint IP addresses, authentication method, local and remote networks and so on. For detailed information about available commands on the User tunnel profile menu, see the *Command Reference*.

When prompted for the IKE profile name, press TAB to view available profiles.

```
>> IKE Profile 1#../botunprof

Enter bo tunnel profile number (1-4096):1

Creating BO Tunnel Profile 1
Enter name of BO tunnel profile:bo tunnel profile 1

Enter name of IKE profile:ike profile 1

<reference IKE profile here>
```

3. Enter the local endpoint's public IP address.

You should previously have configured one or several Portal IP addresses (or VIPs) for the current VPN under

```
/cfg/vpn #/ips
```

.

```
Choose which VIP to use:<press TAB to view available IPs>
```

4. Enter the remote endpoint's public IP address.

```
IP of other end of BO tunnel:
```

5. Enter the name of a previously created access group.

The group's access rules determine which ports and protocols will be available on the remote network.

```
Enter name of AAA group:  
<press TAB to view available groups>
```

6. Enter a remote network that should be accessible with the branch office tunnel.

When the BO Tunnel profile menu is displayed you can enter additional remote (BO) networks using the **remotenets** command.

```
Entering: List networks behind remote BO end  
Enter network IP number:  
Enter netmask:
```

7. Enter a local network from which traffic should be allowed to enter the branch office tunnel.

When the BO Tunnel profile menu is displayed you can enter additional local networks using the **localnets** command.

```
Leaving: List networks behind remote BO end  
Entering: List local (private) networks  
Enter network IP number:  
Enter netmask:
```

Shared Secret Authentication

1. Set the authentication type to sharedsecret.

The authentication type is set to sharedsecret by default. As an alternative, the authentication type can be set to

`cert`

(see the following section).

```
>> BO Tunnel Profile 1#authtype

Current value: sharedsecret
Enter authentication type:
```

2. Enter the shared secret.

This step sets the shared secret at the local endpoint. The same shared secret should be specified at the remote endpoint (for example, a VPN Gateway or similar at the branch office).

```
>> BO Tunnel Profile 1#sharedsecre

Current value: " "

Enter secret:secret
```

3. Apply the changes.

Certificate Authentication

When certificate authentication is used, the local endpoint sends a server certificate to authenticate to the remote endpoint and vice versa. Upon authentication, a value string is extracted from the certificate. This string is matched against a string specified in the endpoint's BO configuration. If a VPN Gateway is used to terminate the tunnel, the string that is used to match the remote certificate's string should be specified with the **remoteid** command.

1. Set the authentication type to cert.

```
>> BO Tunnel Profile 1#authtype

Current value: sharedsecret
Enter authentication type:cert
```

2. Specify the OID (or symbolic name) whose value should be extracted from the remote endpoint's certificate.

Theoretically, if you imported the remote endpoint's certificate to the VPN Gateway you could find out the OIDs, symbolic names and their values for the certificate by using the **/cfg/cert #/subject** command.

Example: **L/localityName (2.5.4.7) = Test** where

localityName

is the TOC="No symbolic name,

2.5.4.7

is the OID and

Test

is the value.

```
>> BO Tunnel Profile 1#certoid
Current value: " "
Cert identity OID within 'subject':2.5.4.7
<example OID>
```

Either the symbolic name (

localityName

in this example) or the OID (

2.5.4.7

in this example) can be specified following the **certoid** command. By pressing **TAB** following the **certoid** command, a list of suggested symbolic names is displayed:

```
commonName, emailAddress, givenName, initials, surname
```

and

```
title
```

```
.
```

In the preceding example, the value specified for

```
localityName
```

in the certificate is

Test

. This value will be extracted from the certificate and matched against the string specified with the **remoteid** command (see following step).

3. Specify the string to match the value extracted from the remote endpoint's certificate.

```
>> BO Tunnel Profile 1#remoteid
Current value: " "
Enter id:Test
<example string>
```

4. Specify which server certificate to use to authenticate the VPN Gateway to the remote endpoint.

To be able to reference the certificate with an index number, the certificate must exist on the VPN Gateway. See the "Certificates and Client Authentication" chapter in the *Users Guide* for detailed instructions on certificate management.

```
>> BO Tunnel Profile 1#../cert

Current value: unset
Enter certificate number (1-1500):
```

5. Specify the CA cert(s) that will be used to authenticate the remote endpoint's certificate.

To be able to reference the CA certificate with an index number, the CA certificate must exist on the VPN Gateway. See the "Certificates and Client Authentication" chapter in the *Users Guide* for detailed instructions on certificate management.

```
>> IPsec#cacerts

Current value: " "

Enter certificate numbers (separated by comma):
```

6. Apply the changes.

```
>> IPsec#apply

Changes applied successfully.
```

For an explanation of BO Tunnel Profile menu commands that have not been covered here, see the *Command Reference*.

RIP Announcement

1. Verify that the current RIP announcement settings are the desired ones.

```
>> IPsec#botunprof 1/ripannouncement

Current value: on
Set RIPv2 announcement (on/off/all):
```

- on:

Branch office networks are announced on the private side through the RIPv2 protocol. The announcement is made on all interfaces for the relevant VPN

except the traffic interface. This setting is required when the cluster consists of several AVGs.

- off:

Branch office networks are not announced on the private side. This setting may cause routing problems when the cluster consists of several AVGs.

- all:

Same as

on

but the announcement is made on all interfaces.

2. Apply the changes.

Information Menu

The Information menu includes a command for viewing the properties of enabled branch office tunnels:

```
>> Main#info/botuns

Number of enabled BO tunnels for all VPNs: 3
----- VPN Number: '1' -----
Number of enabled BO tunnels: 1
Number of BO tunnels in state down: 1 phase1:0 up: 0
BotunProf At host State Enc (KB) Dec (KB) Time
denver(1) 1 down 0 0 07:04:36
----- VPNNumber: '2' -----
Number of enabled BO tunnels: 2
Number of BO tunnels in state down: 0 phase1: 0 up: 1
BotunProf At host State Enc (KB) Dec (KB) Time
austin(2) 1 down 0 0 00:00:05
dallas(1) 2 up 143 138 09:01:25
----- VPN Number: '3' -----
Number of enabled BO tunnels: 0
Number of BO tunnels in state down: 0 phase1: 0 up: 0
BotunProf At host State Enc (KB) Dec (KB) Time
----- VPN Number: '4' -----
Number of enabled BO tunnels: 0 Number of BO tunnels in state down: 0
phase1: 0 up: 0
BotunProf At host State Enc (KB) Dec (KB) Time
```

The output shows the name of the branch office tunnel profile, the AVG host from which the tunnel is set up, the tunnel state (

up, phase1

or

down

), encrypted data in kBytes and decrypted data in kBytes. The

up

tunnel state means that both ISAKMP and IPsec SAs are established, whereas the

phase1

state indicates that only the ISAKMP SA is established).

The output also shows the time the tunnel has been active (hours:minutes:seconds).

Statistics Menu

The Statistics menu includes a number of commands for viewing branch office tunnel performance statistics. The statistics commands related to branch office tunnels begin with

bo

(for example,

bodec

to view decrypted kB per second). The information can be shown on a cluster-wide level, per AVG, per VPN and so on.

```
>> Main#stats/ipsec
```


Chapter 20: Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol (L2TP) is an extension to the Point-to-Point Protocol (PPP), which is an important component for VPN. Using L2TP, an Internet Service Provider (ISP), or other access service, can create a virtual tunnel to link a customer's remote sites or remote users with corporate home networks.

The two endpoints of an L2TP tunnel are L2TP Access Concentrator (LAC) and L2TP Network Server (LNS). The LAC is the initiator of the tunnel and the LNS is the server. After a tunnel is established, the network traffic between the peers is bidirectional. The higher-level protocols pass through the tunnel and to facilitate this, an L2TP session (or call) is established within the tunnel for each higher-level protocol such as PPP. Either the LAC or LNS initiate sessions. The packets exchanged within an L2TP tunnel are categorized as either control packets or data packets.

Configure L2TP

Layer 2 Tunneling Protocol (L2TP) is disabled by default on the VPN Gateway.

Configuring L2TP

Perform the following procedure to configure L2TP:

1. Enable L2TP on the VPN Gateway.

>> Main#cfg/vpn 1/l2tp	(Select L2TP)
>> L2TP#ena	(Enable L2TP)

2. Reference Certificate Authority (CA) certificates used to sign the client certificates if the client certificates are used for VPN client authentication.

You can skip this step if the L2TP client must authenticate through user name, password, or group authentication.

You must store the Certificate Authority (CA) certificate on the VPN Gateway. For more information about certificate management, see *Users Guide*.

This setting applies to all user tunnels in the current VPN.

>> L2TP#cacerts	(Select CA certificates)
Current value: " "	(Current value appears)
Enter certificate numbers (separated by comma):	(Specify the certificate numbers)

3. Reference the server certificates if client certificates are used for VPN client authentication.

You can skip this step if the L2TP client must authenticate through user name, password, or group authentication.

You must store the server certificate on the VPN Gateway. For more information about certificate management, see *Users Guide*.

You can sign the server certificate with a trusted CA certificate.

This setting applies to all user tunnels in the current VPN.

>> L2TP#certs	(Select certificates)
Current value:unset	(Current value appears)
Enter certificate number(1-1500):	(Specify the certificate number)

4. Create an Internet Key Exchange (IKE) profile.

You can create several Internet Key Exchange (IKE) profiles with different settings for encryption, such as NAT traversal. You can usually the default settings for the IKE profile with the IPsec VPN client. For more information about commands on the IKE profile menu, see *Command Reference*.

>> L2TP#ikeprof	(Select the IKE profile)
Enter IKE profile number (1-64):	(Specify the IKE profile number)
Creating IKE Profile 1	(Creates the IKE profile)
Enter name of IKE profile:ike profile 1	(Specify the IKE profile name)

5. Create a user tunnel profile.

The user tunnel defines different criteria for the L2TP tunnel, for example, split tunneling, and client PC control. You can use the default settings for the user tunnel

profile with the L2TP client. For more information about the User tunnel profile menu, see *Command Reference*.

```
>> IKE Profile 1#.. /utunprof (Select User Tunnel)

Enter user tunnel profile number (1-64):1 (Specify profile number)

User Tunnel Profile 1

Enter name of tunnel profile:tunnel (Specify profile name)
profile 1

Enter name of IKE profile:ike profile 1 (Specify the IKE profile
name created)

<reference IKE profile here>
```

6. Map the user tunnel profile to the desired user access group.

Find the desired user access group and then reference the user tunnel profile created earlier. The group name entered by the remote user in the L2TP client must match the group name you select here.

```
>> User Tunnel Profile 1#/cfg/vpn 1/
aaa/group

Enter group number or name: (1-1023)1 (Specify group number or
name)

>> Group 1#l2tp (Select L2TP)

>> L2TP#utunnel (Select user tunnel)

Current value:" " (Displays the current user
tunnel profile)

Name of user tunnel profile:tunnel (Specify user tunnel profile
profile 1 name)
```

7. Enter the group secret (used for group authentication).

The group password entered by the remote user in the L2TP client must match the group secret configured here.

```
>> L2TP#secret

Current value: changeme (Displays the current group
secret)
```

```
Group secret:secret
```

(To change, specify group secret value)

8. Enter the authentication order.

```
>> L2TP#authorder
```

```
Current value: mschapv2, pap
```

(Displays the current authentication order)

```
Enter auth method order (comma separated):
```

(Press TAB to view the authentication order)

```
all pap chap mschapv1 mschapv2
```

Select one of the following as authentication order:

- all: All the authentication orders are selected.
- pap: Password Authentication Protocol (PAP) authenticates a user to a network access server. Point to Point Protocol (PPP) validates a user before allowing them access to server resources.
- chap: Challenge-Handshake Authentication Protocol (CHAP) authenticates a user or network host to an authenticating entity. Challenge-Handshake Authentication Protocol periodically verifies the identity of the client using a three-way handshake, at the time of establishing the initial link, and happens any time afterwards. The verification is based on a shared secret.
- mschapv1: Microsoft Challenge-Handshake Authentication Protocol (CHAP) Version 1 authenticates remote Windows workstations. MS-CHAP authenticators send an 8 octet challenge value field.
- mschapv2: MS-CHAP V2 authenticators send an 16 octet challenge value field.

! Important:

You must configure MSCHAPv1, CHAP or PAP as primary authentication for L2TP with Apple or Android clients. MS-CHAPv2 does not work for L2TP with Apple and Android clients.

9. Set the applicable Dynamic DNS Registration value. The default value is Enabled.

```
>> cfg/vpn <name>/ipsec/utunprof <name>/  
ddnsreg on/off
```

(Select on to enable or off to disable.)

10. Set the status of the Default Radius Group Binding Optional feature. The default setting is Disabled.

```
>> cfg/<vpn #>/ipsec/groupbind on/off
```

(Select on to enable or off to disable.)

11. Apply the changes.
12. Create an IP Pool for remote access.

For more information about creating an IP Pool, see [Create IP Pool](#) on page 323.

13. Create a default IP Pool.

For more information, see [Create a Default IP Pool](#) on page 330.

14. Map the IP Pool.

For more information, see [Map the IP Pool to User Group](#) on page 329.

 **Note:**

To support Active Directory server as authenticate server in L2TP, configure MS-CHAPv2 for LDAP connection on Active Directory server or disable any encrypted authentication method for L2TP.

Chapter 21: Transparent Mode

This chapter describes how to configure the Avaya VPN Gateway (AVG) for use with the Avaya SSL VPN client and the Avaya IPsec VPN client (formerly Contivity VPN client).

What is Transparent Mode?

The term "transparent" is mainly relevant from a user perspective. It means that the remote user will experience network access as if actually sitting within the corporate intranet. No Portal interaction is required.

As opposed to clientless mode, transparent mode requires the user to install one of the following VPN clients:

- The Avaya SSL VPN client
- The Avaya IPsec VPN client (formerly the Contivity VPN client)

The VPN Gateway will act as the VPN server.

Transparent mode supports access to the intranet through legacy TCP- or UDP-based client applications. The following features and services can be used:

- Intranet Web browsing without logging in to the Portal.
- Intranet mail server access through the remote user's native e-mail client software.
- Telnet and SSH access to intranet terminal servers through the remote user's native Telnet or SSH client software.
- Access to a wide range of intranet services built on legacy client/server technology.

Before you start configuring the AVG cluster, you should have performed the initial setup procedure (see the "Initial Setup" chapter in the *Users Guide*).

Avaya SSL VPN Client

As opposed to the Net Direct client (that can be downloaded for each user session and then removed), the SSL VPN client is permanently installed on the remote user's machine. Furthermore, it has a user interface and can be started without the user first having to log on to the Portal.

*** Note:**

From version 7.0 of the VPN Gateway software, the Net Direct client is also available as a client to be installed permanently on the remote user's machine. See [Net Direct](#) on page 87.

The SSL VPN client comes in different versions:

- The LSP (Layered Service Provider) client. Compatible with Windows 98, ME, NT (with IE 5 or later) 2000 and XP. This client does not support UDP. The client is capable of sending version number and OS version to the AVG, which means that untrusted client versions and clients running on untrusted operating systems can be filtered out.
- The TDI (Transport Driver Interface) client. Compatible with Windows 2000 and XP. This client supports UDP as well as TCP. The client is capable of sending version number and OS version to the AVG.
- Old clients, that is, LSP and TDI clients that are not capable of sending version number and OS version to the AVG.

Server Configuration

Start by following the basic instructions in Chapter 2, [Clientless Mode](#) on page 35, on how to set up a VPN. The same configuration applies to both clientless and transparent mode. Then continue with the following steps.

Enable the Desired Client Versions

You can enable or disable client access based on client version.

1. Enable the desired client version.

```
>> Main#cfg/vpn 1/sslclient

>> SSL VPN Client#tdiclient

Current value: off

Allow TDI vpn clients (on/off):on
```

- **tdiclient:** By setting this command to

on

, users with TDI clients installed are allowed to access the VPN. The **tdioslist** and **tdivsn** commands become visible.

- **lspclient:** By setting this command to

on

, users with LSP clients installed are allowed to access the VPN. The **lspolist** and **lspvpn** commands become visible.

- **oldclients:** By setting this command to

on

, users with older SSL VPN clients (that is, LSP/TDI clients that are not capable of sending version number and OS version to the AVG) are allowed to access the VPN.

2. Specify allowed operating systems.

Enter a comma separated list of allowed OSs, e.g. **winxp,win2k**. Only clients running on the specified operating systems will be allowed to connect.

```
>> SSL VPN Client#tdioslist
<or lspolist>

Current value: all
Enter list of allowed OSs for the tdi client:<press TAB to view options>

    all      unknown      winxp      win2k      generic_win
Enter list of allowed OSs for the tdi client:winxp,win2k
```

- **all:**

All client connections are allowed, irrespective of what OS the client runs on.

- **unknown:**

TDI/LSP clients running on an OS that cannot be identified (for example, new OS versions) are allowed to connect.

- **winxp:**

TDI/LSP clients running on Windows XP are allowed to connect.

- **win2k:**

TDI/LSP clients running on Windows 2000 are allowed to connect.

- **win98:**

LSP clients running on Windows 98 are allowed to connect.

- **winnt:**

LSP clients running on Windows NT are allowed to connect.

- **winme:**

LSP clients running on Windows ME are allowed to connect.

- **generic_win:**

TDI/LSP clients running on any other Windows version are allowed to connect.

- integer representing OS ID, e.g.

12:

If a TDI/LSP client tries to connect with an unknown OS version and fails, the log will include details of the client's OS in the form of OS ID number and description. By entering the OS ID number here, client connection will be allowed.

3. Specify minimum client version.

To restrict access to clients with a minimum version number, enter the desired version number.

```
>> SSL VPN Client#tdivsn
<or lspvsn>

Current value: 7.0.0.0
Enter minimum version of the tdi client:7.0.0.1

<example>
```

4. Apply the changes.

Enable Full Access

If not already active, the SSL VPN client can be started from the Portal's **Full Access** page (select **Full Access** on the **Access** tab). This however requires that the Full Access feature is enabled. When the SSL VPN client is started from the **Full Access** page, the remote users does not have to authenticate once again (in the SSL VPN client's login window) because they has already authenticated to the Portal.

For more information about starting the SSL VPN client from the **Full Access** page, see [The Portal from an End-User Perspective](#) on page 51.

1. Follow the instructions for enabling SSL VPN client access previously in this chapter.
2. Enable the Full Access feature for the desired VPN.

```
>> Main#cfg/vpn 1/portal

>> Portal#faccess

>> Full Access#ena
```

3. Apply the changes.

```
>> Full Access#apply
Changes applied successfully
```

*** Note:**

For the Full Access feature to work, the fully qualified domain name (FQDN) of the VPN Gateway must be specified as the server alias in the SSL VPN client (Servers tab>Add). See [4](#) on page 359.

Client Configuration

To ensure that all users (for example, in a specific user group) are provided with the same client settings, install the SSL VPN client and make the desired settings. When done, a configuration file in xml format can be exported and pasted into the CLI or the BBI (described further on). This makes the configuration available for download from the SSL VPN client, using the client's wizard.

This section describes how to configure the SSL VPN client. For options, buttons and so on that are not explained here, see the client's online help.

1. Install the SSL VPN client on your local machine. When installation is complete, the following screen is displayed:



2. Select **Manual configuration** and click **Finish**.
3. On the system tray, double-click the SSL VPN client icon.
The Properties for SSL VPN client window is displayed:
4. Select the **Servers** tab and click **Add**. The following screen is displayed.

5. In the Alias field, enter the VPN's fully qualified domain name (FQDN), e.g. vpn.example.com.

*** Note:**

For the Full Access feature (see page 310) to work with the SSL VPN client, the fully qualified domain name (FQDN) of the VPN Gateway must be specified in the Alias field. Arbitrary aliases like "My intranet" will not work.

6. In the Address field, enter the VPN's Portal IP address.

This IP address should be equivalent to the IP address specified with the `/cfg/vpn #/ips` command.

7. In the Port field, enter 443 (HTTPS) as port number.
8. If required, make the desired settings for firewall traversal.

For users working from a firewall-protected location, there are different options available for firewall traversal. By editing the server properties in the SSL VPN client, you will be able to configure the desired firewall traversal method. See the online help for detailed instructions.

9. Click **OK**, then **Apply**.
10. Select the **Name** redirection tab and click **Add**.

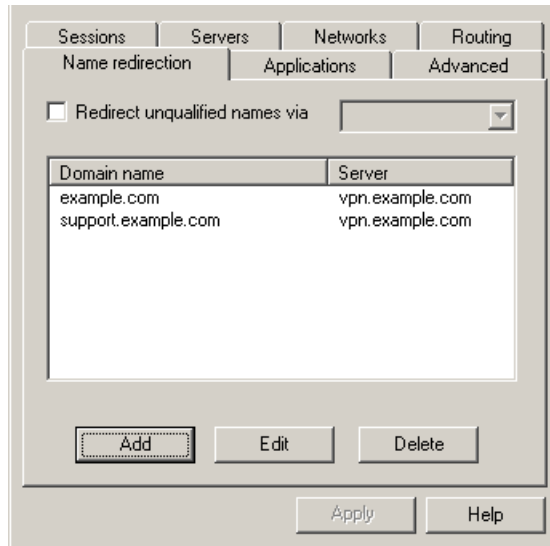
This screen lets you add a domain for redirection of requests to the VPN server.

Example: Enter the domain name **example.com**. This will force all traffic using **example.com** in the address through the VPN server.

Fully qualified domain names (FQDN) can also be used, e.g. **www.example.com**.

11. Click **OK**.
12. Add another domain in the same way.

The domain is added to the list on the **Name redirection** tab.



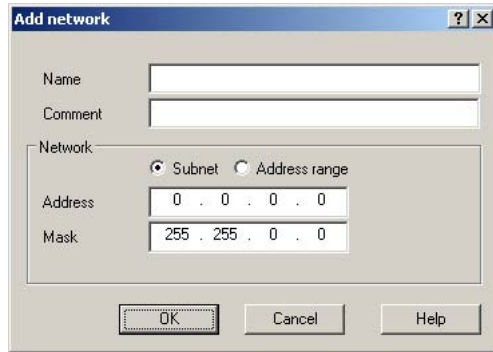
The most qualified domain name in this list will be tried first, irrespective of order.

Example: The domain name **support.example.com** is more qualified than **example.com**. When a domain name is given, the SSL VPN client will check if it matches the most qualified name first, because a less qualified name (like **example.com**) can match the given domain name in any case.

If the remote user requests a domain name that is not listed on the **Name redirection** tab, the client will perform a DNS lookup to resolve the name to an IP address. This IP address will be checked against the routing rules defined on the **Routing** tab (if any).

13. Click **Apply**.
14. To configure IP address routing, proceed to the Networks tab and click Add.

By configuring IP address routing you can specify whether requests to a specific network or address range should be redirected to the AVG server, blocked completely or passed through straight to its destination without the need to authenticate to the AVG server.



The 'Add network' dialog box contains the following fields and controls:

- Name:** A text input field.
- Comment:** A text input field.
- Network:** A section containing two radio buttons: **Subnet** (selected) and **Address range**.
- Address:** A text input field with the value '0 . 0 . 0 . 0'.
- Mask:** A text input field with the value '255 . 255 . 0 . 0'.
- Buttons:** 'OK', 'Cancel', and 'Help' at the bottom.

15. In the **Name** field, enter a suitable name for the network or address range.

This name will later be displayed on the Networks and Routing tabs.

16. In the **Comment** field, enter a description of the network (optional).

17. To register a specific network, select **Subnet**.

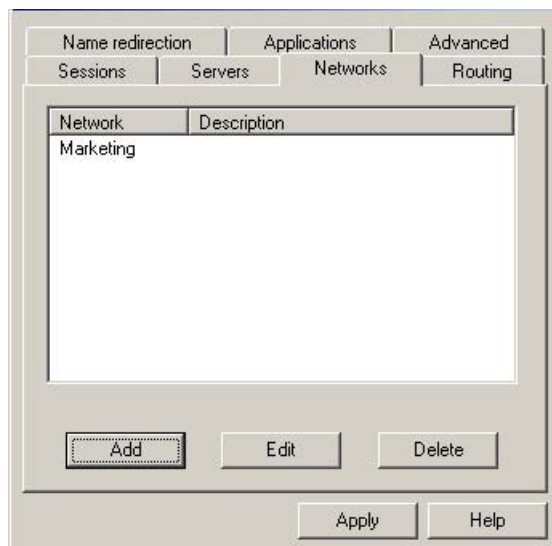
Then enter the network's IP address and subnet mask.

To register a range of networks, select Address range.

Then enter the desired address range in the **From** and **To** fields. Example: To cover the entire Internet, enter 0.0.0.0 in the **From** field and 255.255.255.255 in the **To** field.

18. Click **OK** and **Apply**.

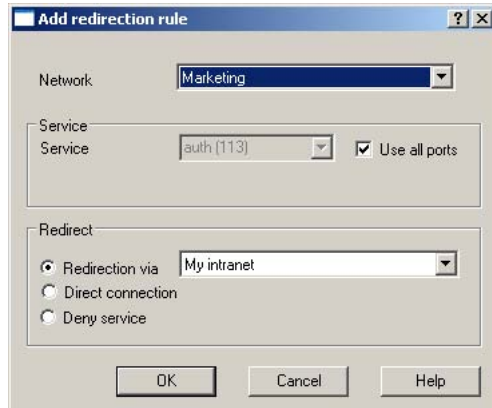
The network is added to the **Networks** tab.



The 'Networks' tab interface shows a table with two columns: 'Network' and 'Description'. The 'Network' column contains the text 'Marketing'. Below the table are buttons for 'Add', 'Edit', and 'Delete'. At the bottom of the window are 'Apply' and 'Help' buttons.

Network	Description
Marketing	

19. Proceed to the **Routing** tab and click **Add**.



20. In the Network list box, select the network for which you wish to add a routing rule.
21. To limit the routing rule to traffic to a specific TCP port, select the desired port in the Service list box (deselect the Use all ports check box first).

If the desired TCP port does not exist in the list, enter the TCP port number directly in the list box. If the routing rule applies to all TCP ports, keep the tick in the Use all ports check box.

22. In the Redirect area, select the desired redirection rule for requests to this network.

- Redirection through. Directs requests to the selected VPN Gateway for authentication, provided the IP address corresponds to selected network or address range.

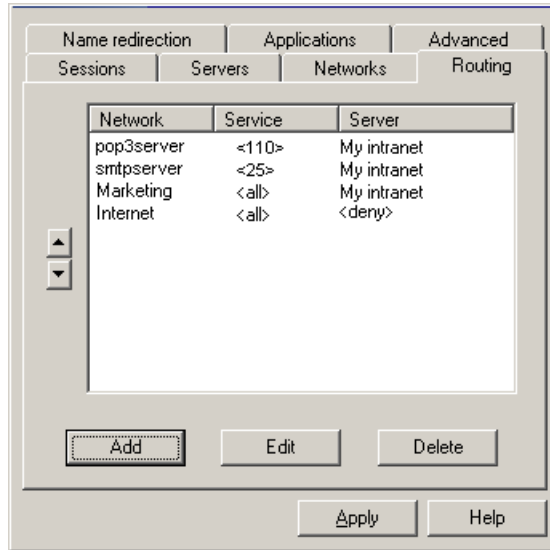
*** Note:**

Requests using domain names listed on the Name direction tab will always be directed to the VPN Gateway.

- Direct connection. Directs the request straight to its destination, without going through the secure VPN Gateway connection.
- Deny service. Any request with an IP address corresponding to a network or address range with this option selected will be denied.

23. Click **OK** and **Apply**.
24. Add another routing rule in the same way (start by defining the network or address range on the Networks tab).

The routing rules are displayed on the **Routing** tab.



The preceding routing rules say traffic destined for the intranet POP3 and SMTP mail servers as well as requests to the marketing network should be redirected through the VPN Gateway. Internet traffic is denied.

Export the Configuration File

When you have configured the SSL VPN client, you can export the configuration as an xml file and paste it into the CLI (or BBI).

1. Complete the configuration of the SSL VPN client and click **Apply**.
2. Select the **Advanced** tab and click the **Export config** button.
3. Save the file in xml format.

If needed, several configuration files can be produced and exported if different user groups have different requirements.

4. Open the xml file in a text editor, e.g. Notepad and copy the contents.
5. Paste the xml file into the CLI.

Having pasted the xml file, press ENTER to create a new line. Then type three periods (...) and press ENTER once again.

```
>> Main#cfg/vpn #/sslclient/xmlconfig
```

Write or paste the text, press Enter to create a new line, and then type "..."(without the quotation marks) to terminate.

```
> > <?xml version="1.0" encoding="utf-8" ?>
> <configuration name="XtraNet">
>   <global>
>     <unqualifiedNameResolution>vpn.example.com</unqualified
NameResolution>
>     <autoStart>1</autoStart>
```

```

> </global>
> <server name="vpn.example.com">
>   <hostname>10.1.82.146</hostname>
>   <port>443</port>
>   <firewall>
>     <method>0</method>
>   </firewall>
>   <security>
>     <ssl3>on</ssl3>
>     <tls1>off</tls1>
>     <ssl3ciphers>65535</ssl3ciphers>
>   </security>
> </server>
> <domain name=".example.com">
>   <server>vpn.example.com</server>
> </domain>
> <domain name=".support.example.com">
>   <server>vpn.example.com</server>
> </domain>
> </configuration>
> ...

>> SSL Client#

```

6. Apply the changes.

```

>> SSL Client#apply

Changes applied successfully.

```

The configuration is now available to remote users with the SSL VPN client installed. The configuration can be downloaded using the client's wizard (see next section). To install the client, the user must have administrator privileges.

Client Configuration Using Wizard

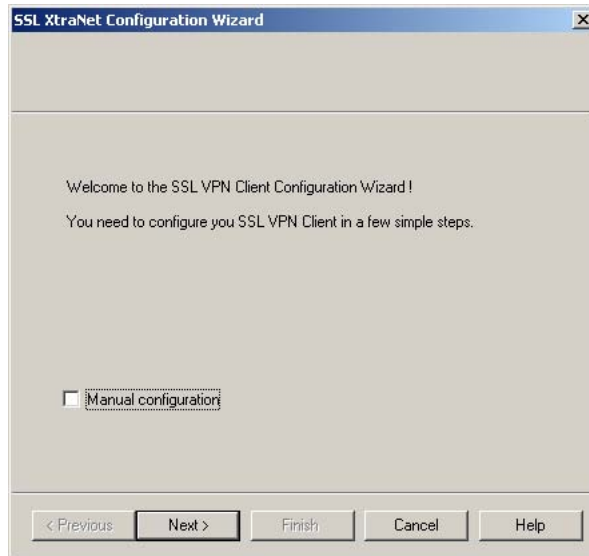
If a configuration file has been produced and the contents have been pasted into the CLI (or BBI), remote users can download the configuration from the VPN Gateway through the SSL VPN client's wizard.

Note that this requires the VPN Gateway to be configured with a portal server, which is normally the case. (An exception is the configuration example described in the section [Transparent Mode Without Portal](#) on page 382.)

The following instructions are directed to the remote user:

1. Install the SSL VPN client.

The wizard is displayed as the first screen.



2. If not, open the wizard by double-clicking the SSL VPN client icon on the system tray, go to the **Advanced** tab and click the **Wizard** button.
3. Click **Next**.
4. Specify the VPN's Portal IP address or domain name.
5. Click **Next**.

The configuration is imported from the VPN Gateway.

SSL VPN Client from a User Perspective

1. Start the SSL VPN client.

Double-click the SSL VPN client icon on your desktop or select the SSL VPN client program from the Start menu.

The SSL VPN client icon appears on the system tray.

2. Connect to the desired server by entering a domain name or IP address in a TCP- or UDP-based application, for example, a web browser.

The SSL VPN client checks if the requested destination matches a domain name, network or IP address range configured in the SSL VPN client. If so, and if the client's routing rules say that requests for this network should be redirected to the VPN Gateway server for authentication, the following dialog box appears:



3. Enter your user name and password and click **OK**.

Supplied credentials are checked against the configured authentication scheme, for example, RADIUS or the VPN's local authentication database.

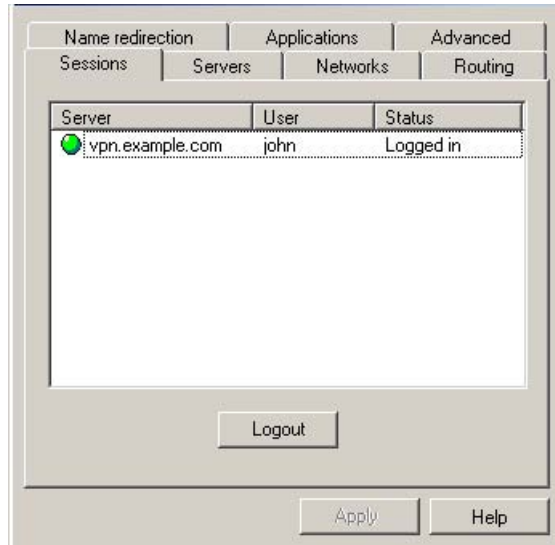
The **Service** list box may contain options for directing the user to a specific authentication database if several such databases exist in the configuration. In the CLI, this is configured in using the `/cfg/vpn #/aaa/auth #/display` command.

When the remote user is successfully authenticated, a secure SSL tunnel is set up between the remote user's machine and the VPN Gateway. The requested resource is displayed (for example, an intranet web page). If the user is not authorized to the resource, an error message will be displayed instead. If the requested address does not match a domain name, network or IP address range configured in the client, the user is directed straight to the destination without passing the VPN Gateway.

4. To logout from the VPN session, right-click the SSL VPN client icon on the system tray and select Properties.

The Properties for SSL VPN Client window is displayed.

5. Select the **Sessions** tab.



The name of the logged in user is displayed.

6. Click **Logout**.

*** Note:**

The remote user is automatically logged out from the session if the idle timeout or maximum session length values are exceeded. These values can be specified on VPN level (using the `/cfg/vpn #/aaa/idlettl` and `sessionttl` commands), on group level (using the `/cfg/vpn #/aaa/group #/idlettl` and `sessionttl` commands) or on extended profile level (using the `/cfg/vpn #/aaa/group #/extend #/idlettl` and `sessionttl` commands).

Avaya IPsec VPN Client

For users with the Avaya IPsec VPN client (formerly the Contivity VPN client) installed, access to intranet resources can be made available through the VPN Gateway through a secure IPsec connection.

Server Configuration

To enable use of the IPsec VPN client, follow the instructions in [Clientless Mode](#) on page 35. The same basic configuration steps for setting up a VPN applies to both clientless and transparent mode. Then continue with the following steps.

*** Note:**

User name and password authentication is only supported if the user exists in the AVG 's local database.

Enable IPsec

IPsec connectivity is disabled by default on the VPN Gateway.

Another way of configuring IPsec is to use the IPsec Quick Setup wizard (`/cfg/vpn # /ipsec/quick`).

1. Enable IPsec on the VPN Gateway.

This step enables IPsec tunnel encryption mode. Transport mode is not supported by the AVG software.

```
>> Main#cfg/vpn 1/ipsec
>> IPsec#ena
```

2. If client certificates are used for VPN client authentication, reference the CA certificate(s) that was used to sign the client certificate(s).

This step can be skipped if the IPsec VPN client should authenticate through user name/password or group authentication.

The CA certificate must be stored on the VPN Gateway. For detailed information about certificate management, see the "Certificates and Client Authentication" chapter in the *Users Guide*.

This setting will apply to all user tunnels in the current VPN.

```
>> IPsec#cacerts

Current value: " "

Enter certificate numbers (separated by comma):
```

3. If client certificates are used for VPN client authentication, reference the server certificate.

This step can be skipped if the IPsec VPN client should authenticate through user name/password or group authentication.

The server certificate must be stored on the VPN Gateway. For detailed information about certificate management, see the "Certificates and Client Authentication" chapter in the *Users Guide*.

The server certificate must be signed by a CA certificate that is a trusted CA certificate on the client machine.

This setting will apply to all user tunnels in the current VPN.

```
>> IPsec#cert

Current value:unset

Enter certificate number (1-1500):
```

4. Create an IKE profile.

This step creates an IKE profile. If needed, several different IKE profiles can be created with different settings for encryption, NAT traversal and so on. The default settings for the IKE profile are usually fine for use with the IPsec VPN client. For detailed information about available commands on the IKE profile menu, see the *Command Reference*.

```
>> IPsec#ikeprof

Enter IKE profile number (1-64):1

Creating IKE Profile 1
Enter name of IKE profile:ike profile 1
```

5. Create a user tunnel profile.

This step creates a user tunnel profile. The user tunnel defines different criteria for the IPsec tunnel, for example, split tunneling, client PC control and so on. The default settings for the user tunnel profile are usually fine for use with the IPsec VPN client. For detailed information about available commands on the User tunnel profile menu, see the *Command Reference*.

When prompted for the IKE profile name, press TAB to view available profiles.

```
>> IKE Profile 1#.. /utunprof

Enter user tunnel profile number (1-64):1

Creating User Tunnel Profile 1
Enter name of tunnel profile:tunnel profile 1

Enter name of IKE profile:ike profile 1

<reference IKE profile here>
```

6. Map the user tunnel profile to the desired user access group.

Find the desired user access group and reference the user tunnel profile you have previously created. The group name entered by the remote user in the IPsec VPN client should match the group name selected here. When prompted for the user tunnel profile name, press TAB to view available profiles.

```
>> User Tunnel Profile 1#/cfg/vpn 1/aaa/group

Enter group number or name: (1-1023)1

>> Group 1#ipsec

>> IPsec#utunnel

Current value: " "

Name of user tunnel profile:tunnel profile 1
```

7. Enter the group secret (used for group authentication).

The group password entered by the remote user in the IPsec VPN client should match the group secret configured here.

```
>> IPsec#secret

Current value: changeme

Group secret:secret
```

8. Apply the changes.

Create IP Pool

The IP pool comes into play when the remote user tries to access a host using the Avaya IPsec VPN client. A new IP address has to be assigned as source IP for the unencrypted connection between the VPN Gateway and the destination host. Optionally, specific network attributes for this connection can also be defined.

Several IP pools can be configured, each with a unique ID number and unique properties. By mapping the desired IP pool to a user group, you can create different methods for IP address and network attributes assignment for different user groups.

One of the configured IP pools should be selected as the default IP pool for the VPN. Groups for which no IP pool is assigned (IP pool number=0) will use the default IP pool.

The IP pools are used to assign IP addresses for Net Direct access as well (see [Net Direct](#) on page 87). If you have already configured an IP pool for use with Net Direct, this pool can also be used for the IPsec VPN client.

Create the IP pool.

Network attributes (including IP address) can be assigned either locally (from the AVG), from an external RADIUS server or from an external DHCP server.

When you configure an IP pool for the first time, you will enter a wizard. Depending on the choice you make for pool mechanism (that is,

```
local  
,  
radius  
or  
dhcp
```

), different questions will be displayed in the wizard.

```
>> Main#/cfg/vpn 1/ippool  
  
Enter Pool number or name (1-1023):1  
  
Creating Pool 1  
Select one of local, radius, dhcp:  
  
<select the desired pool mechanism here>
```

The pool mechanism setting is equivalent to the **type** command in the Pool menu.

You can associate an IP pool with a particular host in a clustered environment. For more information, see [Configure host IP pool](#) on page 330.

Configure IP Address Range and Local Network Attributes

If you set the pool mechanism to

```
local
```

, you should configure the desired IP address range. You can also configure network attributes to be retrieved from the AVG when the client connects.

If you set the source of IP assignment to

```
radius
```

```
or
```

```
dhcp
```

, continue with the relevant section (see the following pages) instead.

1. Configure an IP address range.

```
Set the lower ip for the pool range:10.1.82.140  
  
Set the upper ip for the pool range:10.1.82.150
```

2. If needed, change the default proxy ARP setting.

```
Set proxyarp (on/off/all) [on]:
```

- **on:**

Means that the VPN Gateway that handed out the IP address (from the IP pool) for a specific client connection will respond to ARP requests on behalf of the IPsec VPN client for return traffic. The VPN Gateway then acts as a router and forwards IP packets to the client through the existing tunnel. Proxy ARP is used on all interfaces for the relevant VPN except the traffic interface. This is the default setting.

- **off.**

Return traffic will not be able to reach its destination unless specific routes are configured.

- **all.**

Same as

on

but proxy ARP is used on all interfaces.

3. Configure network attributes (optional).

The Net Direct client normally works fine without adding specific network attributes. You can however specify the desired attributes on the Network attributes menu if needed.

```
>> Pool 1#netattr
```

- **netmask:**

Sets the network mask for the client. The network mask should cover the IP address range specified in step 1. The default network mask is

255.255.255.0

.

- **primary/secondary NBNS server:**

Sets the IP address of a primary NBNS server (NetBIOS Name Server). Used if the IPsec VPN client should use a specific NBNS server to have computer names resolved into IP addresses. NBNS servers provide WINS (Windows Internet Naming Service) which is part of the Microsoft Windows NT server environment.

- **primary/secondary DNS server:**

Sets the IP address of a primary DNS server. Use this command if the IPsec VPN client should use a specific DNS server to have domain names resolved into IP addresses. If no (primary or secondary) DNS server is specified here, the DNS server specified for the VPN to which the remote user belongs will be

used. The command to use is `/cfg/vpn #/adv/dns/servers`. (This option is only possible if a Secure Services Partitioning license is loaded). If only a default DNS server is specified (using the `/cfg/sys/dns/servers` command), this will be used.

- name of client DNS domain:

Lets you specify the name of the domain used while an IPsec user tunnel is connected. It ensures that domain lookup operations point to the correct domain. This is particularly important for clients that use Microsoft Outlook or Exchange, to ensure that the mail server is mapped to the correct domain.

4. Enable the IP Pool.

```
>> Pool 1#ena
```

5. Apply the changes.
6. The next step is to map the IP pool to a group, or make it the default IP pool for the VPN.

Continue with the section [Map the IP Pool to User Group \(Optional\)](#) on page 96.

Configure RADIUS IP Pool

If you set the pool mechanism to radius (as described in the section [Create IP Pool](#) on page 90), you should configure the VPN Gateway to retrieve network attributes from a RADIUS server.

How to configure a RADIUS server is described in the section [RADIUS Authentication](#) on page 119 in [Authentication Methods](#) on page 117.

To configure the VPN Gateway to retrieve network settings (including client IP address) through RADIUS attributes from an external RADIUS server, use the `/cfg/vpn #/aaa/auth # /radius/netattr` command. A minimum requirement is to configure retrieval of client IP address and primary DNS server. You can retrieve a number of network attributes, for example, primary/secondary DNS server, primary/secondary NBNS server and so on.

The following instructions assume that you continue with the IP pool wizard after having chosen

radius

as the pool mechanism.

1. If needed, change the default proxy ARP setting.

```
Set proxyarp (on/off/all) [on]:
```

- on:

Means that the VPN Gateway that handed out the IP address (from the IP pool) for a specific client connection will respond to ARP requests on behalf of the

IPsec VPN client for return traffic. The VPN Gateway then acts as a router and forwards IP packets to the client through the existing tunnel. Proxy ARP is used on all interfaces for the relevant VPN except the traffic interface. This is the default setting.

- `off`.

Return traffic will not reach its destination unless specific routes are configured.

- `all`.

Same as

`on`

but proxy ARP is used on all interfaces.

2. Enable the IP Pool.

```
>> Pool 1#ena
```

3. Configure fallback network attributes (optional).

```
>> Pool 1#netattr
```

For IP pools of the

`radius`

and

`dhcp`

types, network attributes can be configured on the AVG as fallback values if the RADIUS or DHCP server does not return a specific setting for a network attribute. This is done in the same way as for IP pools of the

`local`

type (see [3](#) on page 373 on [3](#) on page 373 for instructions).

4. Apply the changes.
5. The next step is to map the IP pool to a group, or make it the default IP pool for the VPN.

Continue with the section [Map the IP Pool to User Group \(Optional\)](#) on page 96.

Configure DHCP IP Pool

If you set the pool mechanism to

dhcp

(as described in the section [Create IP Pool](#) on page 90, you should configure to retrieve network attributes from a DHCP server.

The following instructions assume that you continue with the IP pool wizard after having chosen

dhcp

as the pool mechanism.

1. Configure the external DHCP server IP address.

```
Entering: DHCP menu
Entering: DHCP servers menu
DHCP server IP address: 10.1.82.100
Leaving: DHCP servers menu
```

2. If needed, change the default proxy ARP setting.

```
Set proxyarp (on/off/all) [on]:
```

- on:

Means that the VPN Gateway that handed out the IP address (from the IP pool) for a specific client connection will respond to ARP requests on behalf of the IPsec VPN client for return traffic. The VPN Gateway then acts as a router and forwards IP packets to the client through the existing tunnel. Proxy ARP is used on all interfaces for the relevant VPN except the traffic interface. This is the default setting.

- off.

Return traffic will not reach its destination unless specific routes are configured.

- all.

Same as

on

but proxy ARP is used on all interfaces.

3. Enable the IP Pool.

```
>> Pool 1#ena
```

4. Configure fallback network attributes (optional).

```
>> Pool 1#netattr
```

For IP pools of the

radius

and

dhcp

types, network attributes can be configured on the AVG as fallback values if the RADIUS or DHCP server does not return a specific setting for a network attribute. This is done in the same way as for IP pools of the

local

type (see [3](#) on page 373 for instructions).

5. Apply the changes.

The next step is to map the IP pool to a group, or make it the default IP pool for the VPN. Continue with the next section.

Map the IP Pool to User Group

As mentioned on [Create IP Pool](#) on page 90, several IP pools with different mechanisms (that is,

local

,

radius

or

dhcp

) can be configured. By mapping the IP pools to different user groups you can provide different ways of assigning IP address and network attributes depending on the user's group membership.

One of the configured IP pools should be selected as the default IP pool for the VPN. Groups for which no IP pool is assigned (IP pool number=0) will use the default IP pool. How to create a default IP pool is described in the next section.

This is how to map an IP pool to a user group:

1. Map the IP pool to the desired user group.

```
>> Main#cfg/vpn 1/aaa/group 1/ippool
```

```
Current value: 0
IP pool number:1
```

2. Map the next IP pool to another group in the same way.
3. Apply the changes.

Create a Default IP Pool

One of the configured IP pools should be selected as the default IP pool for the VPN. Groups for which no IP pool is assigned (IP pool number=0) will use the default IP pool.

1. Configure an existing IP pool as the default IP pool.

```
>> Main#cfg/vpn 1/aaa/defippool

Current value: 0
IP pool number:1
```

2. Apply the changes.

Enable Full Access Tab

If not already active, the user can launch the IPsec VPN client from the **Full Access** page by selecting **Full Access** on the Portal's **Access** tab. This however requires that the Full Access feature is enabled. The client is started in the background and instructed to connect to an Avaya VPN Router server (in

contivity

IPsec mode) or to the VPN Gateway (in

native

IPsec mode). The remote user does not have to authenticate once again because they have already authenticated to the Portal.

For more information about starting the IPsec VPN client from the **Full Access** page, see [The Portal from an End-User Perspective](#) on page 51.

1. Follow the instructions for enabling IPsec VPN client access previously in this chapter.

Note that this is not required if users are to run the IPsec VPN client towards an Avaya VPN Router (formerly Contivity).

2. Enable Full Access for the desired VPN.

```
>> Main#cfg/vpn 1/portal
>> Portal#faccess
>> Full Access#ena
```

3. Select IPsec mode.

To instruct the Avaya IPsec VPN client to connect to an Avaya VPN Router (formerly Contivity), select

```
contivity
```

mode. Then proceed to [4](#) on page 379.

To instruct the client to connect to the VPN Gateway, select

```
native
```

mode. This completes the Full Access configuration. Apply the changes.

```
>> Full Access#ipsecmode
Current value: native
Enter ipsec mode (native/contivity)
```

4. Configure the VPN Router server IP address.

The following steps are only required if

```
contivity
```

IPsec mode is selected in step [3](#) on page 379.

```
>> Full Access#Contip
Current value: 0.0.0.0
Enter Contivity IP address:
<VPN Router IP address>
```

5. For group authentication to the VPN Router, configure the desired user group name.

```
>> Full Access#Contid
Current value: " "
Enter Contivity group ID:
```

6. Enter the shared secret used for group authentication.

```
>> Full Access#Contpass

Current value: " "

Enter Contivity group password:
```

7. Apply the changes.

```
>> Full Access#apply

Changes applied successfully
```

Client Configuration

The Avaya IPsec VPN client can authenticate to the VPN Gateway in three ways:

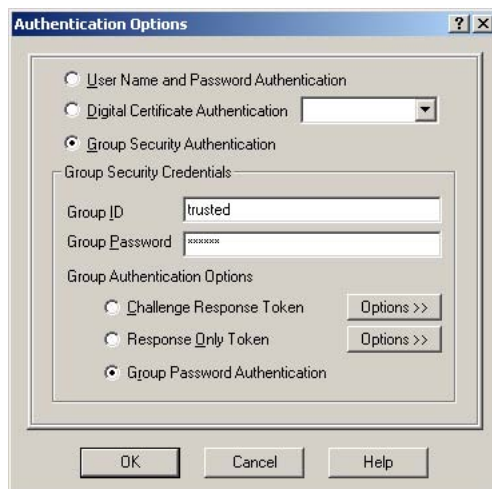
- Group authentication
- User name and password authentication
- Client certificate authentication

Group Authentication

1. Create a new profile on the IPsec VPN client.

On the **File** menu, select **New** and enter an appropriate connection name along with user name and password. In the **Destination** field, enter the VPN's IP address or DNS name.

2. On the **Options** menu, select **Authentication Options**.



3. Select the **Group Security Authentication** option.
4. In the **Group ID** field, enter the name of the user group.
5. In the **Group Password** field, enter the shared secret created in the section [Server Configuration](#) on page 368.
6. Under **Group Authentication Options**, verify that Group Password Authentication is selected.
7. Click **OK**.
8. Click **Save**.

User Name and Password Authentication

1. Create a new profile on the IPsec VPN client.
On the **File** menu, select **New** and enter an appropriate connection name along with user name and password. In the **Destination** field, enter the VPN's IP address or DNS name.
2. Click **Save**.

 **Note:**

User name and password authentication is only supported if the user exists in the AVG's local database.

Client Certificate Authentication

1. Create a new profile on the IPsec VPN client.
On the **File** menu, select **New** and enter an appropriate connection name along with user name and password. In the **Destination** field, enter the VPN's IP address or DNS name.
2. On the **Options** menu, select **Authentication Options**.
3. Select the **Digital Certificate Authentication** option.
4. In the list box to the right, select **MS CAPI**.
5. Click **OK**.
The IPsec VPN client's main window is redisplayed. The **User Name** field is now changed to **Certificate**.
6. Next to the Certificate field, click the icon depicted in the following steps and select **Open**.



Available client certificates are displayed.

7. Select the desired client certificate and click **OK**.
8. Click **Save**.

Transparent Mode Without Portal

If both Portal and SSL VPN client support is the desired option, it is sufficient to follow the configuration instructions in [Clientless Mode](#) on page 35 and [Avaya SSL VPN Client](#) on page 355 in this chapter.

If you wish to configure the AVG cluster to support the SSL VPN client software exclusively, that is, eliminate support for the Portal, follow the instructions in this chapter. First however, you should read the section [Avaya SSL VPN Client](#) on page 355 in this chapter. Note that the portal-less configuration does not support automatic download of the configuration using the SSL VPN client wizard.

The following diagram shows how transparent mode is implemented and used.

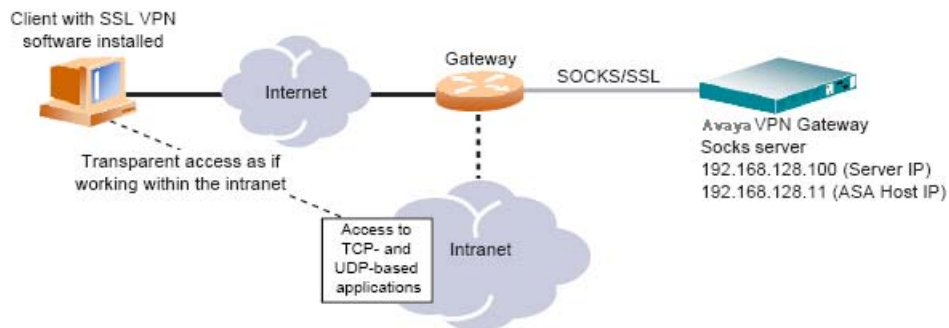


Figure 8: VPN in Transparent Mode Without Portal

Configure a VPN

1. Create a VPN.

The IP address you are prompted for here relates to a portal server, which is automatically created when you create a VPN. In this configuration example we will configure a SOCKS server instead, because portal support should not be enabled.

```
# /cfg/vpn 1
```

```

Creating VPN 1

Enter server ips (comma separated):<press ENTER to skip>

Clear list? (yes/no) [no]:<press ENTER>

```

2. Disable the portal server.

```

>> VPN 1#server

>> Server#dis

```

3. Apply your changes

```

>> Server#apply

Changes applied successfully

```

Create and Configure a SOCKS Server

Only one VPN can be mapped to a socks server so if you plan to use several VPNs, you will have to create several different virtual SSL servers of the socks type.

1. Create a virtual SSL server of the SOCKS type.

This step creates a virtual server on the VPN Gateway. Each virtual server listens to a specific TCP port and is connected to an IP address in the virtual server's IP list.

Specify a virtual server number not currently in use by an existing virtual server. To view the numbers and related names of all configured virtual servers in the AVG cluster, use the **/info/servers** command.

```

# /cfg/ssl/server

Enter virtual server number: (1-)1

Creating new server 1#

```

2. Specify the type of virtual server.

This step specifies that virtual server 1 is a server of the socks type. When the server type is changed to socks, the default listen port number value will automatically be changed to 1080.

```

>> Server 1#type

```

```
Current value: generic
Type (generic/http/socks):socks
```

3. Specify the certificate to be used by the socks server.

You are prompted to type the index number of an existing certificate. To view all certificates currently added to the AVG by index number and name, use the **/info/certs** command. For more information about how to add a certificate to the AVG, see the "Certificates and Client Authentication" chapter in the *Users Guide*.

```
>> Server 1#ssl
>> SSL Settings#cert
Current value: <not set>
Enter certificate number: (1-1500)1
```

* Note:

If the certificate you specify is a chained certificate, you need to first add the CA certificates up to and including the root CA certificate, and then specify the CA certificate chain of the server certificate. For more information about how to construct the server certificate chain, see the **cachain** command under "SSL Server SSL Configuration" in the *Command Reference*.

4. Configure the DNS settings for the socks server.

This step specifies the default DNS domain name for the socks server. Typically, the default DNS domain can be derived from the fully qualified domain name that is registered in DNS for the virtual server IP (VIP) address.

A DNS search domain can also be specified. The search domain(s) you specify is automatically appended to the host names a remote user types in the various address fields in legacy applications (provided a match is found).

```
>> SSL Settings#../dns
>> DNS Settings#search
Current value: " "
Enter search domains (separated by comma):example.com
```

5. Map the socks server to a VPN.

This step maps the socks server to the configured VPN.

```
>> DNS Settings#../socks
>> Socks Settings#vpn
Current value: " "
Enter vpn number: (1-256)1
```

6. Apply the changes.

```
>> Socks Settings#apply
Changes applied successfully.
```

Configure the Socks Server for Standalone Mode

When the VPN Gateway is used without an Application Switch, the server must be set to standalone mode.

1. Enable stand-alone mode for the socks server.

```
# /cfg/ssl/server 1/standalone
Current value: off
Standalone mode (on/off):on
```

2. Configure the IP address of the socks server.

```
>> Server 1#vips
Current value: " "
Enter server ips (comma separated):
<IP address>
```

3. Apply the changes.

```
>> Server 1#apply
Changes applied successfully
```

Now you have created the basis for transparent mode access without a portal. What remains to be done is to configure one or more authentication methods, add user groups with access rules and configure the SSL VPN client to connect to the AVG cluster.

Transparent Mode without Portal but with Application Switch

When the AVG is used for SSL acceleration, it typically requires support of an Application Switch for traffic redirection. With this setup, standalone mode should not be enabled. Only one VIP can be assigned to the virtual SSL server and this VIP should be mapped to the Application Switch.

If you want to deploy the VPN feature with an Application Switch, you need to modify the AVG configuration described earlier in the previous section.

This configuration example assumes that you have two AVGs in the cluster, and that the AVGs are connected to an Application Switch.

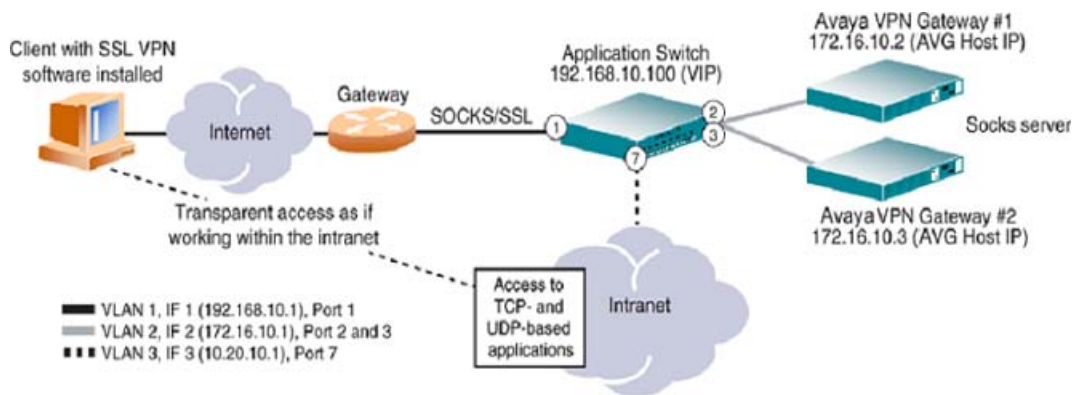


Figure 9: VPN in Transparent Mode without Portal but with Application Switch

Configure the AVG

1. Disable standalone mode if it is currently enabled.

```
# /cfg/ssl/server 1/standalone
Current value: on
Standalone mode (on/off):off
```

2. Apply the changes.

```
>> Server 1#apply
```

Configure the Application Switch

Create the Necessary VLANs

In this configuration, there will be three VLANs: VLAN 1 for the Application Switch that connects to the Internet, VLAN 2 for the AVG devices, and VLAN 3 for the intranet. Because VLAN 1 is the default, only VLAN 2 and VLAN 3 requires additional configuration.

1. Configure VLAN 2 to include Application Switch ports leading to the AVG devices.

```
# /cfg/vlan 2
>> VLAN 2#add 2
Port 2 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]:Y
>> VLAN 2#add 3
Port 3 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]:Y
>> VLAN 2#ena
```

2. Configure VLAN 3 to include the Application Switch port leading to the intranet.

```
# /cfg/vlan 3
>> VLAN 3#add 7
Port 7 is an UNTAGGED port and its current PVID is 1.
Confirm changing PVID from 1 to 2 [y/n]:Y
```

3. Disable Spanning Tree Protocol (STP) for the AVG ports 2 and 3.

```
# /cfg/stp/port 2
>> Spanning Tree Port 2#off
>> Spanning Tree Port 2#../port 3
>> Spanning Tree Port 3#off
```

Configure One IP Interface for Each VLAN

1. Configure an IP interface for client traffic on the Application Switch with VLAN 1.

```
# /cfg/ip/if 1

>> IP Interface 1#addr 192.168.10.1

>> IP Interface 1#mask 255.255.255.0

>> IP Interface 1#broad 192.168.10.255

>> IP Interface 1#vlan 1

>> IP Interface 1#ena
```

*** Note:**

If you prefer, you can reverse the order of the first two commands (**add** and **mask**) in the following example. By entering the mask first, the Application Switch will automatically calculate the correct broadcast address for you. The calculated broadcast address is displayed immediately after you provide the IP address of the interface, and will be applied together with the other settings when you execute the **apply** command.

2. Configure an IP interface for AVG traffic with VLAN 2.

```
# /cfg/ip/if 2

>> IP Interface 2#addr 172.16.10.1

>> IP Interface 2#mask 255.255.0.0

>> IP Interface 2#broad 172.16.255.255

>> IP Interface 2#vlan 2

>> IP Interface 2#ena
```

3. Configure an IP interface for intranet traffic with VLAN 3.

```
# /cfg/ip/if 3

>> IP Interface 3#addr 10.20.10.1

>> IP Interface 3#mask 255.255.255.0

>> IP Interface 3#broad 10.20.10.255
```

```
>> IP Interface 3#vlan 3
>> IP Interface 3#ena
```

4. Apply the changes.

```
# apply
```

*** Note:**

Make sure the VPN Gateways are configured to use the IP address of IP interface 2 on VLAN 2 as their default gateway. For more information about gateway configuration, see the **gateway** command under "iSD Host Configuration" in the *Command Reference*.

Configure the AVG Load Balancing Parameters

Set and enable the IP addresses of the VPN Gateways, and create a group in the switch for load balancing.

1. Define each VPN Gateway as a real server and specify the real server IP address.

The real server IP (RIP) addresses you specify in this case correspond to the IP address you assigned to each VPN Gateway during the initial setup. To view the real IP address of each VPN Gateway in the cluster, you can use the **/info/isdlist** command

```
# /cfg/slb/real 1
>> Real server 1#rip 172.16.10.2
>> Real server 1#ena
>> Real server 1#../real 2
>> Real server 2#rip 172.16.10.3
>> Real server 2#ena
```

2. Create a real server group and add the real servers (the VPN Gateways in this case) to the group.

```
# /cfg/slb/group 1
>> Real server group 1#add 1
```

```
>> Real server group 1#add 2
```

3. Set the load balancing metric and health check type for real server group 1.

```
# /cfg/slb/group 1

>> Real server group 1#metric hash

>> Real server group 1#health sslh
```

4. Set and enable the IP address for Virtual Server 1, enable service on port 1080 (socks), and assign server group 1 (the VPN Gateways) to this service.

```
# /cfg/slb/virt 1

>> Virtual Server 1#vip 192.168.10.100

>> Virtual Server 1#ena

>> Virtual Server 1#service 1080

>> Virtual Server 1 1080 Service#group 1
```

5. Enable client processing on port 1 leading to the Internet.

```
# /cfg/slb/port 1

>> SLB Port 1#client ena
```

6. Turn on Layer 4 processing.

```
# /cfg/slb/on
```

7. Apply the changes.

```
# apply
```

Configure Filters, Apply and Save the Application Switch Configuration

1. Create a filter to redirect client SOCKS traffic intended for port 1080 on the Virtual Server IP (VIP) address.

When this filter is added to the switch port leading to the Internet, incoming socks traffic destined for the virtual server IP address is redirected to the VPN Gateways in real server group 1.

```
# /cfg/slb/filt 100
>> Filter 100#dip 192.168.10.100
>> Filter 100#dmask 255.255.255.255
>> Filter 100#proto tcp
>> Filter 100#dport 1080
>> Filter 100#action redir
>> Filter 100#group 1
>> Filter 100#rport 1080
>> Filter 100#ena
```

2. Create a default filter to allow all other traffic.

```
# /cfg/slb/filt 224
>> Filter 224#sip any
>> Filter 224#dip any
>> Filter 224#proto any
>> Filter 224#action allow
>> Filter 224#ena
```

3. Add the filters to the client port leading to the Internet.

This step adds the HTTPS redirect filter and the default allow filter to the client port leading to the Internet.

```
# /cfg/slb/port 1
>> SLB Port 1#add 100
>> SLB Port 1#add 224
>> SLB Port 1#filt ena
```

4. Apply and save the Application Switch configuration changes.

```
# apply # save
```


Chapter 22: Configure Portal Guard

The Portal Guard feature is an easy way of "converting" an existing HTTP site to generate HTTPS links, secure cookies and so on. The Avaya VPN Gateway (AVG) will not only handle the SSL processing but also see to it that all existing web links are rewritten to HTTPS. This eliminates the need to rewrite each link manually.

This feature can for example, be used to accelerate an existing web Portal or any HTTP site where SSL offload and HTTP to HTTPS rewrite is the desired option. This site and any web sites or web applications launched from the site will now be available from the Internet through the VPN Gateway. All client traffic will be protected with SSL and internal applications and sites do not need to be modified to support access from Internet clients. Access rules are used to limit which internal sites can be reached through Portal Guard.

When the Portal Guard feature is used, the AVG's authentication system is turned off. To access the backend web server, the remote user should enter the SSL VPN Portal's IP address or host name. The user will then be redirected to the backend web server for authentication, without first having to log in to the SSL VPN Portal.

* Note:

The Portal Guard feature is only available if a Portal Guard license has been loaded.

HTTP to HTTPS Rewrite

Using Portal Guard, any link that the remote user clicks while being logged in to the backend server is rewritten to include the AVG rewrite prefix.

Both relative site links (e.g. `/site/file.html`) and absolute site links (e.g. `http://inside.example.com/site/file.html`) will be rewritten.

The AVG rewrite prefix (boldface) is added to the link properties as shown in the following sections: `https://vip.example.com/http/inside.example.com/site/file.html`

Initial Setup

Before enabling the Portal Guard feature you should perform an initial setup of the system. Set up the system as a one-armed configuration and run the VPN Quick Setup wizard. The initial setup procedure is described in Chapter 3, "Initial Setup" in the *Command Reference*.

Running the VPN Quick Setup wizard will provide you with a basic configuration including a test user and a test certificate so that you can test that the SSL VPN Portal is accessible. To view the other settings provided by the wizard, see [Clientless Mode](#) on page 35.

Add a Signed Server Certificate to the AVG

The "Certificates and Client Authentication" chapter in the *Users Guide* provides all the information you need for generating certificate signing requests, adding certificates to the AVG, generating and revoking client certificates, as well as configuring the AVG to require client certificates.

When the signed server certificate has been added to the AVG, it should be mapped to the portal server. The certificate (1) that is currently mapped to your portal server is a test certificate. Type in the number corresponding to the signed certificate that you have added to the AVG.

```
# /cfg/vpn 1/server/ssl

>> SSL Settings#cert

Current value: 1

Enter certificate number: (1-1500)2
```

Update DNS Server

The local DNS server should be updated with the domain name used for the VPN, and be configured to perform reverse DNS lookups.

License Key

To enable the Portal Guard feature in the AVG software, a license key must be obtained from Avaya. To obtain the license keys, you have to provide the MAC address of each VPN Gateway for which a license should be installed.

For instructions about how to obtain the MAC address and how to paste the license key, see [Licenses](#) on page 26 in [Customize the Portal](#) on page 249.

Configure a Default Group

Remote users requesting the AVG Portal to reach the corporate web Portal will automatically be placed in a default group. Before you enable the Portal Guard feature you should configure this group on the VPN Gateway and provide the relevant access rules for the group.

*** Note:**

Be careful when defining the access rules for the default group so that user access is truly limited to the specified intranet web site and allowed links on that web site.

Instructions on how to configure groups and access rules is in [Groups, Access Rules and Profiles](#) on page 157.

Configure Portal Acceleration

To configure portal acceleration of an existing Portal, proceed as follows:

1. Turn off authentication for the AVG Portal.

```
>> Main#cfg/vpn 1/server/portal/authentica  
  
Current value: on  
User authentication (on/off):off
```

2. Set the IP address or host name (and path) of the secure web Portal to which requests should be redirected.

This step sets the backend web server host address and path (if required) when authentication is disabled.

```
>> Portal Settings#dhost  
  
Current value: []  
Enter portal default backend host:inside.example.com/  
portal.html
```

3. Set the protocol used to access the backend host.

```
>> Portal Settings#dscheme  
  
Current value: http  
Enter portal default backend scheme (http/https):
```

4. Reference the default group you have previously created.

```
>> Portal Settings#dgroup  
  
Current value: " "  
  
Enter group name:
```

5. Apply the changes.

```
>> Portal Settings#apply  
  
Changes applied successfully.
```

Glossary

Access Rules	When a user tries to log in to the virtual SSL VPN server, either through the Portal page or through a VPN client, their group membership determines the access rights to different servers and applications on the intranet. This is done by associating one or more access rules (each containing parameters such as allowed network, ports and paths) with a group.
ARP	Address Resolution Protocol. A network layer protocol used to convert an IP address into a physical address, such as an Ethernet address. A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address.
AVG	Avaya VPN Gateway.
BWM	Bandwidth Management (BWM) enables administrators to allocate a portion of the available bandwidth for specific users or groups. The bandwidth policies take lower and upper bound. The lower bound (soft limit) is guaranteed and the upper bound (hard limit) is available according to the requirement. The BWM provides bandwidth policy management for user traffic and IPsec Passthrough.
Base Profile	Refers to links and access rules specified for a user group directly under the Group level. If extended profiles are used, the base profile's links and access rules will be appended to the extended profile's links and access rules.
Branch Office Tunnel	Secure IPsec tunnel between two VPN Gateways (or cluster of VPN Gateways) or similar devices. The tunnel is automatically established when traffic destined for specific remote networks is detected, provided traffic was initiated from a network allowed to send traffic through the tunnel. BO tunnels can for example, be set up between a main office and a branch office.
CA (Certificate Authority)	A trusted third-party organization or company that issues digital certificates. The role of the CA in this process is to guarantee that the entity granted the unique certificate is, in fact, who claims to be.
CLI (Command Line Interface)	The text-based interface on the VPN Gateway, presented to the user after having logged in. The CLI can be accessed through a console connection or remote connection (Telnet or SSH). The CLI is used for collecting information and configuring the VPN Gateway.
Cluster (of AVGs)	A cluster is a group of VPN Gateways that share the same configuration parameters. There can be more than one cluster in the network, each with its own set of

parameters and services to be used with different real servers. Every cluster has a Management IP address (MIP).

Console Connection

A connection to the VPN Gateway established through the console port.

CRL (Certificate Revocation List)

A list containing the serial numbers of revoked client certificates. Each CA issues and maintains their own CRLs. If you generate client certificates on the VPN Gateway, you can also create your own CRL.

CSR (Certificate Signing Request)

A request for a digital certificate, sent to a CA. On the VPN Gateway, you can generate a CSR from the command line interface by using the `request` command.

DCE (Data Communications Equipment)

A device that communicates with a Data Terminal Equipment (DTE) in RS-232C communications.

DER (Distinguished Encoding Rules)

A process for unambiguously converting an object specified in ASN.1 (such as an X.509 certificate, for example) into binary values for storage or transmission on a network.

Digital Certificate

The digital equivalent of an ID card used in conjunction with a public key encryption system. Digital certificates are issued by trusted third parties known as certificate authorities (CAs), after verifying that a public key belongs to a certain owner. The certification process varies depending on the CA and the level of certification.

Digital Signature

A digital guarantee that a document has not been altered, as if it were carried in an electronically-sealed envelope. The "signature" is an encrypted digest of the text that is sent with the text message. The recipient decrypts the signature digest and recomputes the digest from the received text. If the digests match, the message is proved intact and tamper free from the sender.

A digital signature ensures that the document originated with the person signing it and that it was not tampered with after the signature was applied. However, the sender could still be an impersonator and not the person who claims to be. To verify that the message was indeed sent by the person claiming to send it requires a digital certificate (digital ID) which is issued by a certification authority.

DIP (Destination IP) Address

The destination IP address of a frame.

DPort (Destination Port)

The destination port number, linking the incoming data to the correct service. For example, port 80 for HTTP, port 443 for HTTPS, port 995 for POP3S.

DTE (Data Terminal Equipment)

A device that controls data flowing to or from a computer. The term is most often used in reference to serial communications defined by the RS-232C standard. This standard defines the two ends of the communication channel as being a DTE and

DCE device. However, using a null-modem cable, a DTE to DTE communication channel can also be established between, for example, two computers.

Extended Profile	Extended profiles can be defined for a user group if other links and access rules should apply when the user authenticates by means of a specific authentication method or when connecting from a specific IP address or network.
HTTP Proxy	Java applet accessible on the Portal page's Advanced tab, enabling links executed on complex intranet Web pages (containing plugins like Flash, Shockwave and Java applets) to be sent through a secure connection to the SSL server for redirection.
L2TP	Layer 2 Tunneling Protocol (L2TP) acts as a data link layer protocol for tunneling network traffic between two peers over an existing network or Internet.
Master	A VPN Gateway in a cluster that is in control of the MIP address, or can take over the control of the MIP address should another master fail. Configuration changes in the cluster are propagated to other members through the master VPN Gateways.
MIB (Management Information Base)	An SNMP structure that describes which groups and objects that can be monitored on a particular device.
MIP (Management IP) Address	An IP address that is an IP alias to a master VPN Gateway in a cluster of VPN Gateways. The MIP address identifies the cluster and is used when making configuration changes through a Telnet or SSH connection or through the Browser-Based Management Interface (BBI).
Net Direct Client	The Net Direct client is an SSL VPN client that can be downloaded from the Portal for each user session. As opposed to the LSP and TDI versions of the SSL VPN client, the Net Direct client does not have a user interface. Another difference is that the Net Direct client is packet-based, while the SSL VPN clients uses system calls. The packet-based solution supports more applications (for example, Microsoft Outlook).
Network Access Protection	Network Access Protection (NAP) is a Microsoft® technology which enforces system health requirements for clients trying to access private network.
Nslookup	A utility used to find the IP address or host name of a machine on a network. To use the <code>nslookup</code> command on the VPN Gateway, it must have been configured to use a DNS server.
NTP (Network Time Protocol)	A protocol used to synchronize the real-time clock in a computer. There are numerous primary and secondary servers on the Internet that are synchronized to the Coordinated Universal Time (UTC) through radio, satellite or modem.
Passphrase	Passphrases differ from passwords only in length. Passwords are usually short, from six to ten characters. Short passwords may be adequate for logging onto computer systems that are programmed to detect a large number of incorrect guesses, but they are not safe for use with encryption systems. Passphrases are usually much

longer—up to 100 characters or more. Their greater length makes passphrases more secure.

PEM (Privacy Enhanced Mail)

A standard for secure e-mail on the Internet. It supports encryption, digital signatures and digital certificates as well as both private and public key methods. Keys and certificates are often stored in the PEM format.

Ping (Packet INternet Groper)

A utility used to determine whether a particular IP address is online.

PKCS #12

A standard for storing private keys and certificates.

PKI (public key infrastructure)

Short for public key infrastructure, a system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction. PKIs are currently evolving and there is no single PKI nor even a single agreed-upon standard for setting up a PKI. However, nearly everyone agrees that reliable PKIs are necessary before electronic commerce can become widespread.

A PKI is also called a trust hierarchy.

Portal

The Portal web page is displayed following a successful login to a virtual SSL VPN server of the portal type. The Portal contains different tabs from where the user can access various intranet resources such as web, mail and file servers.

Portal Guard

The Portal Guard feature is an easy way of "converting" an existing HTTP site to generate HTTPS links, secure cookies and so on. The VPN Gateway will not only handle the SSL processing but also see to it that all existing web links are rewritten to HTTPS. This eliminates the need to rewrite each link manually.

Port Forwarder

Applies to the SSL VPN feature. Java applet accessible on the Portal page's Advanced tab, enabling transparent access to applications through a secure connection. By specifying an arbitrary port number on the client along with the desired intranet host and port number, the user can access an intranet application by connecting to localhost on the specified port number.

Secure Portable Office

The Secure Portable Office (SPO) client provides VPN access from portable storage such as USB compliant flash memory and CD ROM.

Secure Service Partitioning

Feature designed to partition a cluster of VPN Gateways into separate VPNs. The idea is to give service providers (ISPs) the possibility to host multiple VPN customers on a shared Remote Access Services (RAS) platform.

Setup Utility

When turning on a VPN Gateway the very first time, the Setup utility starts up automatically. The Setup utility is used for performing a basic configuration of the VPN Gateway. The Setup utility first presents you with the choice of setting up the AVG as a single device, or to add the VPN Gateway to an existing cluster.

If you perform a reinstallation of the AVG software, you will also enter the Setup Utility after the VPN Gateway has rebooted.

SIP (Source IP) Address	The source IP address of a frame.
Slave	A VPN Gateway that depends on a master VPN Gateway in the same cluster for proper configuration.
SNMP (Simple Network Management Protocol)	A network monitoring and control protocol. Data is passed from SNMP agents, which are hardware and/or software processes reporting activity in each network device (a VPN Gateway, for example), to the workstation console (or SNMP manager) used to oversee the network. The SNMP agents return information in a MIB (Management Information Base), which is a data structure that defines what information is obtainable from the device.
SOCKS	<p>A generic, proxy protocol for TCP/IP-based networking applications. The SOCKS protocol provides a flexible framework for developing secure communications by easily integrating other security technologies, for example, SSL.</p> <p>SOCKS includes two components, the SOCKS server and the SOCKS client. The SOCKS server is implemented at the application layer, while the SOCKS client is implemented between the application and transport layers. The basic purpose of the protocol is to enable hosts on one side of a SOCKS server to gain access to hosts on the other side of a SOCKS server, without requiring direct IP reachability.</p>
SPort (Source Port)	The source destination port, linking the incoming data to the correct service. For example, port 80 for HTTP, port 443 for HTTPS, port 995 for POP3S.
SSH (Secure Shell)	A program used to log into another computer over a network, execute commands in a remote machine, and move files from one machine to another. SSH provides strong authentication and secure communications over insecure channels.
SSL (Secure Sockets Layer) Protocol	The SSL protocol is the leading security protocol on the Internet. It runs above the TCP/IP protocol and below higher-level protocols such as HTTP or IMAP. SSL uses TCP/IP on behalf of the higher-level protocols and, in the process, allows an SSL-enabled server to authenticate itself to an SSL-enabled client.
SSL VPN client	Windows application with SOCKS support. When installed on a user's computer, transparent access (not through the Portal page) to intranet applications is enabled.
TLS (Transport Layer Security)	The TLS protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.
Traceroute	A utility used to identify the route used for station-to-station connectivity across the network.

Trap	If a trap is defined in the MIB, a trap message is sent from the SNMP agent to the SNMP manager when the trap is triggered. A trap can for example define a hardware failure in a monitored device.
Tunnel Guard	Tunnel Guard is an application that maintains checking that the required components (executables, DLLs, configuration files, and so on.) are installed and active on the remote user's machine.
URI (Uniform Resource Identifier)	The addressing technology from which URLs are created. Technically, URLs such as HTTP:// and FTP:// are specific subsets of URIs, although the term URL is mostly heard.
VIP (Virtual IP) Address	An IP address that the remote user should connect to access the Portal (in clientless mode) or simply the VPN (in transparent mode).
Virtual SSL Server	A virtual SSL server handles a specific service on the VPN Gateway, such as HTTPS, SMTPS, IMAPS, or POP3S. You can create up to 256 virtual SSL servers per AVG cluster. To authenticate itself towards clients making requests for the specified service, the virtual SSL server is configured to use a digital certificate.
VLAN (Virtual Local Area Network)	VLANs are commonly used to split up groups of network users into manageable broadcast domains, to create logical segmentation of workgroups, and to enforce security policies among logical segments.
X.509	A widely-used specification for digital certificates that has been a recommendation of the ITU since 1988.
X11 Forwarding	The X Window System (commonly X11 or X) is a windowing system for bitmap displays. It is the standard toolkit and protocol to build graphical user interfaces on Unix, Unix-like operating systems and OpenVMS, and is available for almost all modern operating systems. The VPN Gateway supports secure display of X11 across the Internet by way of X11 Forwarding, supported by the SSH applet on the Portal's Advanced tab and the Terminal link type.