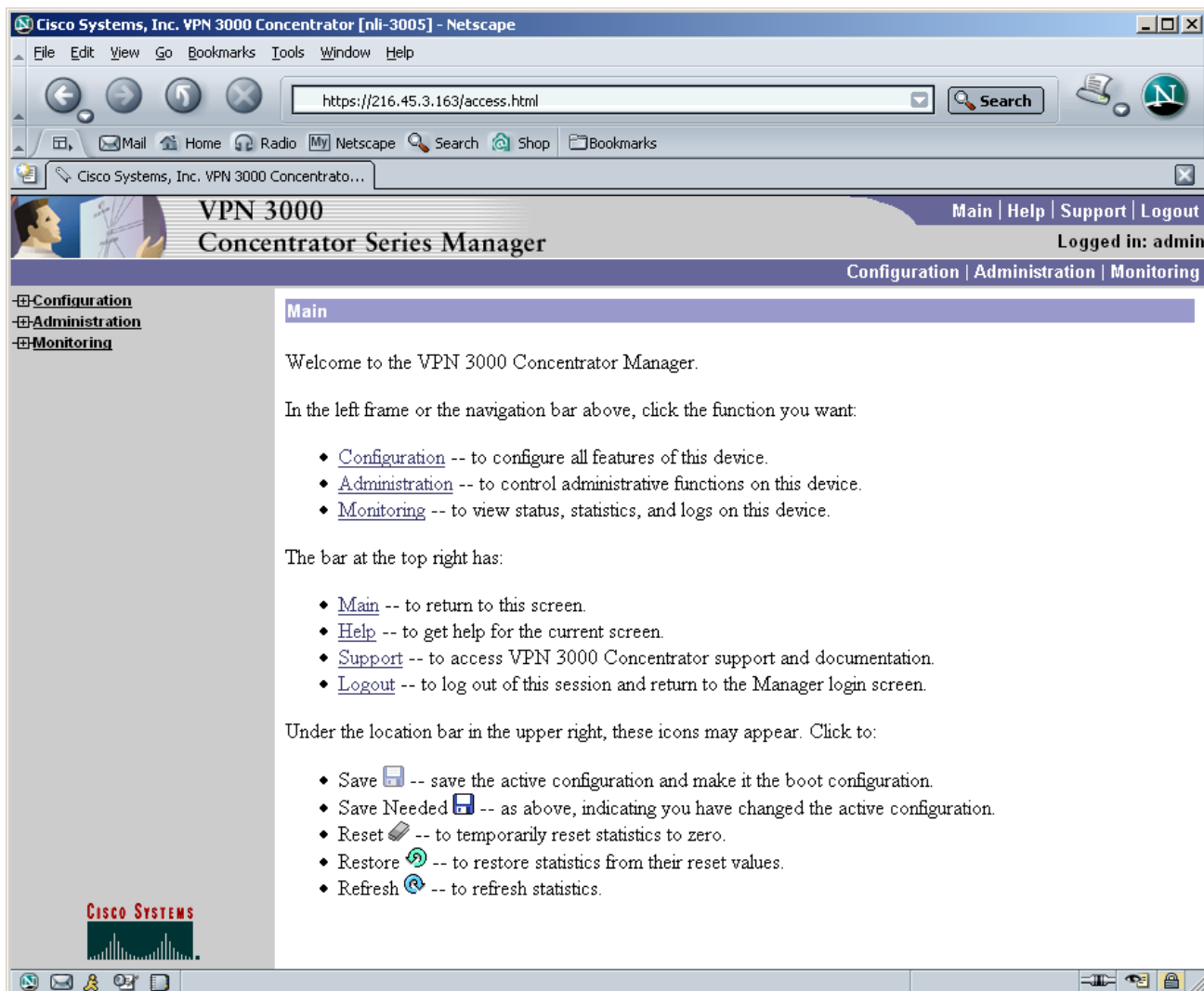


VPN 3000 Concentrator

Overview

The VPN 3000 Concentrator is used primarily for VPN clients. It can also be configured for LAN-to-LAN VPN's. To access the concentrator, you can use either a console cable and make some configuration changes through the CLI. But, most of the functionality is not available through the CLI. You will be required to get familiar with the GUI using a web browser. However, this GUI is quite intuitive and if you are already familiar with VPN configuration, you will find configuring this device to be fairly simple.

There are 3 main sections to the VPN 3000: Configuration, Monitoring, and Administration. Configuration allows you to configure all the features of the concentrator including interfaces, system parameters, users, and policy. Administration allows you to administer sessions, control access rights, manage files, manage certificates, software updates, and system reboots. Monitoring allows you to view routing tables, filters, logs, system status, sessions, and statistics.



The screenshot shows a Netscape browser window displaying the Cisco VPN 3000 Concentrator Series Manager. The browser's address bar shows the URL `https://216.45.3.163/access.html`. The page title is "Cisco Systems, Inc. VPN 3000 Concentrator [nli-3005] - Netscape". The main content area is titled "VPN 3000 Concentrator Series Manager" and includes a navigation bar with links for "Main", "Help", "Support", and "Logout". The user is logged in as "admin". The left sidebar contains a navigation menu with "Configuration", "Administration", and "Monitoring". The main content area is titled "Main" and contains the following text:

Welcome to the VPN 3000 Concentrator Manager.






In the left frame or the navigation bar above, click the function you want:

- [Configuration](#) -- to configure all features of this device.
- [Administration](#) -- to control administrative functions on this device.
- [Monitoring](#) -- to view status, statistics, and logs on this device.

The bar at the top right has:

- [Main](#) -- to return to this screen.
- [Help](#) -- to get help for the current screen.
- [Support](#) -- to access VPN 3000 Concentrator support and documentation.
- [Logout](#) -- to log out of this session and return to the Manager login screen.

Under the location bar in the upper right, these icons may appear. Click to:

- Save  -- save the active configuration and make it the boot configuration.
- Save Needed  -- as above, indicating you have changed the active configuration.
- Reset  -- to temporarily reset statistics to zero.
- Restore  -- to restore statistics from their reset values.
- Refresh  -- to refresh statistics.

The bottom of the page features the Cisco Systems logo and a taskbar with various system icons.

Reset the VPN Concentrator to Factory Defaults

Depending on the requirements of the exam, you may need to reset the concentrator back to factory defaults. However, be aware this is a simple, but fairly lengthy process. Since time is of the essence you may not want to consider this option. We would assume you will be given a concentrator with a blank configuration. But, do not count on it. If you do reset the system, you can accept the defaults for almost every question. The only important one to answer is the IP addresses. Since you cannot configure some of the options through the GUI it is important that the concentrator be reachable using HTTP and its inside IP address. Once you have access to the inside IP address through the web browser, you can enable HTTPS on the outside interface.

Step 1. Login as Administrator. Type 2 for Administration. Type 3 for System Reboot.

```
Login: admin
Password:
```

```
                Welcome to
                Cisco Systems
                VPN 3000 Concentrator Series
                Command Line Interface
                Copyright (C) 1998-2003 Cisco Systems, Inc.
```

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit
```

```
Main -> 2
```

```
1) Administer Sessions
2) Software Update
3) System Reboot
4) Reboot Status
5) Ping
6) Access Rights
7) File Management
8) Certificate Management
9) Back
```

```
Admin -> 3
```

```
1) Cancel Scheduled Reboot/Shutdown
2) Schedule Reboot
3) Schedule Shutdown
4) Back
```

Step 2. Type 2 for Reboot and ignore the Config file. This is effectively the same as changing a router's configuration register to 0x2142.

```
Admin -> 2
```

```
1) Save active Configuration and use it at Reboot
2) Reboot without saving active Configuration file
3) Reboot ignoring the Configuration file
4) Back
```

```
Admin -> 3
```

```
1) Cancel Scheduled Reboot/Shutdown
2) Reboot Now
3) Reboot in X minutes
4) Reboot at time X
5) Reboot wait for sessions to terminate
```

6) Back

Admin -> 2

```
126 09/16/2003 14:34:02.490 SEV=1 REBOOT/1 RPT=1
Reboot scheduled immediately.
Done
```

```
Login: admin
Password:
```

```
                Welcome to
                Cisco Systems
VPN 3000 Concentrator Series
                Command Line Interface
Copyright (C) 1998-2003 Cisco Systems, Inc.
```

- 1) Configuration
- 2) Administration
- 3) Monitoring
- 4) Save changes to Config file
- 5) Help Information
- 6) Exit

```
Main ->
131 09/16/2003 14:34:11.210 SEV=1 REBOOT/6 RPT=1
Rebooting VPN 3000 Concentrator now.
```

Resetting System...

[Connection to vpn closed by foreign host]

Step 3. Once the 3000 reboots you will be booted from your console connection. If you are using a 2511 or an access server you will have to reconnect. Login using the default admin/admin username and password when the box is finished booting.

```
Dev-Rack1# vpn
Translating "vpn"
Trying vpn (1.1.1.1, 2011)... Open
```

```
...
Loading image .....
Verifying image checksum .....
Active image loaded and verified...
Starting loaded image...
Starting power-up diagnostics...
```

```
...
pSH+ Copyright (c) Integrated Systems, Inc., 1992.
Cisco Systems, Inc./VPN 3000 Concentrator Version 4.0.1.Rel May 06 2003 13:13:03
Features:
Initializing VPN 3000 Concentrator ...
Waiting for CAPI initialization to complete...
Initialization Complete...Waiting for Network...
```

```
1 09/16/2003 14:34:39.270 SEV=1 EVENT/37 RPT=1
Reset Reason : 2 (Hardware-Reset)
```

```
Login: admin
Password:
```

```
                Welcome to
                Cisco Systems
VPN 3000 Concentrator Series
                Command Line Interface
Copyright (C) 1998-2003 Cisco Systems, Inc.
```

Step 4. Answer the prompts for basic system setup. You can accept the defaults for most of the prompts. If the value in the brackets is the desired setting simply hit enter to accept the default.

```
-- : Set the time on your device. The correct time is very important,
-- : so that logging and accounting entries are accurate.

-- : Enter the system time in the following format:
-- :      HH:MM:SS. Example 21:30:00 for 9:30 PM

> Time

Quick -> [ 14:34:45 ] 12:32:00

-- : Enter the date in the following format.
-- : MM/DD/YYYY Example 06/12/1999 for June 12th 1999.

> Date

Quick -> [ 09/16/2003 ]

-- : Set the time zone on your device. The correct time zone is very
-- : important so that logging and accounting entries are accurate.

-- : Enter the time zone using the hour offset from GMT:
-- : -12 : Kwajalein  -11 : Samoa    -10 : Hawaii    -9 : Alaska
-- :  -8 : PST       -7 : MST      -6 : CST       -5 : EST
-- :  -4 : Atlantic  -3 : Brasilia -2 : Mid-Atlantic -1 : Azores
-- :   0 : GMT       +1 : Paris    +2 : Cairo     +3 : Kuwait
-- :  +4 : Abu Dhabi +5 : Karachi  +6 : Almaty    +7 : Bangkok
-- :  +8 : Singapore +9 : Tokyo    +10 : Sydney   +11 : Solomon Is.
-- : +12 : Marshall Is.

> Time Zone

Quick -> [ -5 ] -8

1) Enable Daylight Savings Time Support
2) Disable Daylight Savings Time Support

Quick -> [ 1 ] 1
```

Step 5. Configure the interfaces and IP addresses.

This table shows current IP addresses.

Intf	Status	IP Address/Subnet Mask	MAC Address
Ether1-Pri	Not Configured	0.0.0.0/0.0.0.0	
Ether2-Pub	Not Configured	0.0.0.0/0.0.0.0	

```
-----
DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured
```

** An address is required for the private interface. **

```
> Enter IP Address

Quick Ethernet 1 -> [ 0.0.0.0 ] 192.168.1.201

Waiting for Network Initialization...

> Enter Subnet Mask

Quick Ethernet 1 -> [ 255.255.255.0 ]

1) Ethernet Speed 10 Mbps
2) Ethernet Speed 100 Mbps
3) Ethernet Speed 10/100 Mbps Auto Detect

Quick Ethernet 1 -> [ 3 ]

1) Enter Duplex - Half/Full/Auto
2) Enter Duplex - Full Duplex
3) Enter Duplex - Half Duplex
```

```

Quick Ethernet 1 -> [ 1 ]

> MTU (68 - 1500)

Quick Ethernet 1 -> [ 1500 ]

1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Save changes to Config file
4) Continue
5) Exit

Quick -> 2

This table shows current IP addresses.

-----
Intf           Status      IP Address/Subnet Mask      MAC Address
-----
Ether1-Pri|    UP        | 192.168.1.201/255.255.255.0 | 00.90.A4.08.00.2B
Ether2-Pub|Not Configured|      0.0.0.0/0.0.0.0         |
-----

DNS Server(s): DNS Server Not Configured
DNS Domain Name:
Default Gateway: Default Gateway Not Configured

> Enter IP Address

Quick Ethernet 2 -> [ 0.0.0.0 ] 216.45.3.163

> Enter Subnet Mask

Quick Ethernet 2 -> [ 255.255.255.0 ]

1) Ethernet Speed 10 Mbps
2) Ethernet Speed 100 Mbps
3) Ethernet Speed 10/100 Mbps Auto Detect

Quick Ethernet 2 -> [ 3 ]

1) Enter Duplex - Half/Full/Auto
2) Enter Duplex - Full Duplex
3) Enter Duplex - Half Duplex

Quick Ethernet 2 -> [ 1 ]

> MTU (68 - 1500)

Quick Ethernet 2 -> [ 1500 ]

1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Save changes to Config file
4) Continue
5) Exit

Quick -> 3

1) Modify Ethernet 1 IP Address (Private)
2) Modify Ethernet 2 IP Address (Public)
3) Save changes to Config file
4) Continue
5) Exit

Quick -> 4

```

Step 6. Configure the hostname, DNS, and gateway settings.

```

-- : Assign a System Name (hostname) to this device.
-- : This may be required for DHCP.

> System Name

Quick -> nli-3005

-- : Specify a local DNS server, which lets you enter hostnames
-- : rather than IP addresses while configuring.

> DNS Server

```

```
nli-3005: Quick -> [ 0.0.0.0 ]
-- : Enter your Internet domain name; e.g., yourcompany.com
> Domain
nli-3005: Quick -> ccbootcamp.com
> Default Gateway
nli-3005: Quick -> 216.45.3.1
```

Step 7. Enable PPTP, L2TP, and IPSec if desired.

```
-- : Configure protocols and encryption options.
-- : This table shows current protocol settings
```

PPTP	L2TP
Enabled	Enabled
No Encryption Req	No Encryption Req

```
1) Enable PPTP
2) Disable PPTP

nli-3005: Quick -> [ 1 ]

1) PPTP Encryption Required
2) No Encryption Required

nli-3005: Quick -> [ 2 ]

1) Enable L2TP
2) Disable L2TP

nli-3005: Quick -> [ 1 ] 2

1) Enable IPSec
2) Disable IPSec

nli-3005: Quick -> [ 1 ]
```

Step 8. Configure address assignment for tunnels.

```
-- : Configure address assignment for PPTP, L2TP and IPSec.

1) Enable Client Specified Address Assignment
2) Disable Client Specified Address Assignment

nli-3005: Quick -> [ 2 ]

1) Enable Per User Address Assignment
2) Disable Per User Address Assignment

nli-3005: Quick -> [ 2 ]

1) Enable DHCP Address Assignment
2) Disable DHCP Address Assignment

nli-3005: Quick -> [ 2 ]

1) Enable Configured Pool Address Assignment
2) Disable Configured Pool Address Assignment

nli-3005: Quick -> [ 2 ]
```

Step 9. Configure VPN user authentication and VPN groups.

```
-- : Specify how to authenticate users

1) Internal
```

- 2) RADIUS
- 3) NT Domain
- 4) SDI
- 5) Kerberos/Active Directory
- 6) Continue

nli-3005: Quick -> [1]

Current Users

No Users

- 1) Add a User
- 2) Delete a User
- 3) Continue

nli-3005: Quick -> 1

> User Name

nli-3005: Quick -> **cisco**

> Password

nli-3005: Quick -> *********

Verify -> *********

Current Users

1. cisco

- 1) Add a User
- 2) Delete a User
- 3) Continue

nli-3005: Quick -> 3

> IPSec Group Name

nli-3005: Quick -> **ccbootcamp**

> IPSec Group Password

nli-3005: Quick -> *********

Verify -> *********

Step 10. Change the admin password.

-- : We strongly recommend that you change the password for user admin.

> Reset Admin Password

nli-3005: Quick -> [*****] *********

Verify -> *********

Step 11. Save changes to config file and exit.

- 1) Goto Main Configuration Menu
- 2) Save changes to Config file
- 3) Exit

nli-3005: Quick -> 2

1) Goto Main Configuration Menu

2) Save changes to Config file

3) Exit

nli-3005: Quick -> 3

Done

Password Recovery

Step 1. Connect your PC to the console cable. Use the same settings you would use for a router (9600 baud, 8 data bits, no parity, 1 stop bit, hardware flow control, VT100 emulation).

Step 2. Login to the concentrator using the current admin password. If you do not know this password, you will need to power off the concentrator and power back on.

```
Login: admin
Password:
```

```

                Welcome to
                Cisco Systems
VPN 3000 Concentrator Series
                Command Line Interface
Copyright (C) 1998-2003 Cisco Systems, Inc.
```

```
1) Configuration
2) Administration
3) Monitoring
4) Save changes to Config file
5) Help Information
6) Exit
```

```
nli-3005: Main -> 2
```

```
1) Administer Sessions
2) Software Update
3) System Reboot
4) Reboot Status
5) Ping
6) Access Rights
7) File Management
8) Certificate Management
9) Back
```

```
nli-3005: Admin -> 3
```

```
1) Cancel Scheduled Reboot/Shutdown
2) Schedule Reboot
3) Schedule Shutdown
4) Back
```

```
nli-3005: Admin -> 2
```

```
1) Save active Configuration and use it at Reboot
2) Reboot without saving active Configuration file
3) Reboot ignoring the Configuration file
4) Back
```

```
nli-3005: Admin -> 1
```

```
1) Cancel Scheduled Reboot/Shutdown
2) Reboot Now
3) Reboot in X minutes
4) Reboot at time X
5) Reboot wait for sessions to terminate
6) Back
```

```
nli-3005: Admin -> 2
```

```
595 09/27/2003 12:18:30.290 SEV=1 REBOOT/1 RPT=1
Reboot scheduled immediately.
Done
```

```
600 09/27/2003 12:18:48.160 SEV=1 REBOOT/6 RPT=1
Rebooting VPN 3000 Concentrator now.
```



```
Resetting System...
```

```
[Connection to vpn closed by foreign host]
```

Step 3. If your connection is terminated, quickly reconnect. Look for the 3 dots immediately following Starting power-up diagnostics. Enter Ctrl-C when you see these dots. Enter 1 to Reset Passwords. The password will be reset to factory default.

```
Dev-Rack1# vpn
Translating "vpn"
Trying vpn (1.1.1.1, 2011)... Open

...
Loading image .....
Verifying image checksum .....
Active image loaded and verified...
Starting loaded image...
Starting power-up diagnostics...
```

```
...
Main Menu Options
-----
1 - Reset Passwords
Q - Quit Main Menu
```

```
Resetting passwords...
Passwords have been reset...
```

Step 4. Enter Q to quit and have the system come up normally. Login with the default username and password. The default username is admin and the default password is also admin.

```
Main Menu Options
-----
1 - Reset Passwords
Q - Quit Main Menu
```

```
Q
pSH+ Copyright (c) Integrated Systems, Inc., 1992.
Cisco Systems, Inc./VPN 3000 Concentrator Version 4.0.1.Rel May 06 2003 13:13:03
Features:
Initializing VPN 3000 Concentrator ...
Waiting for CAPI initialization to complete...
Initialization Complete...Waiting for Network...
```

```
1 09/27/2003 12:34:46.080 SEV=1 EVENT/37 RPT=1
Reset Reason : 2 (Hardware-Reset)

4 09/27/2003 12:34:46.310 SEV=3 IP/1 RPT=1
IP Interface 1 status changed to Link Up.

5 09/27/2003 12:34:46.330 SEV=3 IP/1 RPT=2
IP Interface 2 status changed to Link Up.

6 09/27/2003 12:34:46.900 SEV=3 IP/2 RPT=1
IP Interface 1 status changed to Link Down.

7 09/27/2003 12:34:47.900 SEV=3 IP/2 RPT=2
IP Interface 2 status changed to Link Down.

8 09/27/2003 12:34:48.900 SEV=3 IP/1 RPT=3
IP Interface 1 status changed to Link Up.

9 09/27/2003 12:34:48.900 SEV=3 IP/1 RPT=4
IP Interface 2 status changed to Link Up.
```

```
Login: admin
Password:
```

```
Welcome to
Cisco Systems
```

- 1) Configuration
- 2) Administration
- 3) Monitoring
- 4) Save changes to Config file
- 5) Help Information
- 6) Exit

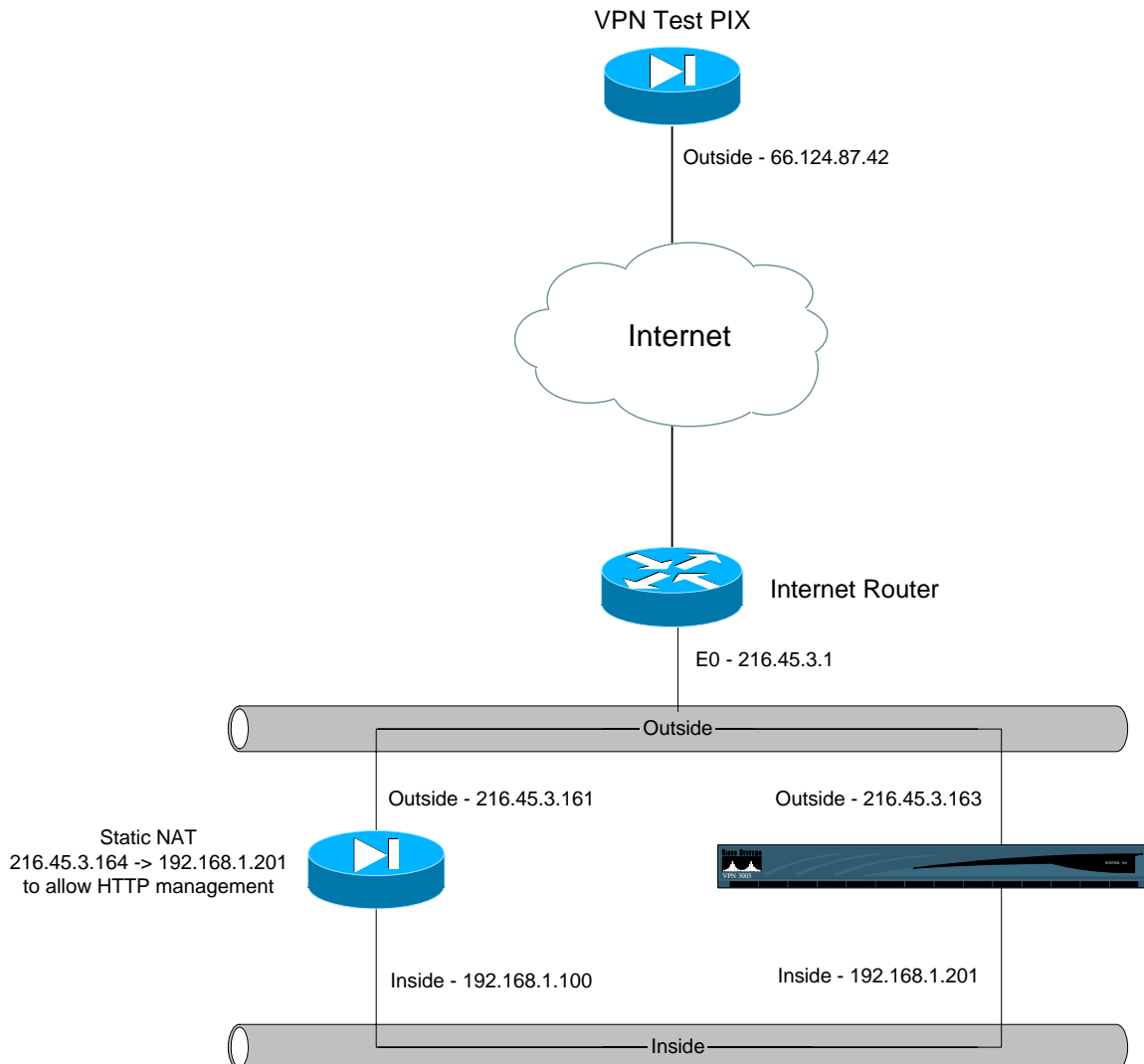
nli-3005: Main ->

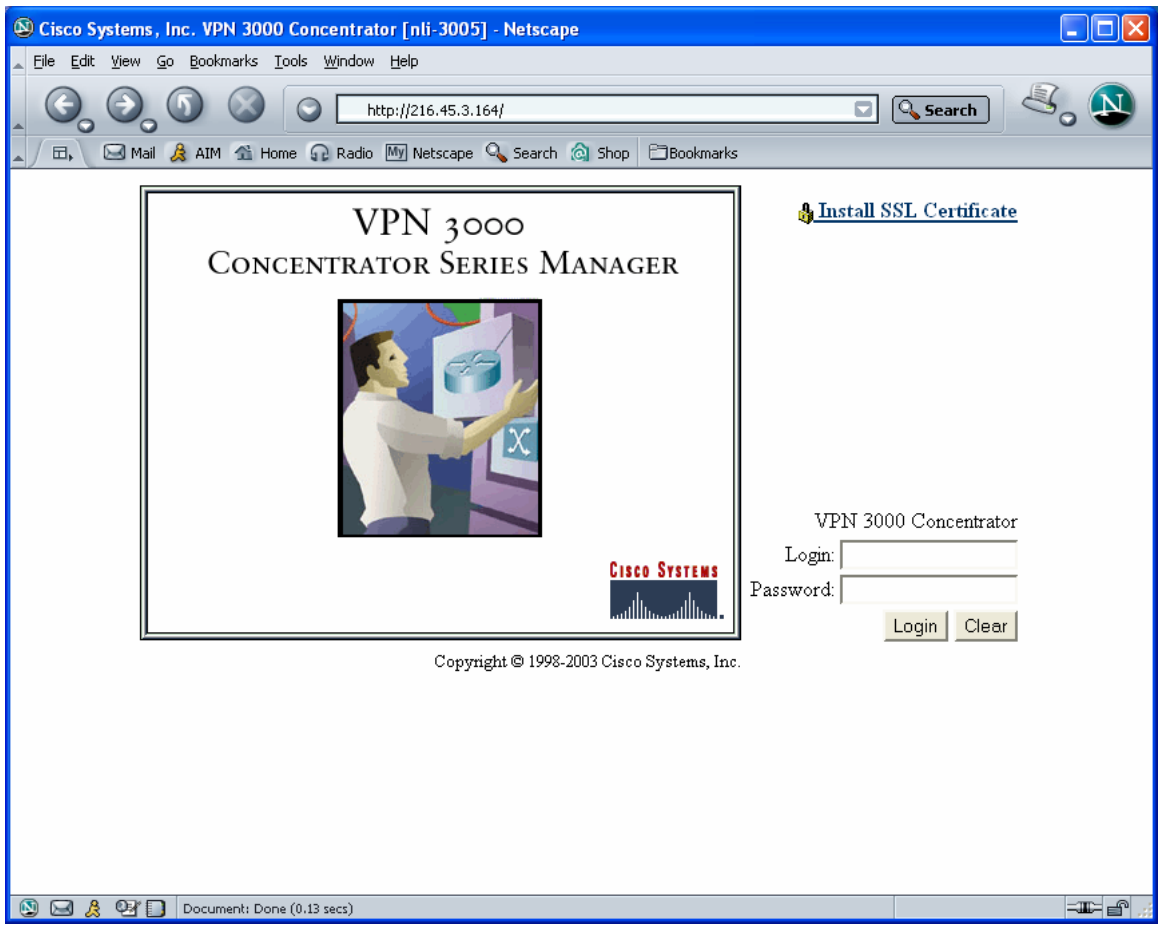
Configuring SSL

Step 1. Open a web browser to the inside IP address. You can configure the 3000 through the outside interface, but it must be enabled. By default, the concentrator will deny all management connections to the outside. You can configure the 3000 to allow HTTPS and SSH to the outside.

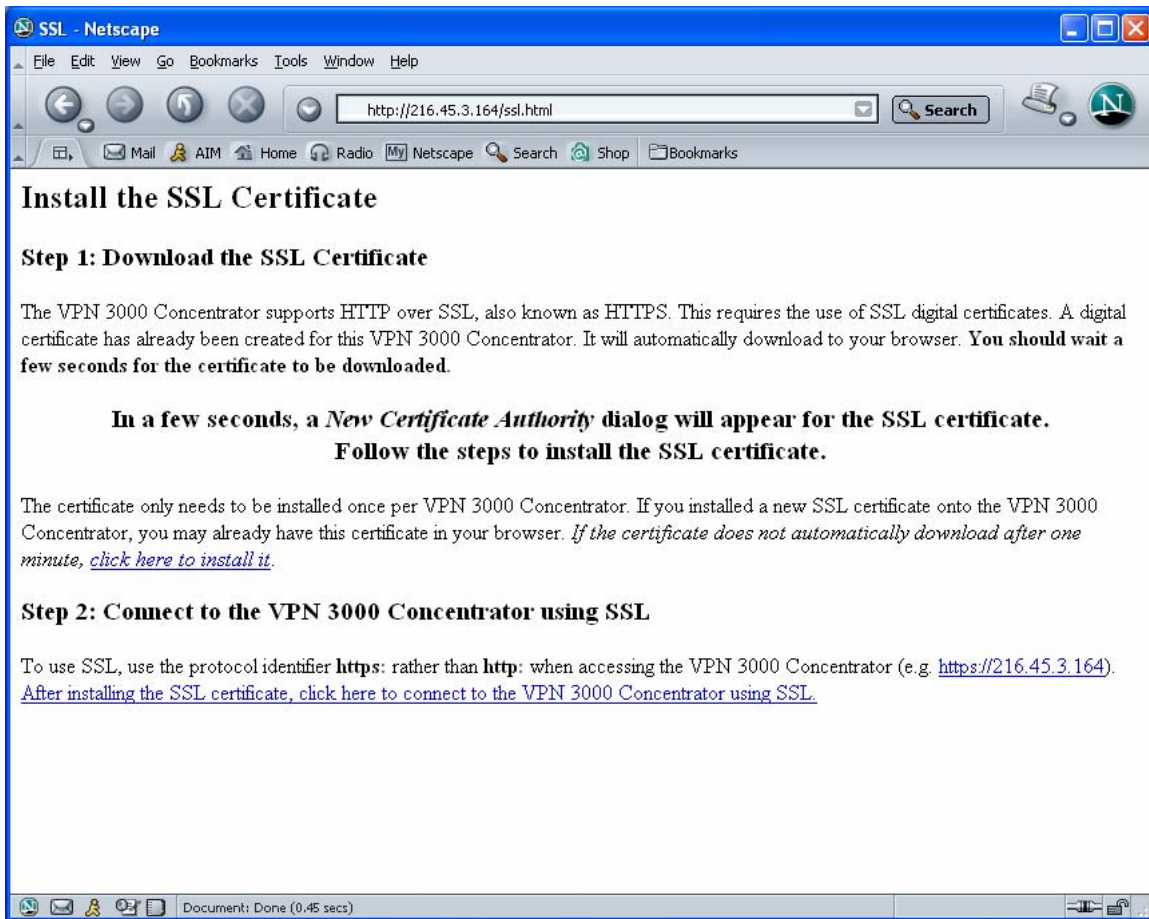
Figure x shows the layout of our VPN network. This was setup using the Internet and not a lab network. It is important to pay close attention to the layout particularly the static NAT.

Figure x. VPN Test Network





Step 2. Click on Install SSL Certificate. Wait for the certificate to download.



Step 3. Click OK to trust the CA.



Step 4. Click the radio button to Accept this certificate. Click OK.



Step 5. Click OK if you receive this security error. This is due to NAT.



Step 6. Connect to the 3000 using HTTPS.



Cisco Systems, Inc. VPN 3000 Concentrator [nli-3005] - Netscape

File Edit View Go Bookmarks Tools Window Help

https://216.45.3.164/index.html Search

Mail AIM Home Radio My Netscape Search Shop Bookmarks

VPN 3000 CONCENTRATOR SERIES MANAGER



VPN 3000 Concentrator

Login:

Password:

Copyright © 1998-2003 Cisco Systems, Inc.

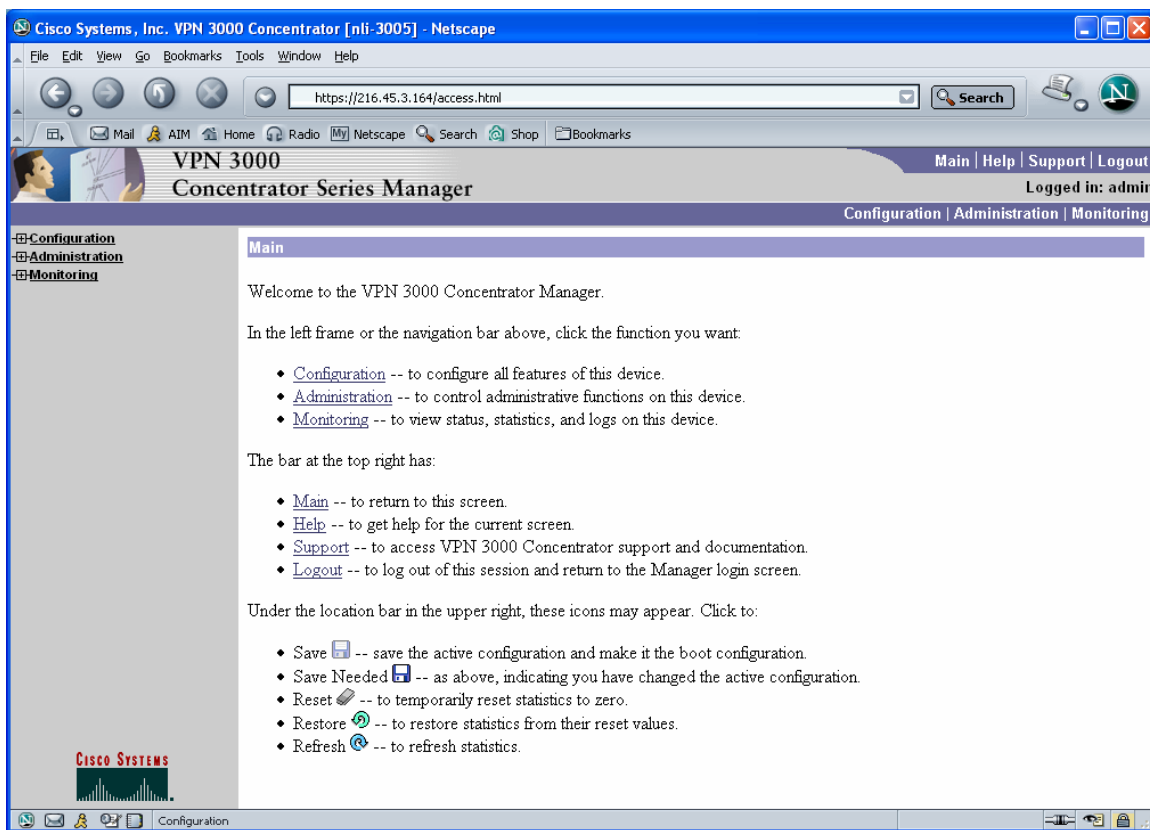
Document: Done (83.049 secs)

Configuring a Basic LAN-To-LAN VPN

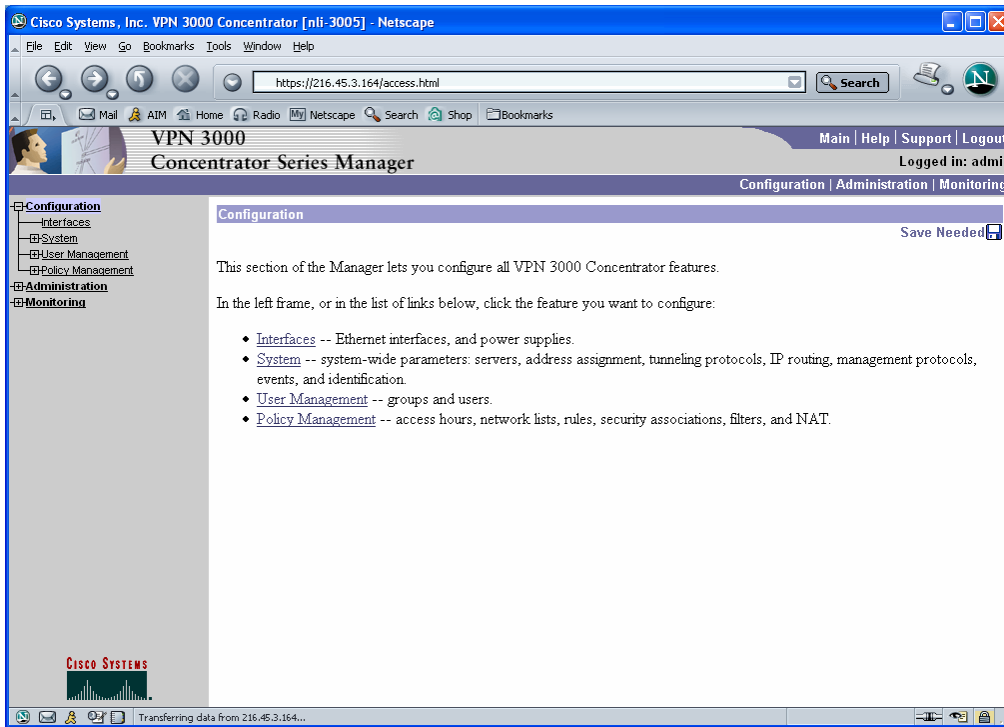
Step 1. Configure your PIX or Router for IPSec. This is already covered in Chapter XX. Below is the relevant PIX configuration used in this example.

```
access-list nonat permit ip 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
access-list VPN_3005 permit ip 192.168.2.0 255.255.255.0 192.168.1.0 255.255.255.0
ip address outside 66.124.87.42 255.255.255.248
ip address inside 192.168.0.1 255.255.255.0
nat (inside) 0 access-list nonat
crypto ipsec transform-set netcg esp-3des esp-sha-hmac
crypto map VPN 10 ipsec-isakmp
crypto map VPN 10 match address VPN_3005
crypto map VPN 10 set peer 216.45.3.163
crypto map VPN 10 set transform-set netcg
crypto map VPN interface outside
isakmp enable outside
isakmp key ***** address 216.45.3.163 netmask 255.255.255.255
isakmp identity address
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash md5
isakmp policy 10 group 1
isakmp policy 10 lifetime 86400
```

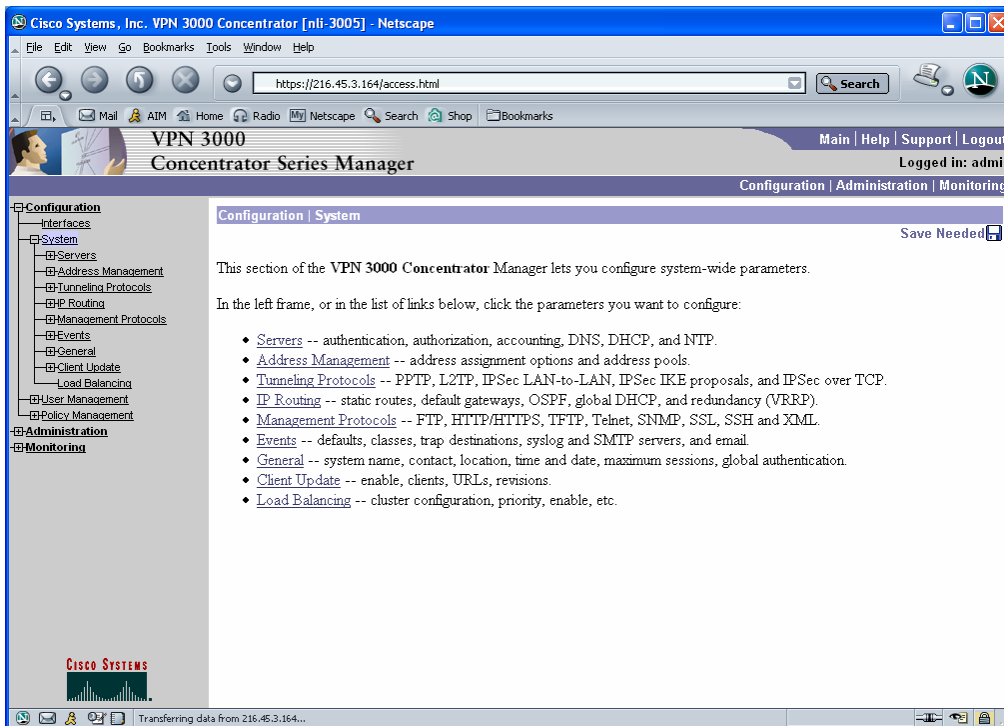
Step 2. Logon to the VPN concentrator using a web browser. You cannot configure LAN-to-LAN tunnels using the console. Once logged in, click Configuration.



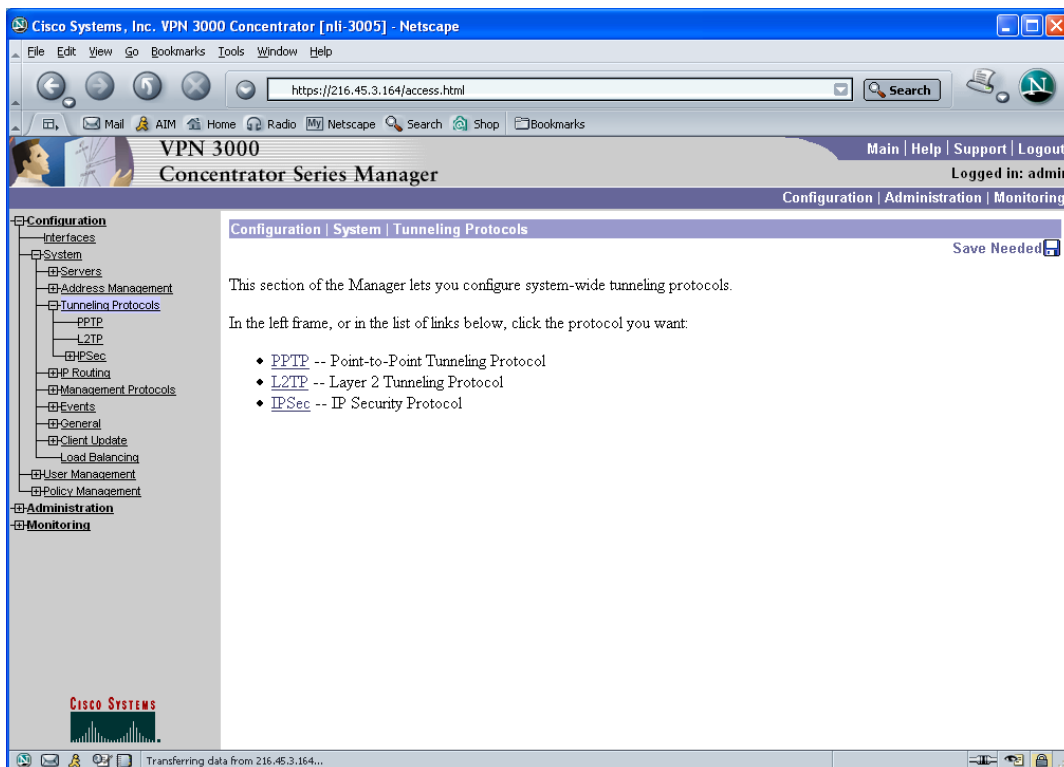
Step 3. Click System.



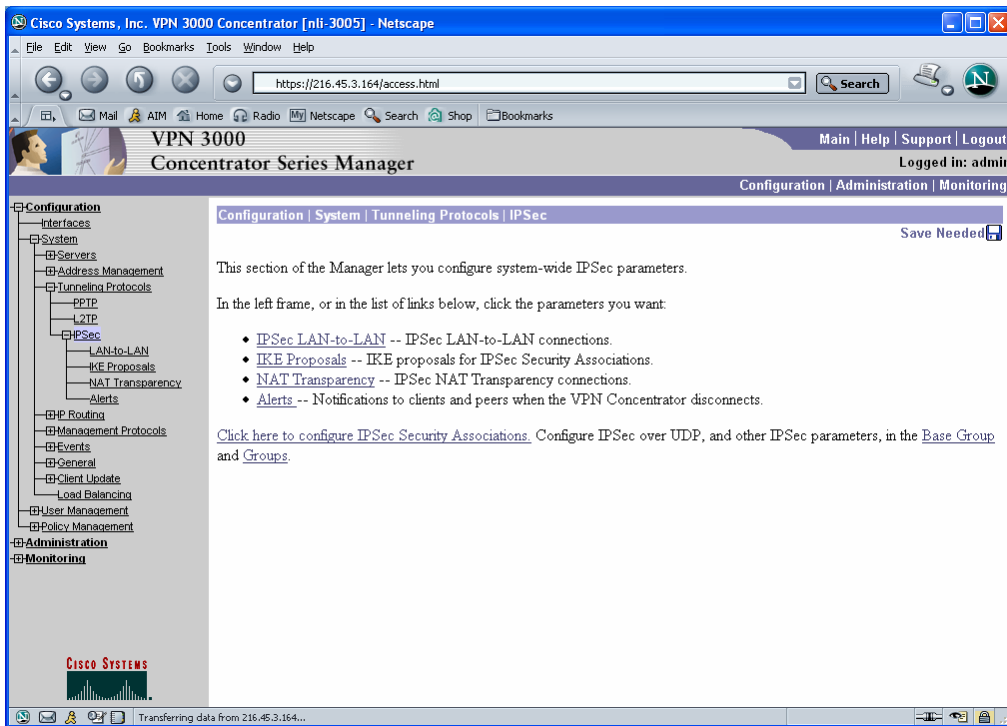
Step 4. Click Tunneling Protocols



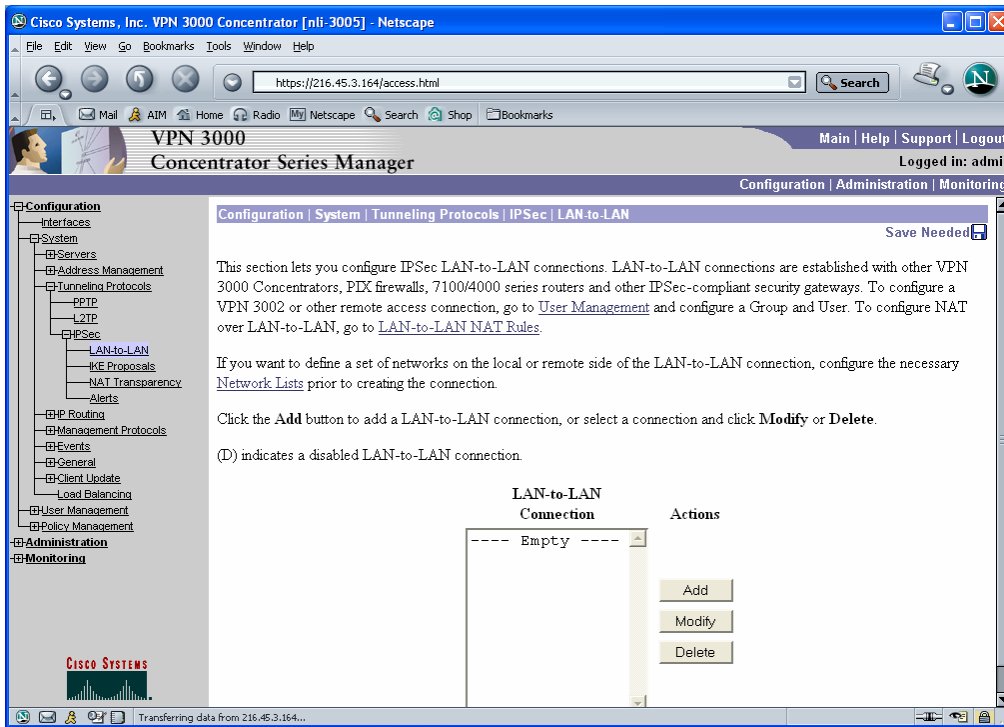
Step 5. Click IPsec



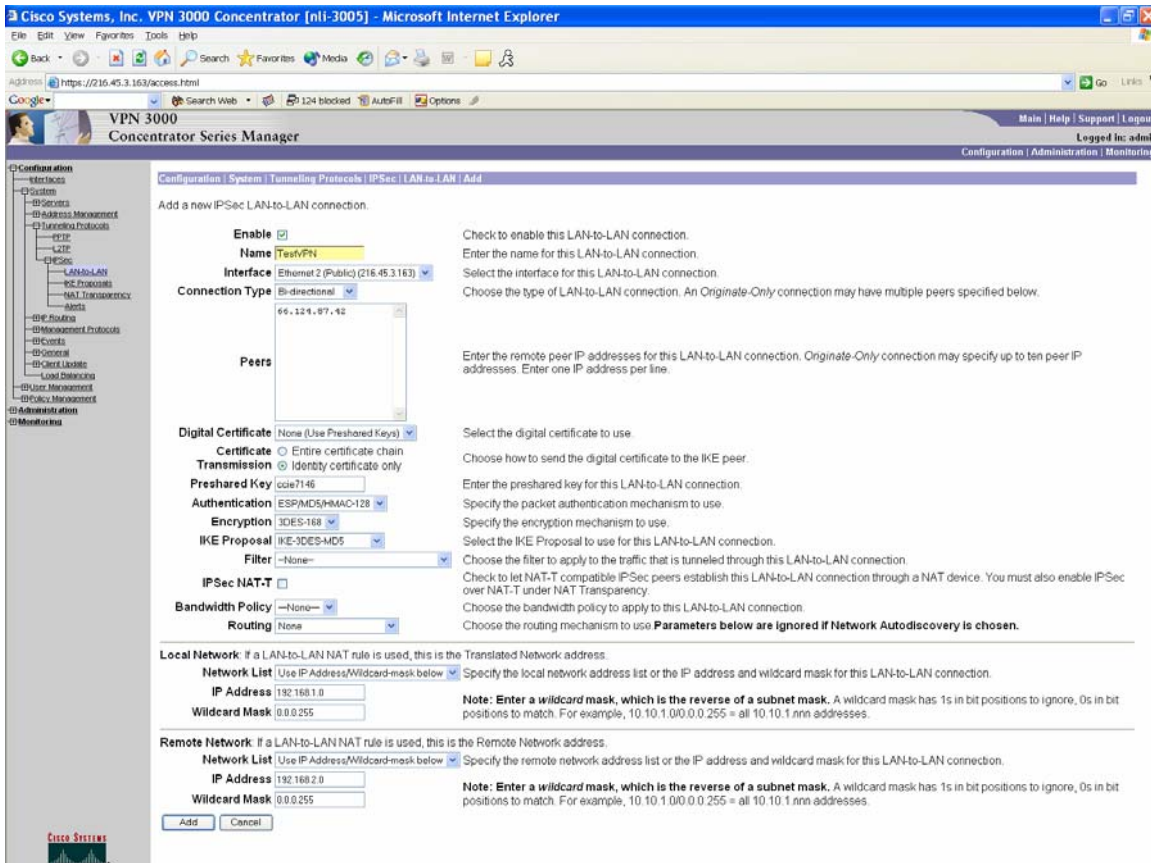
Step 6. Click IPsec LAN-to-LAN



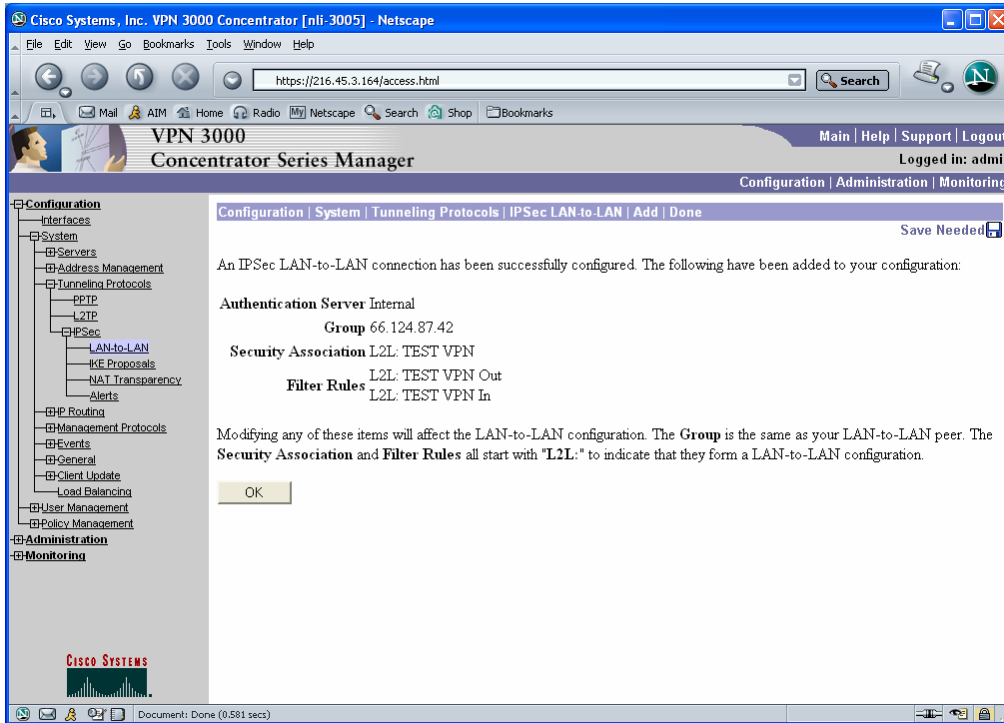
Step 7. Click Add.



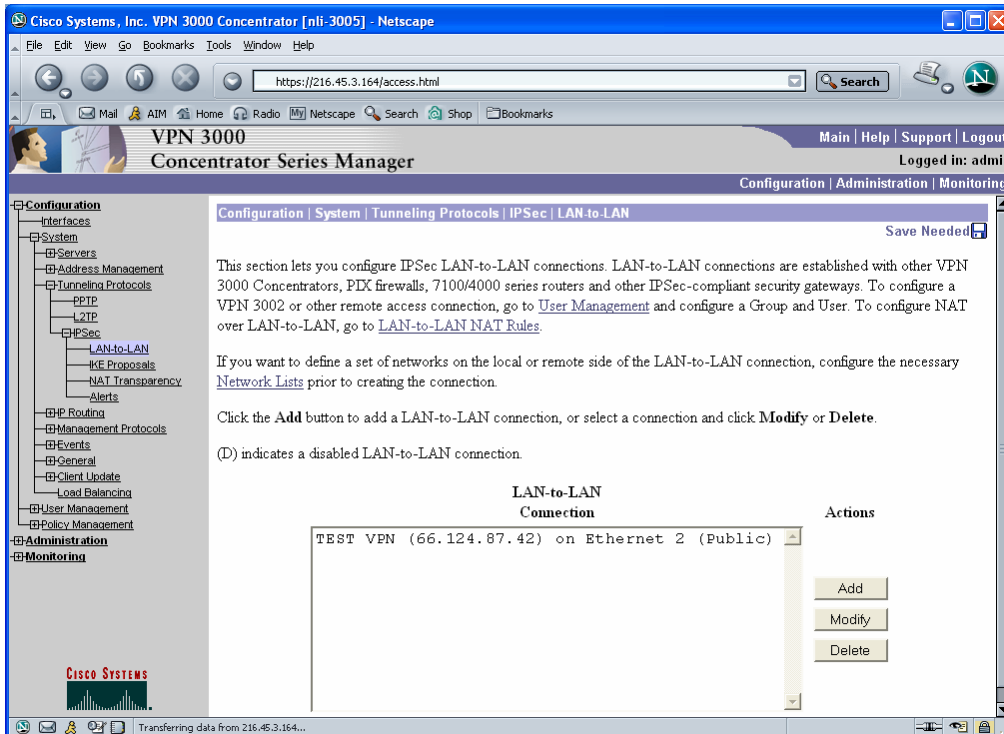
Step 8. Complete the appropriate values. The click Add.



Step 9. Click OK.



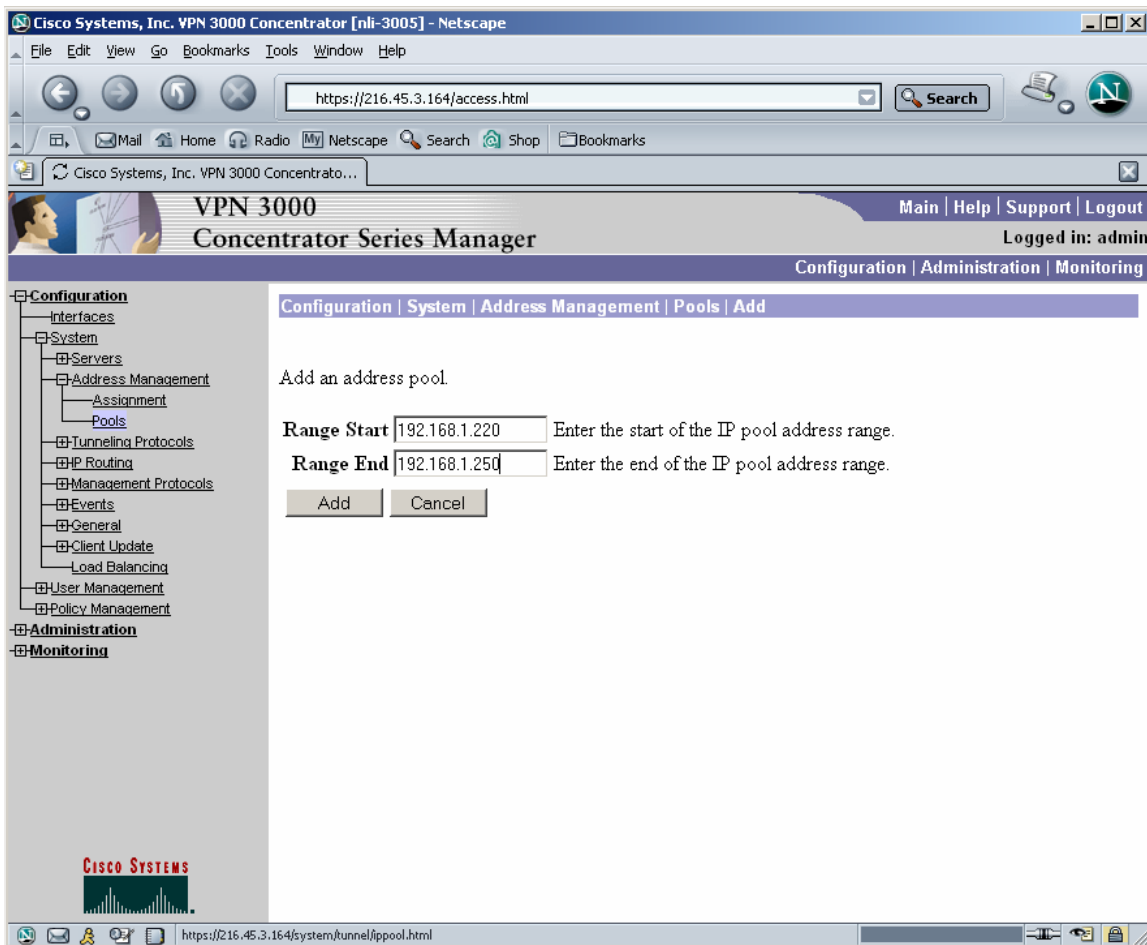
Step 10. VPN setup is complete.



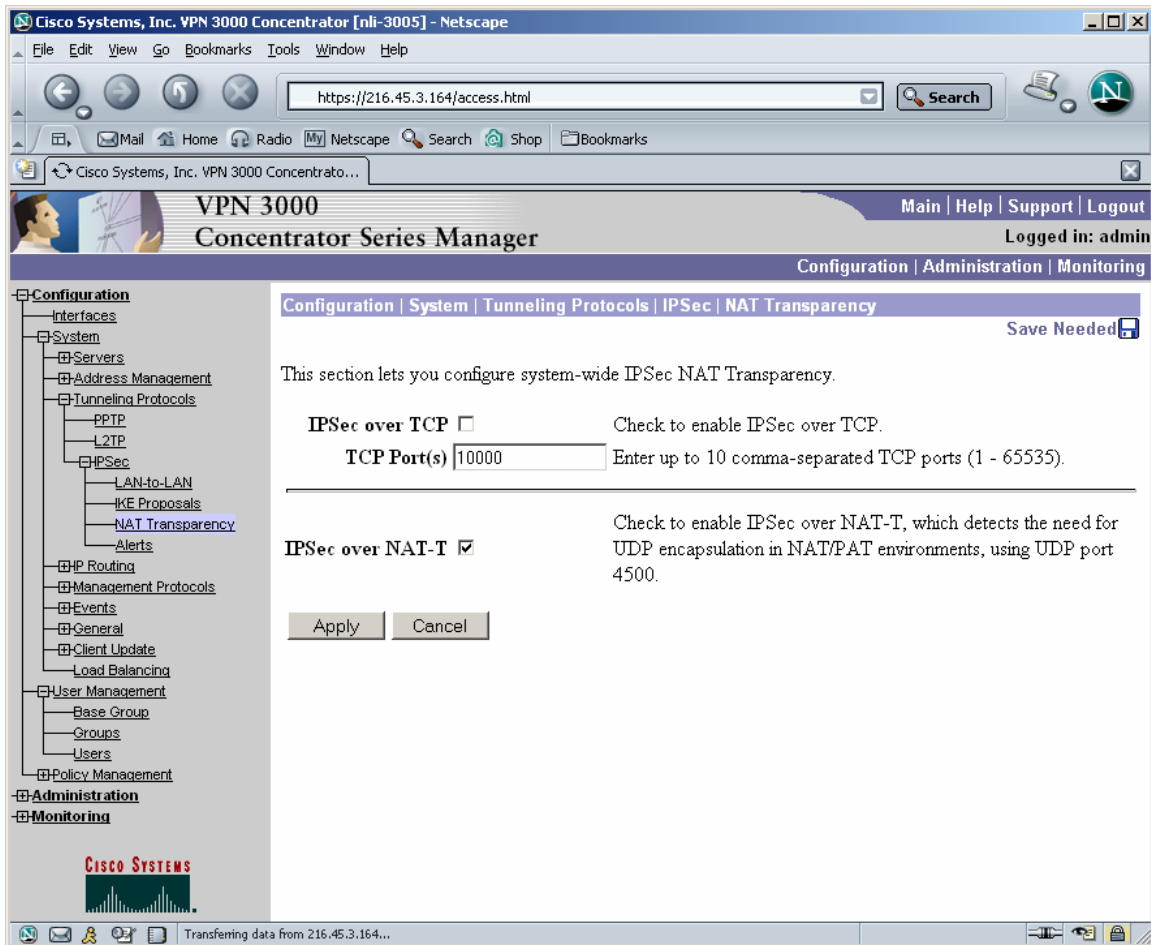
Configuring the 3000 for VPN 4.0 Clients

Step 1. Logon to the VPN concentrator using a web browser. You cannot configure VPN clients using the console.

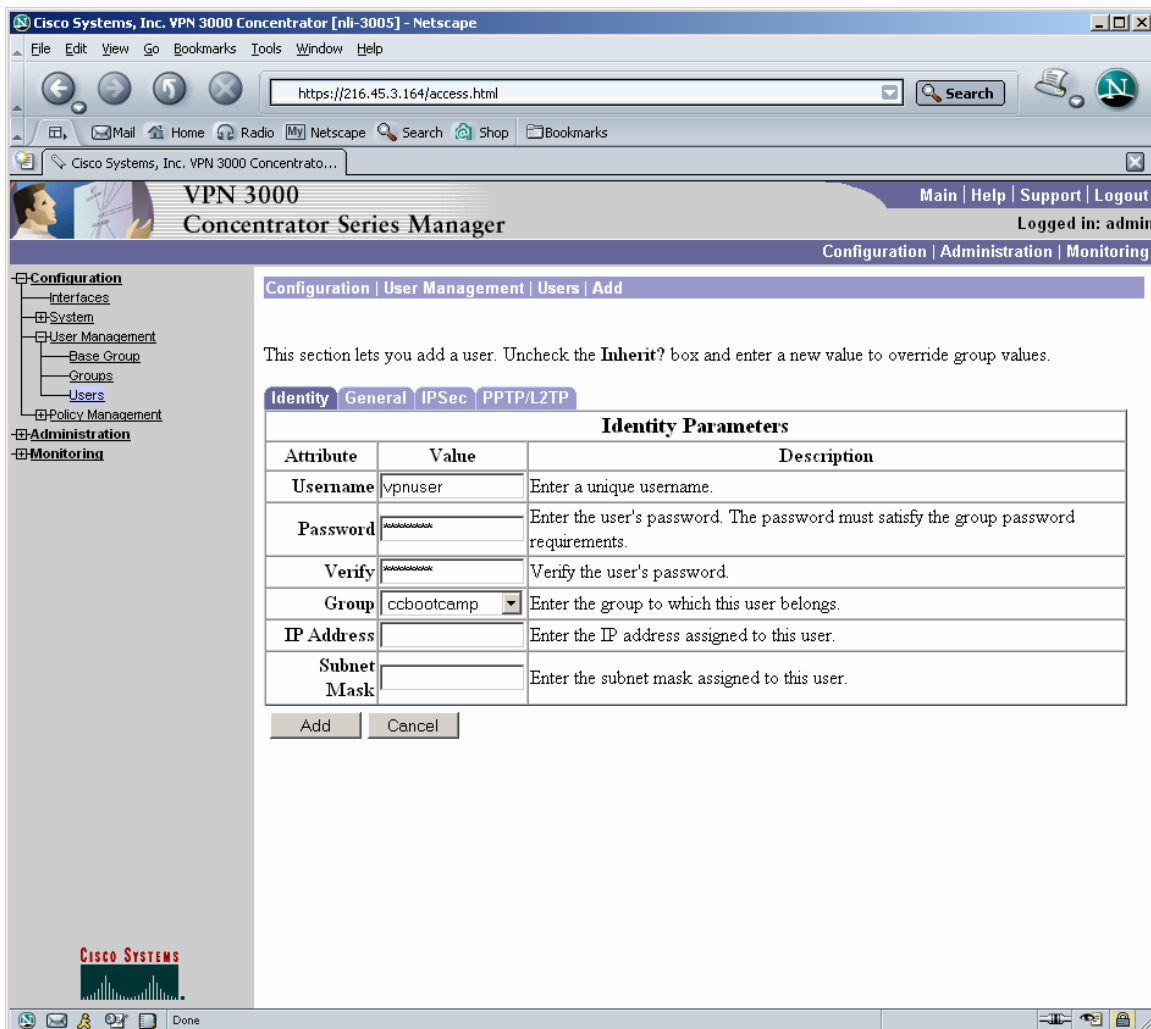
Step 2. Configure an Address Pool or some other method of assigning VPN clients an IP address. Click Configuration > System > Address Management > Address Pools.



Step 3. Enable NAT Transparency. This step is optional, but if your client is behind a firewall running PAT you will need this option enabled.



Step 4. Add VPN users. Assigning the user to a Group. The rest of the tabs and their settings can be left at default.



Allowing Split Tunneling

By default, the 3000 will tunnel all traffic between the VPN client and the 3000. This is a more secure method, but all the user's web browsing and other traffic not destined for the remote network will come through the 3000. Depending on the requirements given, this may not be desirable. To allow only traffic destined for the remote internal network to traverse the VPN is called split tunneling. In our example, the remote internal network is 192.168.1.0 /24. We want traffic destined for this network from the VPN client to be encrypted. All other traffic should use the VPN client's normal default gateway.

Step 1. To configure split tunneling, we must first define which networks we want to be allowed or not allowed over the tunnel. Click Policy Management > Network Lists > Add.

Step 2. Configure the specific networks you want to allow or deny from being encrypted. Click Add.

Cisco Systems, Inc. VPN 3000 Concentrator [nli-3005] - Netscape

File Edit View Go Bookmarks Tools Window Help

https://216.45.3.164/access.html

VPN 3000 Concentrator Series Manager

Main | Help | Support | Logout

Logged in: admin

Configuration | Administration | Monitoring

Configuration | Policy Management | Traffic Management | Network Lists | Add

Configure and add a new Network List. Click on **Generate Local List** to generate a network list based on routing entries on the Private interface.

List Name: Allow Split Tunnel

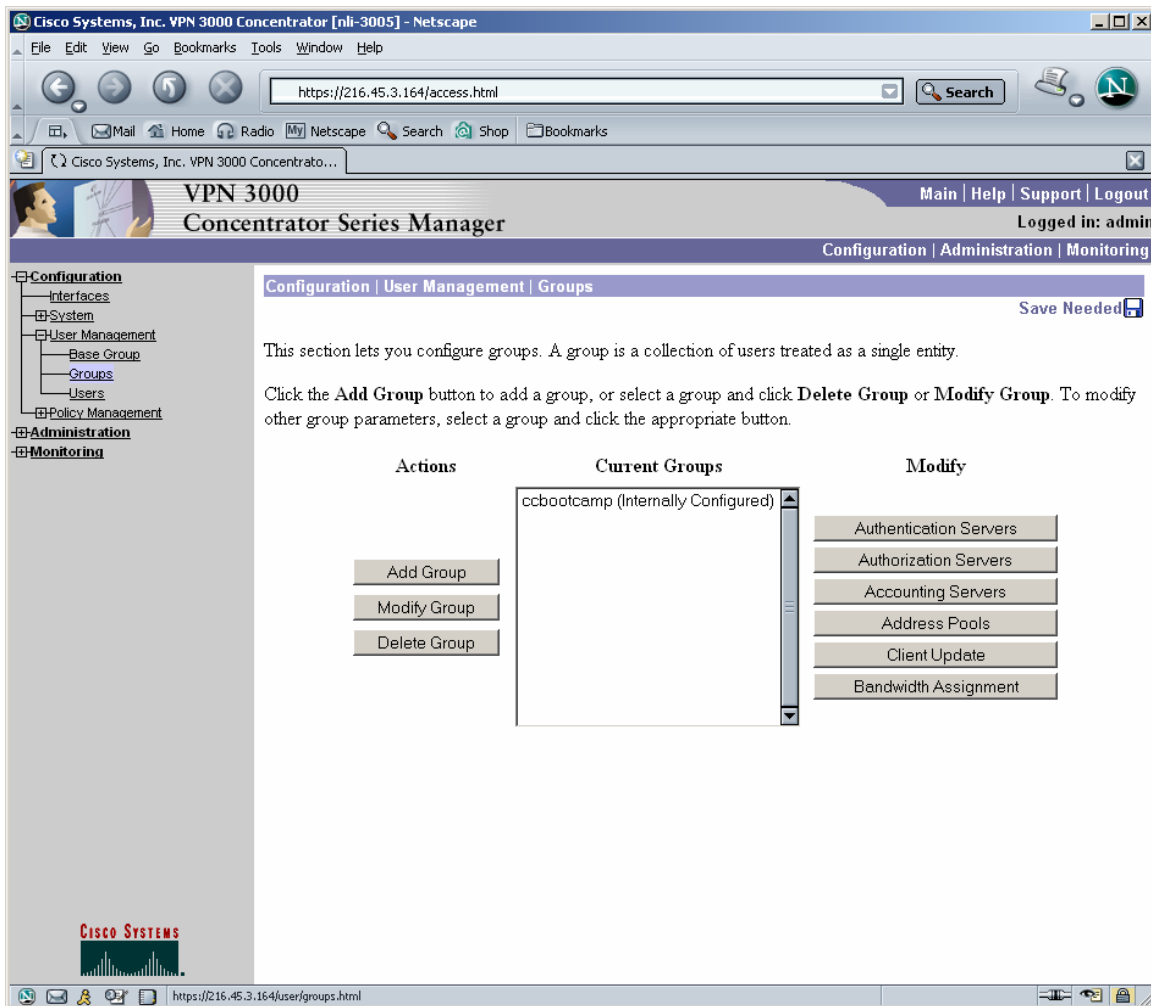
Network List: 192.168.1.0/0.0.0.255

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

- 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, 10.10.1.0/0.0.255 = 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.

Add Cancel Generate Local List

Step 3. Once you have created the Network List, you have to apply it to a VPN Group. Click User Management > Groups.



Step 4. Click the Client Config tab. Scroll down to the section titled Common Client Parameters. Click the radio button Only tunnel networks in the list. Then click the drop down next to Split Tunneling Network List and select the list created in Step 2. Click Apply at the bottom of the page.

Cisco Systems, Inc. VPN 3000 Concentrator [nli-3005] - Netscape

https://216.45.3.164/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
- Administration
- Monitoring

Identity General IPsec Client Config Client FW HW Client PPTP/L2TP

Client Configuration Parameters

Cisco Client Parameters			
Attribute	Value	Inherit?	Description
Banner		<input checked="" type="checkbox"/>	Enter the banner for this group.
Allow Password Storage on Client	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow the IPsec client to store the password locally.
IPsec over UDP	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to allow a client to operate through a NAT device using UDP encapsulation of ESP.
IPsec over UDP Port	10000	<input checked="" type="checkbox"/>	Enter the UDP port to be used for IPsec through NAT (4001 - 49151, except port 4500, which is reserved for NAT-T).
IPsec Backup Servers	Use Client Configured List	<input checked="" type="checkbox"/>	<ul style="list-style-type: none"> Select a method to use or disable backup servers. Enter up to 10 IPsec backup server addresses/names starting from high priority to low. Enter each IPsec backup server address/name on a single line.
Microsoft Client Parameters			
Intercept DHCP Configure Message	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to use group policy for clients requesting Microsoft DHCP options.
Subnet Mask	255.255.255.255	<input checked="" type="checkbox"/>	Enter the subnet mask for clients requesting Microsoft DHCP options.
Common Client Parameters			
Split Tunneling Policy	<input type="radio"/> Tunnel everything <input type="checkbox"/> Allow the networks in list to bypass the tunnel <input checked="" type="radio"/> Only tunnel networks in the list	<input type="checkbox"/>	Select the method and network list to be used for Split Tunneling. Tunnel Everything: Send all traffic through the tunnel. Allow the networks in the list to bypass the tunnel: The VPN Client may choose to send traffic to addresses in this list to the client's LAN. Send all other traffic through the tunnel. NOTE: This setting only applies to the Cisco VPN Client. Tunnel networks in the list: Send traffic to addresses in this list through the tunnel. Send all other traffic to the client's LAN.
Split Tunneling Network List	Allow Split Tunnel	<input type="checkbox"/>	

Transferring data from 216.45.3.164...

*****This document is being provided as a pre-release for those customers that have bought the CCIE Security Lab Guide. This material is currently being updated and when it is complete a new version of the Lab Guide will be printed. If you have any comments or questions about this document please email john@netcinc.com**