



Avaya CAD-SV

Configuring Nortel Contivity 1100 VPN Router to Support Avaya 96xx series IP Phones.

Issue 1.0
10th October 2009

ABSTRACT

These Application Notes describe the steps to configure the Nortel Contivity 1100 VPN Router to Support Avaya 96xx series IP Phones.

TABLE OF CONTENTS

1.	Introduction.	3
1.	NETWORK TOPOLOGY.....	4
2.	EQUIPMENT AND SOFTWARE VALIDATED	6
3.	NORTEL VPN ROUTER 1100 CONFIGURATION	7
4.	AVAYA 96XX SERIES IP PHONE CONFIGURATION	15
4.1	96xx series IP Phone Firmware	15
4.2	Configuring Avaya 96xx series IP Phone	15
4.3	“46xxsettings.txt” File	17
5.	VERIFICATION.....	21
6.	TROUBLE SHOOTING	22
6.1	IKE Phase 1 no response.	22
6.2	Incorrect IKE Phase 2	22
6.3	Phone displaying “connecting...”.....	23
7.	CONCLUSION	24
8.	REFERENCES.....	24

1. Introduction.

These Application Notes describe the steps to configure the Nortel Contivity 1100 VPN Router to support IPSec Tunnel termination using Local Credential authentication for Avaya 96xx series IP Phone.

Avaya 96xx series IP Phone has software based IPSec Virtual Private Network (VPN) client integrated into the firmware of an Avaya 96XX Series IP Telephone. This capability allows Avaya IP Telephone to be plugged in and used over a secure IPSec VPN from any broadband Internet connection. End users experience the same IP telephone features as if they were using the telephone in the office. Avaya IP Telephone models supporting the Avaya 96xx series IP Phone firmware include the 9620, 9620C, 9620L, 9630, 9640, 9650, 9650C and 9670. Please Note that 9610 does not support VPN. Please Note that VPN feature is supported in H.323 based IP phones and not SIP based. Also Spice 3.1 H.323 phones are supported in Avaya Communication Manager 3.1, Build 4.0+.

Release 3.1 of the Avaya 96xx series IP Phone firmware, used in these Application Notes, extends the support of head-end VPN gateways to include Nortel VPN Router (formerly known as Nortel Contivity) platforms. The configuration steps described in these Application Notes utilize a Nortel VPN Router 1100.

The Avaya 96xx series IP Phone utilizes the Internet Key Exchange (IKE) Protocol for IPSec tunnel establishment and authentication with the Nortel VPN Router.

CHAPTER 1.

1. NETWORK TOPOLOGY

The below Figure 1 describes the general test setup diagram to configure the 96xx series IP phone with the Nortel vpn gateway.

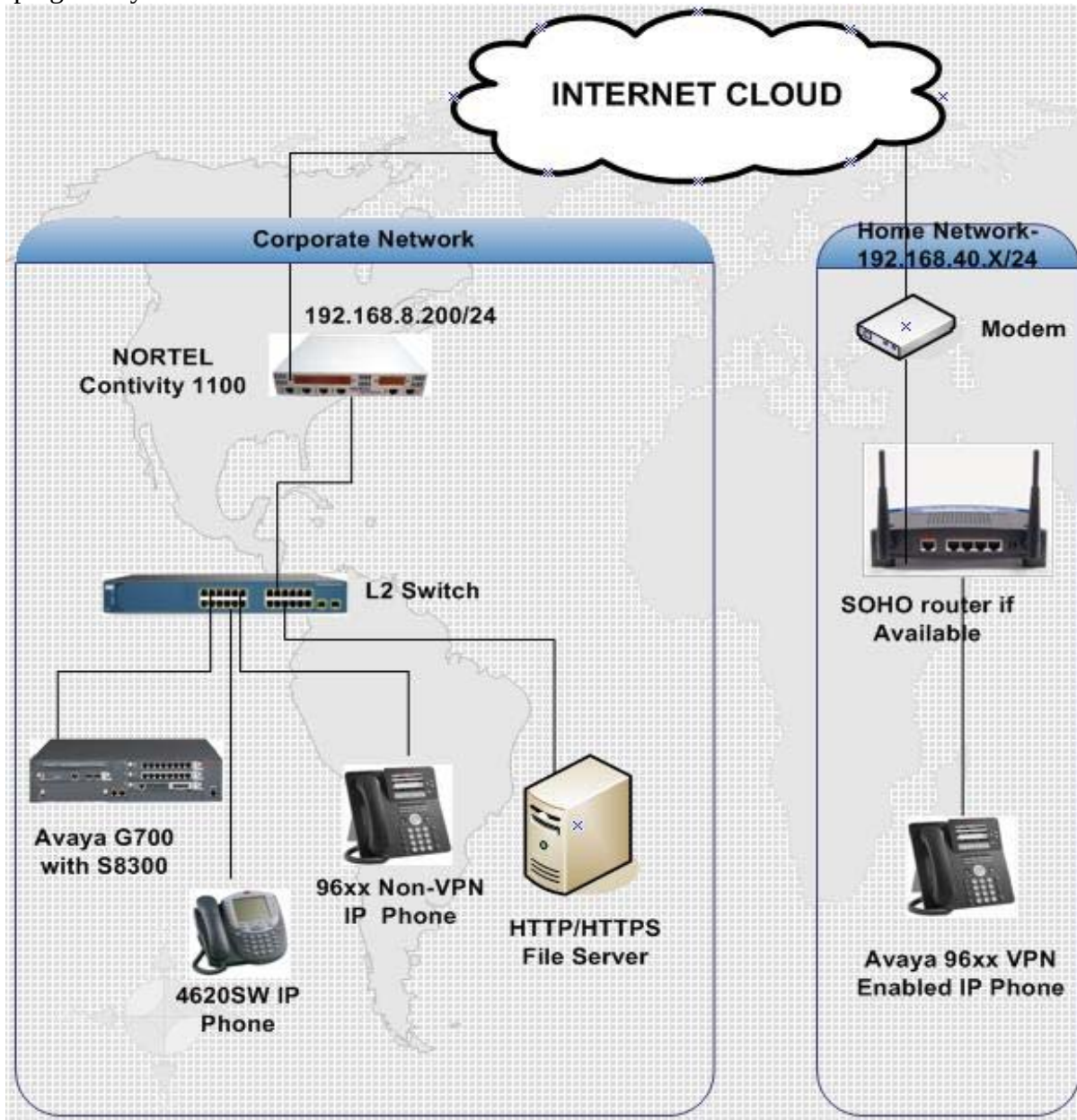


Figure 1: High level test diagram for Implementation of 96xx series avaya IP phones with Nortel contivity 1100.

The sample network implemented for these Application Notes is shown in Figure 1. The Corporate IP Network location contains the Nortel Contivity 1100 VPN Router functioning as perimeter security device and VPN head-end. The Avaya S8730 Server and Avaya G700 Media Gateway are also located at the Corporate IP Network.

The Avaya 96xx series VPN Enabled IP Phones are located in the public network and configured to establish an IPSec tunnel to the Public IP address of the Nortel VPN Router. The Nortel VPN Router will assign IP addresses to the 96xx series IP Phones. The assigned IP addresses, also known as the inner addresses, will be used by the 96xx series IP Phones when communicating inside the IPSec tunnel and in the private corporate network to Avaya Communication Manager.

CHAPTER 2

2. EQUIPMENT AND SOFTWARE VALIDATED

Table 1 lists the equipment and software/firmware versions used in the sample configuration provided.

Equipment	Software Version
Avaya G700 Media Gateway with S8300.	Avaya Communication Manager 3.1 Build 4.0 and above.
Avaya 96xx Telephone	Release 3.1
Nortel Contivity 1100 Software Version	V06_00.310+

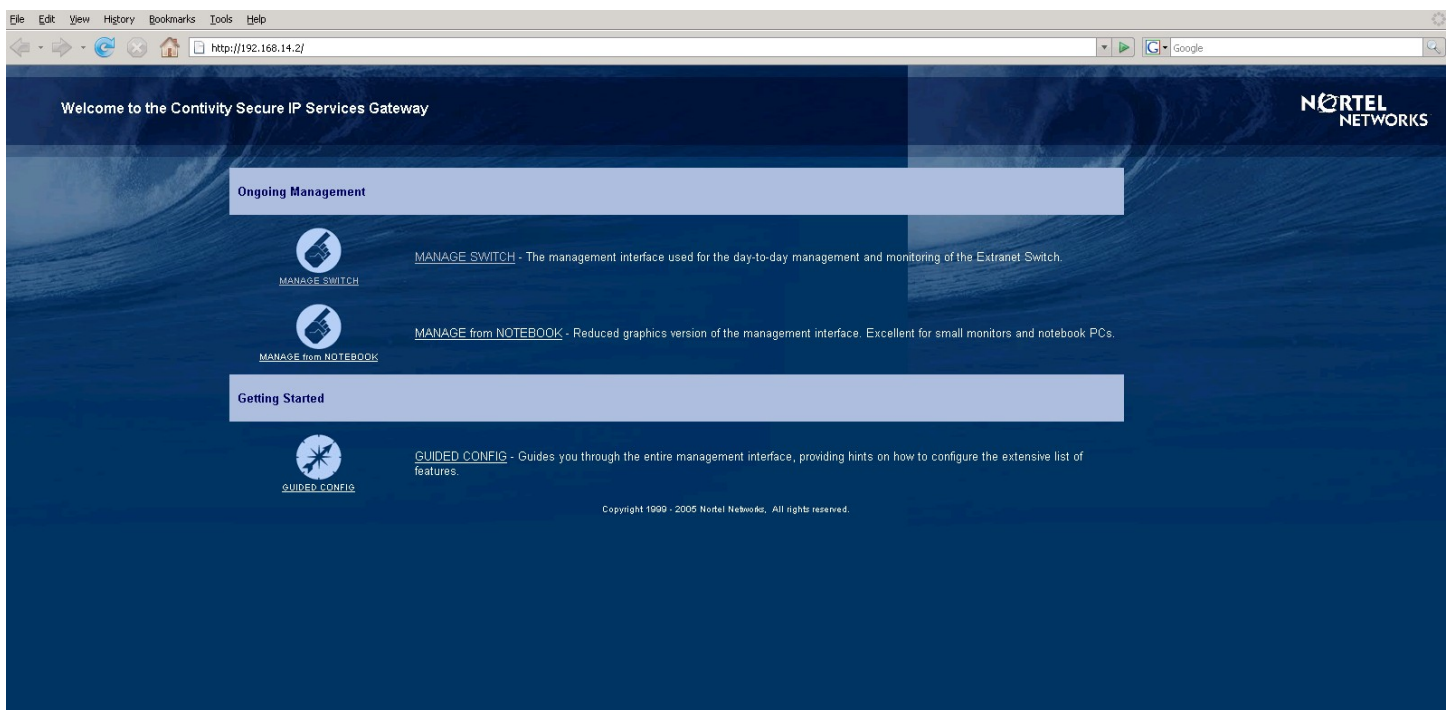
Table 1 – Equipment Version Information

CHAPTER 3.

3. NORTEL VPN ROUTER 1100 CONFIGURATION

These Application Notes assume the Nortel VPN Router has been configured with basic IP connectivity and is connected into the network. The Nortel VPN Router 1100 depicted in Figure-2 has been configured with IP address 192.168.14.2 as its Management IP address.

1. From a web browser, enter the URL of the Nortel VPN Router (management) interface, <http://<Management IP address of VPN Router>> and the following Nortel VPN Router screen appears. Select **MANAGE SWITCH** and log in using a user name with administrative privileges in the pop-up window (not shown).



2. The below screen shows the LAN interface IP address configuration used in the sample network. One private interface with IP address 192.168.14.3/24 and one public interface with IP address 192.168.8.200/30 are used in the sample network.

LAN Interfaces

Interface	Description	State	Type	Actions
Fast Ethernet		Enabled	Private	Configure Statistics

[Add Multinet](#)

IP Address	Subnet Mask	Interface Filter	Type	Actions
192.168.14.3	255.255.255.0	permit all (Contivity Interface Filter in use)	Primary	Edit Delete

Interface	Description	State	Type	Actions
Slot 1 Interface 1		Enabled	Public	Configure Statistics

[Add Multinet](#)

IP Address	Subnet Mask	Interface Filter	Type	Actions
192.168.8.200	255.255.255.0	permit all (Contivity Interface Filter in use)	Primary	Edit Delete

3. Select **SERVICES AVAILABLE** from the left panel menu. Make sure IPsec is enabled (default) for at least the public interface.

Services

Allowed Services

Tunnel Type	Public	Private
IPsec	☒	☒
PPTP	☒	☒
L2TP & L2F	☒	☒
Firewall User Authentication	☐	☐

4. The screen capture below shows the Default Routes defined under ROUTING STATIC ROUTES in the sample network. One default route to gateway 192.168.14.1 on the Private side and the other default route to gateway 192.168.8.1 on the public side.

192.168.14.2 - Contivity Secure IP Services Gateway - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites

Address http://192.168.14.2/manage/manager.htm Go Links »

SYSTEM
SERVICES
ROUTING
QOS
PROFILES
SERVERS
ADMIN
STATUS
HELP

STATIC ROUTES
OSPF
RIP
BGP
ROUTE MAP
INTERFACES
MULTICAST
VRRP
CONFIGURATION
ROUTE TABLE
ACCESS LIST
POLICY
CLIENT-ADDR-DIS
INTERFACE GRP
NAT

Static Routes

LOGOFF

Static Routes

Enabled ☒

OK Cancel

Default Routes

Type	Gateway Address	Interface	Admin State	Cost	Action	
Private	192.168.14.1	Fast Ethernet	Enabled	10	Edit	Delete
Public	192.168.8.1	Slot 1 Interface 1	Enabled	10	Edit	Delete

Add Public Route Add Private Route

Validate Public Default Routes ☐ Ping Interval 30 Seconds

OK Cancel

Static Routes through Physical Interfaces

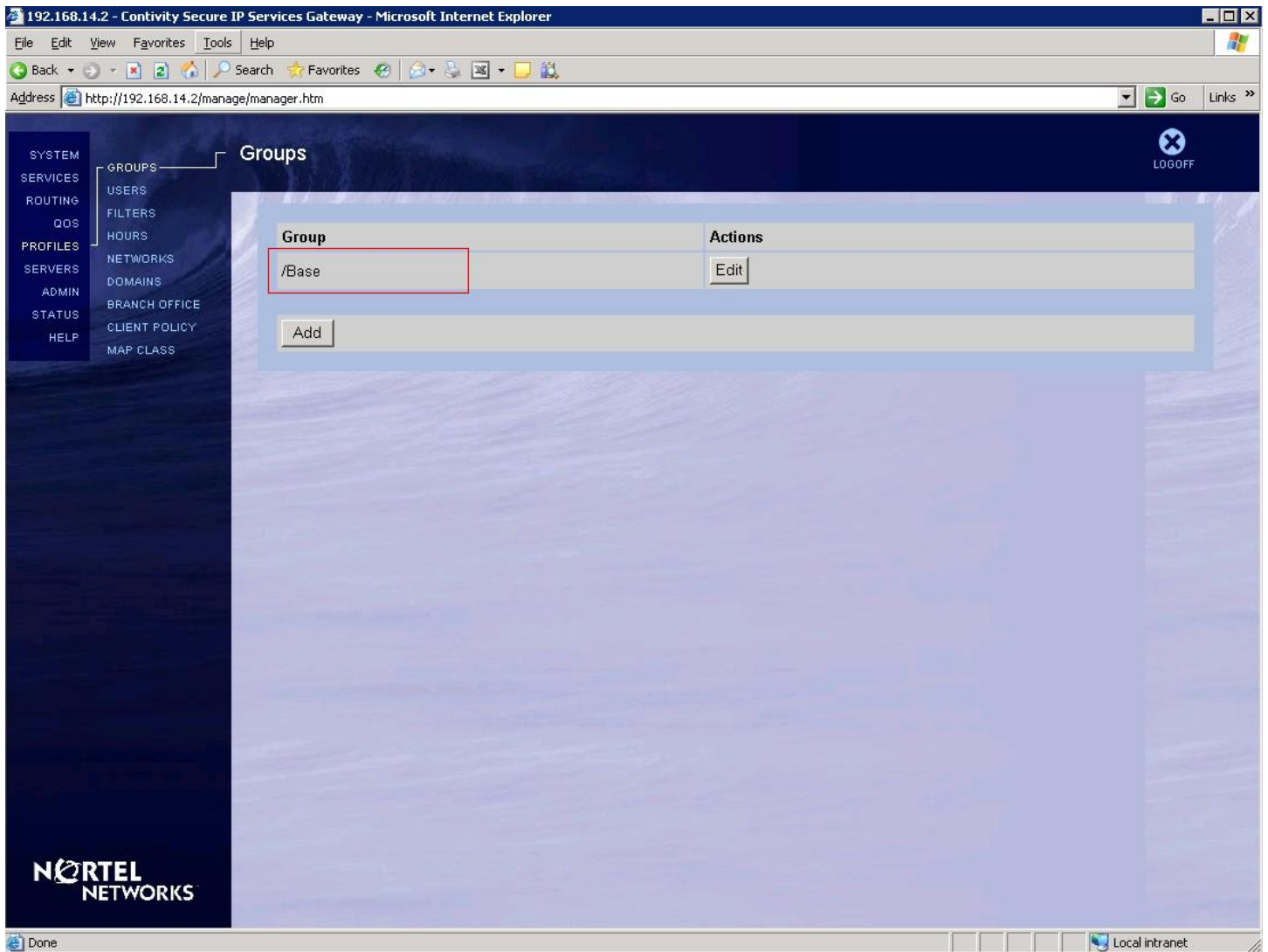
IP Address	Subnet Mask	Gateway Address	Interface	Admin State	Cost	Action
Add						

Show Branch Office Routes Show DoD Routes Show PPPoE Routes

NORTEL NETWORKS

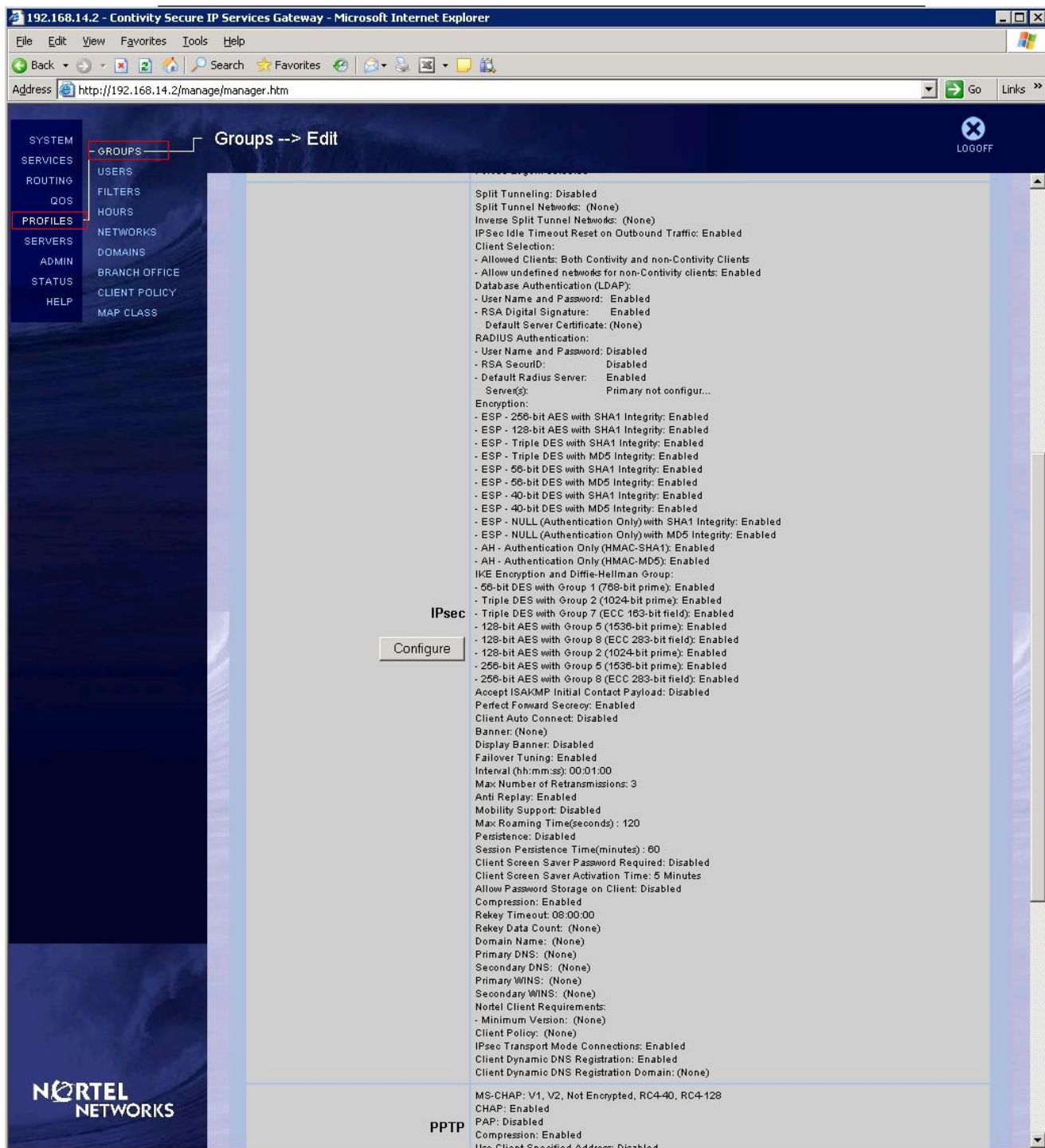
Done Local intranet

5. /BASE group was defined for use in the sample network.



6. The abbreviated screen capture below shows the IPsec configuration used for the above /BASE group. The **Encryption** is set to **ESP – Triple DES with MD5 Integrity**. The encryption will need to match Avaya 96xx

series IP Phones setting in **Section 5.2**



7. Create new users by selecting PROFILES USERS from the left panel menu. The 96xx series IP phone will use this user ID to log in. Each 96xx series IP phone should have its own user ID.

192.168.14.2 - Contivity Secure IP Services Gateway - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://192.168.14.2/manage/manager.htm

SYSTEM
SERVICES
ROUTING
QOS
PROFILES
SERVERS
ADMIN
STATUS
HELP

GROUPS
USERS
FILTERS
HOURS
NETWORKS
DOMAINS
BRANCH OFFICE
CLIENT POLICY
MAP CLASS

User Management

LOGOFF

Group /Base Display

User Search

☒ Last Name
☐ User ID
☐ Admin Rights
☐ LDAP

Search Group
Search All

Previous Next Add User [More Reports](#)

	Last	First	Actions
1	sasi		Edit Delete
1	vpn		Edit Delete
2	vpn		Edit Delete
3	vpn		Edit Delete
4	vpn		Edit Delete
5	vpn		Edit Delete
c	sasi		Edit Delete
jamadar	wasim		Edit Delete
s	ganesh		Edit Delete

Add User

NORTEL NETWORKS

Done Local intranet

8. The following abbreviated screen capture shows the values used for a user, vpn1, who belongs to the /Base group. The User ID of vpn1 is composed of the 96xx series IP phone extension and the user name to facilitate tracking.

192.168.14.2 - Contivity Secure IP Services Gateway - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites

Address http://192.168.14.2/manage/manager.htm Go Links

SYSTEM
SERVICES
ROUTING
QOS
PROFILES
SERVERS
ADMIN
STATUS
HELP

GROUPS
USERS
FILTERS
HOURS
NETWORKS
DOMAINS
BRANCH OFFICE
CLIENT POLICY
MAP CLASS

User Management --> Edit User

LOGOFF

General

First Last

Name vpn 1

Group /Base

Static IP Address Static Subnet Mask

Remote User

Note: The static IP subnet mask is used for IPsec connections only

User Accounts

	User ID	Password	Confirm Password	Expires (Days)	Status
IPsec	vpn1			Never	
PPTP					
L2TP					
L2F					
Firewall User Authentication					

Must Change Password at Next Logon ☐ (Nortel IPSEC Client Only)

L2TP/IPsec Data Protection

Require Own IPsec Credentials ☐

IPsec Certificate Credentials

Remote Identity

Valid Issuer Certificate Authority

(No issuer CAs available)

Subject Distinguished Name

☒ Relative

Common Name Org Unit Organization

Locality State/Province Country

Email Address

NORTEL NETWORKS

Done Local intranet

9. Select **SERVICES USER IP ADDR** from the left panel menu to define a DHCP scope to be assigned to Avaya 96xx series IP Phones. The sample configuration defined an IP address pool for the “Contivity” pool with an IP address range from 192.168.14.220 to 192.168.14.228 to be assigned to Avaya 96xx series IP phones.

SYSTEM
SERVICES
ROUTING
QOS
PROFILES
SERVERS
ADMIN
STATUS
HELP

RADIUS AUTH
RADIUS ACCT
LDAP
LDAP Proxy
USER IP ADDR
DHCP RELAY
DHCP

Remote User IP Address Pool

LOGOFF

DHCP

☒ Any External DHCP Server
☐ Internal DHCP Server
☐ Specified DHCP Server

DHCP Server

Primary	0.0.0.0	Not Configured
Secondary	0.0.0.0 *Optional	Not Configured
Tertiary	0.0.0.0 *Optional	Not Configured

DHCP Cache Size 1

Immediate Address Release ☒

DHCP Blackout Interval* 300 (seconds) *Amount of time before an address is available for reissue.

Override Blackout Interval when no addresses are available ☒

Address Pool

Pools	Start	End	Subnet Mask	Total	In Use	Action
contivity	192.168.14.220	192.168.14.228	255.255.255.0	9	1	Edit Delete

Add

Address Pool Blackout Interval* 0 (seconds) *Amount of time before an address is available for reissue.

If Named Pool Unavailable:*

☐ Failover to Default pool
☒ Deny address request

*Indicates action if named pool is absent or empty

OK

Cancel

4. AVAYA 96XX SERIES IP PHONE CONFIGURATION

4.1 96xx series IP Phone Firmware

The Avaya 96xx series (3.1) VPN-Enabled IP Phone firmware must be installed on the phone prior to the phone being deployed in the remote location. Refer to [1] and [2] for details on installing 96xx series IP Phone firmware. The firmware version of Avaya IP telephones can be identified by viewing the version displayed on the phone upon boot up or when the phone is operational by selecting the **Options** hard button → **View IP Settings** → soft button **Miscellaneous** → soft button → **Right arrow** hard button. The Application file name displayed denotes the installed firmware version.

As displayed in **Table 1**, 96xx series IP Phone firmware includes “3_1” in the name. This allows for easy identification of firmware versions incorporating VPN capabilities.

4.2 Configuring Avaya 96xx series IP Phone

The Avaya 96xx series IP Phone configuration can be administered centrally from an HTTP server through 46xxsettings.txt file (mentioned in section 5.3) or locally on the phone. These Application Notes utilize the local phone configuration method. Refer to [1] and [2] for details on a centralized configuration.

1. There are two methods available to access the **VPN Configuration Options** menu from the 96xx series IP Phone.

[A]. During Telephone Boot: -

During the 96xx series IP Phone boot up, “*” key can be used to enter the Configuration mode is displayed on the telephone screen as shown below.

100 Mbps Ethernet * to program

(Please note that the “*” key can also be used to enter the configuration mode till tunnel building procedures is not complete). When the * key is pressed, it will ask for “Enter Code:” we need to Press Mute Button + PROCPSWD (default 27238) (**Mute + 2-7-2-3-8 + #**) and then press # to Enter into the phone configuration mode.

Go to “ADDR” (Address Procedures) and update it with the below details.

Phones IP Address	0.0.0.0 (Will be assigned from the IP pool configured on the VPN gateway or by the Internal DHCP server if the VPN gateway is configured as DHCP Relay).
-------------------	--

Call Servers IP Address	192.168.1.201 (Avaya Communication manager IP address).
Router IP Address	0.0.0.0 (Will be assigned by the VPN gateway or by the Internal DHCP server if the VPN gateway is configured as DHCP Relay).
Subnet Mask	0.0.0.0 (Will be assigned by the VPN gateway or by the Internal DHCP server if the VPN gateway is configured as DHCP Relay).
Http Server	A.B.C.D (Internal HTTP server IP address in dotted decimal format from the network which contains the Avaya Communication Manager).
Https Server IP Address	A.B.C.D (Internal HTTPS server IP address in dotted decimal format from the network which contains the Avaya Communication Manager).
802.1Q	Auto
VLAN ID	0
VLAN Test	60

Press Exit to come out of the “ADDR” procedures.

2. Scroll down to the last option VPN. Note that the VPN configuration parameters will not be edited until the value of “VPNPROC” parameter is set to 2. (To do this open the upload directory of file server, open the file 46xxsettings.txt file and append it with “SET VPNPROC 2” and upload this new 46xxsettings.txt file into the avaya 96xx IP phone). It is recommended to set the value of VPNPROC to 2 while uploading the vpn enabled binary into the phone. Use Right Navigation key to go to the next screen options. (Note that the values will not be saved until Right-Navigation key is pressed even if “Save button is pressed”). The External addresses will be reflected only after rebooting the phone.

The configuration values of one of the 96xx series IP Phones used in the sample configurations are shown in **Table 2** below.

No.	Option	Value
1	VPN	Enabled
2	VPN Vendor	Nortel
3	Gateway Address	192.168.8.200 (FQDN or the IP Address (in dotted decimal format) of the VPN gateway ‘Untrust’ Interface)
4	External Phone IP Address	192.168.40.143 (Phone IP address from the list of the local home network IP addresses).
5	External Router	192.168.40.1 (External Router IP address of the home Network).
6	External Subnet Mask	255.255.255.0 (External Subnet Mask of the home Network).
7	External DNS Server	0.0.0.0 (Provided by the local Service Provider)
8	Encapsulation	4500-4500
9	Copy TOS	NO
10	Auth. Type:	Local Credentials.
11	VPN User Type:	Any
12	VPN User:	Vpn1 (vpn username)

13	Password Type:	Save in Flash
14	User Password:	***** (I.e. Remote User password i.e. vpn1 as per our notes).
15	IKE ID Type:	Key-ID
16	IKE Xchg Mode:	Aggressive
17	IKE DH Group:	1
18	IKE Encryption Alg:	Any
19	IKE Auth. Alg. :	Any
20	IKE Config. Mode:	Enabled
21	IPsec PFS DH Group:	1
22	IPsec Encryption Alg:	Any
23	IPsec Auth. Alg.:	Any
24	Protected Network:	0.0.0.0/0
25	IKE Over TCP:	Never

[B] While phone is operational in vpn enabled Mode.

Press “Mute button + procpwd + #” to enter the craft procedures and follow the above steps to program the vpn enabled phone.

4.3 “46xxsettings.txt” File

The 46xxsetting.txt file contains variable values used by the 96xx phone during the setup of the IPsec VPN tunnel. The variables specific Nortel for Local credentials authentication are listed below. Descriptions of each variable and the values used in the sample configuration are shown.

```
#####
## VPN Mode
## 0: Disabled, 1: Enabled.
#####
SET NVVPNMODE 1
#####
## Vendor.
## 1: Juniper/Netscreen,      2: Cisco
## 3: Checkpoint/ Nokia    4: Other
## 5: Nortel.
#####
SET NVVPNSVENDOR 5
#####
## Encapsulation Type.
## 0: 4500-4500,              1: Disabled
## 2: 2070-500,
## 4: RFC (500-500)
#####
SET NVVPNENCAPS 0
#####
## Copy TOS.
## 1: Yes,                    2: No
#####
SET NVVPNCOPYTOS 2
#####
## Authentication Type.
```

```

##
## [For Cisco/Juniper/Checkpoint/Other]
## 3: PSK,                      4: PSK with Xauth
## 5: RSA signatures with Xauth, 6: Hybrid Xauth
## 7: RSA signatures.
##
## [Nortel Authentication Type]
## 1: Local credentials,        2: Radius Credentials.
## 3: Radius SecureID,          4: Radius Axent.
#####
SET NVVPNAUTHTYPE 1
#####
## VPN User Type.
## 1: Any,                      2: User
#####
SET NVVPNUSERTYPE 2
#####
## VPN User name.
#####
SET NVVPNUSER vpn1
#####
## Password Type.
## 1: Save in Flash,            2: Erase on reset
## 3: Numeric OTP,              4: Alpha-Numeric OTP
## 5: Erase on VPN termination.
#####
SET NVVPNPSWDTYPE 1
#####
## User Password.
#####
SET NVVPNPSWD vpn1
#####
## IKE ID (Group Name).
#####
SET NVIKEID base
#####
## Preshared Key (Group Password).
#####
#SET NVIKEPSK
#####
## IKE ID Type.
## 1: IPv4_ADDR,                2: FQDN
## 3: USER_FQDN,                9: DER_ASN1_DN
## 11: Key ID
#####
SET NVIKEIDTYPE 11
#####
## IKE Xchg Mode.
## 1: Aggressive,               2: Identity Protect.
#####
SET NVIKEXCHGMODE 1
#####
## IKE DH Group.
#####
SET NVIKEDHGRP 1

```

```
#####
## IKE Encryption Algo.
## 1: AES-128,          2: 3DES
## 3: DES              4: AEs-192
## 5: AES-256          0: Any
#####
SET NVIKEP1ENCALG 0
#####
## IKE Auth algo.
## 0: Any,              1: MD5
## 2: SHA-1
#####
SET NVIKEP1AUTHALG 0
#####
## IKE Config Mode.
## 0: Enabled,          1: Disabled.
#####
SET NVIKECONFIGMODE 0
#####
## IPsec PFS DH group.
#####
SET NVPFSDHGRP 1
#####
## IPsec Encryption Algo.
## 1: AES-128,          2: 3DES
## 3: DES              4: AEs-192
## 5: AES-256          6: None
## 0: Any
#####
SET NVIKEP2ENCALG 0
#####
## IPsec Authentication Algo.
## 0: Any,              1: MD5
## 2: SHA-1
#####
SET NVIKEP2AUTHALG 0
#####
## Protected Network.
#####
SET NVIPSECSUBNET 0.0.0.0/24
#####
## IKE Over TCP.
## 0: Never,            1: Auto
## 2: Always
#####
SET NVIKEOVERTCP 1
#####
## Craft access
## 0: Enabled,          1: only view option is available?
#####
SET PROCSTAT 0
#####
## VPN craft access
## 0: disabled,         1: view only
## 2: View and edit.
#####
```

SET VPNPROC 2

```
#####  
## Call Server address  
#####  
##SET MCIPADD 192.168.1.162  
#####  
## Craft code  
#####
```

SET PROCPSWD 27238

```
#####  
## VPN craft access code  
#####  
##SET NVVPNCODE 876  
#####  
## SNMP String  
#####  
##SET SNMPSTRING public  
#####
```

5. VERIFICATION.

The active VPN sessions to the Nortel VPN Router can be viewed by selecting **Status Sessions** from the left panel menu of the web management interface.

Active IPsec tunnels are shown in the **Current End User Sessions** of the display. The abbreviated screen capture below shows the **Current End User Session** of three 96xx series IP Phones with active tunnels to the Nortel VPN Router.

The screenshot displays the Nortel VPN Router web management interface. On the left, a navigation menu includes SYSTEM, SERVICES, ROUTING, PROFILES, SERVERS, ADMIN, **STATUS**, and HELP. The **STATUS** menu is expanded, showing sub-items: SESSIONS, SYSTEM, HEALTH CHECK, STATISTICS, SYSTEM LOG, and EVENT LOG. The **SESSIONS** sub-item is selected, leading to the 'Active Sessions' page. At the top right, there is a 'LOGOFF' button. Below the navigation menu, a 'Display' dropdown menu is set to 'All Sessions'. The main content area is divided into several sections:

- End User Summary:** A table showing session counts for different protocols and users.
- Branch Office Summary:** A table showing session counts for different protocols and branch offices.
- Current Branch Office Sessions:** A table showing active sessions for the current branch office.
- Current End User Sessions:** A table showing active sessions for the current end user, with a search bar and filters.

The 'Current End User Sessions' table is highlighted with a red border. It contains the following data:

User	Type	UID	IP Address Assigned Public	IPX Address	Start	Kbytes	Packets	Links	Action
vpn 2	IPSEC	vpn2	192.168.14.228 192.168.8.148		09/18/2009 03:34:16	In: 85 Out: 85	In: 1461 Out: 1459		Log Off Details
admin	Admin HTTP	admin	192.168.14.14		09/18/2009 03:08:25				Log Off

6. TROUBLE SHOOTING

This section offers some common configuration mismatches between the 96xx series IP Phone and the Nortel VPN Router to assist in troubleshooting. The key events of the logs are highlighted in bold. The Nortel VPN Router log messages were generated using the “Original” Display Mode. Nortel VPN Router log messages can be access through **STATUS EVENT LOG** from the main web management interface.

6.1 IKE Phase 1 no response.

If we given user name are incorrect we will get VPN Tunnel Failure Message.

VPN tunnel failure		
Retry	Details	Sleep

If we press **Retry** Soft key again it will retry to establish the tunnel.

If we press **Details** Soft key.

We can see IKE Phase 1 no response

IKE Phase 1 no response		
Restart	Program	Back

Press **Program** soft key it will redirect to Craft Code Screen

Enter Code:
= OK

Give Craft Code and it will redirect to **Craft Procedures** Screen here select **VPN** and press **Start** soft key Press forward soft key on the phone and check the IKE Exchange mode, Check **IKE Phase1** parameters on VPN gateway and phone is correct or not, Check the IP pool is configured properly and also same pool name it is mentioned in Profiles -- >Groups -- > Base -- > Edit -- > Connectivity -- > Address pool.

6.2 Incorrect IKE Phase 2

If we given incorrect IKE Phase 2 Settings then we will get VPN Tunnel Failure Message

VPN tunnel failure		
Retry	Details	Sleep

If we press **Retry** soft key again it will retry to establish the tunnel.

If we press **Details** soft key we can see **Invalid configuration screen**.

Invalid configuration

Restart

Program

Back

Press **Program** soft key it will redirect to Craft Code Screen

Enter Code:

= OK

Give Craft Code and it will redirect to **Craft Procedures** Screen here select **VPN** and press **Start** soft key
Press forward soft key on the phone and it will go to IKE Phase 2 Screen, here check the IKE Phase 2 Screen
Settings is correct or not.

6.3 Phone displaying “connecting...”

This issue can be resolved by the administrators who have access to the Avaya Communication manager and Nortel VPN Gateway. Open the web interface of the Nortel VPN gateway. Check the entered routes are correct. Check that the phone requests are able to reach the ACM and also phone gets response from the ACM (Trace using any sniffing software e.g. Ethereal/wireshark). Open up the 46xxsettings.txt file and enter “SET VPNTTS 0”. Reboot the phone with the correct file server IP address.

7. CONCLUSION

The Avaya 96xx series IP Phone combined with Nortel VPN Router 1100 security appliance provides a secure solution for remote worker telephony over any broadband Internet connection. The Avaya 96xx series IP Phone Local Credentials implementation for Nortel VPN Router security appliances demonstrated successful interoperability with the Nortel VPN Router.

8. REFERENCES

Avaya Solution & Interoperability Test Lab:

Configuring Nortel VPN Router to Support Avaya VPNremote Phones – Issue 1.0

Avaya Application Notes and Resources Web Site:

<http://www.avaya.com/gcm/master-usa/en-us/resource/>

Avaya Product Support Web Site:

<http://support.avaya.com/japple/css/japple?PAGE=Home>

Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.
