VPNremote Phone Administrators Guide
Cisco Gateway

May 9, 2006

Table of Contents

1. Introduction

The VPNremote Phone is a product from Avaya which provides remote communication capabilities for small office and home (SOHO) users. It provides users with the ability to connect to corporate communications systems from anywhere with internet access.

The advantage of the VPNremote Phone is that it provides communications which is independent of the users PC and without opening the corporate network to unauthorized access.

This document covers Cisco configuration

2. Communication Manager and Network Administration

From an administrative perspective, the VPNremote Phone is seen as just another extension on Communication Manager. The phone could have a DID or non-DID number and it is designed to behave just like an IP Telephone connected inside the corporate network.

Deploying a VPN Phone really consists of only two main steps. These are 1) administering a new extension and 2) administering access to the VPN network.

Single Extension:
If the end user works remotely full time then a single extension can be configured for an IP Telephone.

Bridged Extension:
When bridged extensions are used, there are actually two phone numbers (DID, non-DID, or combination of the two) but they act as a single phone. When you receive a call, both phones ring. When you have a message, the message waiting light appears on both phones.

One reason to use a bridged extension is when the user has both an office phone and a home office. With bridged extensions, their office phone is a DID number and their VPNremote Phone is a non-DID number and they are bridged together.

Since the VPNremote phones are remotely connecting it is a good idea to place the VPNremote Phone extensions on their own IP Network Region. Due to a wide range of home network ISP bandwidths, a codec setting of G.729 with 3 Frames per Packet is suggested. This allows for a larger range of users to use the service.

CM Levels
Version 3.0 or later

See Reference links for more details.

3. VPN Gateway

VPNremote Phone Beta release 2 from Avaya requires that an Avaya Security Gateway (SG), Cisco VPN Concentrator or a Juniper gateway is used for the central VPN gateway.
.

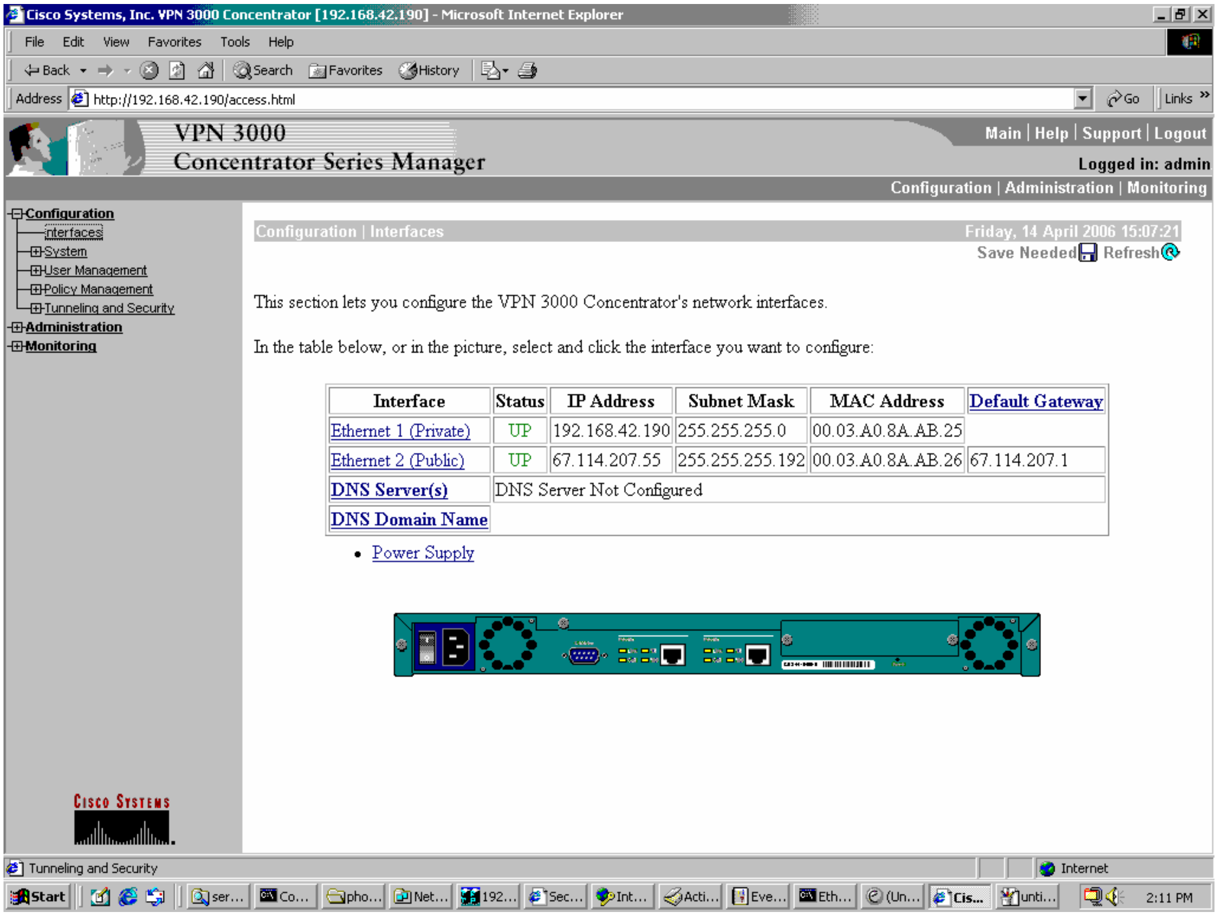
The basic configuration to support VPNemote phone would require the following:

1. Public and private interfaces configured
2. Static routes if needed
3. User accounts for local authentication or external authentication using Radius
4. VPN which includes your local networks, all users and the IKE and IPSec policies
5. IP address pool

Cisco Gateway

The following shows the basic VPN configuration that would be needed on Cisco VPN gateways.

Interfaces


Cisco Systems, Inc. VPN 3000 Concentrator [192.168.42.190] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://192.168.42.190/access.html
Go Links
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Policy Management
Tunneling and Security
Administration
Monitoring
Configuration | Interfaces
Friday, 14 April 2006 15:07:21
Save Needed Refresh
Cisco Systems
Tunneling and Security
Internet
Start
2:11 PM

This section lets you configure the VPN 3000 Concentrator's network interfaces.

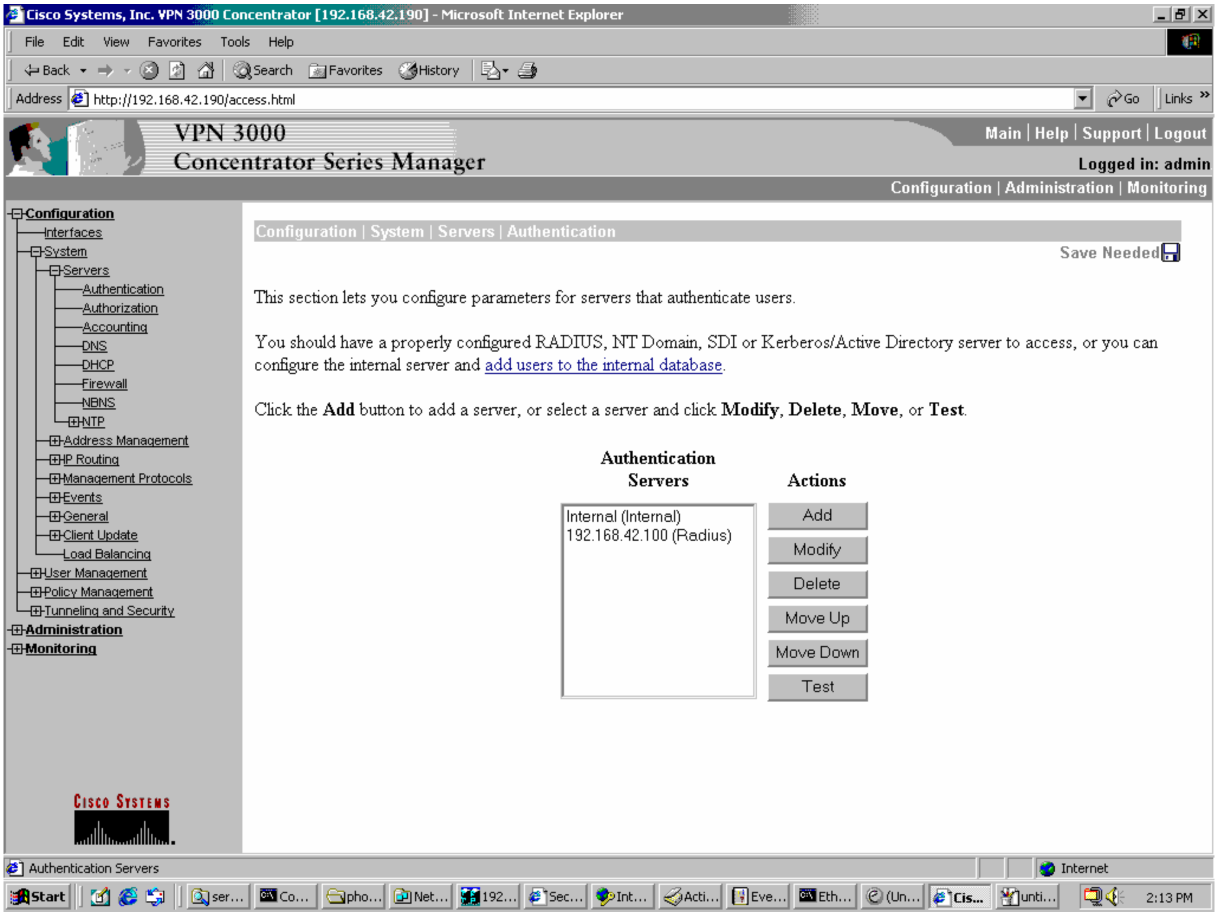
In the table below, or in the picture, select and click the interface you want to configure:

Interface	Status	IP Address	Subnet Mask	MAC Address	Default Gateway
Ethernet 1 (Private)	UP	192.168.42.190	255.255.255.0	00.03.A0.8A.AB.25	
Ethernet 2 (Public)	UP	67.114.207.55	255.255.255.192	00.03.A0.8A.AB.26	67.114.207.1
DNS Server(s)	DNS Server Not Configured				
DNS Domain Name					

- Power Supply

Authentication Servers:

Configure the Authentication servers for either internal authentication or external Radius authentication.



This section lets you configure parameters for servers that authenticate users.

You should have a properly configured RADIUS, NT Domain, SDI or Kerberos/Active Directory server to access, or you can configure the internal server and add users to the internal database.

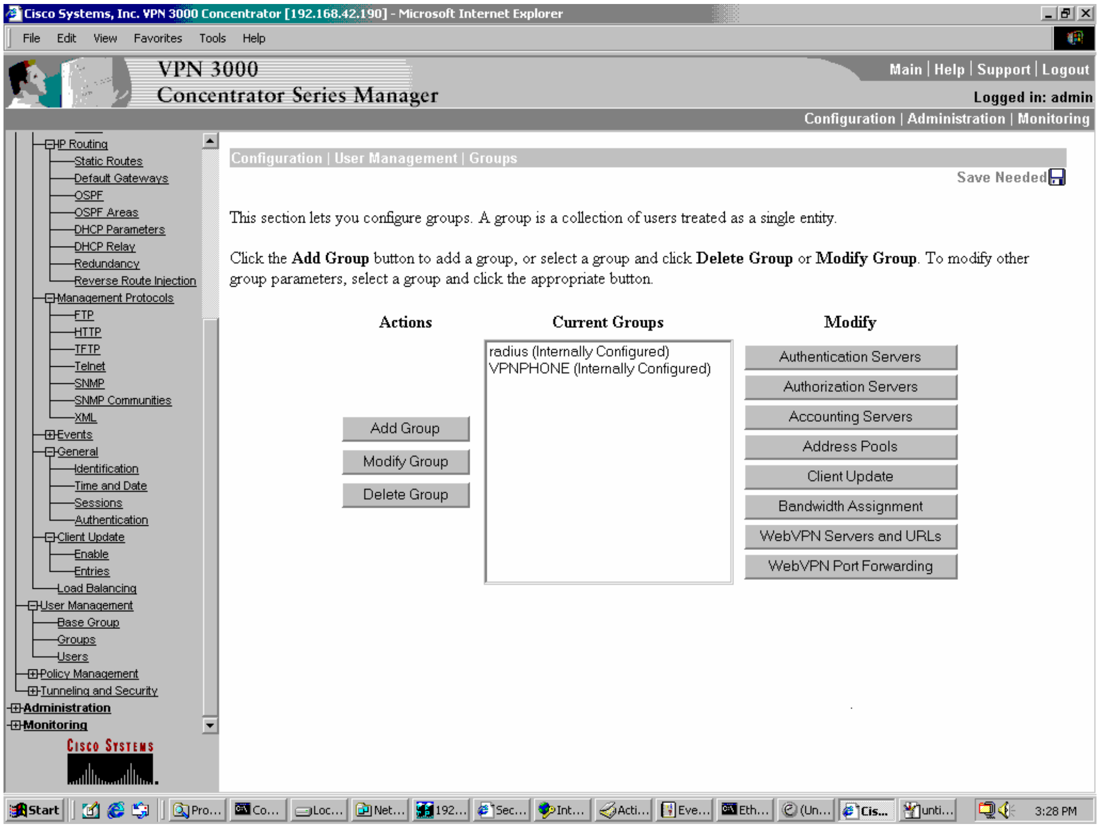
Click the **Add** button to add a server, or select a server and click **Modify**, **Delete**, **Move**, or **Test**.

Internal (Internal)
192.168.42.100 (Radius)

Group Configuration:

A group name can be configured to used with either internal users which are authenticated by the Cisco or a group used for external Radius authentication. Configured under the option User Management.

VPNremote Phone



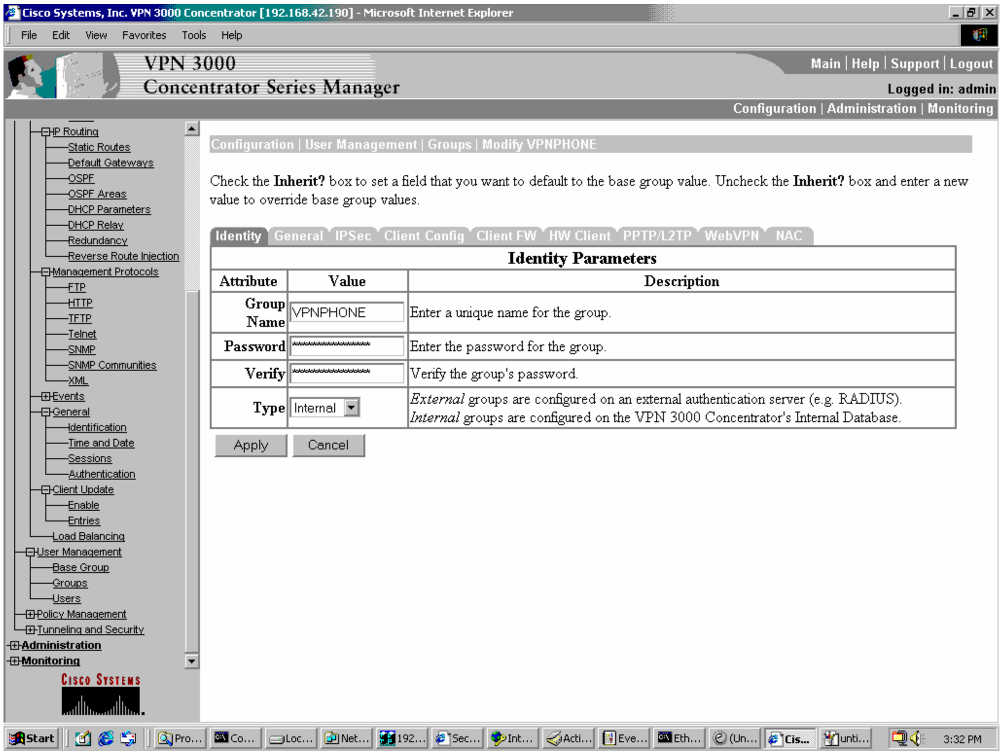
Configuration | User Management | Groups

This section lets you configure groups. A group is a collection of users treated as a single entity.

Click the **Add Group** button to add a group, or select a group and click **Delete Group** or **Modify Group**. To modify other group parameters, select a group and click the appropriate button.

Actions **Current Groups** **Modify**

radius (Internally Configured)
VPNPHONE (Internally Configured)



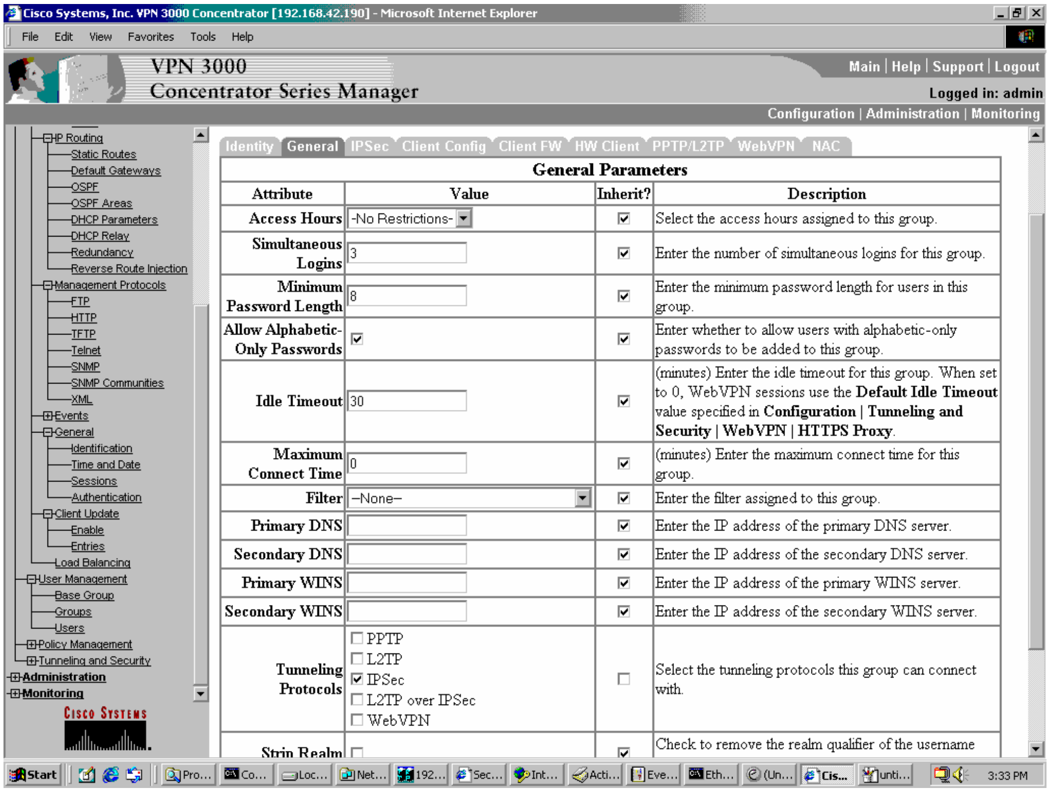
Configuration | User Management | Groups | Modify VPNPHONE

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity Parameters

Attribute	Value	Description
Group Name	VPNPHONE	Enter a unique name for the group.
Password	****************	Enter the password for the group.
Verify	****************	Verify the group's password.
Type	Internal	*External* groups are configured on an external authentication server (e.g. RADIUS). *Internal* groups are configured on the VPN 3000 Concentrator's Internal Database.

VPNremote Phone

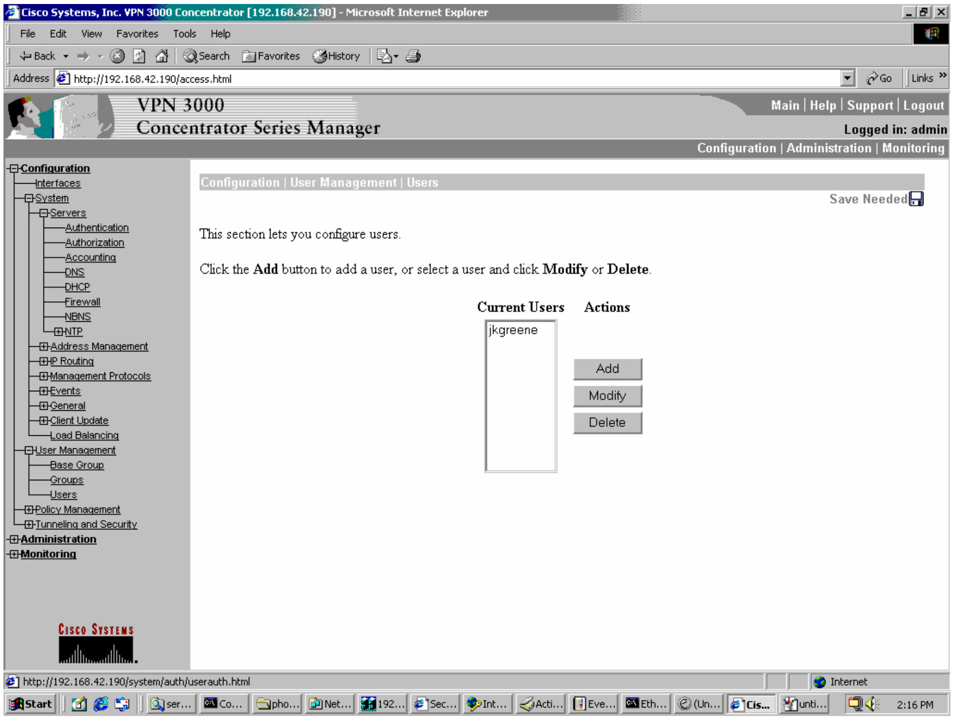


General Parameters

Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	☑	Select the access hours assigned to this group.
Simultaneous Logins	3	☑	Enter the number of simultaneous logins for this group.
Minimum Password Length	8	☑	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	☑	☑	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	☑	(minutes) Enter the idle timeout for this group. When set to 0, WebVPN sessions use the **Default Idle Timeout** value specified in **Configuration** | **Tunneling and Security** | **WebVPN** | **HTTPS Proxy**.
Maximum Connect Time	0	☑	(minutes) Enter the maximum connect time for this group.
Filter	–None–	☑	Enter the filter assigned to this group.
Primary DNS		☑	Enter the IP address of the primary DNS server.
Secondary DNS		☑	Enter the IP address of the secondary DNS server.
Primary WINS		☑	Enter the IP address of the primary WINS server.
Secondary WINS		☑	Enter the IP address of the secondary WINS server.
Tunneling Protocols	□ PPTP □ L2TP ☑ IPSec □ L2TP over IPSec □ WebVPN	□	Select the tunneling protocols this group can connect with.
Strip Realm	□	☑	Check to remove the realm qualifier of the username

Internal User:

Configure users under the User management option.



Configuration | User Management | Users

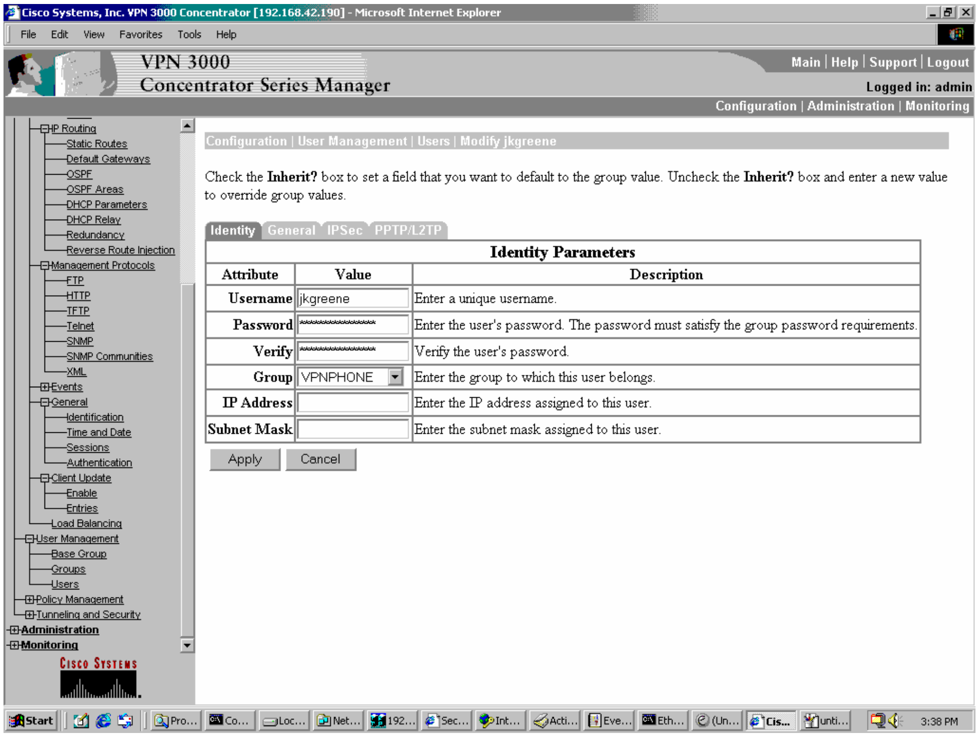
Save Needed

This section lets you configure users.

Click the **Add** button to add a user, or select a user and click **Modify** or **Delete**.

Current Users	Actions
jkgreene	Add Modify Delete

VPNremote Phone

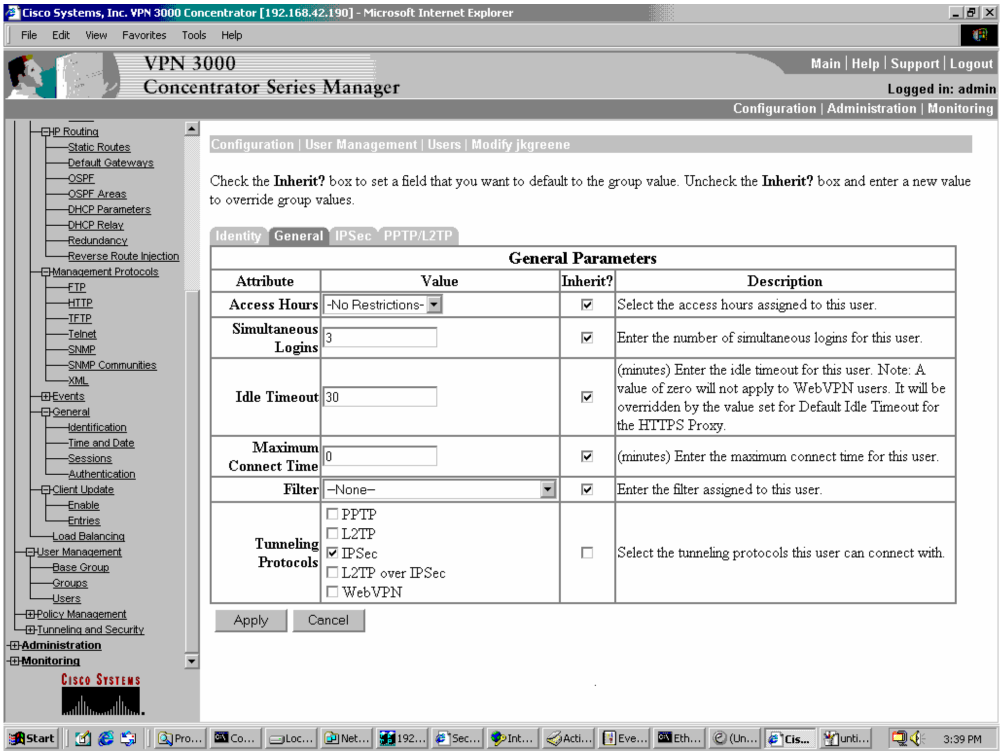


Configuration | User Management | Users | Modify jkgreene

Check the **Inherit?** box to set a field that you want to default to the group value. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity Parameters

Attribute	Value	Description
Username	jkgreene	Enter a unique username.
Password	******************	Enter the user's password. The password must satisfy the group password requirements.
Verify	******************	Verify the user's password.
Group	VPNPHONE	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.



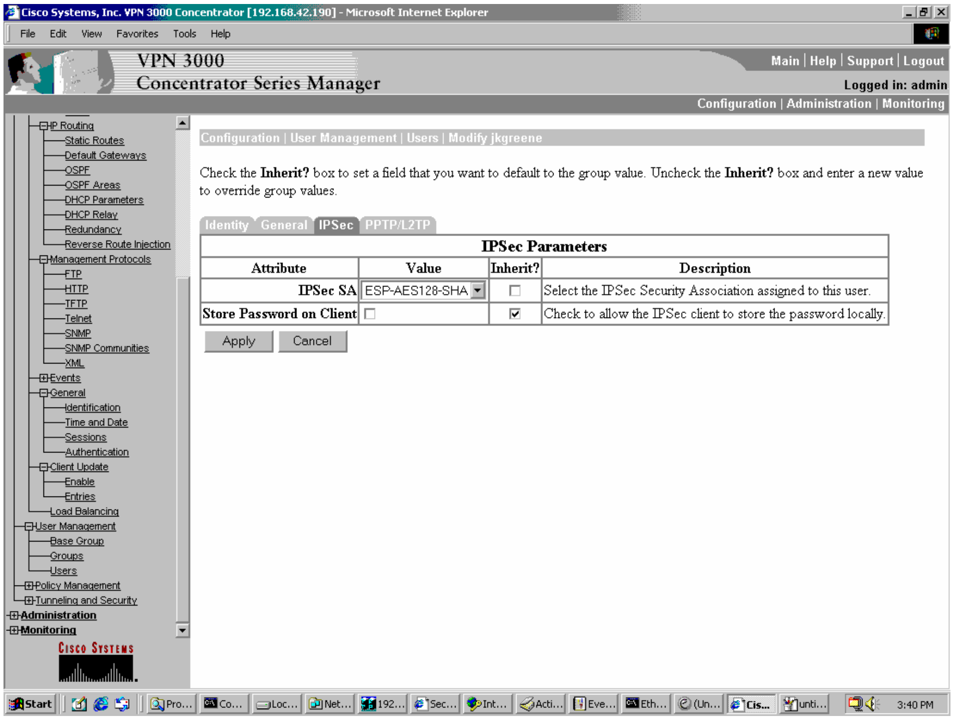
Configuration | User Management | Users | Modify jkgreene

Check the **Inherit?** box to set a field that you want to default to the group value. Uncheck the **Inherit?** box and enter a new value to override group values.

General Parameters

Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	☑	Select the access hours assigned to this user.
Simultaneous Logins	3	☑	Enter the number of simultaneous logins for this user.
Idle Timeout	30	☑	(minutes) Enter the idle timeout for this user. Note: A value of zero will not apply to WebVPN users. It will be overridden by the value set for Default Idle Timeout for the HTTPS Proxy.
Maximum Connect Time	0	☑	(minutes) Enter the maximum connect time for this user.
Filter	–None–	☑	Enter the filter assigned to this user.
Tunneling Protocols	□ PPTP □ L2TP ☑ IPSec □ L2TP over IPSec □ WebVPN	□	Select the tunneling protocols this user can connect with.

VPNremote Phone



Configuration | User Management | Users | Modify jkgreene

Check the **Inherit?** box to set a field that you want to default to the group value. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity | General | IPSec | PPTP/L2TP

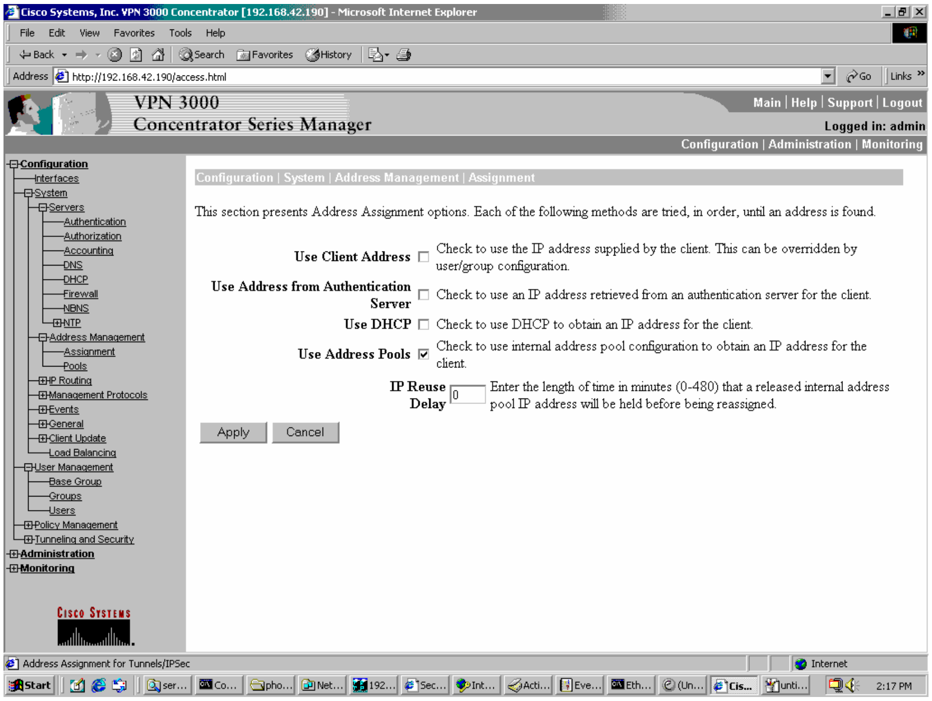
IPSec Parameters

Attribute	Value	Inherit?	Description
IPSec SA	ESP-AES128-SHA	□	Select the IPSec Security Association assigned to this user.
Store Password on Client	□	☑	Check to allow the IPSec client to store the password locally.

Apply | Cancel

IP Address Pool Configuration

Enable the option to use the client IP address pool under the Address Management option.



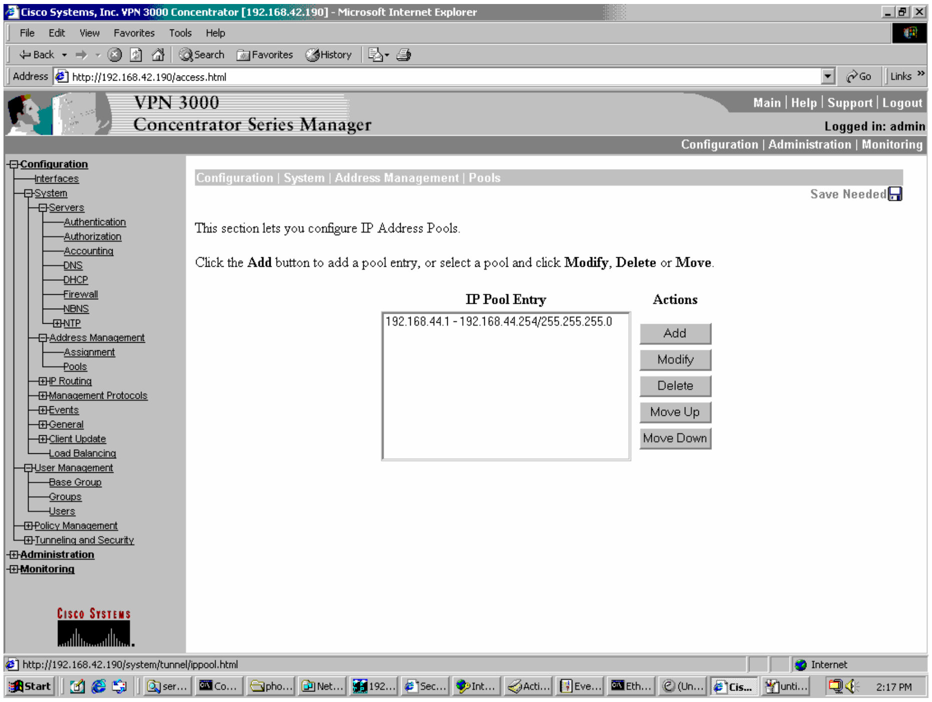
Configuration | System | Address Management | Assignment

This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.

Use Client Address	□	Check to use the IP address supplied by the client. This can be overridden by user/group configuration.
Use Address from Authentication Server	□	Check to use an IP address retrieved from an authentication server for the client.
Use DHCP	□	Check to use DHCP to obtain an IP address for the client.
Use Address Pools	☑	Check to use internal address pool configuration to obtain an IP address for the client.
IP Reuse Delay	0	Enter the length of time in minutes (0-480) that a released internal address pool IP address will be held before being reassigned.

Apply | Cancel

Configure the Client IP address range.



Cisco Systems, Inc. VPN 3000 Concentrator [192.168.42.190] - Microsoft Internet Explorer

Address http://192.168.42.190/access.html

VPN 3000 Concentrator Series Manager

Logged in: admin

Configuration | System | Address Management | Pools

Save Needed

This section lets you configure IP Address Pools.

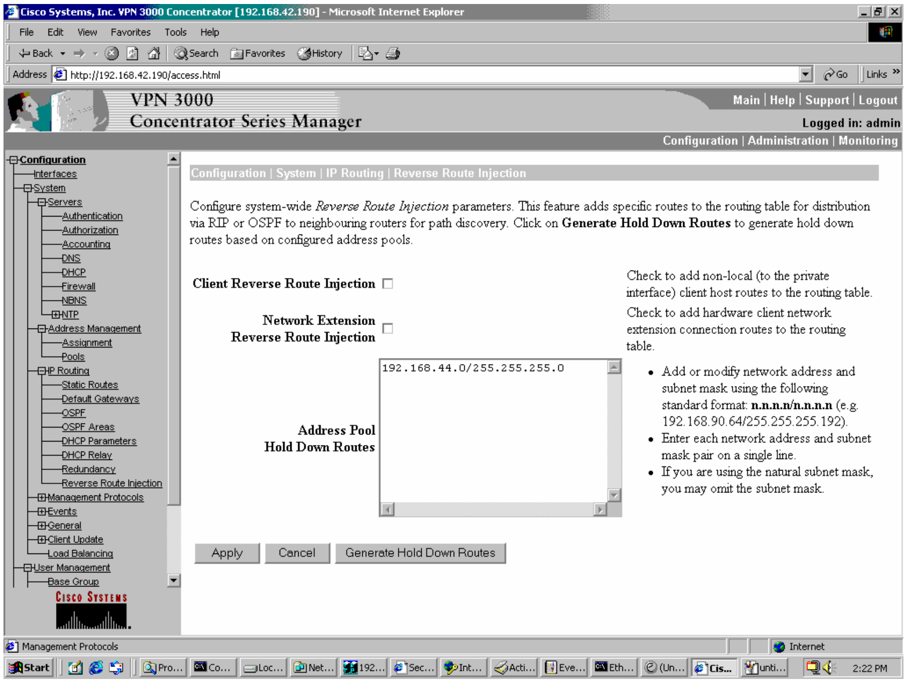
Click the **Add** button to add a pool entry, or select a pool and click **Modify**, **Delete** or **Move**.

IP Pool Entry

192.168.44.1 - 192.168.44.254/255.255.255.0

http://192.168.42.190/system/tunnel/ippool.html

The Reverse route injection must be configured under the Routing option. Click on the “Generate Hold Down routes” for configuration.



Cisco Systems, Inc. VPN 3000 Concentrator [192.168.42.190] - Microsoft Internet Explorer

Address http://192.168.42.190/access.html

VPN 3000 Concentrator Series Manager

Logged in: admin

Configuration | System | IP Routing | Reverse Route Injection

Configure system-wide *Reverse Route Injection* parameters. This feature adds specific routes to the routing table for distribution via RIP or OSPF to neighbouring routers for path discovery. Click on **Generate Hold Down Routes** to generate hold down routes based on configured address pools.

Client Reverse Route Injection □ Check to add non-local (to the private interface) client host routes to the routing table.

Network Extension Reverse Route Injection □ Check to add hardware client network extension connection routes to the routing table.

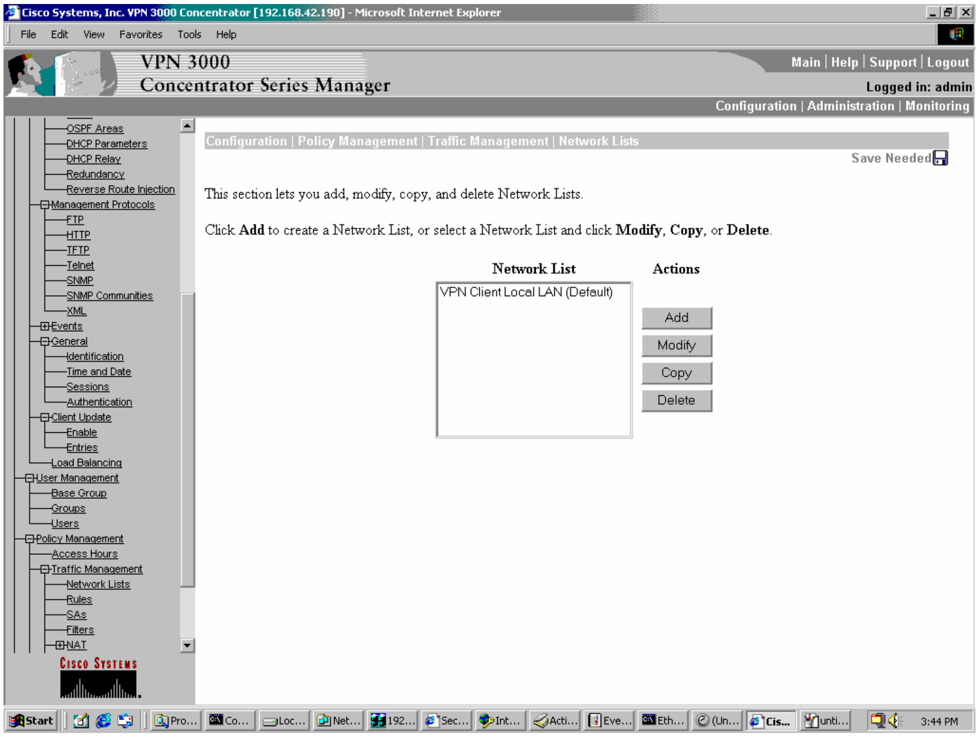
Address Pool Hold Down Routes: 192.168.44.0/255.255.255.0

- Add or modify network address and subnet mask using the following standard format: **n.n.n.n/n.n.n.n** (e.g. 192.168.90.64/255.255.255.192).
- Enter each network address and subnet mask pair on a single line.
- If you are using the natural subnet mask, you may omit the subnet mask.

Management Protocols

Network List

The network list defines all the networks that are protected by the gateway on the private side. Using a network of 0.0.0.0/0.0.0.0 provides support for all private networks and simplifies the configuration.



Configuration | Policy Management | Traffic Management | Network Lists

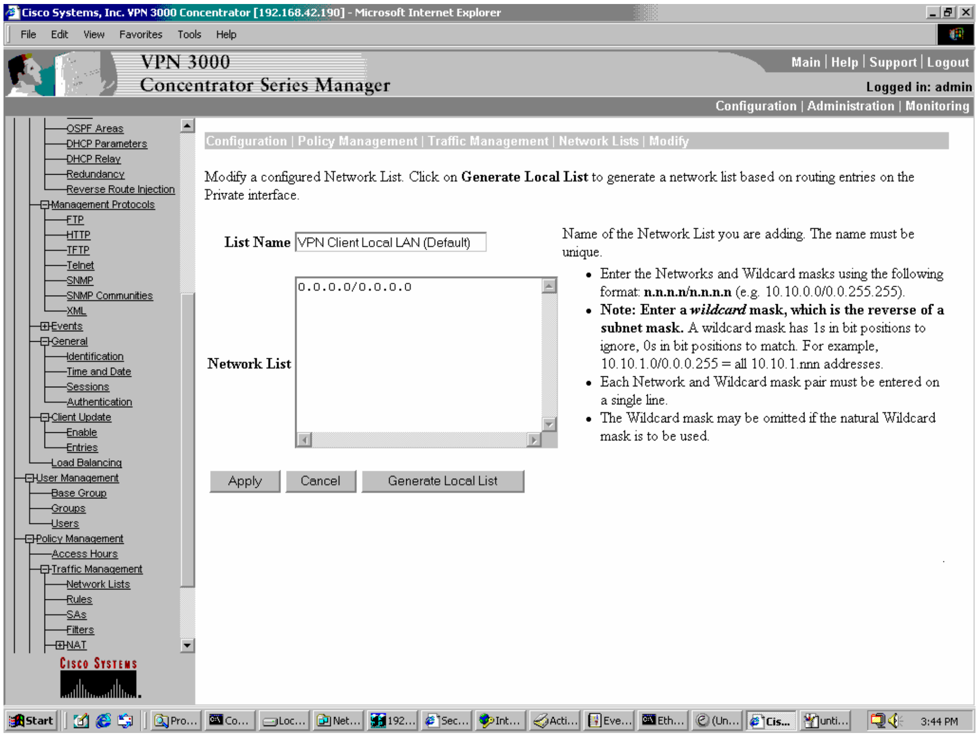
Save Needed

This section lets you add, modify, copy, and delete Network Lists.

Click **Add** to create a Network List, or select a Network List and click **Modify**, **Copy**, or **Delete**.

Network List: VPN Client Local LAN (Default)

Actions



Configuration | Policy Management | Traffic Management | Network Lists | Modify

Modify a configured Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name: VPN Client Local LAN (Default)

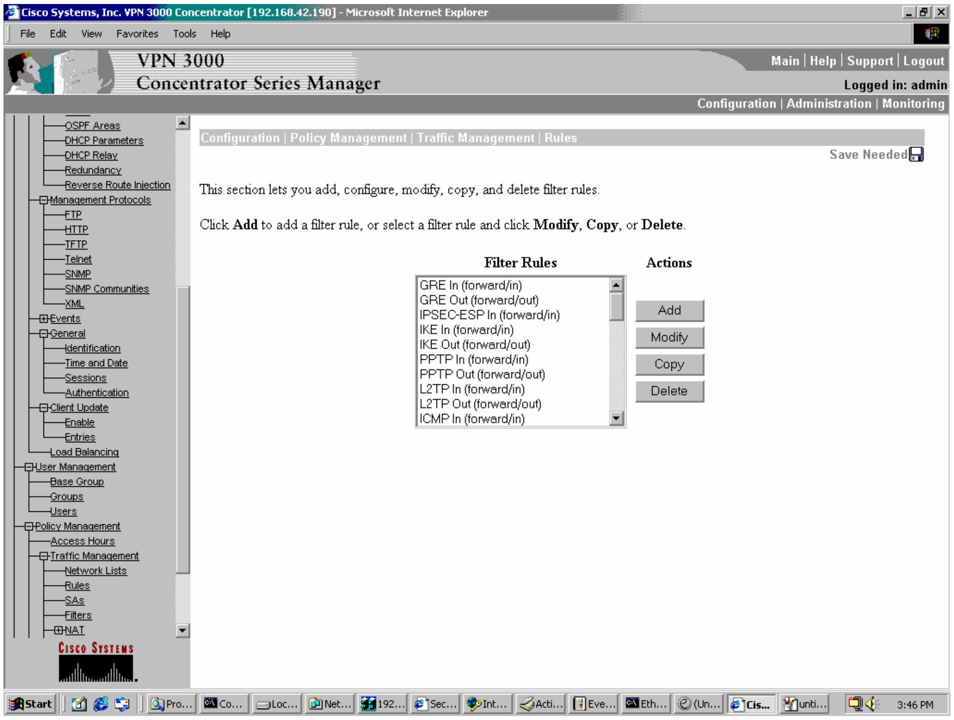
Name of the Network List you are adding. The name must be unique.

Network List: 0.0.0.0/0.0.0.0

- Enter the Networks and Wildcard masks using the following format: **n.n.n.n/n.n.n.n** (e.g. 10.10.0.0/0.0.255.255).
- **Note: Enter a *wildcard* mask, which is the reverse of a subnet mask.** A wildcard mask has 1s in bit positions to ignore, 0s in bit positions to match. For example, 10.10.1.0/0.0.0.255 = all 10.10.1.nnn addresses.
- Each Network and Wildcard mask pair must be entered on a single line.
- The Wildcard mask may be omitted if the natural Wildcard mask is to be used.

Traffic Manager

Configure the traffic filter rules to define what traffic will be allowed. The default rules cover the standard VPN rules required.



Configuration | Policy Management | Traffic Management | Rules

Save Needed

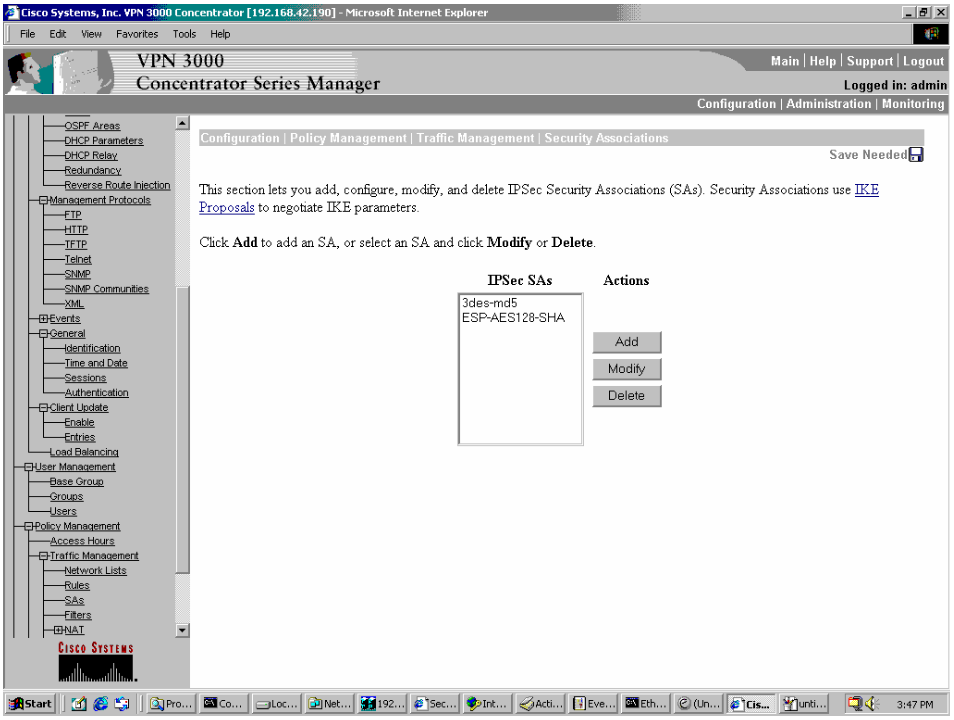
This section lets you add, configure, modify, copy, and delete filter rules.

Click **Add** to add a filter rule, or select a filter rule and click **Modify**, **Copy**, or **Delete**.

Filter Rules **Actions**

GRE In (forward/in)
GRE Out (forward/out)
IPSEC-ESP In (forward/in)
IKE In (forward/in)
IKE Out (forward/out)
PPTP In (forward/in)
PPTP Out (forward/out)
L2TP In (forward/in)
L2TP Out (forward/out)
ICMP In (forward/in)

Configure the IKE and IPSec encryption type for the VPN



Configuration | Policy Management | Traffic Management | Security Associations

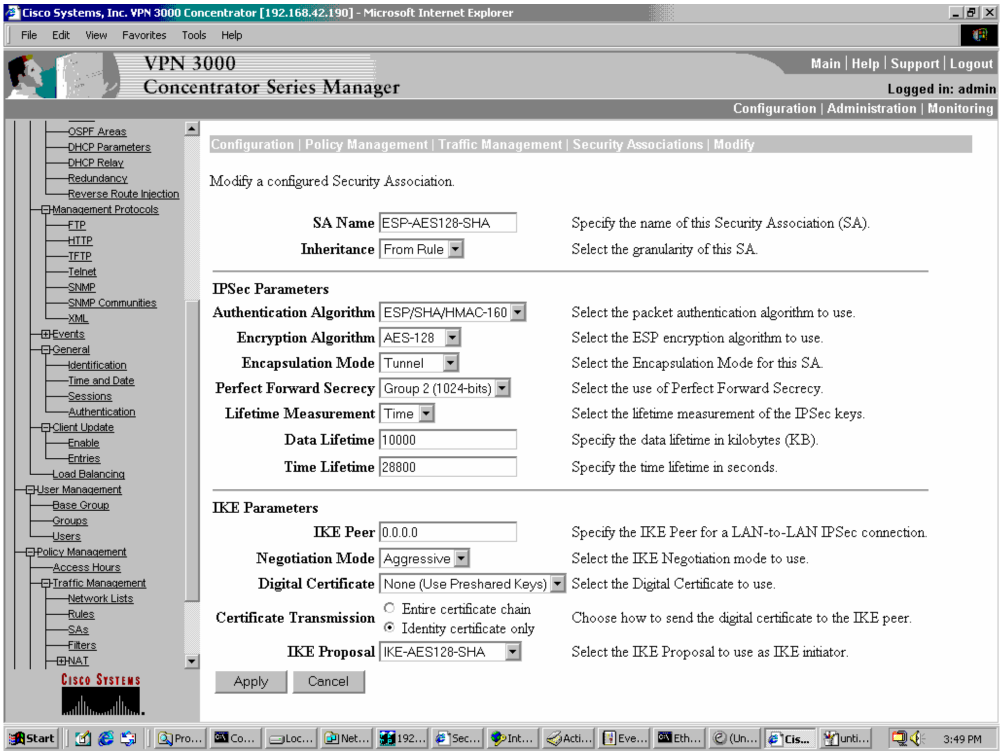
Save Needed

This section lets you add, configure, modify, and delete IPSec Security Associations (SAs). Security Associations use IKE Proposals to negotiate IKE parameters.

Click **Add** to add an SA, or select an SA and click **Modify** or **Delete**.

IPSec SAs **Actions**

3des-md5
ESP-AES128-SHA



Configuration | Policy Management | Traffic Management | Security Associations | Modify

Modify a configured Security Association.

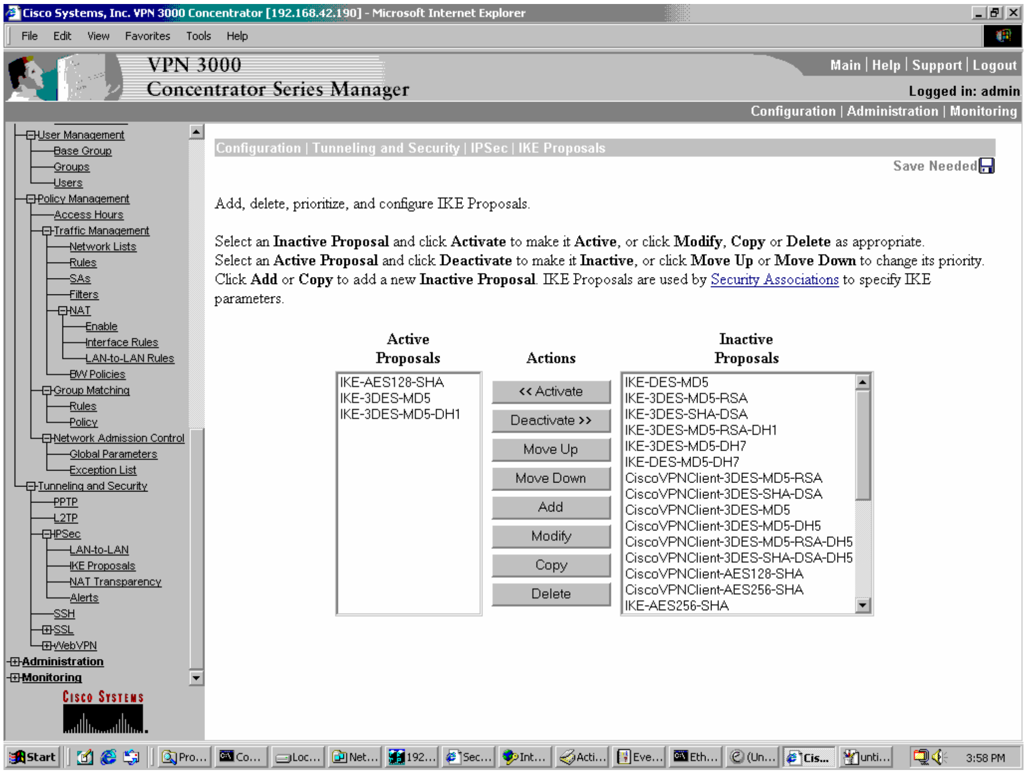
SA Name	ESP-AES128-SHA	Specify the name of this Security Association (SA).
Inheritance	From Rule	Select the granularity of this SA.

IPSec Parameters

Authentication Algorithm	ESP/SHA/HMAC-160	Select the packet authentication algorithm to use.
Encryption Algorithm	AES-128	Select the ESP encryption algorithm to use.
Encapsulation Mode	Tunnel	Select the Encapsulation Mode for this SA.
Perfect Forward Secrecy	Group 2 (1024-bits)	Select the use of Perfect Forward Secrecy.
Lifetime Measurement	Time	Select the lifetime measurement of the IPSec keys.
Data Lifetime	10000	Specify the data lifetime in kilobytes (KB).
Time Lifetime	28800	Specify the time lifetime in seconds.

IKE Parameters

IKE Peer	0.0.0.0	Specify the IKE Peer for a LAN-to-LAN IPSec connection.
Negotiation Mode	Aggressive	Select the IKE Negotiation mode to use.
Digital Certificate	None (Use Preshared Keys)	Select the Digital Certificate to use.
Certificate Transmission	○ Entire certificate chain ● Identity certificate only	Choose how to send the digital certificate to the IKE peer.
IKE Proposal	IKE-AES128-SHA	Select the IKE Proposal to use as IKE initiator.



Configuration | Tunneling and Security | IPSec | IKE Proposals

Save Needed

Add, delete, prioritize, and configure IKE Proposals.

Select an **Inactive Proposal** and click **Activate** to make it **Active**, or click **Modify**, **Copy** or **Delete** as appropriate.
Select an **Active Proposal** and click **Deactivate** to make it **Inactive**, or click **Move Up** or **Move Down** to change its priority.
Click **Add** or **Copy** to add a new **Inactive Proposal**. IKE Proposals are used by Security Associations to specify IKE parameters.

Active Proposals	Actions	Inactive Proposals
IKE-AES128-SHA IKE-3DES-MD5 IKE-3DES-MD5-DH1	<< Activate Deactivate >> Move Up Move Down Add Modify Copy Delete	IKE-DES-MD5 IKE-3DES-MD5-RSA IKE-3DES-SHA-DSA IKE-3DES-MD5-RSA-DH1 IKE-3DES-MD5-DH7 IKE-DES-MD5-DH7 CiscoVPNClient-3DES-MD5-RSA CiscoVPNClient-3DES-SHA-DSA CiscoVPNClient-3DES-MD5 CiscoVPNClient-3DES-MD5-DH5 CiscoVPNClient-3DES-MD5-RSA-DH5 CiscoVPNClient-3DES-SHA-DSA-DH5 CiscoVPNClient-AES128-SHA CiscoVPNClient-AES256-SHA IKE-AES256-SHA

4. VPNremote Phone Setup

- When the phone reboots, when you see the screen that says " * to program" press the the * key
- Press the # key until you see the screen that says "VPN Configuration, * to modify". Press the * key.
- Select option "Profile"
- Select option "Modify"
- Select desired profile. i.e "Cisco Xauth with PSK"
- Select "Done"
- Select User Name and configure user id
- Select option 'Password" and configure password
- Select option " Group Name" and enter group name provide by administrator and save (You may need to press the large right arrow key to see this)
- Select option " Group PSK " and enter group pre-shared key provided by the administrator, save
- Press the large right arrow key until you see the option IKE Parameters, use soft key to select
- Select DH group key and change value to desired value provided by administrator and press Done
- Select option " IPSec Parameters", change DH group to desired value and press Done.
- Select Done and restart your phone. It will now connect to the new gateway.

5. Deployment Recommendations

All phones must be upgraded to the VPNremote phone firmware on the corporate network before deployment to user. This will allow the phone to be prepared for the user to complete the configuration specific to his needs. This is done by having a HTTP or TFTP server on the corporate network that is accessible.

HTTP and TFTP Servers
Copy all preconfigured upgrade, setting and binary files provided with the VPNremote firmware to the server.

Since Remote firmware upgrades takes longer than local upgrades, sufficient number of TFTP servers must be available to support the user population or upgrades will need to be performed staggered.

IP Telephone Conversion
Plug the phone into the corporate network until it comes up. Once up modify the group number by entering “mute 47687#”. Configure the address of the TFTP server and reboot the phone. The phone now will upgrade it’s firmware to the VPNremote phone firmware. The group number is defined by the administrator and configure in the setting and vpnupgrade.scr files.

Configuration for the VPNremote phone can be delivered by HTTP/TFTP servers as listed above.

6. Supported Phone Models

The following is a list of supported phone models that the VPNremote phone firmware is supported on.

4610SW, 4620SW, 4621SW, 4622SW, 4625SW

7. Errors

The following lists possible error messages that may be seen on the VPNremote phone and possible steps to take to resolve the issue.

Error message	Possible Solution
Authentication failure, User Blocked	Wait for 3-5 minutes and try to reconnect.
Invalid password OR user name	Confirm the correct user name or password is being entered
Phone brand rejected by SG	Phone branding is not configured on gateway you are connecting to, confirm the VPN server address.
VPN Topology not supported	Multiple central site devices configured which is not a supported configuration. (This error should not be seen in Avaya)
Empty Gate Keeper List	No call server addresses configured. Use MUTE addr# to confirm setting
TCP/IP Connection Failure	Confirm VPN server address is correct. Use MUTE vpnmod# Confirm the Gateway is available Confirm VPNremote Phone has internet connectivity Disable 802.1q. Use MUTE addr# Check local router to see if IPSec pass thru is enabled

8. Firewalls

The following is a list of all ports and protocols that must be permitted to pass through any local or remote firewall.

TCP 1443, UDP 500, UDP 2070, UDP 4500, IP Protocol 50 (esp)

9. Troubleshooting

1. Authentication Failures

- Check User ID and password configured on phone
- Check Event log on Security gateway
- Check Configured User ID and password on Gateway
- If external authentication is used such as Radius, check connectivity between SG and Radius and Radius User configuration

3. TCP/IP Connection Failure

- Confirm VPN server address is correct.
- Confirm the Gateway is available
- Confirm VPNremote Phone has internet connectivity

4. SSL Connection Failure

- Confirm ssl 1443 is not blocked by external device
- Confirm Security Gateway is accepting ssl connections

5. General Phone Errors and Behaviors

- Contact DHCP/TFTP administrator, L2Q parms in option 43/176 or xxx.SCR script file have looping conditions, caused by the Gateway address set to 0.0.0.0
- Loading ……. is not seen during startup and mute light flashes
  1. Check the boot code version. Older version such as 1.9x is not compatible with the latest 2.3 GA version.

6. IKE and IPSec Negotiation Failures

- Enable IKE Logging on the Security Gateway

7. Phone fails to register

- Confirm the VPN tunnel was built
  1. Check if SAs are built on Security gateway
  2. When the VPNremote Phone starts, does it access the TFTP server through the VPN tunnel? If it does then the tunnel is up to that network. Check to see if the call server is on the same subnet as the TFTP server. If configured IP group in Security Gateway covers all networks, then access should be available.

10. References

Information on 4600 Series IP Telephones
http://www.avaya.com/gcm/master-usa/en-us/products/offers/4600_series_ip_telephones.htm

Information on the SG203 and SG208 Product Line
http://www.avaya.com/gcm/master-usa/en-us/products/offers/sg203_sg208_security_gateways.htm

Security and Avaya Communication Manager Media Servers
http://support.avaya.com/elmodocs2/s8700/docs/Media_Server_Security.pdf

Avaya IP Telephony Implementation Guide for CM3.0
http://support.avaya.com/elmodocs2/comm_mgr/r3/IP_GUIDE_3.0.pdf

IP Telephony Deployment Guide
http://support.avaya.com/elmodocs2/comm_mgr/r3/pdfs/245600_3_4_1.pdf

Administrator Guide for Communication Manager
http://support.avaya.com/elmodocs2/comm_mgr/r3/pdfs/03_300509_1.pdf

VPNremote Phone Administrators Guide
http://support.avaya.com/elmodocs2/4600/19_600753_1.pdf

DSLreports – test internet connection speeds
http://www.dslreports.com/tools