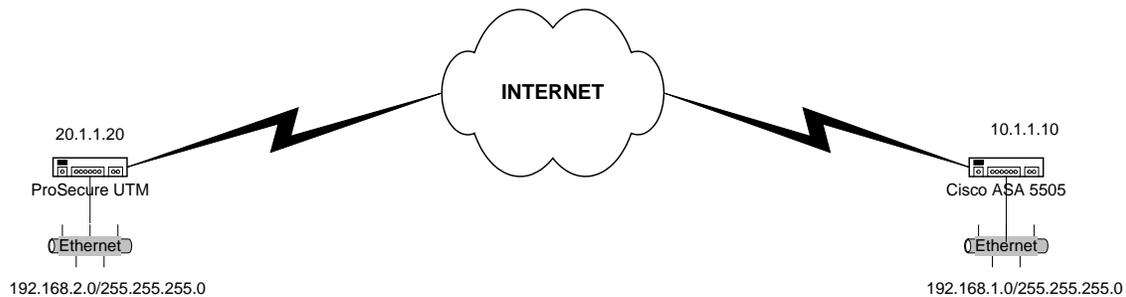


Netgear ProSecure UTM to Cisco ASA 5505 VPN Guide

This document is a step-by-step instruction for setting up a VPN between Netgear ProSecure UTM and Cisco ASA 5505 firewall. These instructions are provided “as is”. Netgear doesn’t provide support for configuring VPN between Netgear routers and Non-Netgear VPN devices.

The instruction is verified with Netgear ProSecure UTM25 and Cisco ASA 5505.

Scenario:



Both the Netgear ProSecure UTM and the Cisco ASA 5505 firewall are connected to Internet with a public IP address assigned to the WAN interface. The VPN is configured with the following parameters:

	Netgear ProSecure UTM	Cisco ASA 5505 Firewall
Local IKE identity	20.1.1.20	10.1.1.10
Remote IKE identity	10.1.1.10	20.1.1.20
Local VPN subnet	192.168.2.0	192.168.1.0
Local VPN subnet netmask	255.255.255.0	255.255.255.0
Encryption algorithm	3DES	3DES
Authentication algorithm	SHA-1	SHA
Pre-shared key	123456789	123456789
IKE mode	Main mode	Main mode

The above parameters are specific to our network settings. User will need to change the parameters to match their network setting such as IP addresses of the VPN gateways and the local area network IP addresses. You can also choose a different encryption algorithm or authentication algorithm. A different pre-shared key is also recommended. You need to make sure the same encryption/authentication algorithm and pre-shared key are specified in both the Netgear routers and ASA 5505 firewall’s VPN policy.

I. Configure the Netgear ProSecure UTM:

1. Log in to the Netgear ProSecure UTM.
2. Click on **VPN Wizard** under the VPN menu.
 - Enter a descriptive name for the VPN policy in the **Connection Name and Remote IP Type** textbox. It is only being used to help user manage the IKE polices. For our example, 'toCisco'.
 - Enter a pre-shared key. We used 123456789.
 - Enter the remote IP address of the ASA 5505 firewall under **End Point Information**.
 - Enter the remote LAN subnet and mask under **Secure Connection Remote Accessibility**. We used 192.168.1.1 255.255.255.0 – the ASA 5505's LAN subnet.
 - Click Apply.

The screenshot shows the Netgear ProSecure UTM VPN Wizard configuration page. The page is titled "VPN Wizard" and has a navigation bar with tabs for "IKE Policies", "VPN Policies", "VPN Wizard", "Mode Config", and "RADIUS Client". A "VPN Wizard Default Values" link is also present. The main content area is divided into four sections, each with a question mark icon in the top right corner:

- About VPN Wizard:** Contains a paragraph explaining the wizard's purpose and a section titled "This VPN tunnel will connect to the following peers:" with radio buttons for "Gateway" (selected) and "VPN Client".
- Connection Name and Remote IP Type:** Contains two text input fields: "What is the new Connection Name?" (value: toCisco) and "What is the pre-shared key?" (value: 123456789, with a note "(Key Length 8 - 49 Char)"). Below these is a section titled "This VPN tunnel will use following local WAN Interface:" with radio buttons for "WAN 1" (selected) and "WAN 2".
- End Point Information:** Contains two text input fields: "What is the Remote WAN's IP Address or Internet Name?" (value: 10.1.1.10) and "What is the Local WAN's IP Address or Internet Name?" (value: 20.1.1.20).
- Secure Connection Remote Accessibility:** Contains two text input fields: "What is the remote LAN IP Address?" (value: 192.168.1.1) and "What is the remote LAN Subnet Mask?" (value: 255.255.255.0).

You should see the following IKE policy:

Edit IKE Policy ➔ Add New VPN Policy

Operation succeeded.

<p>Mode Config Record</p> <p>Do you want to use Mode Config Record?</p> <p><input type="radio"/> Yes <input checked="" type="radio"/> No</p> <p>Select Mode Config Record: <input type="text"/></p> <p>view selected</p>	<p>General</p> <p>Policy Name: <input type="text" value="toCisco"/></p> <p>Direction / Type: <input type="text" value="Both"/></p> <p>Exchange Mode: <input type="text" value="Main"/></p>
<p>Local</p> <p>Select Local Gateway: <input checked="" type="radio"/> WAN1 <input type="radio"/> WAN2</p> <p>Identifier Type: <input type="text" value="Local Wan IP"/></p> <p>Identifier: <input type="text" value="20.1.1.20"/></p>	<p>Remote</p> <p>Identifier Type : <input type="text" value="Remote Wan IP"/></p> <p>Identifier: <input type="text" value="10.1.1.10"/></p>

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Authentication Method: Pre-shared key RSA-Signature

Pre-shared key: (Key Length 8 - 49 Char)

Diffie-Hellman (DH) Group:

SA-Lifetime (sec):

Enable Dead Peer Detection: Yes No

Detection Period: (Seconds)

Reconnect after failure count:

Extended Authentication

XAUTH Configuration

None
 Edge Device
 IPsec Host

Authentication Type:

Username:

Password:

You should see the following VPN policy (NOTE – you need to adjust the SA Lifetime to 28800):

Edit VPN Policy

Operation succeeded.

General

Policy Name:

Policy Type:

Select Local Gateway: WAN1 WAN2

Remote Endpoint: IP Address:
 FQDN:

Enable NetBIOS?
 Enable RollOver?

Enable Keepalive: Yes No

Ping IP Address:

Detection period: (Seconds)

Reconnect after failure count:

Traffic Selection

This field is not editable, because netbios is selected.

Local IP: Remote IP:

Start IP Address: Start IP Address:

End IP Address: End IP Address:

Subnet Mask: Subnet Mask:

Manual Policy Parameters

SPI-Incoming: (Hex, 3-8 Chars) SPI-Outgoing: (Hex, 3-8 Chars)

Encryption Algorithm: Integrity Algorithm:

Key-In: Key-In:

Key-Out: Key-Out:

(DES-8 Char & 3DES-24 Char) (MD5-16 Char & SHA-1-20 Char)

Auto Policy Parameters

SA Lifetime:

Encryption Algorithm: Integrity Algorithm:

PFS Key Group:

Select IKE Policy:

These instructions are tested with the ASA 5505 firewall starting in its factory default setting. We have only configured the firewall's WAN interface IP address and the default gateway before setting up the VPN policy. Your ASA 5505 firewall may have existing configurations that need to be modified in order for the VPN to work. For example, firewall rules and NAT (network address translation) rules may interfere with your VPN. Please refer to your Cisco documentation for configuring those settings.

From the Cisco ASA 5505 webGUI:

1. Log in to the Cisco ASA 5505.
2. Click on **VPN Wizard** under the VPN configuration menu.
3. Click on Launch VPN Wizard and then select Site to Site and Next.

The screenshot displays the Cisco ASDM 5.2 for ASA web GUI. The title bar indicates the device is '192.168.1.1'. The interface includes a menu bar (File, Options, Tools, Wizards, Help), a search bar, and a toolbar with icons for Home, Configuration, Monitoring, Back, Forward, Packet Tracer, Refresh, Save, and Help. The left sidebar shows a tree view of configuration options, with 'VPN Wizard' selected under the 'VPN' category. The main content area is titled 'VPN Wizard' and contains the following text:

Use this wizard to configure site-to-site VPN tunnels and remote access VPN tunnels.

Site-to-Site VPN
Use this option to create a VPN tunnel from this ASA to another VPN device. To complete this configuration, you need to know the IP address of the peer device and the pre-shared key or the trustpoint name configured on it.

Remote Access VPN.
Use this option to configure a Remote Access VPN tunnel to this ASA. To complete this configuration, you must know the pre-shared key or the trustpoint name necessary for this tunnel.

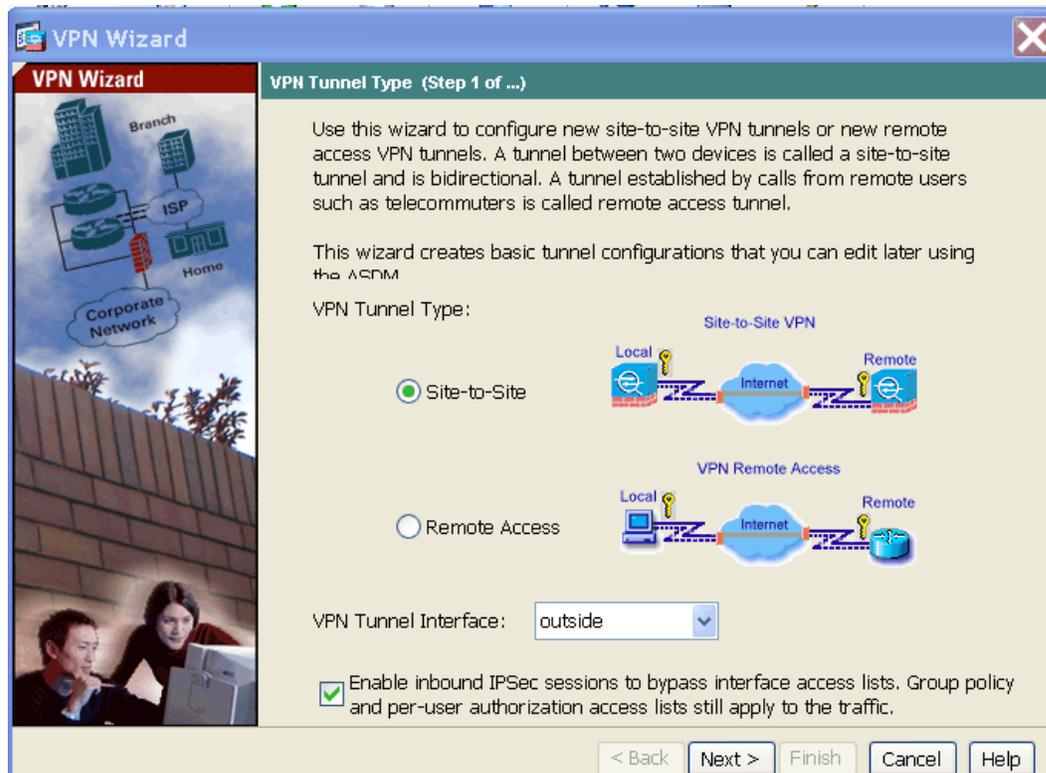
Site-to-Site VPN Diagram: A diagram showing two VPN devices (Local and Remote) connected via an Internet cloud. The Local device is on the left and the Remote device is on the right.

VPN Remote Access Diagram: A diagram showing a Local device connected via an Internet cloud to a Remote device. The Local device is on the left and the Remote device is on the right.

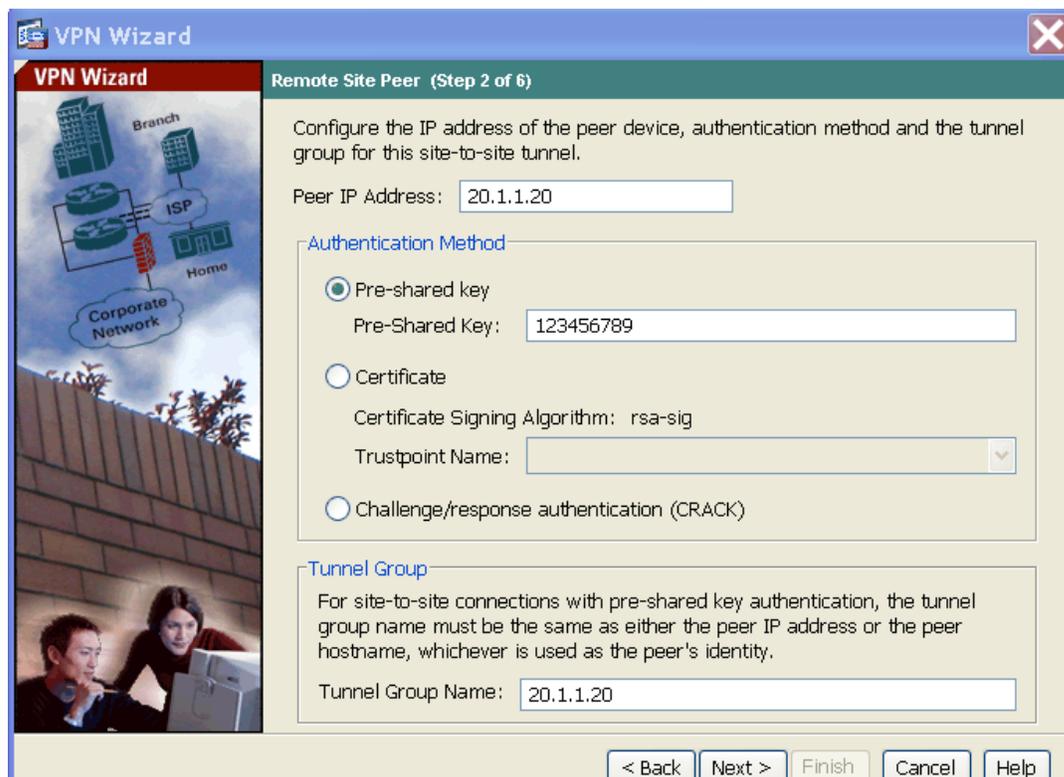
An information icon (i) is present, with the following text: "Only new VPN configurations can be created using this wizard. To edit an existing configuration, switch to the Feature mode and select VPN."

A "Launch VPN Wizard" button is located at the bottom of the main content area.

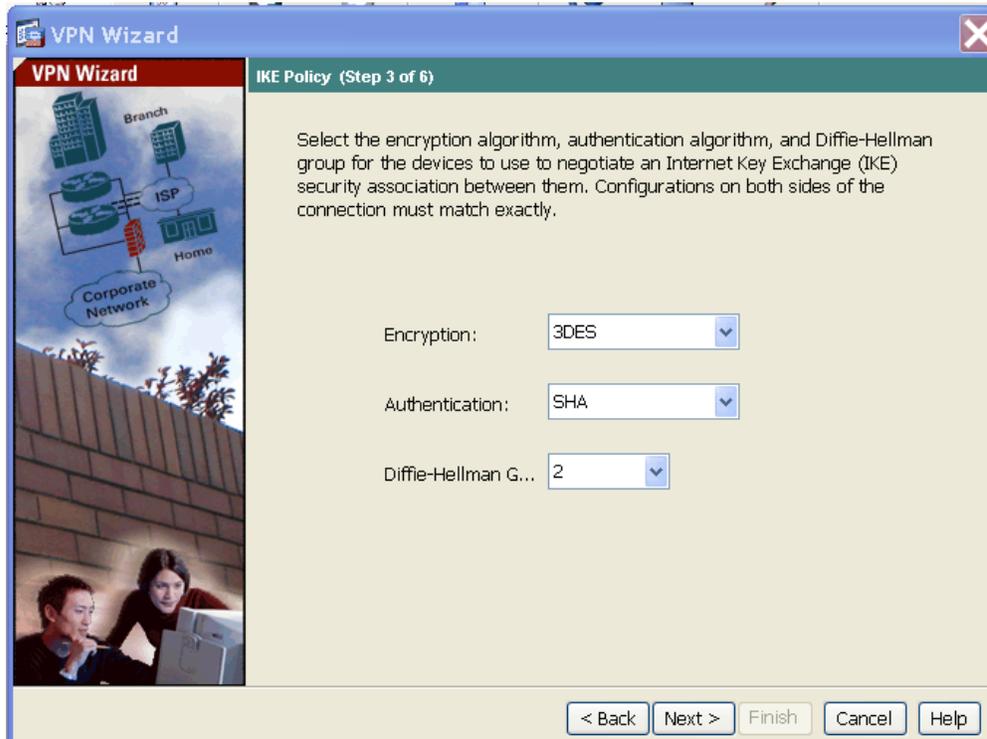
The status bar at the bottom shows "Configuration changes saved successfully.", the user is "<admin>", the page number is "15", and the date/time is "8/13/09 11:37:57 AM UTC".



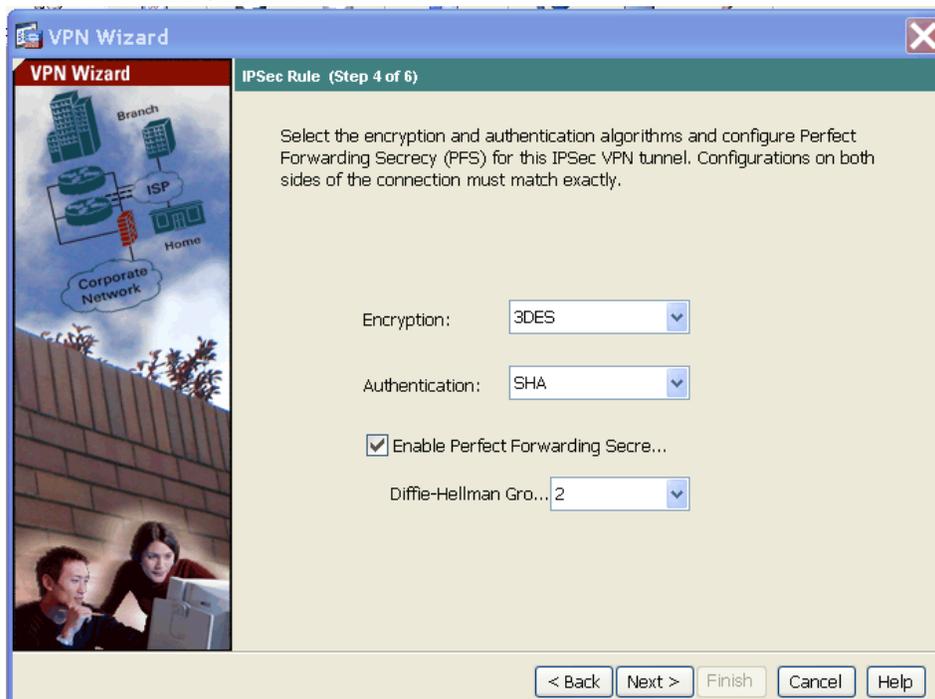
4. Enter the remote WAN IP address of the NETGEAR ProSecure UTM and the same pre-shared key you entered in the Netgear ProSecure UTM.



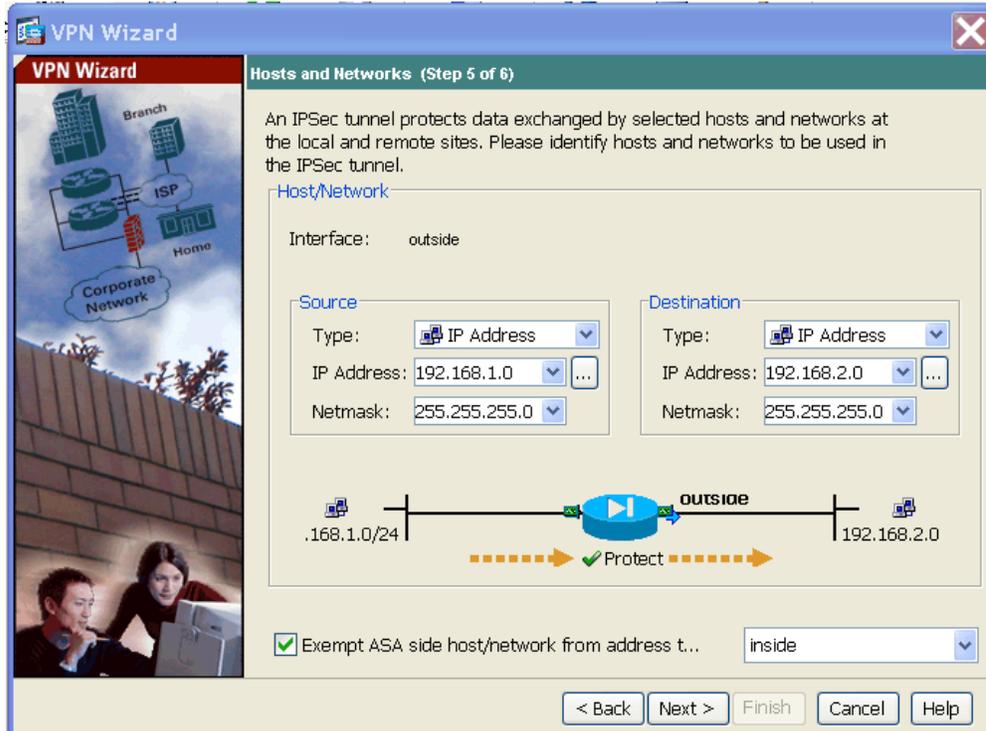
- Specify 3DES for the Encryption, SHA for Authentication and DH Group 2 for the IKE Policy.



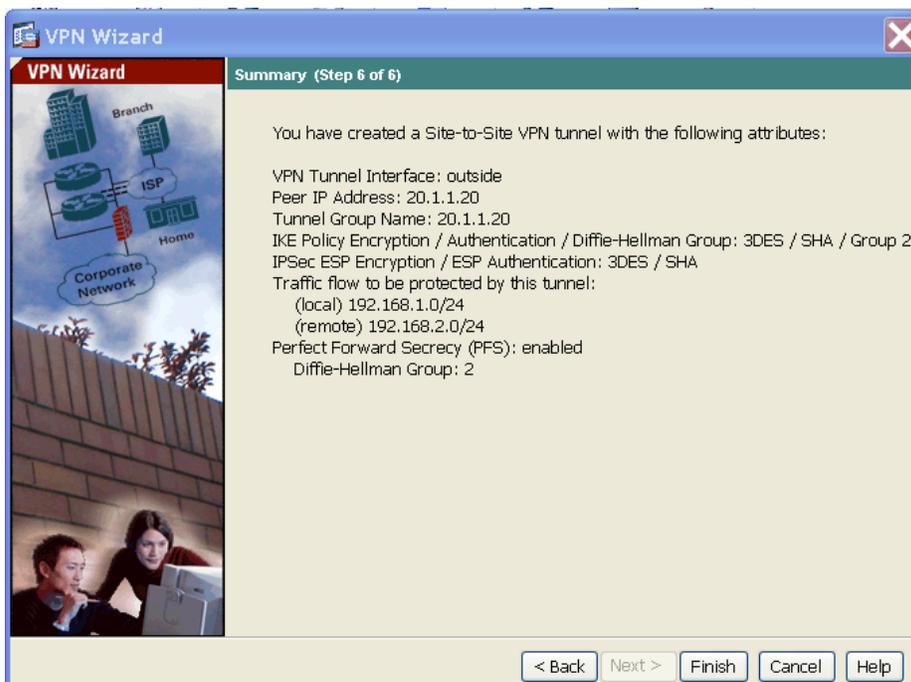
- Specify 3DES for the Encryption, SHA for Authentication and DH Group 2 for the IPsec Policy. Perfect Forwarding Secrecy needs to be checked since we enabled this on the NETGEAR side.



7. Specify the local and remote LAN traffic that will traverse the VPN tunnel.



8. Review your settings and click Finish.



Try to ping one of the devices on either side and the VPN tunnel should be established.