Configuring a Teleworker VPN Client on the Cisco ISA500 Security Appliance

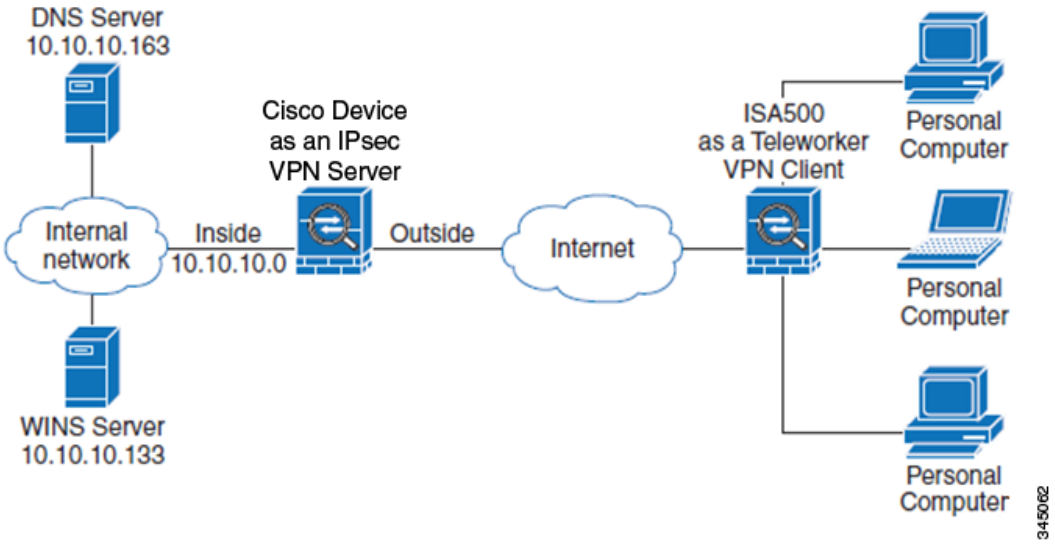
This application note describes how to configure a Teleworker VPN Client on the Cisco ISA500 security appliance. This document includes the following sections:

Overview

The Teleworker VPN Client feature minimizes the configuration requirements at remote locations by allowing the ISA500 to work as a Cisco VPN hardware client so that it receives the VPN security policies on a VPN tunnel from a remote IPsec VPN server. This solution is ideal for remote offices with limited IT support or for large Customer Premises Equipment (CPE) deployments where it is not practical to configure multiple remote devices individually.

Figure 1 shows a Cisco device configured as an IPsec VPN server. When the ISA500 (acting as a Teleworker VPN Client) initiates the VPN connection, the IPsec VPN server pushes the IPsec policies to the client and creates the corresponding VPN tunnel.

Figure 1 IPsec Remote Access with an IPsec VPN Server



Operating Modes

The Teleworker VPN Client supports the following two operating modes. You must specify an operation mode before establishing a connection.

- **Client Mode**
- **Network Extension Mode**

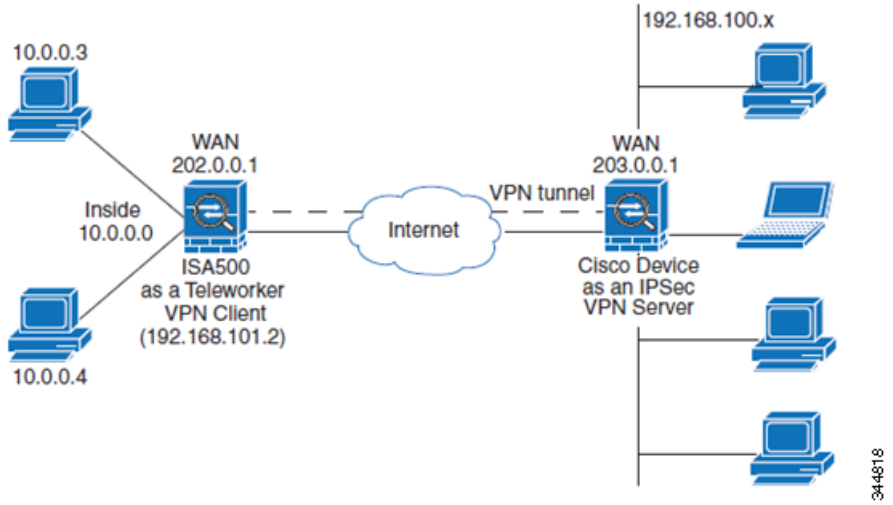
NOTE Both operation modes support split tunneling. Split tunneling allows for secure access to corporate resources through the VPN tunnel in addition to Internet access to an Internet Service Provider (ISP) or other service which eliminates the corporate network from the path for web access.

Client Mode

In client mode, Network Address Translation (NAT) or Private Address Translation (PAT) is performed so that remote computers and other hosts at the end of the VPN tunnel can form a private network. In this mode, the IP addresses in the IP address space of the destination server are not used. Instead, the outside interface of the Teleworker VPN Client is assigned an IP address by the remote server.

Figure 2 illustrates how client mode works. In this example, the ISA500 provides access to two computers assigned IP addresses in the 10.0.0.0 private network space. These computers are connected to the Ethernet interface on the ISA500. The Cisco device (IPsec VPN server) assigns an IP address (192.168.101.2) to the ISA500 (Teleworker VPN Client) which performs NAT or PAT translation over the VPN tunnel so that the computers can access the destination network (192.168.100.x). In this example, the computers (hosts 10.0.0.3 and 10.0.0.4) are translated to (192.168.101.2) but hosts in the remote network (192.168.100.x) are unable to access the computers (hosts 10.0.0.3 and 10.0.0.4). For information about how to configure the ISA500 in client mode, see Configuring the ISA500 in Client Mode, page 4.

Figure 2 IPsec VPN Client Connection



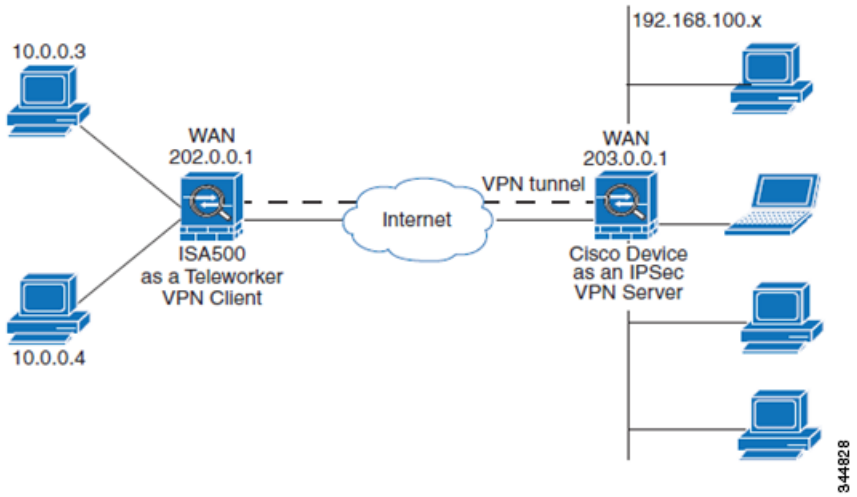
Network Extension Mode

Network Extension Mode (NEM) determines whether the inside hosts relative to the Cisco VPN hardware client (ISA500) are accessible from the corporate network over the VPN tunnel. In NEM mode, the Cisco VPN hardware client obtains a private IP address from a local DHCP server or is configured with a static IP address.

Table 3 illustrates how NEM mode works. In this example, the ISA500 acts as a Cisco VPN hardware client and is connected to a remote IPsec VPN server. The hosts attached to the ISA500 have IP addresses in the 10.0.0.0 private network space. The VPN server does not assign an IP address to the ISA500 (which does not perform NAT or PAT translation over the VPN tunnel). When accessing the remote network (192.168.100.x), the hosts (10.0.0.3) and (10.0.04) are not translated, but the hosts in the remote network (192.168.100.x) can access the hosts (10.0.0.3 and 10.0.04) directly.

The client hosts are assigned IP addresses that are fully routable by the destination network over the VPN tunnel. These IP addresses could be either in the same subnet space as the destination network or in separate subnets, assuming that the destination routers are configured to properly route those IP addresses over the VPN tunnel. For information about how to configure the ISA500 in NEM mode, see Configuring the ISA500 in NEM Mode, page 9.

Figure 3 IPsec VPN Network Extension Connection



Configuring the Teleworker VPN Client

The section describes how to configure the Teleworker VPN Client on the ISA500 in client mode and NEM mode. This configuration requires that you configure two ISA500 security appliances - one as an IPsec VPN server and another ISA500 as a Teleworker VPN Client.

Configuring the ISA500 in Client Mode

- Configuring the ISA500 as an IPsec VPN Server (Client Mode)
- Configuring the ISA500 as Teleworker VPN Client (Client Mode)

Configuring the ISA500 as an IPsec VPN Server (Client Mode)

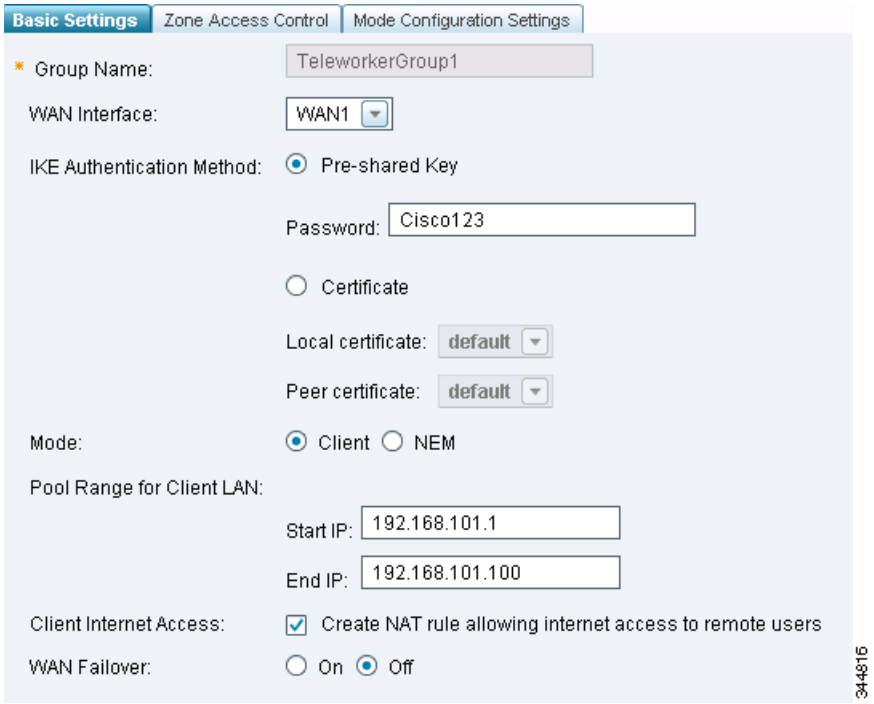
Step 1. Enable IPsec Remote Access.

a. Choose **VPN > IPsec Remote Access.**

b. Click **On** to enable remote access and set the ISA500 as an IPsec VPN server.

c. Click **Save**.

Step 2. Add an IPsec Remote Access group policy by clicking **Add** from the IPsec Remote Access window. This policy is used by the remote VPN clients to establish the VPN connections.



Step 3. From the Basic Settings tab, specify this information:

d. Enter the **Group Name** and **Password**.

e. Click **Client** mode. In this mode, the IPsec VPN server (ISA500) can assign the IP addresses to the outside interfaces of the remote VPN.

f. Enter the starting and ending IP addresses in the **Start IP** and **End IP** fields. These fields define the IP address pool range for the remote VPN clients.

NOTE The IP address space for these addresses must be different than the Teleworker remote client's network or any other remote client's network that is used to establish the VPN connection to the IPsec VPN server. Otherwise, the VPN connection will fail. In this example, the range is 192.168.101.1 to 192.168.101.100.

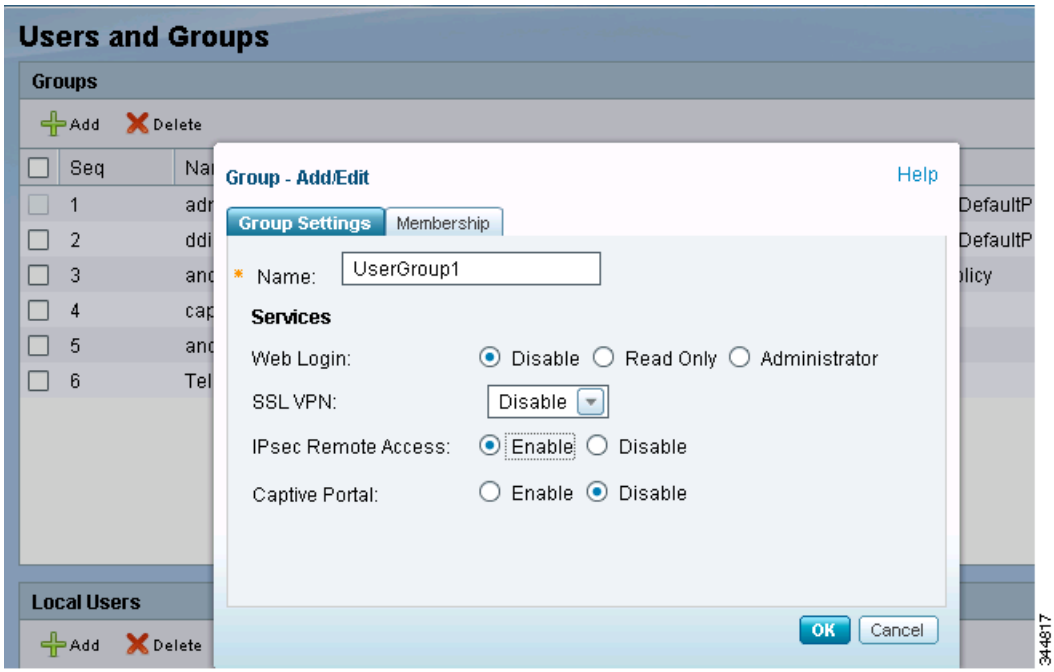
g. Specify the remaining fields or choose the default values.

h. Click **OK** to save your settings.

Step 4. Add a User Group. A user can only belong to one user group and share the same service policy.

a. Choose **Users > Users and Groups**.

b. Click **Add**.



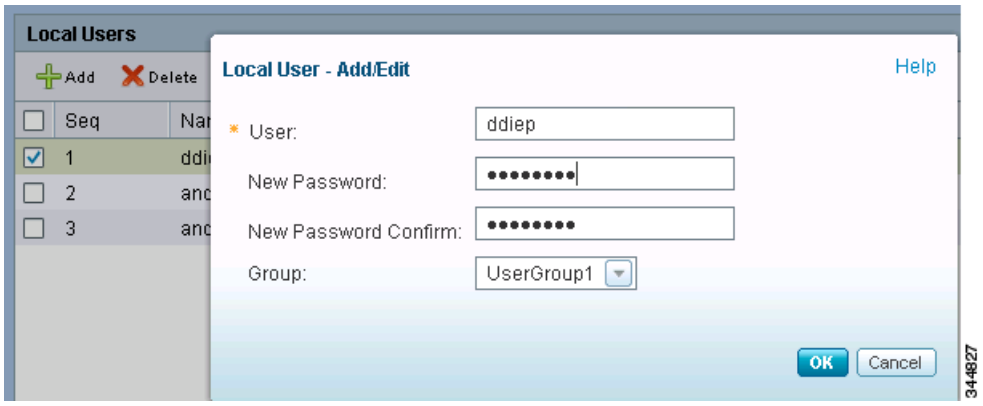
c. Enter a name for the new group. In this example, the new group is UserGroup1.

d. Under Services, **Enable** IPsec Remote Access. This allows the members of the user group at remote sites to establish the VPN tunnels to securely access your network resources.

e. Click **OK** to save your settings.

Step 5. Assign a user to the group that you just created.

a. Under Local Users, click the box next to the user you want to add and then click the pencil icon.



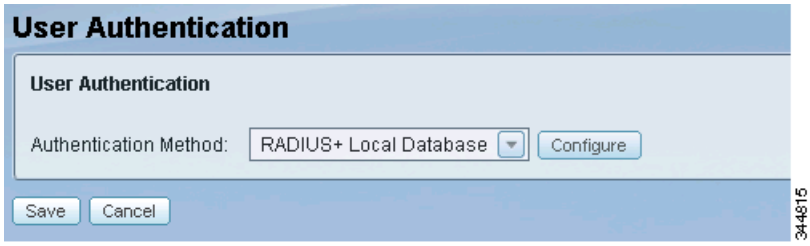
b. Enter and confirm the new user password.

c. Choose the group to which this user belongs. In this example, the group is UserGroup1.

d. Click **OK** to save your settings.

Step 6. Specify the user authentication method.

a. Choose **Users > Users Authentication**.



b. Choose the authentication method from the drop-down menu (LDAP, RADIUS, or Local Database). In this example, because the user credentials were defined locally, Local Database is also included as one of the authentication methods.

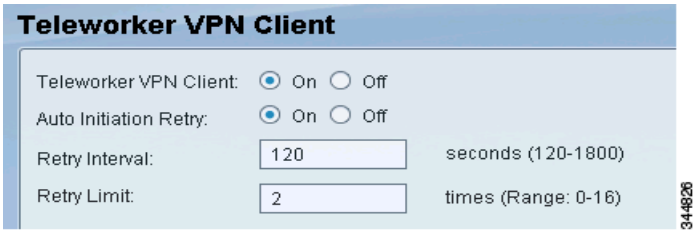
c. Click **Save**.

Configuring the ISA500 as Teleworker VPN Client (Client Mode)

Step 1. Enable the Teleworker VPN Client.

a. Choose **VPN > Teleworker > VPN Client**.

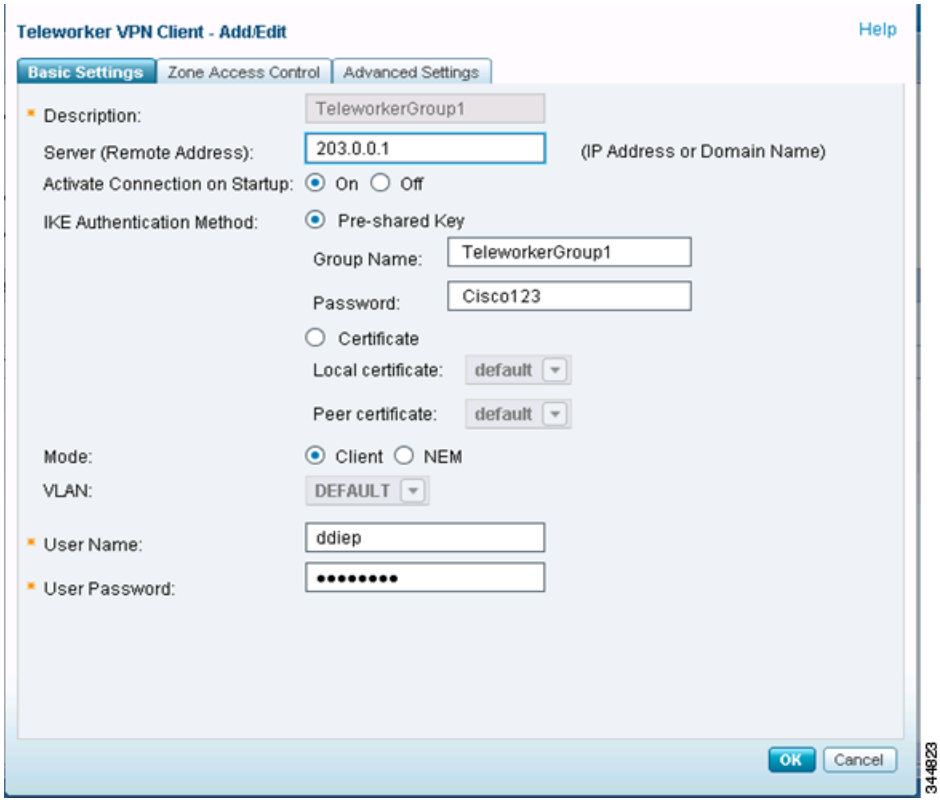
b. Click **On** to enable the client and set the ISA500 as a Teleworker VPN client. Enabling this feature disables site-to-site VPN and IPsec remote access and terminates their connected VPN sessions.



Step 2. Add a Teleworker VPN client.

a. Click **Add** from the Teleworker VPN Client window.

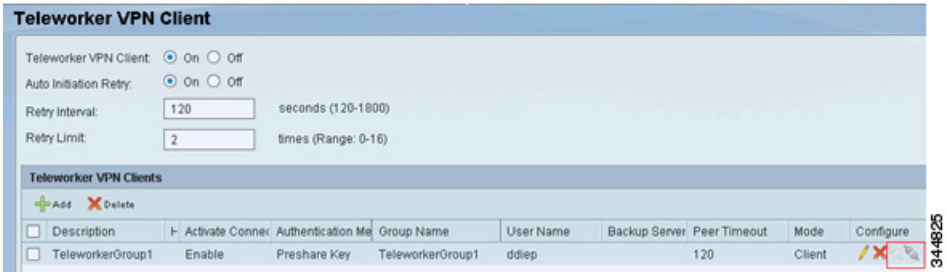
b. Enter the same remote server IP address, group name, group password, user name, and user password that was previously defined on the IPsec remote access server. See Configuring the ISA500 as an IPsec VPN Server (Client Mode), page 4.



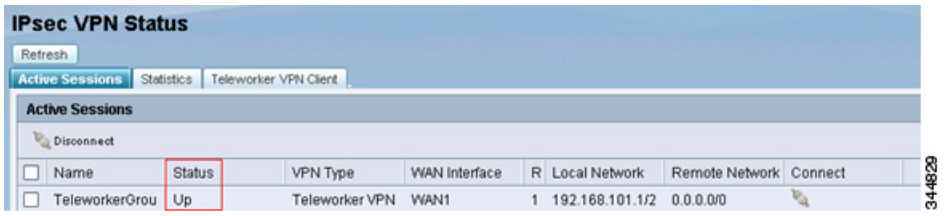
c. Select **Client** mode.

d. Click **OK** to save your settings.

Step 3. Click the **Connect** icon for the group that you just added to activate the connection.



Step 4. Choose **VPN > VPN Status > IPSec VPN Status** to verify the connection. In this example, the Teleworker Group session shows as connected and active (Status Up).

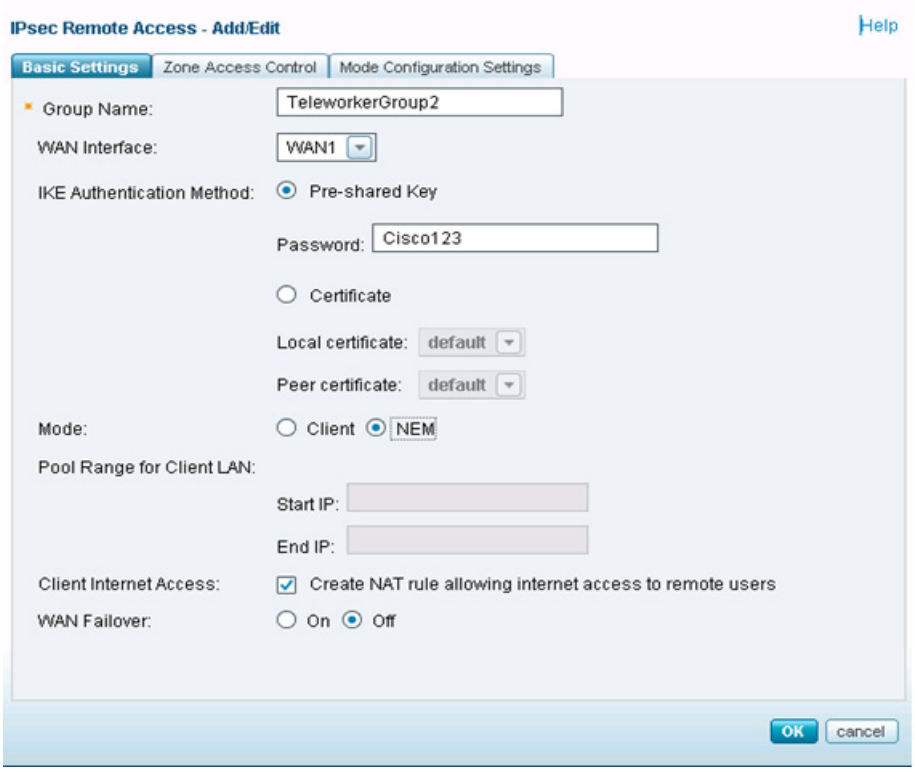


Configuring the ISA500 in NEM Mode

- Configuring the ISA500 as an IPsec VPN Server (NEM Mode)
- Configuring the ISA500 as Teleworker VPN Client (NEM Mode)

Configuring the ISA500 as an IPsec VPN Server (NEM Mode)

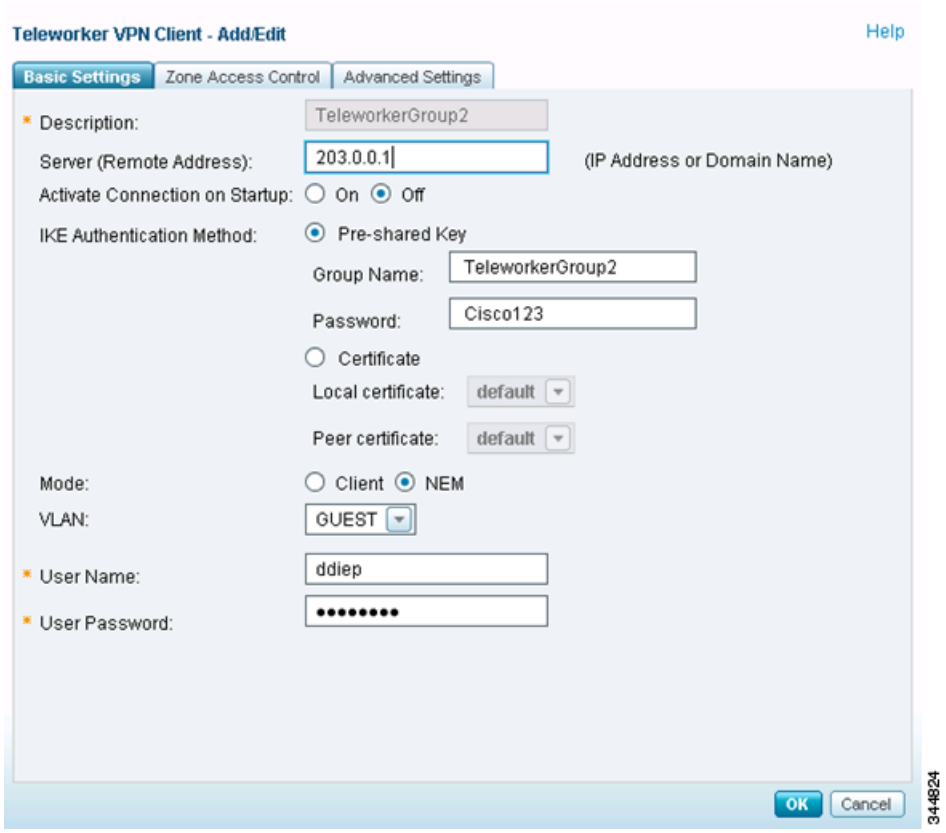
The steps for configuring the ISA500 in NEM mode are the same as those for Client mode. See Configuring the ISA500 as an IPsec VPN Server (Client Mode). The only difference is that you must select NEM mode when adding the IPsec Remote Access group as shown here.



Configuring the ISA500 as Teleworker VPN Client (NEM Mode)

The steps for configuring the ISA500 as a teleworker client in NEM mode are the same as those for client mode. See Configuring the ISA500 as Teleworker VPN Client (Client Mode). The only difference is that you must select NEM mode when adding the Teleworker VPN Client. NEM mode allows host(s) from the server to access a teleworker client's private network space. You can use the Default VLAN, GUEST VLAN, or define a VLAN to be an accessible private network space.

NOTE The Group Name, Password, User Name and User Password must be the same as the IPsec VPN Server (ISA500) configuration. See Configuring the ISA500 as an IPsec VPN Server (NEM Mode), page 9.

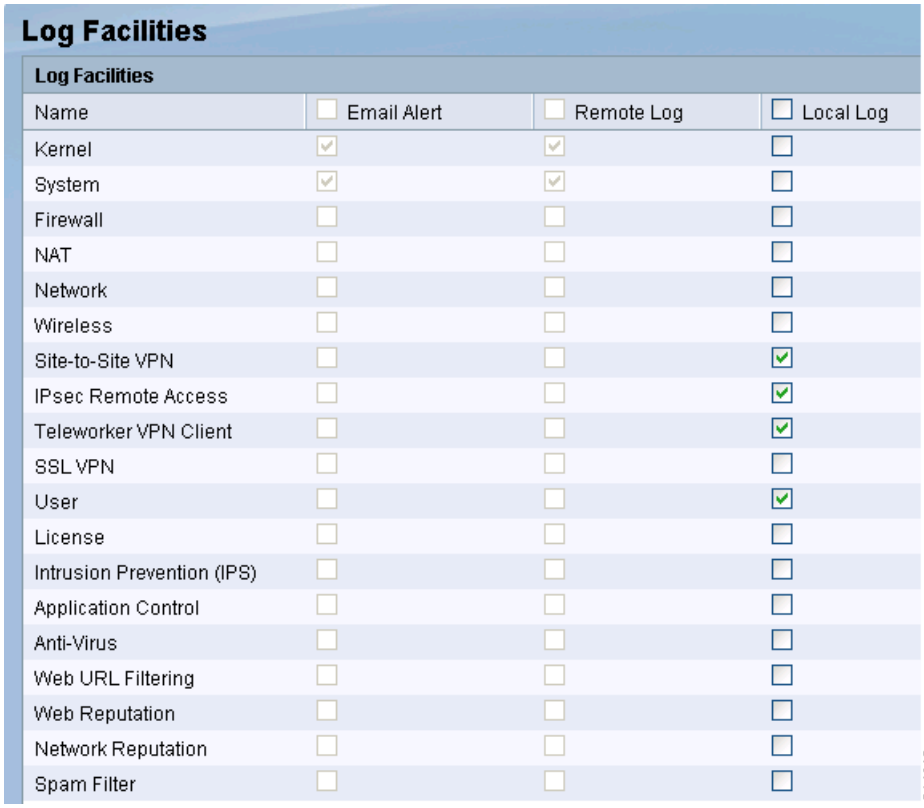


Troubleshooting VPN Connection Problems

You can turn on specific VPN logs for more details if problems occur when establishing a VPN connection. At a minimum, we recommend that you enable log facilities on the IPsec Remote Access server side for troubleshooting purposes.

Step 1. To enable logging, choose **Device Management > Logs > Log Facility**.

Step 2. Under **Local Log**, check the boxes for the feature that you want to troubleshoot. In this example, the logs for Site-to-Site VPN, IPsec Remote Access, Teleworker VPN Client, and User are enabled.



Step 3. Choose **Device Management > Logs > Log Settings**. Set the Local Log Severity level to **Debug** and then click **Save**.

Step 4. Choose **Device Management > Logs > View Logs** to view the logging information. This example shows the logs that were generated from the IPsec Remote Access server side.

```
-VPN Connection is successfully established

13:45:18 - Debug - Site-to-Site VPN: msg=find_host_connection returns
EZVPN_TeleworkerGroup1; (pluto)
13:45:18 - Info - IPsec Remote Access: msg=[IPsec Remote Access][pluto] User
ddiep: Attempting to login; (pluto)
13:45:18 - Info - IPsec Remote Access: msg=[IPsec Remote Access][pluto] User
ddiep: Authentication Successful; (pluto)
13:45:18 - Info - IPsec Remote Access: msg=[IPsec Remote Access][pluto] Assign
a virtual IP address (192.168.101.1)
13:45:19 - Info - IPsec Remote Access: msg=[IPsec Remote Access][pluto]  IPsec
SA established tunnel mode; (pluto)

-Fail to authenticate User credential.
Solution: ensure username or password matched from both sides.

14:45:00 - Err - IPsec Remote Access: msg=[IPsec Remote Access][pluto] User
ddiep1: Authentication Failed: Incorrect Username or Password; (pluto)
14:45:00 - Info - User: user from=ezvpn;result=fail (pluto)
14:45:00 - Info - IPsec Remote Access: msg=[IPsec Remote Access][pluto] User
ddiep1: Attempting to login; (pluto)

-VPN connection failed b/c IPSec Remote Access server has an existing "Client"
group (andrpham1) that was having same IP subnet (192.168.100.x) as current
Teleworker remote IP subnet. This only happen when Teleworker connection is
using "NEM" mode.
Solution: From IPSec Remote Access server, delete "andrpham1" group or change
it to use different subnet other than 192.168.100.x.

17:00:35 - Warning - IPsec Remote Access: msg=Virtual IP 192.168.100.0/24
overlaps with connection EZVPN_andrpham1"" (kind=CK_TEMPLATE) '@andrpham1';
(pluto)
```

For More Information

Product Resources	Location
Product Documentation	www.cisco.com/go/isa500resources
Cisco Small Business Support Community	www.cisco.com/go/smallbizsupport
Cisco Small Business Support and Resources	www.cisco.com/go/smallbizhelp
Phone Support Contacts	www.cisco.com/go/sbsc
Firmware Downloads	www.cisco.com/go/isa500software
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb