Cisco VPN 3000 Series Concentrator oMG Setup Guide For VPN 3000 and oMG-2000 Release 3.9+

oMG

SIERRA WIRELESS®

oMG-ED-071010
1.3
June 17, 2015

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the Sierra Wireless modem are used in a normal manner with a well-constructed network, the Sierra Wireless modem should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Sierra Wireless accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the Sierra Wireless modem, or for failure of the Sierra Wireless modem to transmit or receive such data.

Safety and Hazards

Do not operate the Sierra Wireless modem in areas where cellular modems are not advised without proper device certifications. These areas include environments where cellular radio can interfere such as explosive atmospheres, medical equipment, or any other equipment which may be susceptible to any form of radio interference. The Sierra Wireless modem can transmit signals that could interfere with this equipment.

The driver or operator of any vehicle should not operate the Sierra Wireless modem while in control of a vehicle. Doing so will detract from the driver or operator’s control and operation of that vehicle. In some states and provinces, operating such communications devices while in control of a vehicle is an offence.

Limitations of Liability

This manual is provided “as is”. Sierra Wireless makes no warranties of any kind, either expressed or implied, including any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. The recipient of the manual shall endorse all risks arising from its use.

The information in this manual is subject to change without notice and does not represent a commitment on the part of Sierra Wireless. SIERRA WIRELESS AND ITS AFFILIATES SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE OR ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE ANY SIERRA WIRELESS PRODUCT, EVEN IF SIERRA WIRELESS AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THEY ARE FORESEEABLE OR FOR CLAIMS BY ANY THIRD PARTY.

Notwithstanding the foregoing, in no event shall Sierra Wireless and/or its affiliates aggregate liability arising under or in connection with the Sierra Wireless product, regardless of the number of events, occurrences, or claims giving rise to liability, be in excess of the price paid by the purchaser for the Sierra Wireless product.

Customer understands that Sierra Wireless is not providing cellular or GPS (including A-GPS) services. These services are provided by a third party and should be purchased directly by the Customer.

SPECIFIC DISCLAIMERS OF LIABILITY: CUSTOMER RECOGNIZES AND ACKNOWLEDGES SIERRA WIRELESS IS NOT RESPONSIBLE FOR AND SHALL NOT BE HELD LIABLE FOR ANY DEFECT OR DEFICIENCY OF ANY KIND OF CELLULAR OR GPS (INCLUDING A-GPS) SERVICES.

Patents

This product may contain technology developed by or for Sierra Wireless Inc.

This product may include technology licensed from QUALCOMM®.

This product is manufactured or sold by Sierra Wireless Inc. or its affiliates under one or more patents licensed from InterDigital Group and MMP Portfolio Licensing.

Copyright

Trademarks

Sierra Wireless®, AirPrime®, AirLink®, AirVantage®, WISMO® and the Sierra Wireless and Open AT logos are registered trademarks of Sierra Wireless, Inc. or one of its subsidiaries.

Windows® and Windows Vista® are registered trademarks of Microsoft Corporation.

Macintosh® and Mac OS X® are registered trademarks of Apple Inc., registered in the U.S. and other countries.

QUALCOMM® is a registered trademark of QUALCOMM Incorporated. Used under license.

Other trademarks are the property of their respective owners.

Contact Information

Sales Desk:	Phone:	1-604-232-1488
	Hours:	8:00 AM to 5:00 PM Pacific Time
	Contact:	http://www.sierrawireless.com/sales
Post:	Sierra Wireless 13811 Wireless Way Richmond, BC Canada V6V 3A4	
Technical Support:	Hours:	6:30 AM to 4:30 PM Pacific Time
	Email:	imt-support@sierrawireless.com
	Phone:	1-866-468-2968
	KBase:	http://imt-kbase.sierrawireless.com/
Web:	http://www.sierrawireless.com/	

Consult our website for up-to-date product descriptions, documentation, application notes, firmware upgrades, troubleshooting tips, and press releases: www.sierrawireless.com

Document History

Version	Date	Updates
1.3	June 17 2015	Updated to SWI Template. SWI Logo updates.

Contents

1. Introduction

This document provides an example of how to configure a Cisco VPN 3000 Series Concentrator to interoperate with an oMG1000 system using IPsec. Although differences will arise it may also serve as an example for configuring other Cisco VPN products. The actual model used in the example is the entry level 3005.

It is intended to serve as guide and your actual configuration will need to have different details. It is NOT intended to be a complete setup manual for the VPN 3000 and readers should refer to the CISCO documentation for additional details.

1.1. Who Should Read This Guide

Individuals tasked with configuring a Cisco VPN Server to interoperate with oMG1000 units should pay close attention to the configuration steps. Once the VPN server is correctly configured, the oMG1000 configuration is simple.

1.2. Why you should Read This Guide

There are numerous oMG1000s installations that have been successfully deployed with Cisco VPN servers. However, in almost every case, the most problematic step seems to be the configuration of the VPN server and we have NEVER experienced a situation that was not ultimately corrected by applying a suitable VPN server configuration.

We recommend you start with a new server configuration for your oMGs rather than to expand or modify an existing configuration. That seems to be the most reliable approach.

1.3. Related Publications

Title and Publication Number	Description
oMG1000 Installation Guide oMG-ED-060516	Describes how to install the oMG1000 into a vehicle.
oMG1000 Operation Guide oMG-ED-060416	Describes how to Operate the oMG1000.

2. VPN Principle of Operation

A VPN provides secure (authenticated and encrypted) data communications between end points.

The oMG1000 includes VPN client software that is compatible with the Cisco VPN protocol.

Although the 3005 supports VPN protocols such as PPTP and L2TP the oMG assumes plain-old IPsec mode which supports TCP/IP data communications.

The following firewall settings may need to be “opened” between the client on an oMG and the VPN server. Note these need only be done for an intermediate device (e.g. Service Provider firewall), not on the oMG or on the VPN server:

- UDP ports 500, 1000 and 10000
- IP protocol 50 (ESP)
- TCP port configured for IPsec/TCP
- NAT-T port 4500

3. Reference Network

Figure 1 provides a simplified network diagram that will be used in the example configuration. After successful configuration and commencement of normal operation, the laptop will be able to access the application server over the secure data channel by specifying the latter's IP address.

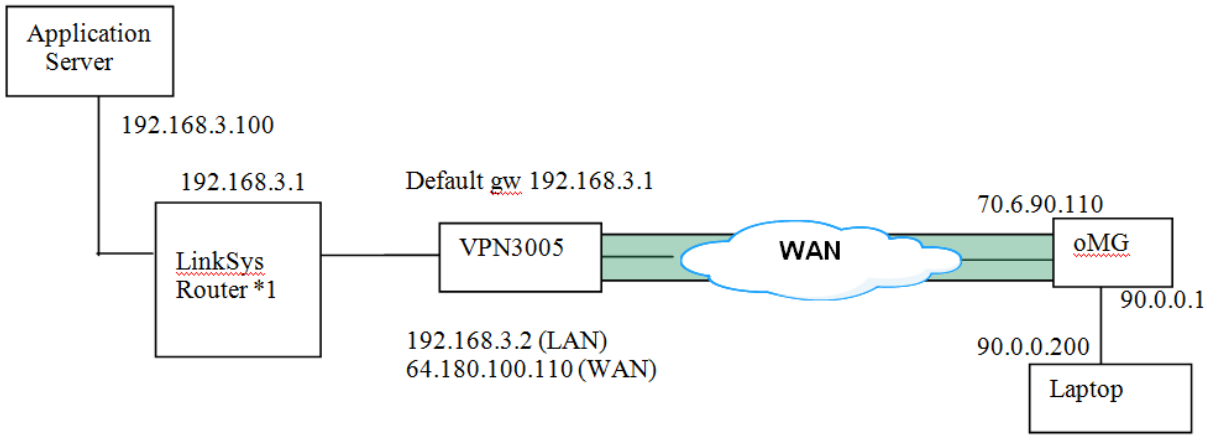


Figure 1 - Simplified Network

*1 Note that the application server and the VPN3005 are both connected to the LAN side of the Linksys unit to eliminate need for enterprise routing setup.

The remainder of this document assumes the simple network in Figure 1 has been established and configured with appropriate subnet masks.

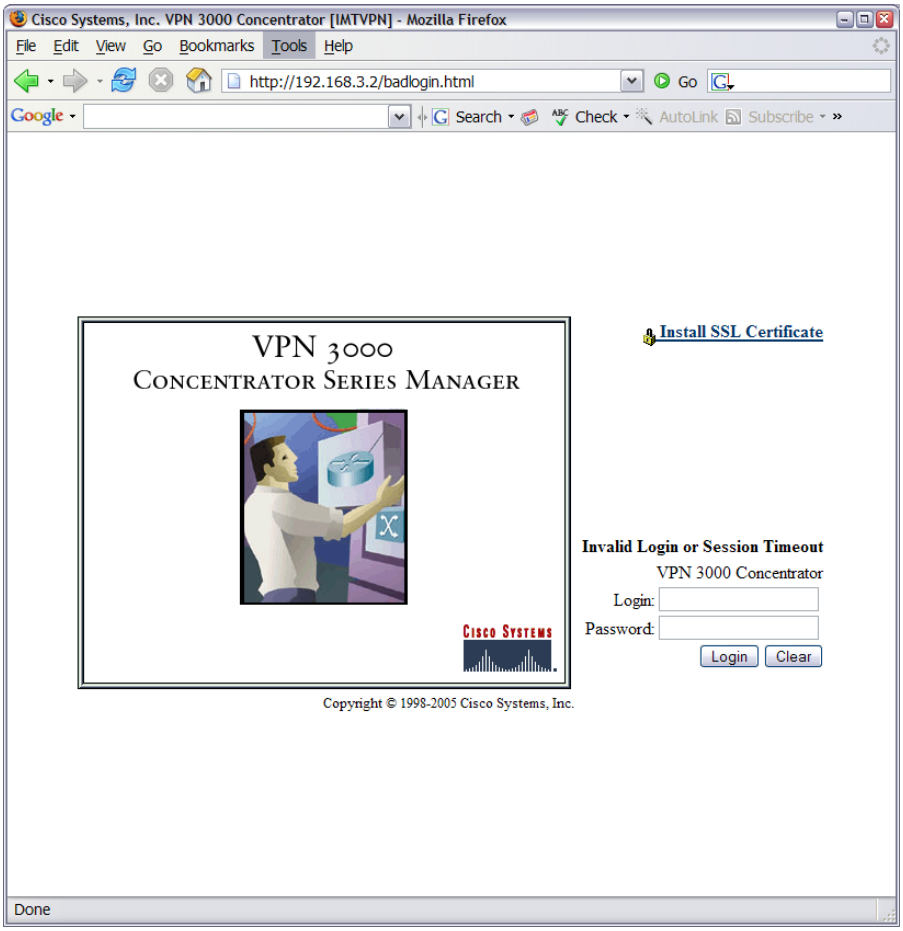
4. VPN SERVER CONFIGURATION

4.1. Login

The 3005 default access is user=admin, password=admin.

Using a PC (Not shown in Figure 1), connect to the LAN side of the VPN server and use a web browser (IE or FireFox).

Supply http://192.168.3.2 as the URL. A screen similar to the one below should appear.

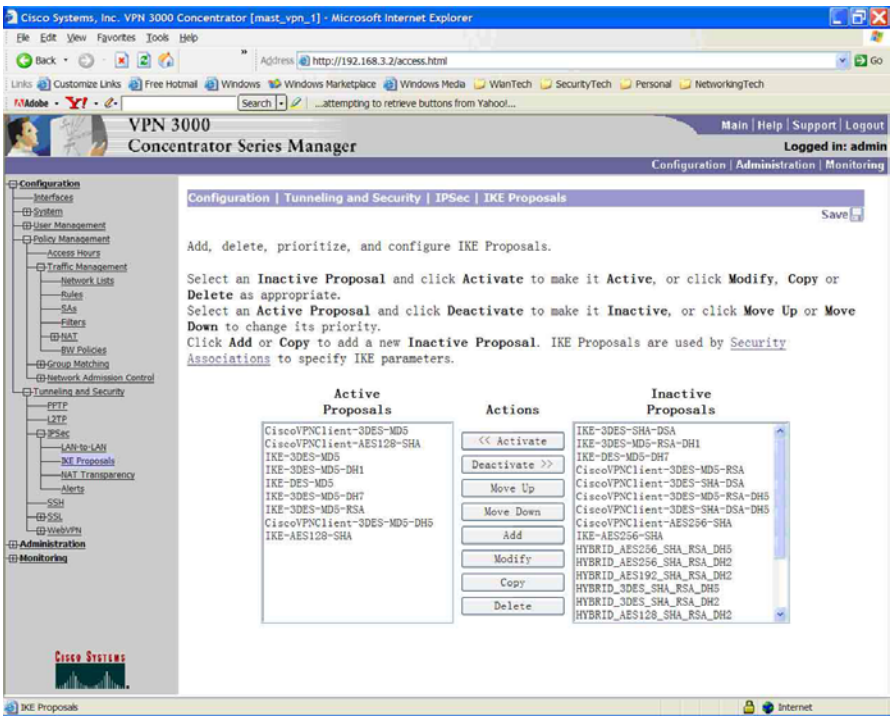


4.2. Active Proposal

Phase 1 of IPsec involves an exchange of security messages using encryption and hashing methods referred to as proposals. This step requires you to specify one that is compatible with the oMG.

Navigate to **Configuration->Tunneling and Security->IPSec->IKE Proposals** and select **CiscoVPNClient-3DES-MD5**.

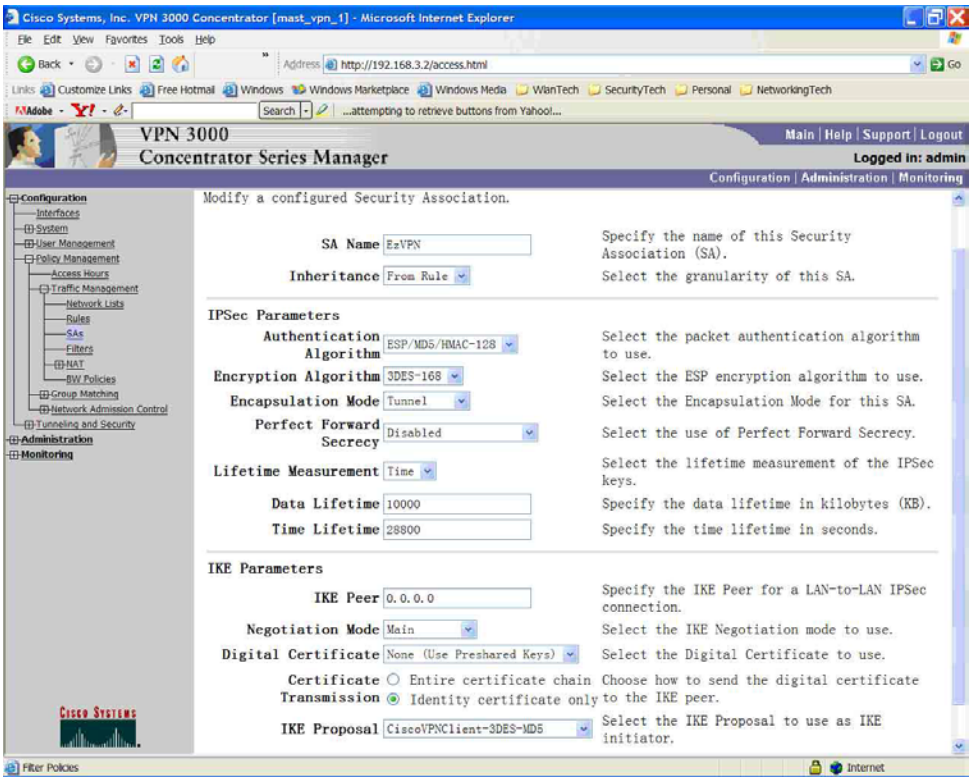
The screen shot is as follows:



4.3. Security Association

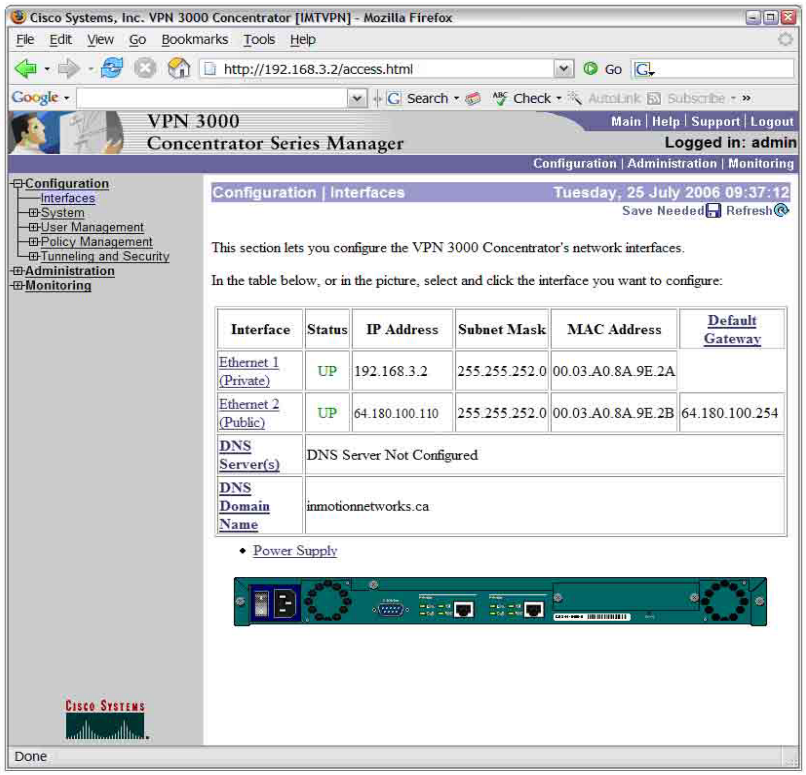
Phase 2 of IPsec requires specification of a security association that establishes the authentication and encryption scheme that will be used for data transfer.

Navigate to **Configuration->Policy Management->Traffic Management->SAs** and specify **ESP/MD5/HMACC-128, 3DES-168** and ensure the IKE parameter from the previous section is matching. The result should be similar to this screen shot:



4.4. Interface Setup

Navigate to **Configuration->Interfaces** and establish Ethernet 1 and 2 as private and public interfaces – examples as below.



4.5. Address Pool

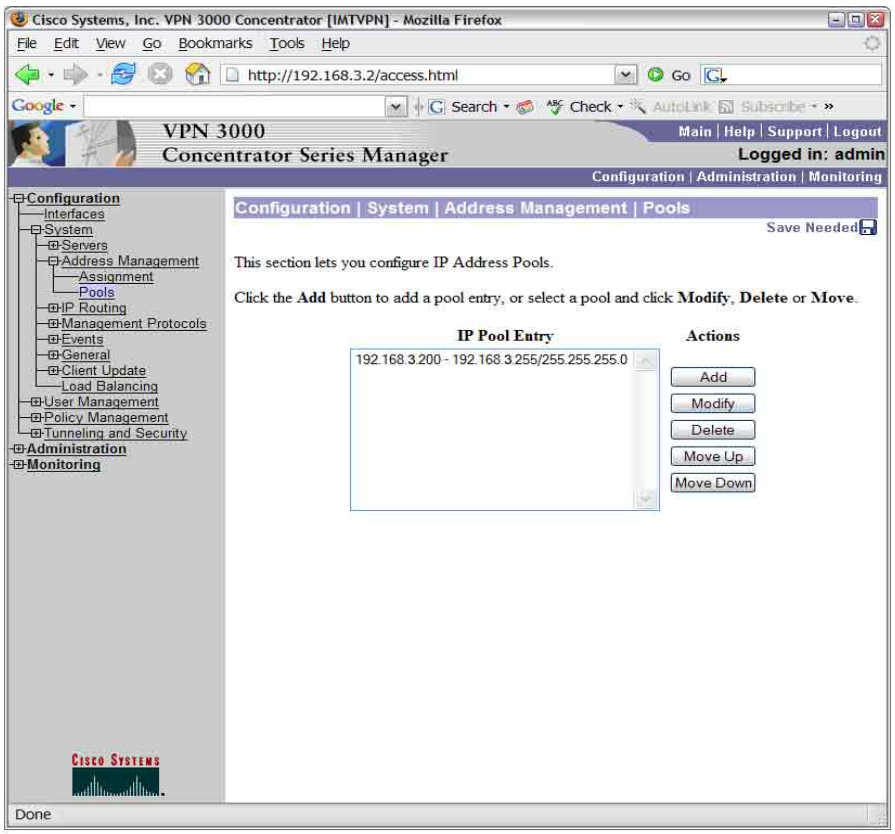
Create an address pool which is an IP address range that can be assigned to remote access clients. The values used must be routable within the enterprise, but not the WAN/Internet.

In our simple example we use an address rang in the same subnet as our simple enterprise network to avoid needing to specify intermediate routing.

Navigate to **configuration -> System->Address Management->Pool** and specify the addresses: In the example network this is:

192.168.3.200 0 192.168.3.255 / 255.255.255.0

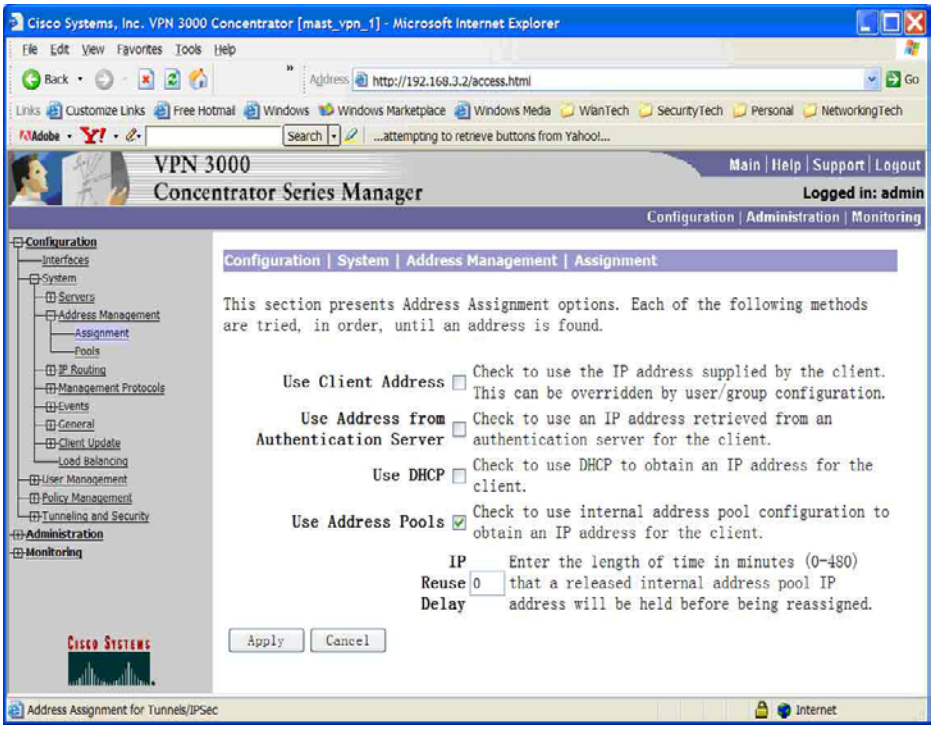
After saving the screen should look like:



4.6. Address Assignment

This step makes the address pool eligible for use.

Navigate to **Configuration->System->Address Management->Assignment** and check the **Use Address Pools** box as in the following shot:

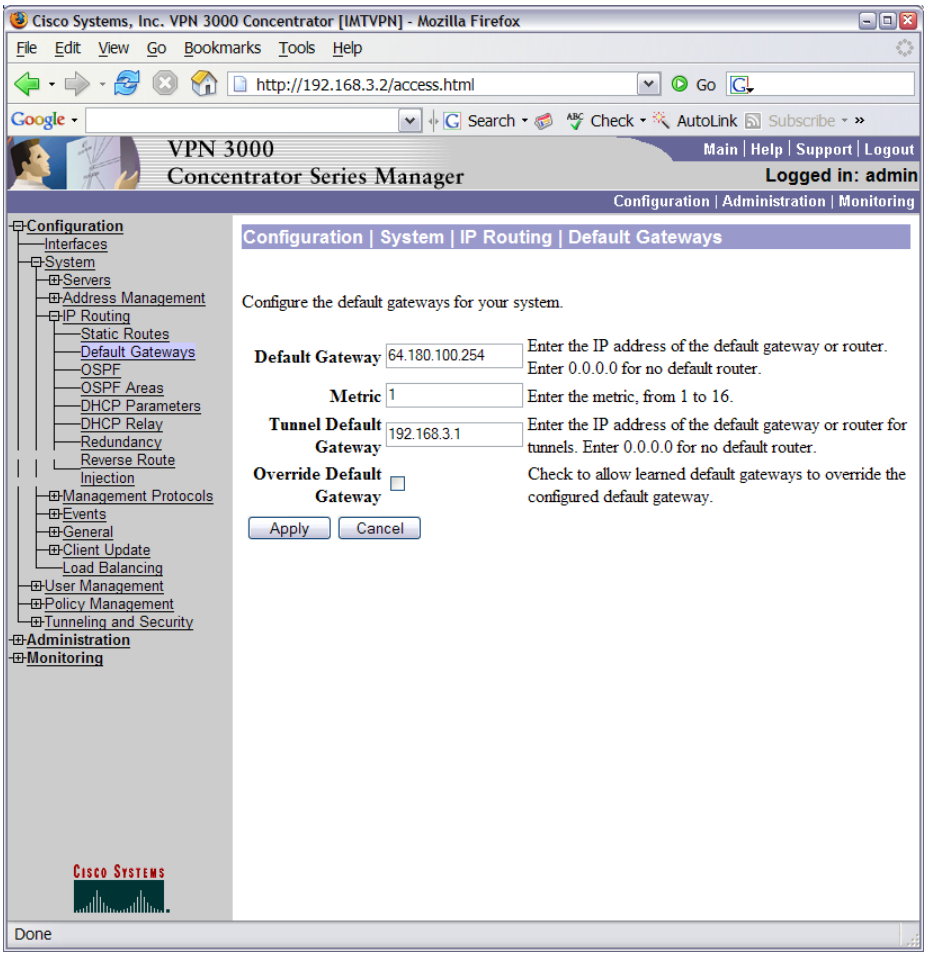


4.7. Default Gateway

A default gateway setting is required to route traffic over the WAN and LAN.

Navigate to **Configuration->System->IP Routing->Default Gateway** and set the values appropriate for your network. In the example case, the *Service Provider Default WAN* gateway is 64.180.100.254 and the *Tunnel DG* is 192.168.3.1.

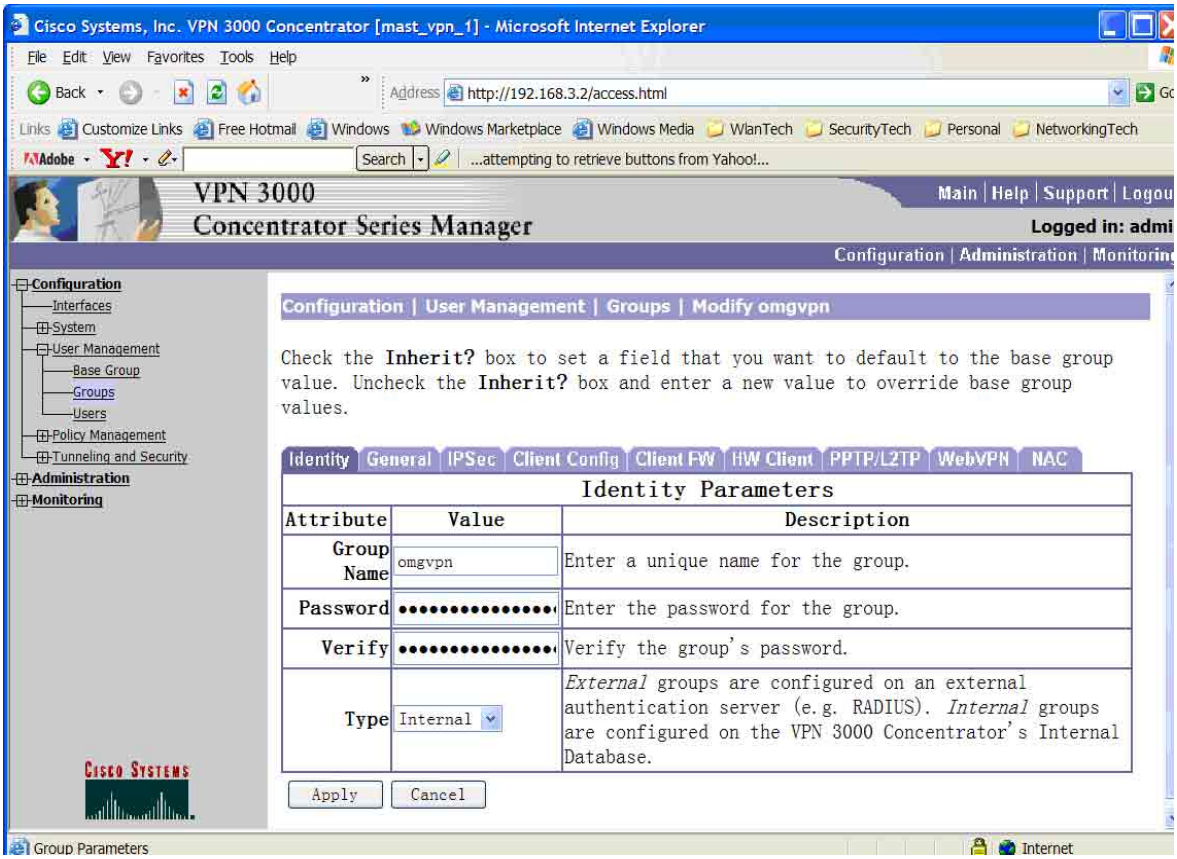
The result should look like:



4.8. Groups

Virtually all oMG customers prefer to use a shared secret approach rather than certificate based authentication. The former requires you to create one or more groups and corresponding users. Typically our customers choose to simplify their administration work load by employing the same group and user name and corresponding passwords for all oMGs.

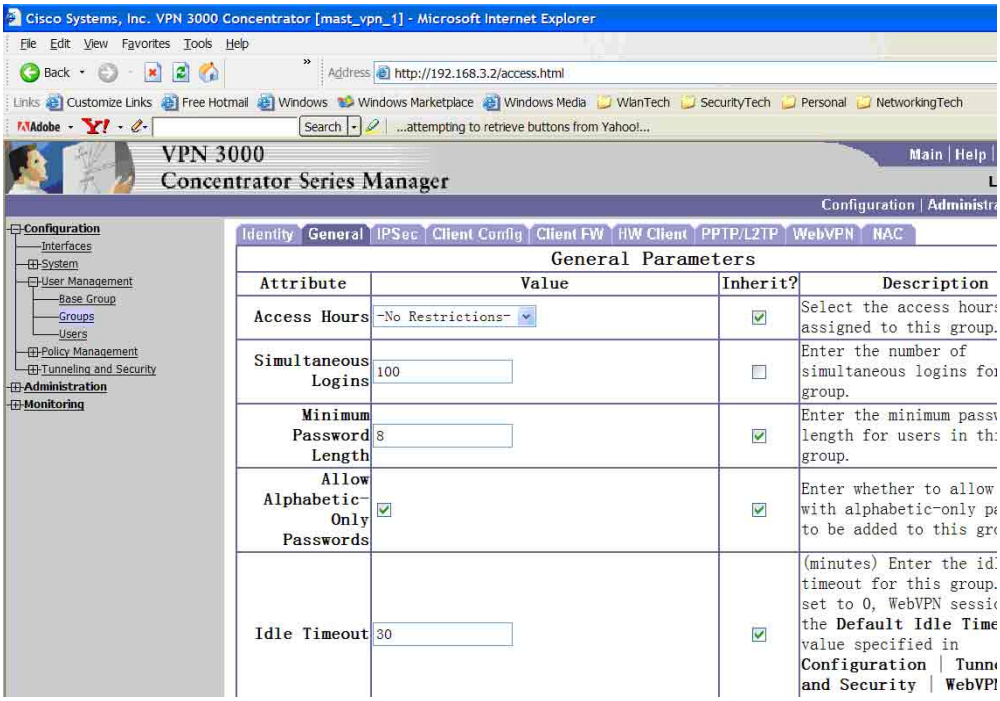
Specify this information by navigating to **Configuration->User Management-Groups**. Select the Identify tab and supply the required information. Repeat the process for the *Users*. The screens are similar and appear like:

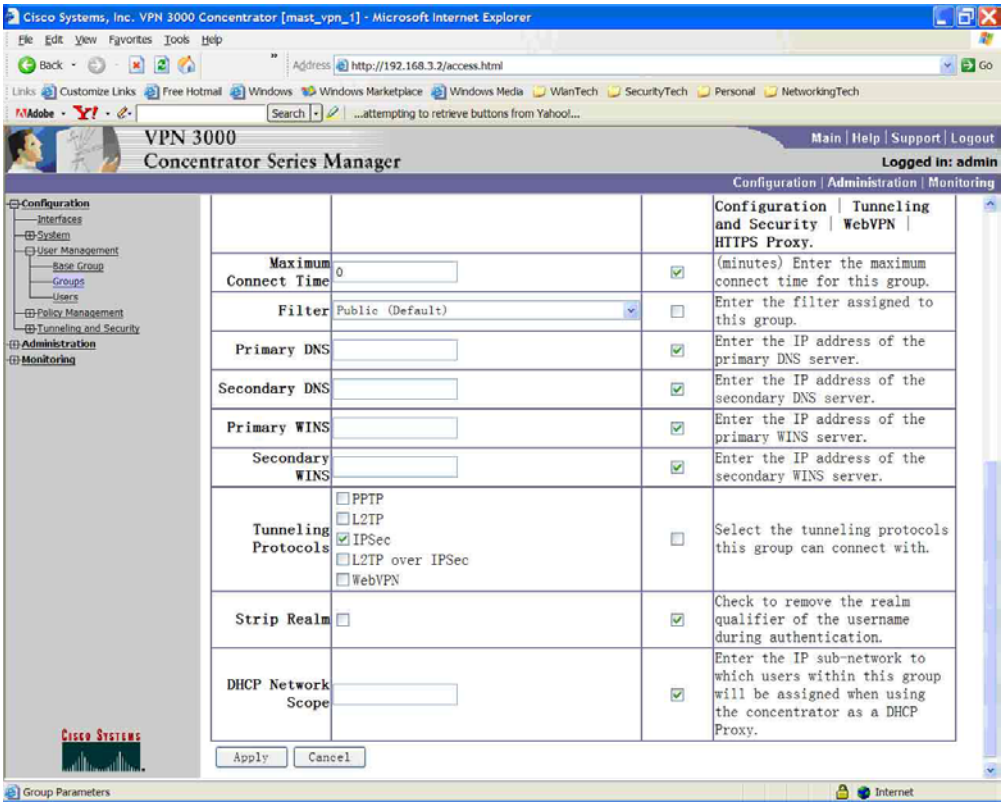


4.9. General Settings

Next select the **GENERAL** tab and ensure the following is set:

- Ensure IPSec is checked
- Filter set to Public
- Enable Simultaneous Logins
  - If mode is single login user shared by all clients, set the number of connections allowed
  - If mode is individual account, leave the connections as default: 3
- Set Allow Alphabet-Only-Passwords as necessary.

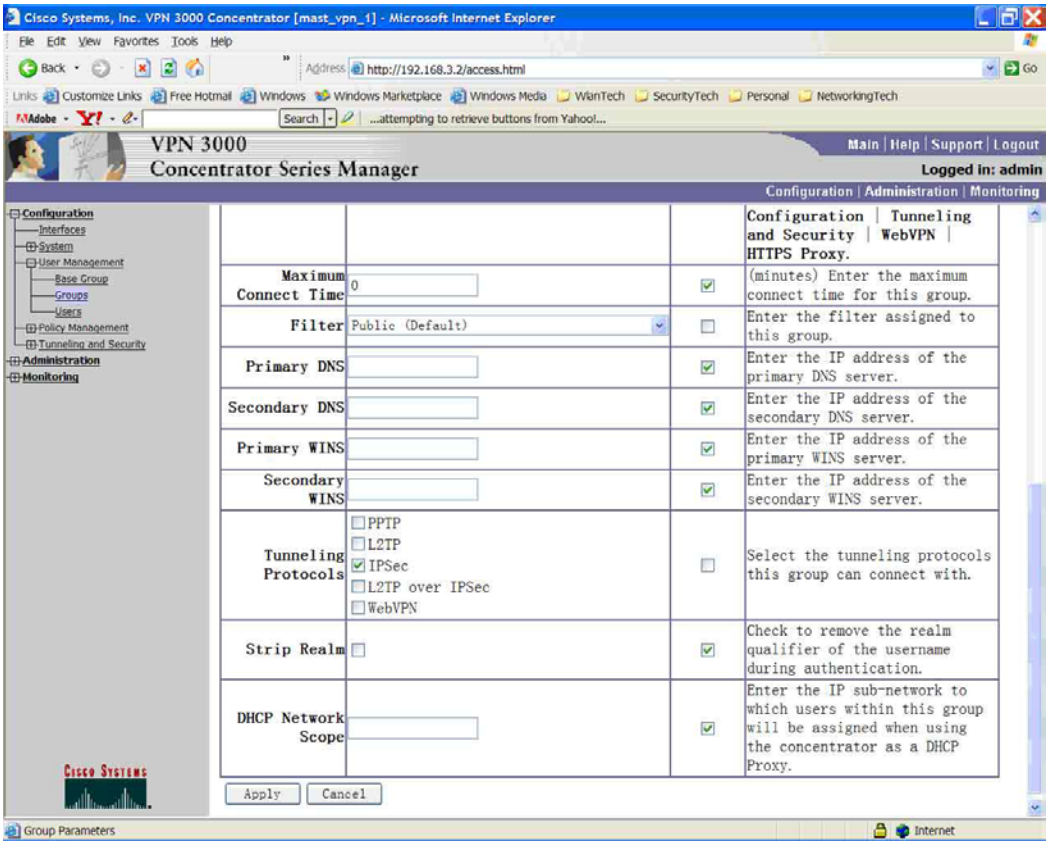

Cisco Systems, Inc. VPN 3000 Concentrator [mast_vpn_1] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://192.168.3.2/access.html
VPN 3000
Concentrator Series Manager
Main | Help
Configuration | Administra
Configuration
Interfaces
System
User Management
Base Group
Groups
Users
Policy Management
Tunneling and Security
Administration
Monitoring
Identity General IPSec Client Config Client FW HW Client PPTP/L2TP WebVPN NAC
General Parameters
Attribute Value Inherit? Description
Access Hours -No Restrictions-
Select the access hours assigned to this group.
Simultaneous Logins 100
Enter the number of simultaneous logins for group.
Minimum Password Length 8
Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords
Enter whether to allow passwords with alphabetic-only passwords to be added to this group.
Idle Timeout 30
(minutes) Enter the idle timeout for this group. If set to 0, WebVPN sessions use the Default Idle Timeout value specified in Configuration | Tunneling and Security | WebVPN


Cisco Systems, Inc. VPN 3000 Concentrator [mast_vpn_1] - Microsoft Internet Explorer
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration | Tunneling and Security | WebVPN | HTTPS Proxy.
Maximum Connect Time 0
(minutes) Enter the maximum connect time for this group.
Filter Public (Default)
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 during authentication.
DHCP Network Scope
Enter the IP sub-network to which users within this group will be assigned when using the concentrator as a DHCP Proxy.
Apply
Cancel
Group Parameters
Internet

4.10. IPSec

This step activates the previously configured Security Association.

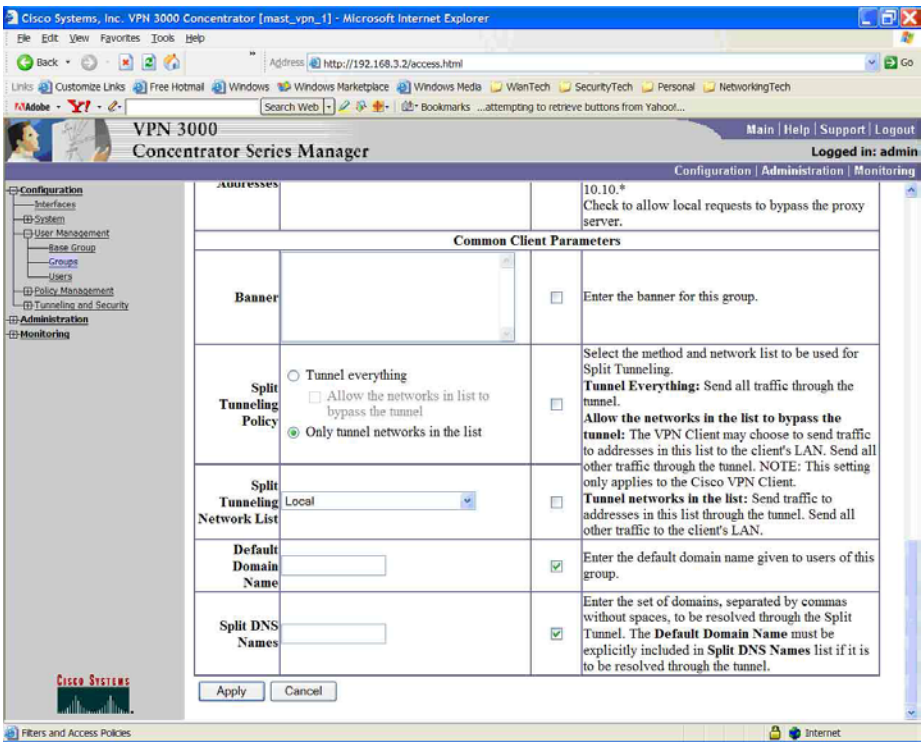
In the *Groups* menu, select the **IPsec Tab** and choose the name you previously assigned for the SA. Ensure tunnel type is *Remote Access* and enable **IKE Keepalives**.



4.11. Client Config

This step establishes IPsec compatibility settings with the client.

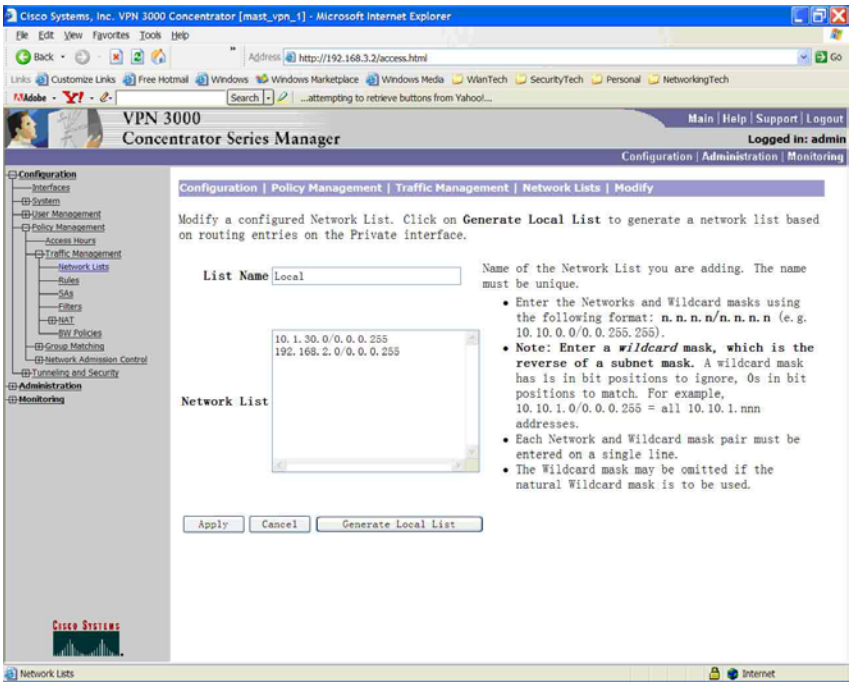
- The following parameters are important for use with oMGs.
- Check **allow password storage** on client.
- Check **Inherit** for IPsec over UDP, leave port 10000 as port to use for NAT.
- Typically, enable split tunnel mode with traffic to the oMM servers going outside the tunnel. This is a very important consideration. Refer to Appendix A for a detailed explanation.



4.12. Network Lists

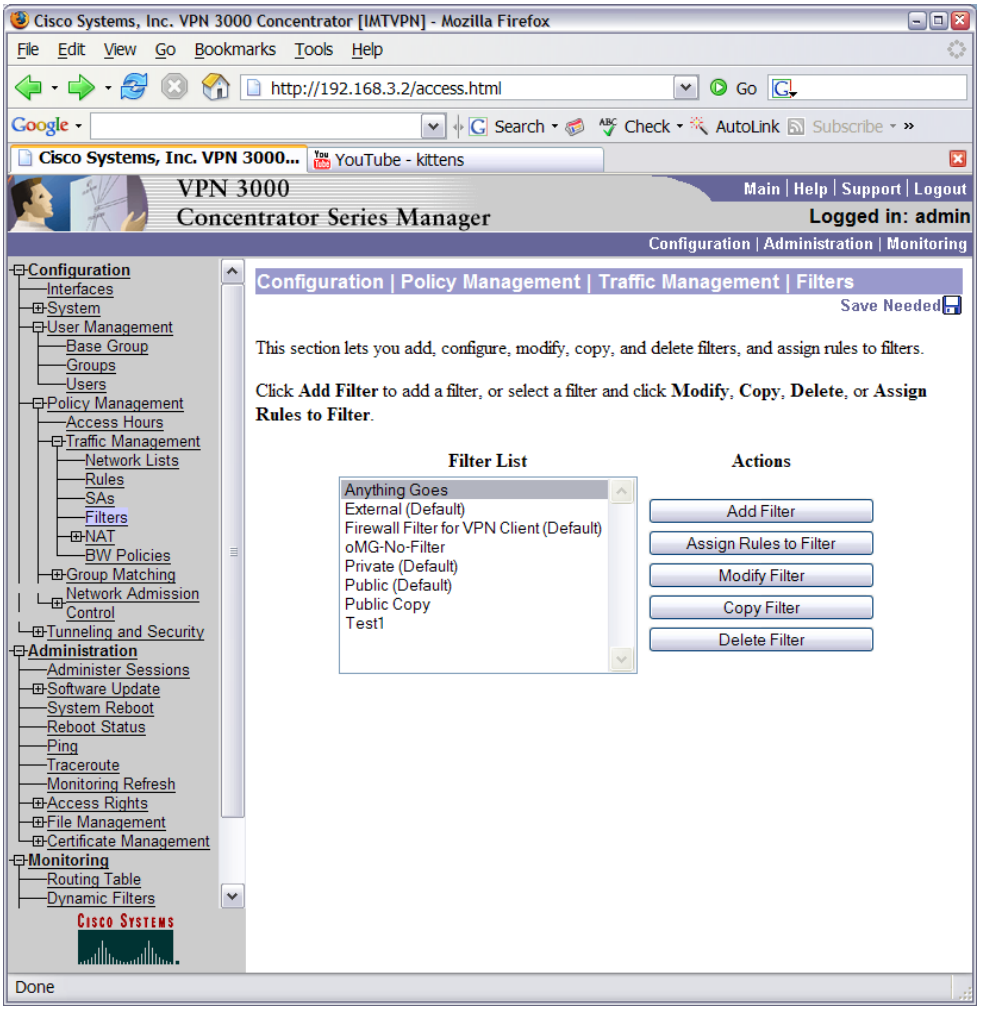
This step specifies details of the spiit tunnel policy.

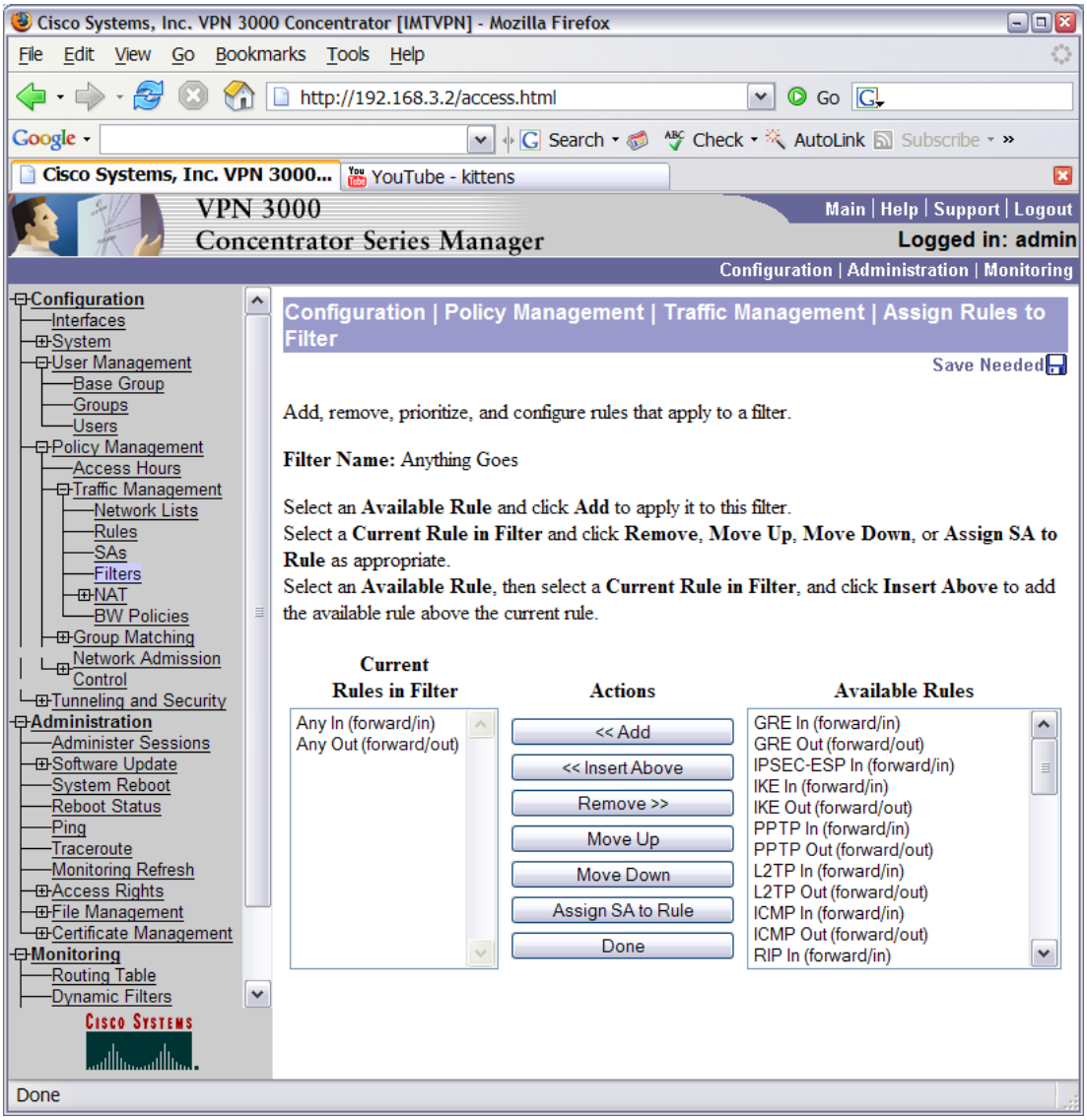
Navigate to **Configuration->Policy Management->Traffic Management-> Network Lists** and supply the address information. The screen should resemble the following:



4.13. Filter

The VPN Concentrator has an integrated firewall that must be configured. This is a common problem area when the VPN seems to be operational but application data does not pass. In the following screens we have chosen a pass everything approach for simplicity.



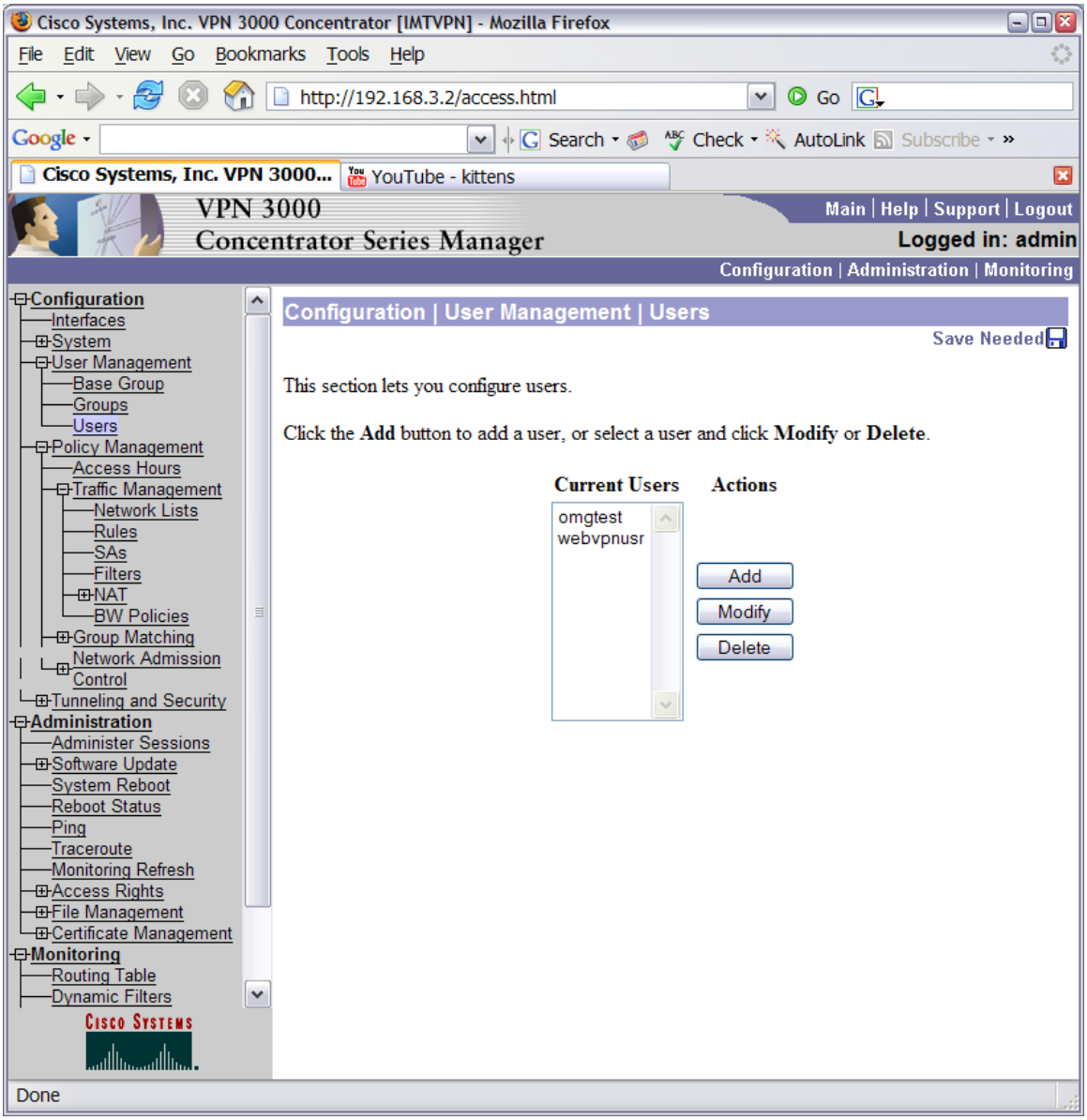


4.14. User Configuration

In this step you complete the client credentials specifications by defining users.

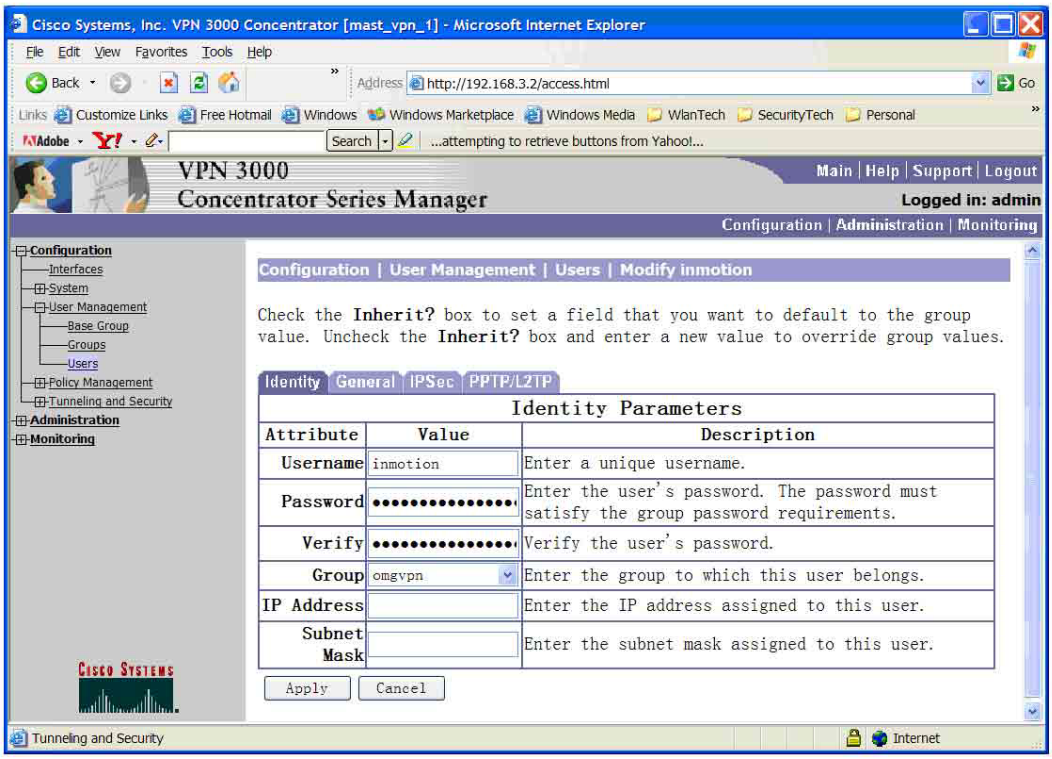
Navigate to **Confguration->User Management->Users** and supply the user information.

The screen should resemble:



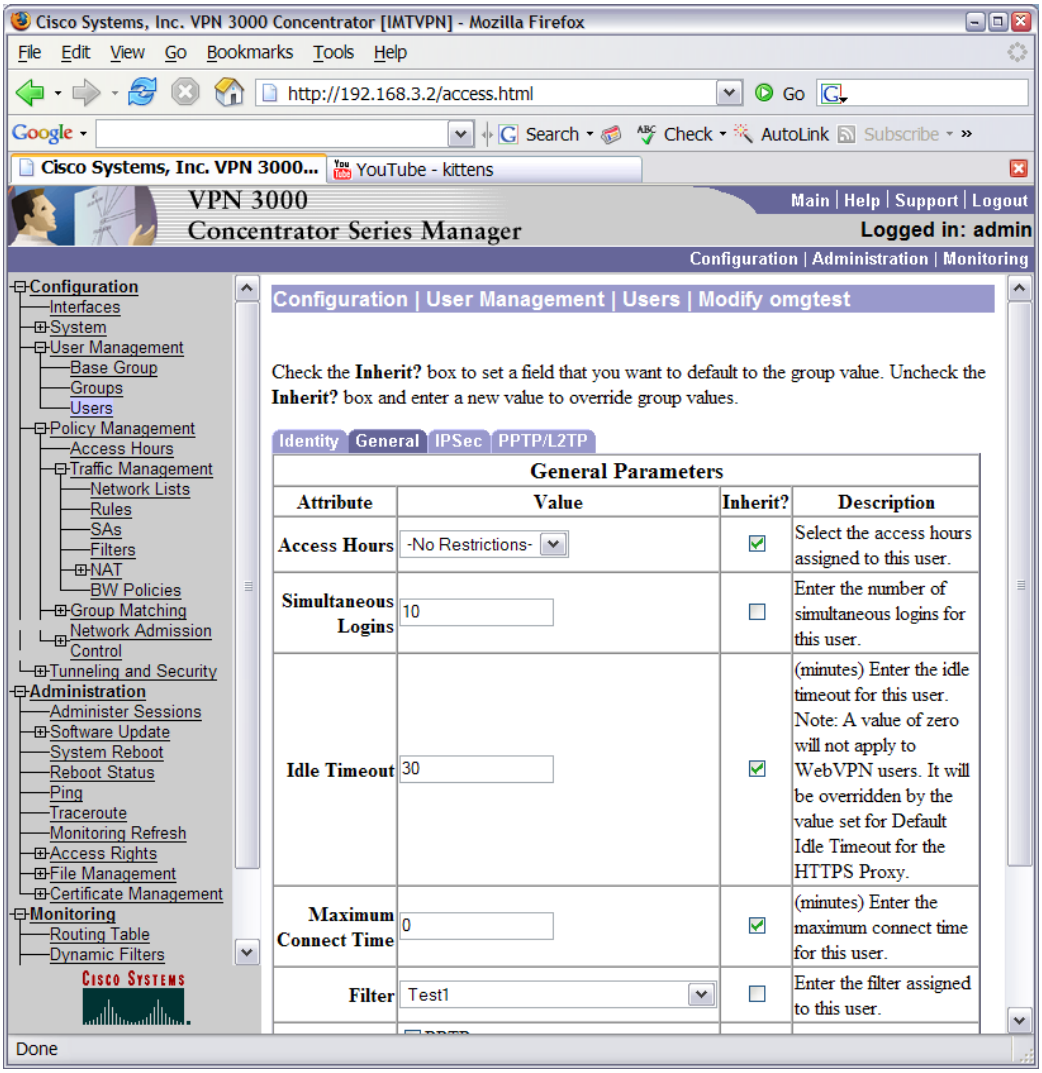
4.15. User Identify

Specify the user details by selecting the **Identify Tab**; choosing your own user name, etc.



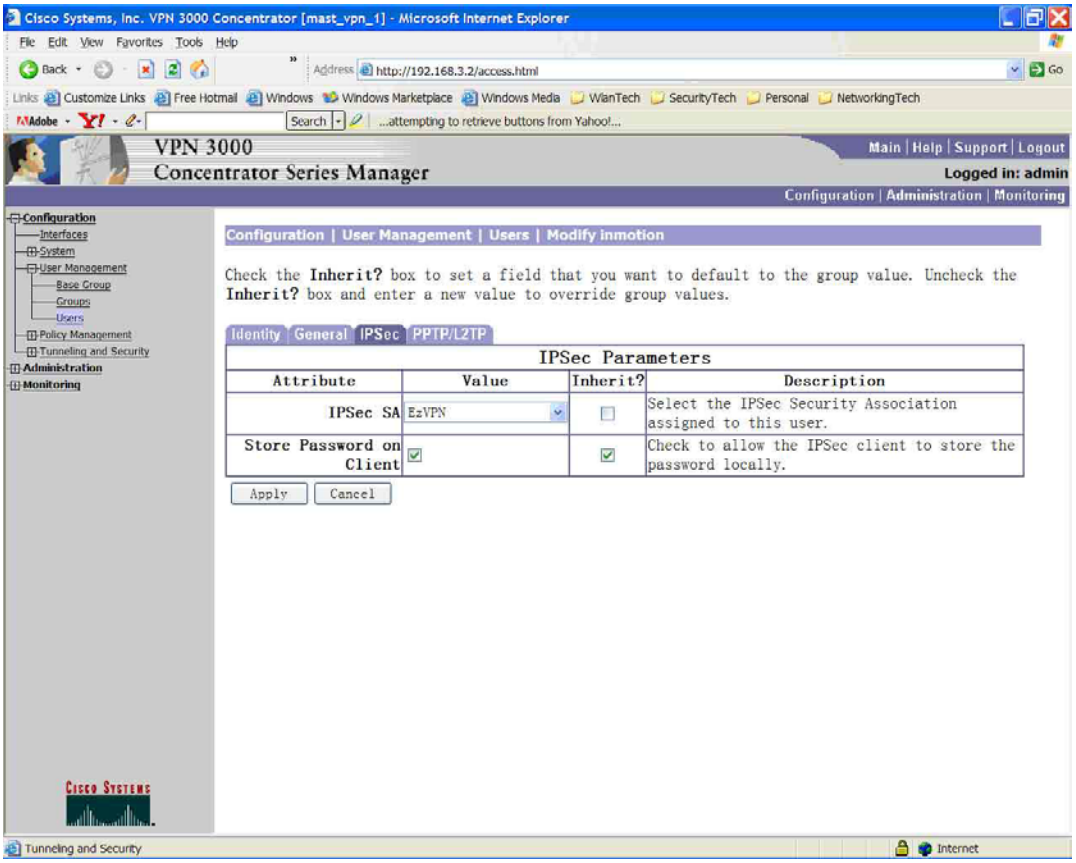
4.16. User General

Specify the name of the filter you previously defined.



4.17. User IPSec

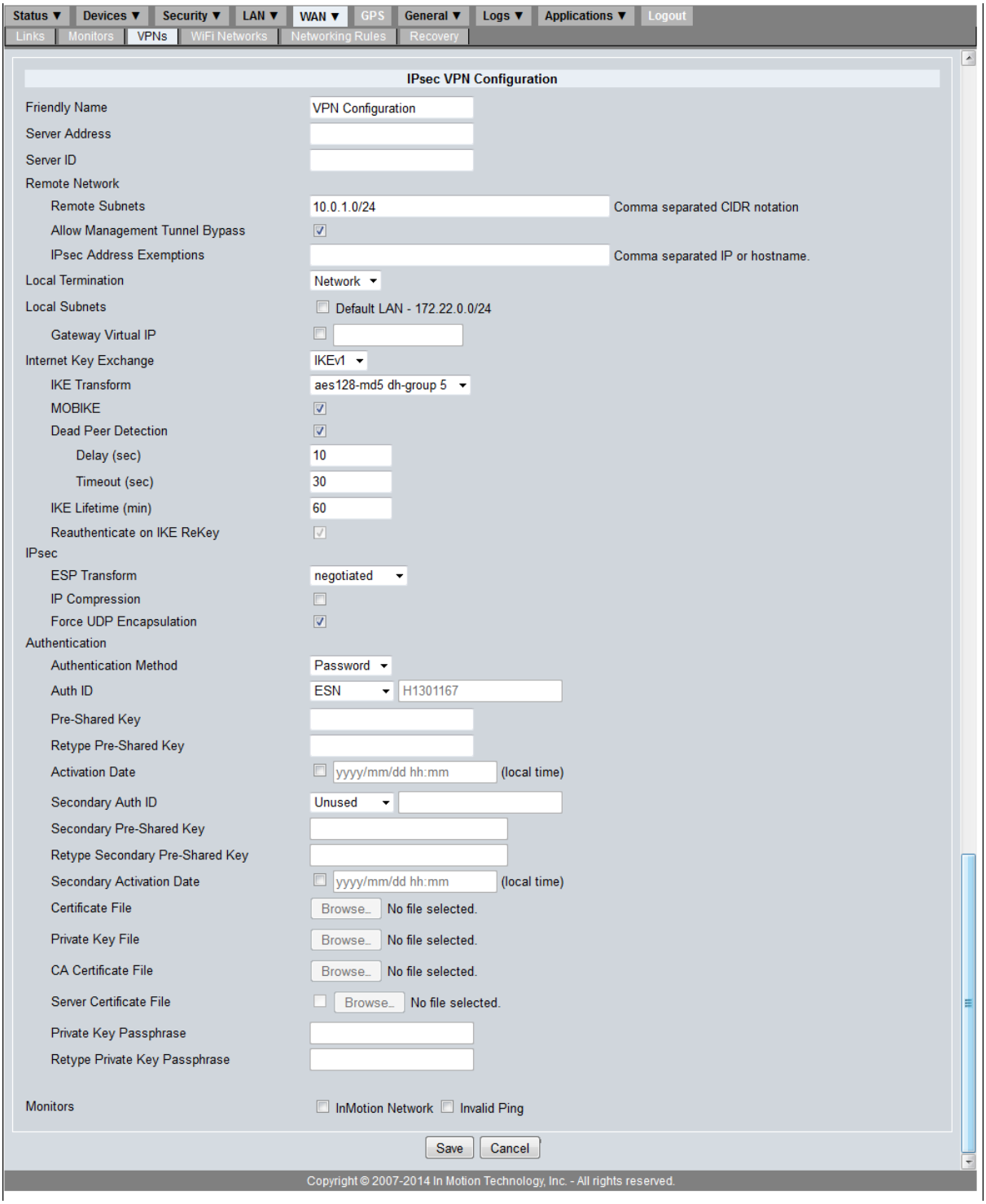
This should inherit from the Group, but ensure that the right SA is selected.


Cisco Systems, Inc. VPN 3000 Concentrator [mast_vpn_1] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://192.168.3.2/access.html
VPN 3000
Concentrator Series Manager
Main | Help | Support | Logout
Logged in: admin
Configuration | Administration | Monitoring
Configuration
Interfaces
System
User Management
Base Group
Groups
Users
Policy Management
Tunneling and Security
Administration
Monitoring
Configuration | User Management | Users | Modify inmotion
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
EzVPN
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
Tunneling and Security
Internet

5. oMG Setup

A pre-requisite to doing this step is to ensure that a WAN interface is correctly configured and verified to be operational without any VPN configuration. **DO NOT SKIP THIS**.

Connect a PC to the oMG LAN and log into the Craft Interface using a web browser and navigate to http://welcome-to-inmotion/MG-LCI.



Fill out the *VPN Configuration* screen settings as follows:

a. **Friendly Name**: Enter a descriptive nickname for the VPN.

b. **Server Address**: Set to the VPN Gateway IP Address (IP address or FQDN).

c. **Server ID**: set to the IP address, hostname, domain name, or fully qualified domain name that the VPN server will use to identify itself to the gateway while negotiating the VPN tunnel or leave blank to use the *Server Address*.

d. **Remote Network**: Set to *Network*.

   i. **Remote Subnets**: Set to the subnet of the enterprise LAN behind the 3000 Series Concentrator using CIDR notation.

   ii. **Allow Management Tunnel Bypass**: Set to enabled. Sierra Wireless strongly recommends this field be enabled. Although it necessitates planning for the management tunnel UDP connection through to the oMM, the benefit is that it allows for an independent means of access to the oMG from the oMM for remote configuration and troubleshooting.

   iii. **IPSec Address Exemptions**: Leave blank. Traffic generated on the oMG to the IP addresses (or FQDN's) defined in this list will not be sent through the IPsec VPN tunnel (where the list is included).

e. **Local Termination**: Set to *Network*.

f. **Local Subnets**: select the LAN segment that is to become part of the VPN.

   i. **Gateway Virtual IP**: Set to enabled and enter the IP address of the oMG within the local subnet.

Note: *For IPSec VPN Host to LAN, set Local Termination to Host. In a Host-to-LAN configuration the oMG will have a single VPN address and all devices on the oMG LAN will be NATTed (address translated) behind that address.*

g. **Internet Key Exchange**: Set to IKEv1.

   i. **IKE Transform**: Set to the desired IKE transform.

   ii. **MOBIKE**: Set to disabled. This is compatible only with IKEV2 and allows the IP addresses associated with IKEv2 and the SA (security association) to be changed without tearing down and re-establishing the VPN connection. This end result is a fast switch of the VPN that has minimal impact to end user data. The 3000 Series Concentrator does not support IKEv2.

   iii. **Dead Peer Detection**: Set to enabled. During idle periods, an "R_U_THERE" packet is sent every delay period. If an "R_U_THERE_ACK" packet has not been received within the timeout period, the peer will be declared dead. When Dead Peer Detection is enabled, the Delay and Timeout time can be set. The default values are 10 and 30 seconds respectively. Note that interoperable DPD is not completely reliable. A VPN link monitor is recommended to assure reliable failure detection and recovery.

      1. **Delay**: Set to 10.

      2. **Timeout**: Set to 30.

   iv. **IKE Lifetime**: Set to 60. The lifetime for the IKE SA (security association). Once the lifetime has been reached a new SA will be negotiated. Either end may initiate the negotiation; both sides need not agree.

   v. **Reauthenticate on IKE ReKey**: This parameter is only available for IKEV2. It specifies if re authentication should be performed when re-keying IKE SA (security association). The Cisco VPN 3000 Series only supports IKEv1, which always performs the authentication.

h. **IPSec**

   i. **ESP Transform**: Set to the desired ESP transform. Note: these two values must be the same on the VPN 3000 Series.

   ii. **IP Compression**: Set to disabled.

iii. **Force UDP Encapsulation**: Set to enabled (default). Sierra Wireless recommends this field be enabled. When the VPN server is behind a firewall, firewall configuration is simplified as the firewall only has to allow ports 500 (IKE) and 4500 (UDP-encapsulated ESP) when UDP encapsulation is employed.

Note: *When UDP encapsulation is not used, protocol 50 must also be allowed for the ESP protocol to pass.*

i. **Authentication**:

i. **Authentication Method**: Set to *Password* to use PSK authentication.

ii. **Auth ID**: Set to *ESN* or *IP address* of the oMG (serial number or IP address). This is used so the VPN gateway can identify the oMG and select the corresponding VPN settings.

iii. **Pre-Shared Key**: Enter a unique pre-shared key. Note that this same value will also later be entered on the VPN gateway side.

iv. **Retype Pre-Shared Key**: Re-enter the unique pre shared key.

v. **Activation Date**: set to the date and time when the current Auth ID and PSK should become the active credentials in a rotating credential system. This must match the corresponding setting that is configured on the Cisco VPN 3000 Series system.

vi. **Secondary Auth ID**: set to *ESN* or *IP address*. It will usually be the same as the Auth ID. This must match the corresponding setting that is configured on the Cisco VPN 3000 Series system.

vii. **Secondary Pre Shared Key**: specify the secondary PSK to use in conjunction with the Pre Shared Key field to provide "rotating" keys for enhanced security. This must match the corresponding setting that is configured on the Cisco VPN 3000 Series system.

viii. **Retype Secondary Pre Shared Key**: retype the secondary pre shared key.

ix. **Secondary Activation Date**: set to the date and time when the *Secondary Auth ID* and PSK should become the active credentials in a rotating credential system. This must match the corresponding setting that is configured on the Cisco VPN 3000 Series system.

x. **Certificate File**: Option disabled for PSK.

xi. **Private Key File**: Option disabled for PSK.

xii. **CA Certificate File**: Option disabled for PSK.

xiii. **Server Certificate File**: Option disabled for PSK.

xiv. **Private Key Passphrase**: Option disabled for PSK.

xv. **Retype Private Key Passphrase**: Option disabled for PSK.

j. **Monitors**: Select the desired monitor to use for this VPN connection. Monitors are required to promptly detect an unusable tunnel, upon which, the VPN will be re-initialized. For more information see the oMG Operation and Configuration Guide.

Tip: *when first testing the VPN, it's recommended that monitors be disabled initially in order to test that all of the other configuration parameters are working properly.*

Click on the **Save** button.

After the oMG is operational and the green LED is on solid, you may be able to verify externally by using the PC to reach the enterprise application (or at least to ping an address on the enterprise private VPN network.

If there are problems, you may be able to diagnose something from the oMG side by logging in to the oMG administration console using Putty.

After login perform */opt/cisco-vpnclient/bin/vpnclient stat* to view a status dump. You should see a reasonable client address at the top of the dump. From the oMG console window try to ping a private VPN address. Note that you should also be able to ping the local client address but that is not a useful test.

Appendix A. Split Tunnel Recommendations

A.1. VPN and Network Management

Split tunneling is the term that describes routing some traffic through the VPN tunnel while allowing other traffic to bypass the tunnel and pass directly to the WAN.

This can be implemented using either inclusion or exclusion lists, as preferred.

The Cisco VPN 3000 series establishes split tunnel policy at the server and pushes the routing information to any VPN client when the tunnel initializes.

Split tunneling is an important consideration for oMG operation from two perspectives:

1. The oMG is designed to communicate with the oMM. The oMM is available as a hosted service or as a Management Appliance that you can operate completely under your control within your enterprise. Although the oMG can function without the connection to the oMM, it is strongly recommended to allow “outside of tunnel” access to the oMM management servers. The addresses of the hosted oMM servers should be verified at installation time. Currently they are:
    a. 64.40.113.48
    b. 64.40.113.142
    c. 216.139.228.216
    d. 216.139.228.216
    e. 64.180.100.213

Similarly, the oMG is designed to periodically verify the integrity of the data path when its WAN link(s) is active. It does this by contacting a ping host, which by default is one of the above oMM servers. When the ping host is disabled the oMG is unable to detect the common condition of when a WAN link has a signal but is unable to pass data.

Without split tunneling, all oMG network management traffic is routed through the VPN concentrator. This typically requires special routing configuration within the enterprise to forward the network management traffic back to the internet. It may also necessitate provisioning of additional network access bandwidth. Therefore most customers specify that the traffic to the oMM servers flows outside the tunnel.

A.2. VPN and DNS interaction

In most situations, the oMG serves up IP addresses via DHCP and performs Name Resolution via DNS for devices attached to its LAN. The DNS service in the oMG is configured as a forwarder so that all name resolution requests are passed upstream to an external DNS server. The upstream DNS server configuration is specified as part of the oMG WAN configuration and this requires particular attention to ensure correct operation.

When operating with a VPN, a device such as a PC attached to the oMG LAN will expect to contact an application server or printer that resides on the private network reachable via the VPN. For example this could be the 10.4.0.0 network. To reach these by name, the best practice is to specify a DNS server on the same network – e.g. 10.4.0.10. When the tunnel is properly configured and operating normally and all peripheral elements are also correct, the PC name resolution requests are serviced by the 10.4.0.10 server.

In the case where DNS is provided over the VPN, that DNS server must supply all name resolution. In particular if a client PC needs to connect to the Internet with a web browser, then the DNS server must provide the required information (by forwarding requests) for the global name space.

Furthermore the DNS servers must specifically resolve the names of the oMM servers – especially the ping host, even if the traffic to the ping host for the active oMG WAN link flows outside the VPN. Note that the ping host name resolution is a special case that can be side-stepped by using an IP address instead of a host name for the ping host.

There is one other ramification of using private DNS. During the transition period from WAN link down to link up to VPN active, there will be an interval where the link is active but the VPN will be not active. During this interval, there will be no name resolution. Depending on the timing configured for ping host, there may be failures. For cellular data connections this is normally not a significant concern since ping host timing is commonly set on the order of over 1 minute for this cycle. However for WAN WIFI connections, it is often set more aggressively to support fast switching between cellular and WIFI. This could lead to unexpected interactions.