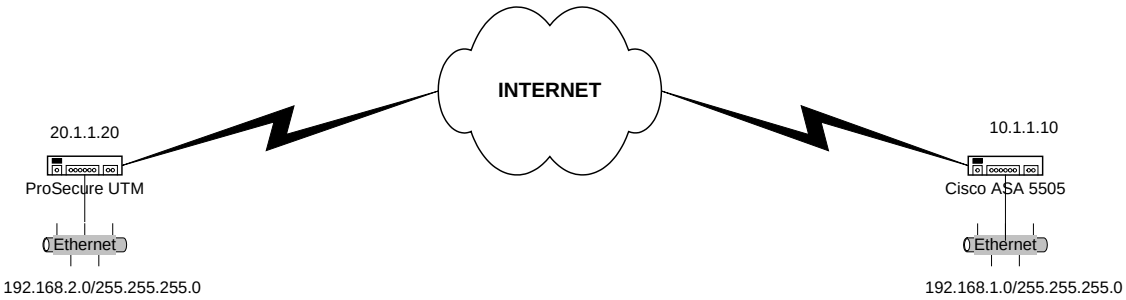
Netgear ProSecure UTM to Cisco ASA 5505 VPN Guide

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:

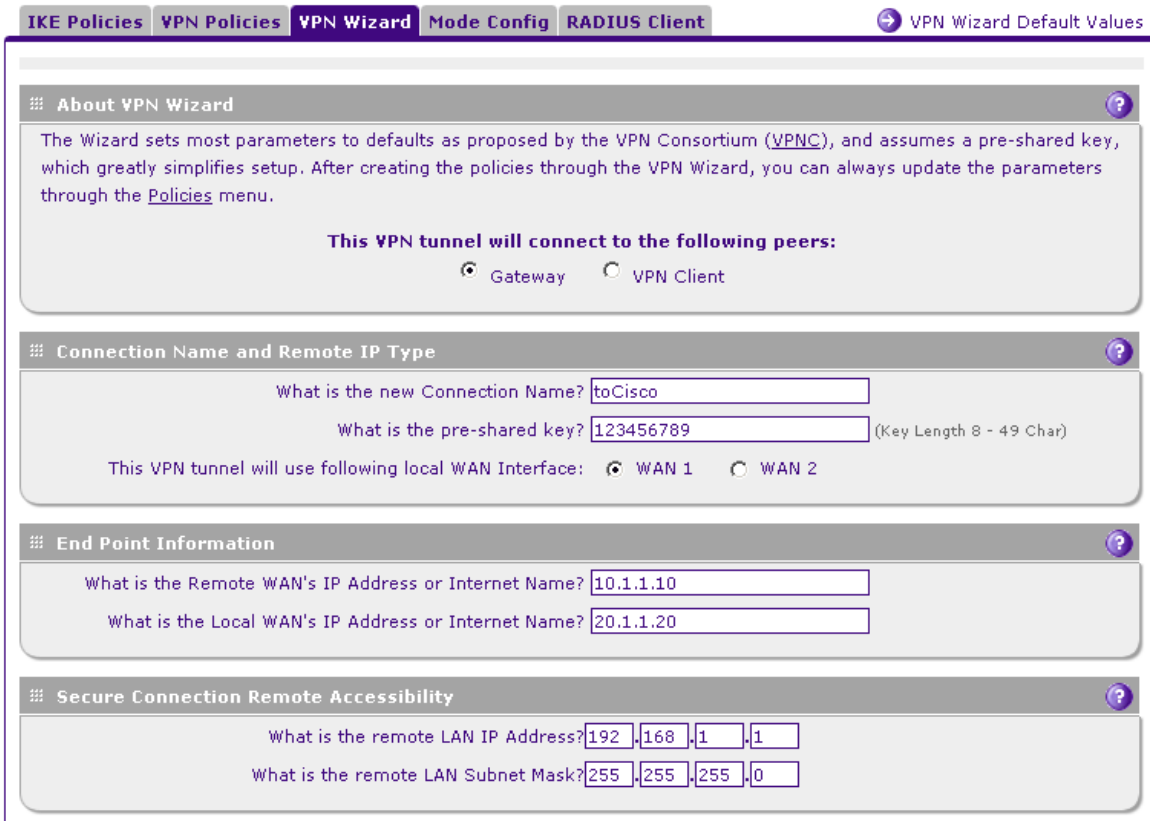
	Netgear ProSecure UTM	Cisco ASA 5505 Firewall
Local IKE identity	20.1.1.20	10.1.1.10
Remote IKE identity	10.1.1.10	20.1.1.20
Local VPN subnet	192.168.2.0	192.168.1.0
Local VPN subnet netmask	255.255.255.0	255.255.255.0
Encryption algorithm	3DES	3DES
Authentication algorithm	SHA-1	SHA
Pre-shared key	123456789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

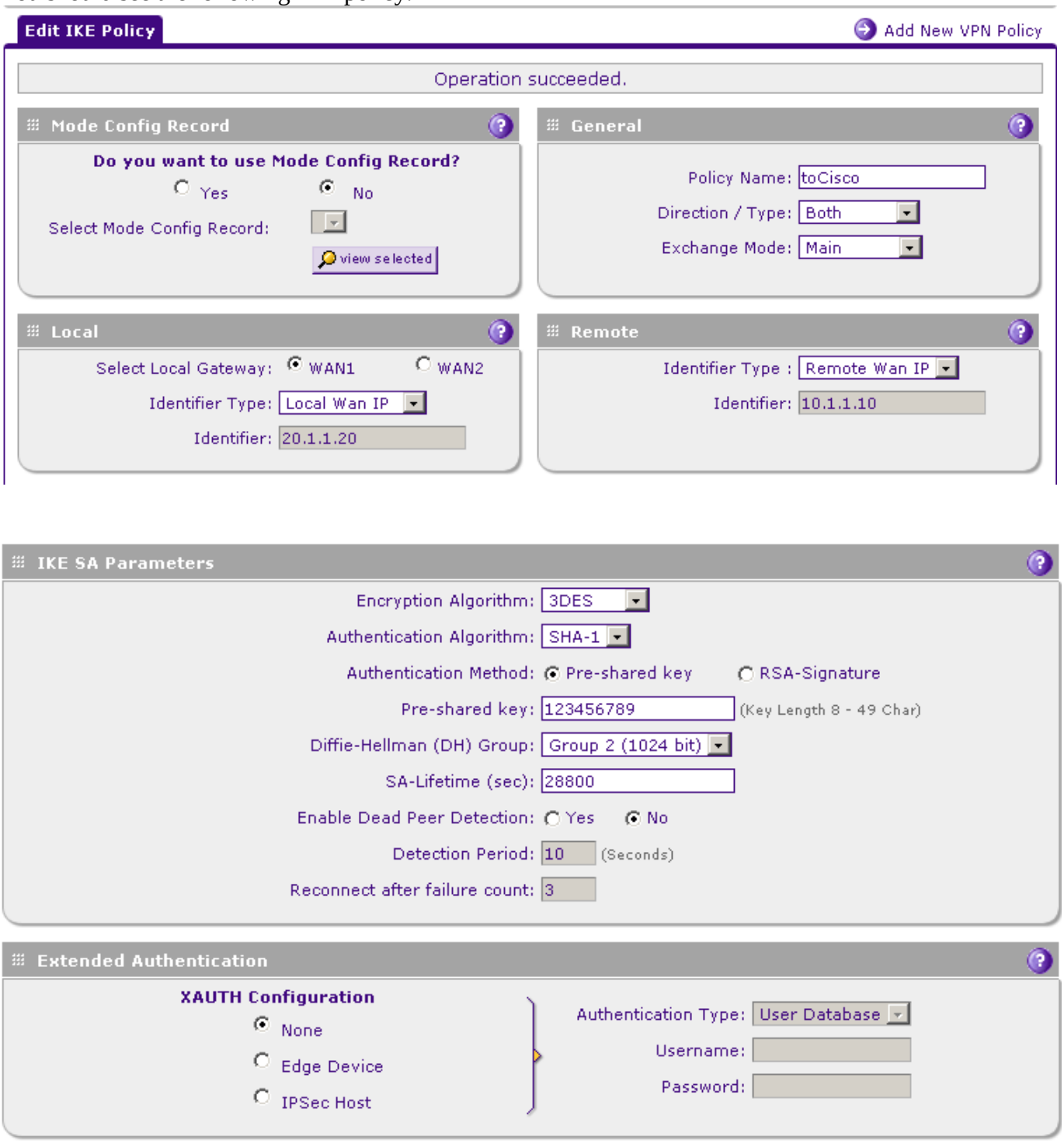
I. Configure the Netgear ProSecure UTM:

1. Log in to the Netgear ProSecure UTM.
2. Click on **VPN Wizard** under the VPN menu.

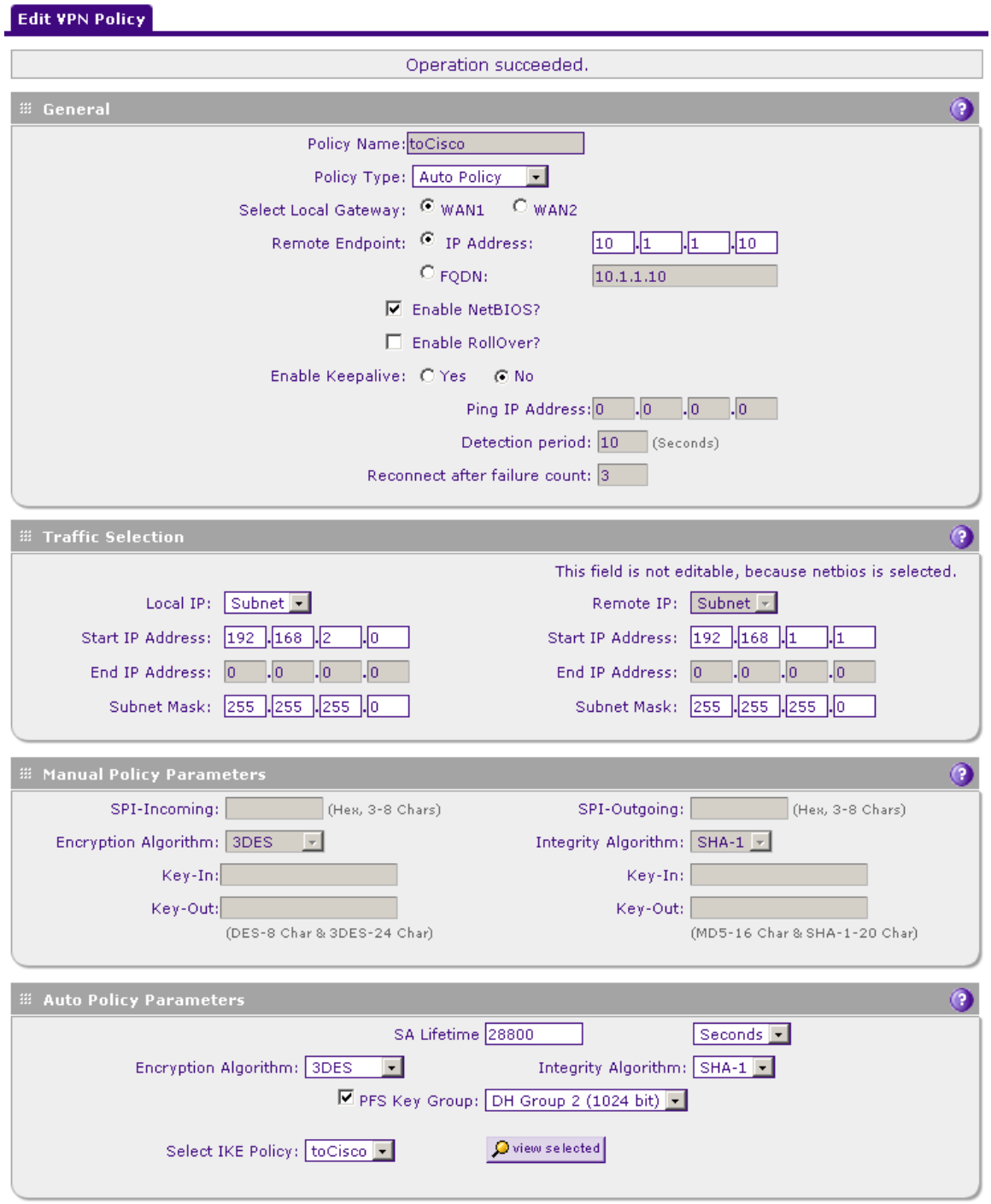
    - Enter a descriptive name for the VPN policy in the **Connection Name and Remote IP Type** textbox. It is only being used to help user manage the IKE polices. For our example, 'toCisco'.
    - Enter a pre-shared key. We used 123456789.
    - Enter the remote IP address of the ASA 5505 firewall under **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.



You should see the following IKE policy:



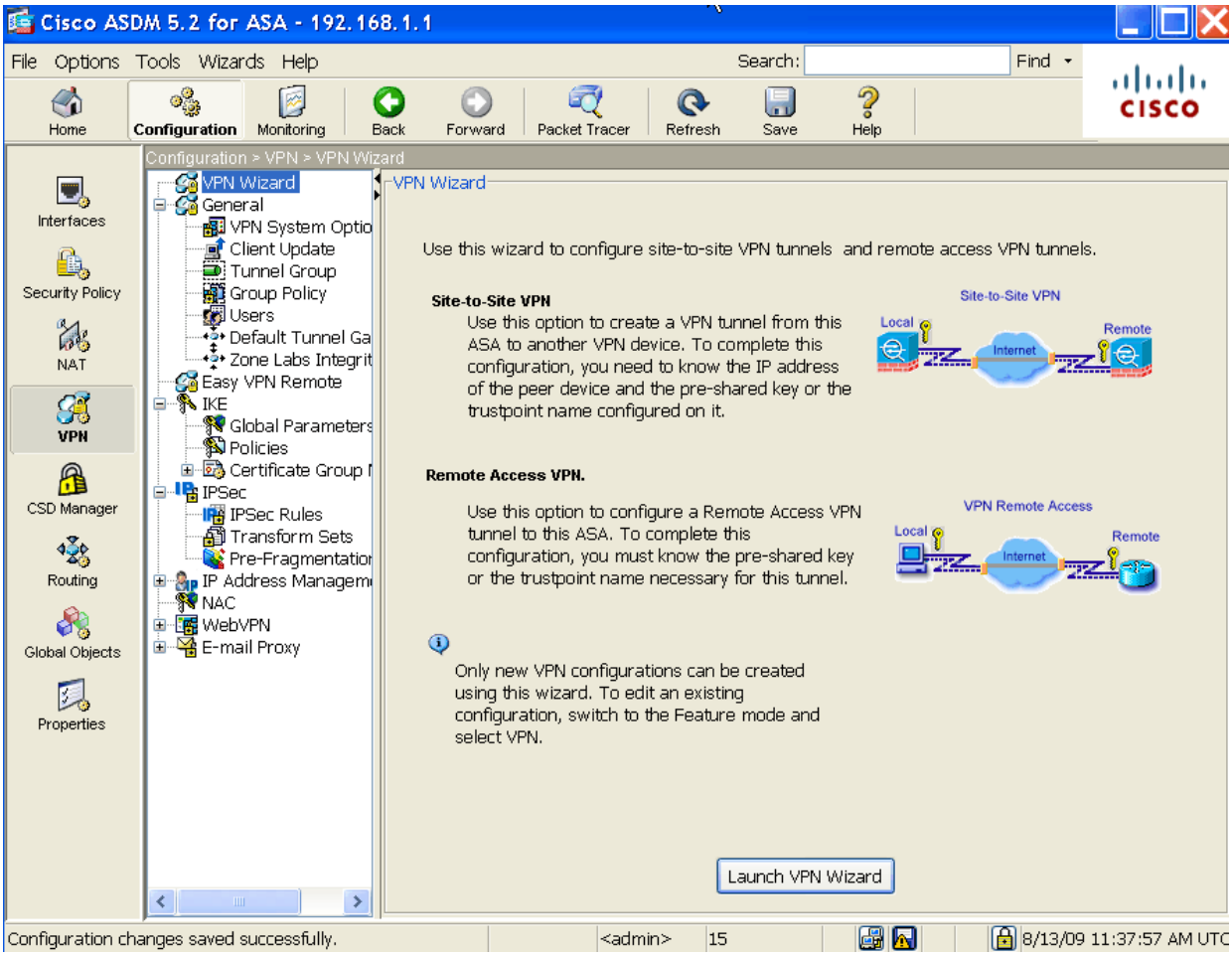
You should see the following VPN policy (NOTE – you need to adjust the SA Lifetime to 28800):

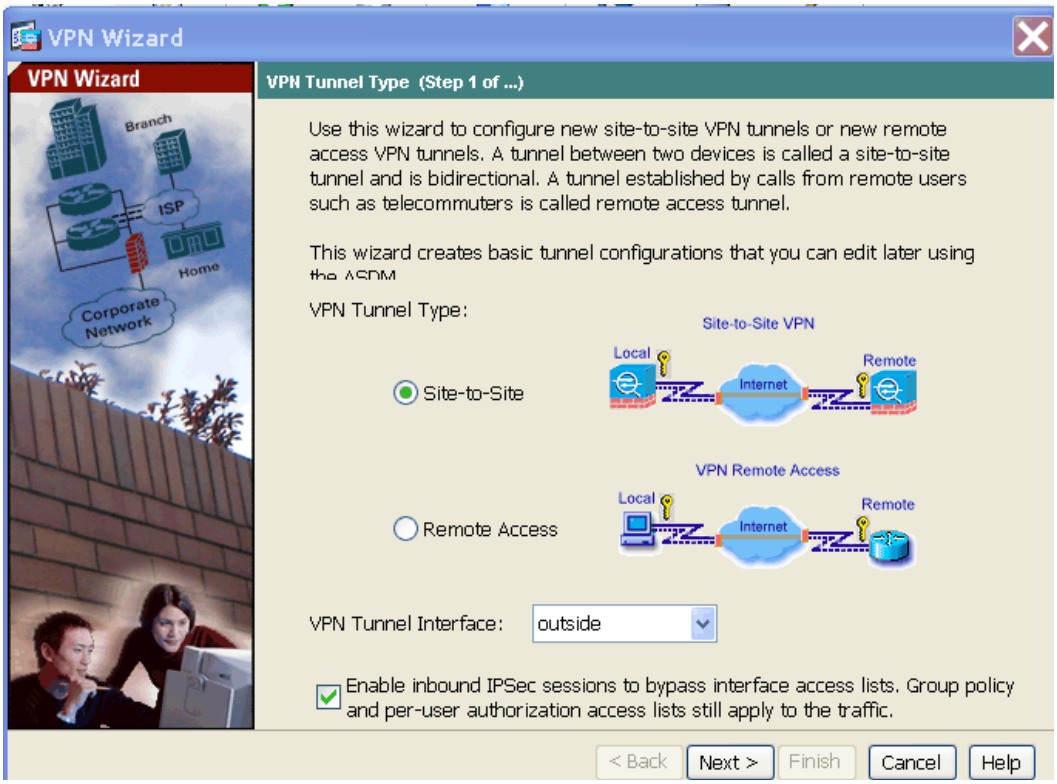


These instructions are tested with the ASA 5505 firewall starting in its factory default setting. We have only configured the firewall's WAN interface IP address and the default gateway before setting up the VPN policy. Your ASA 5505 firewall may have existing configurations that need to be modified 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.

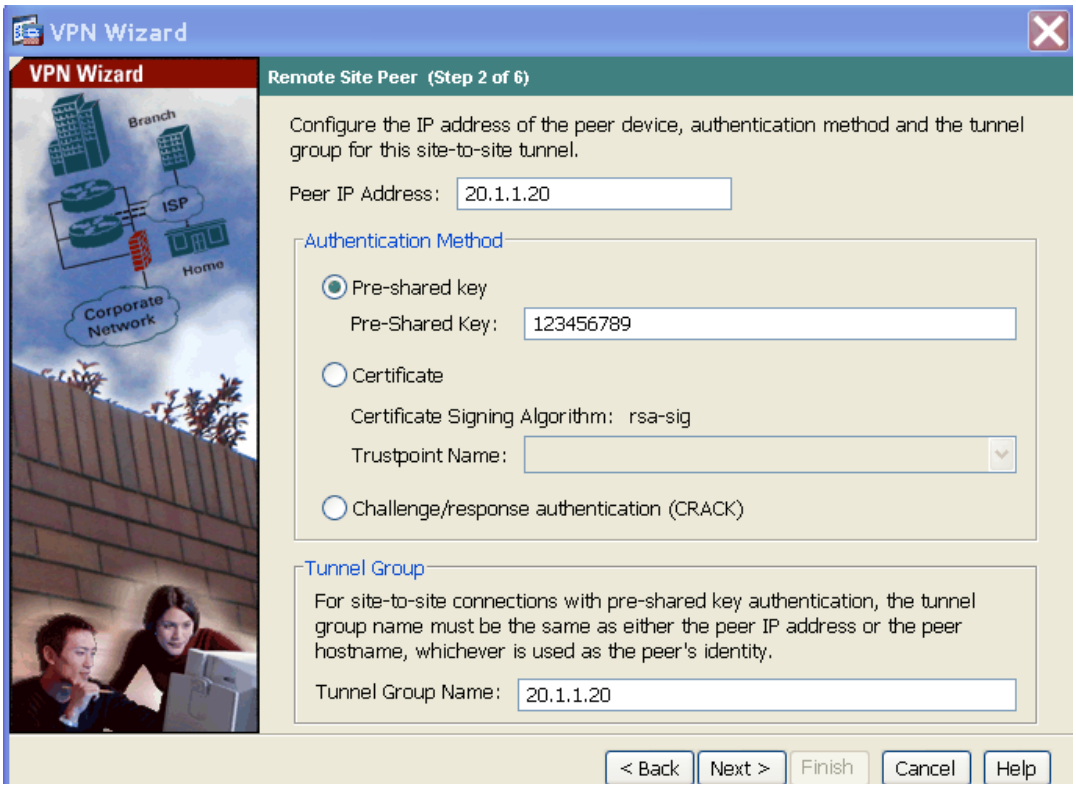
From the Cisco ASA 5505 webGUI:

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.

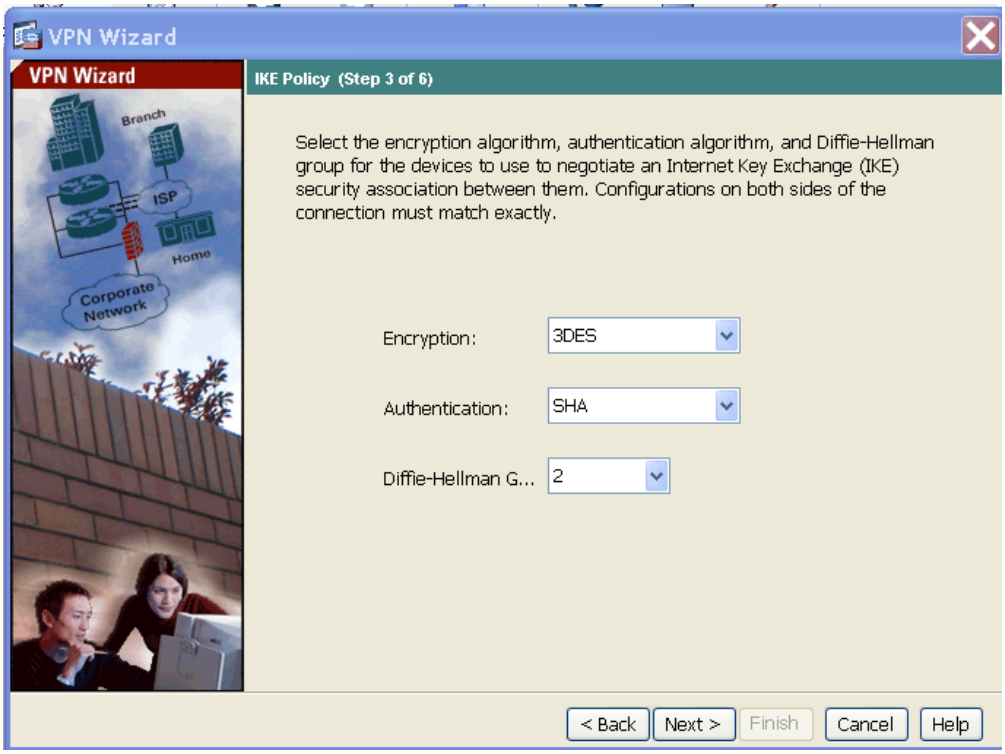




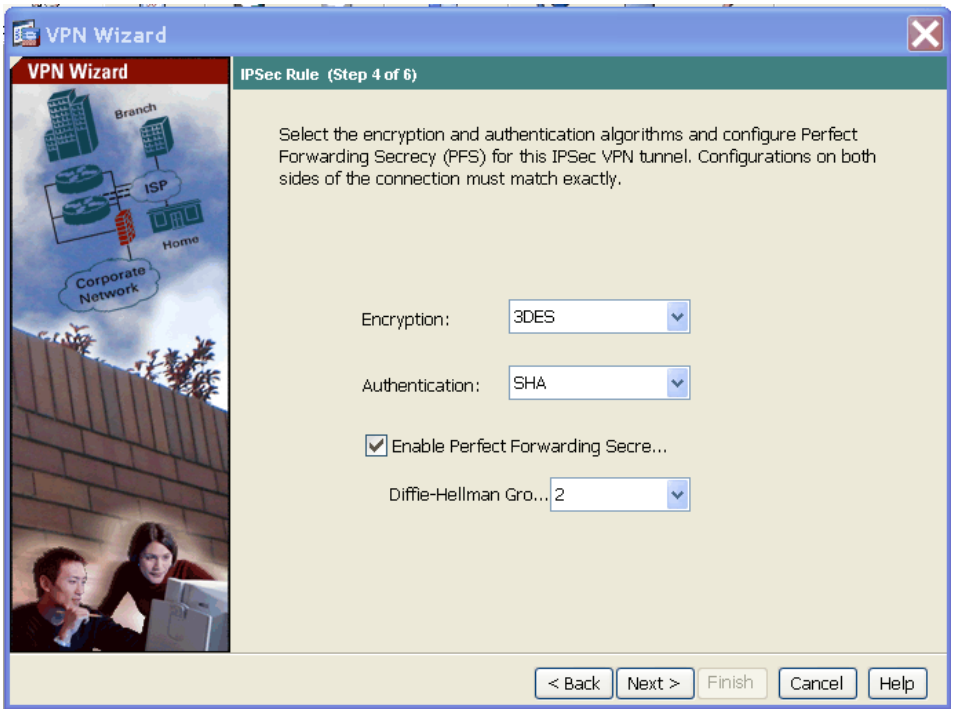
4. Enter the remote WAN IP address of the NETGEAR ProSecure UTM and the same pre-shared key you entered in the Netgear ProSecure UTM.



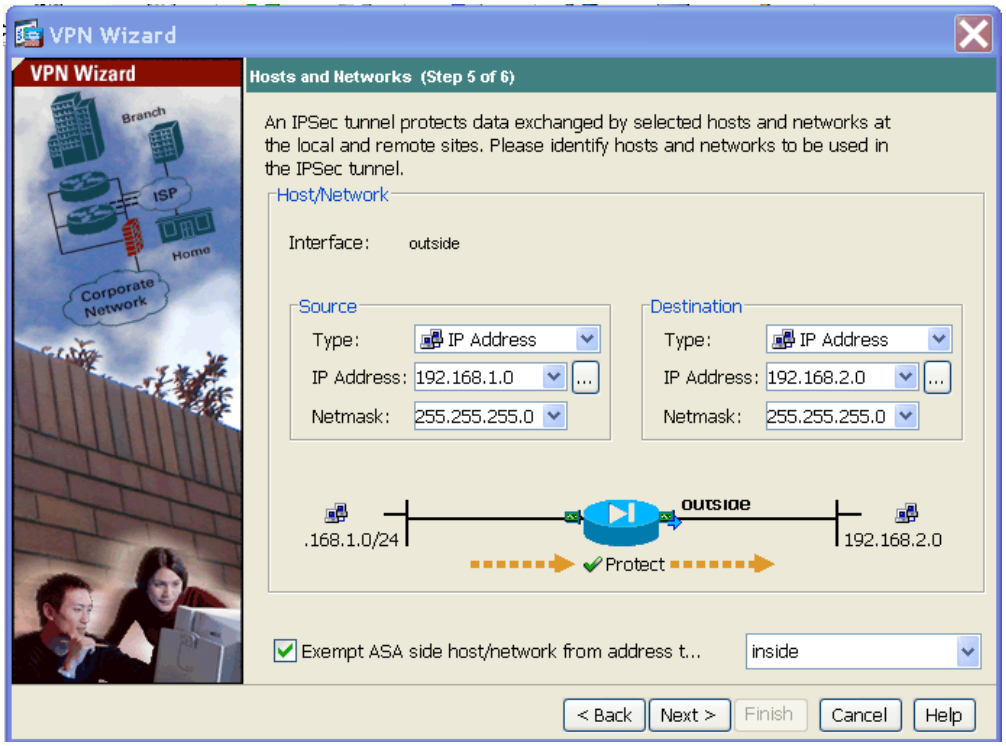
5. Specify 3DES for the Encryption, SHA for Authentication and DH Group 2 for the IKE Policy.



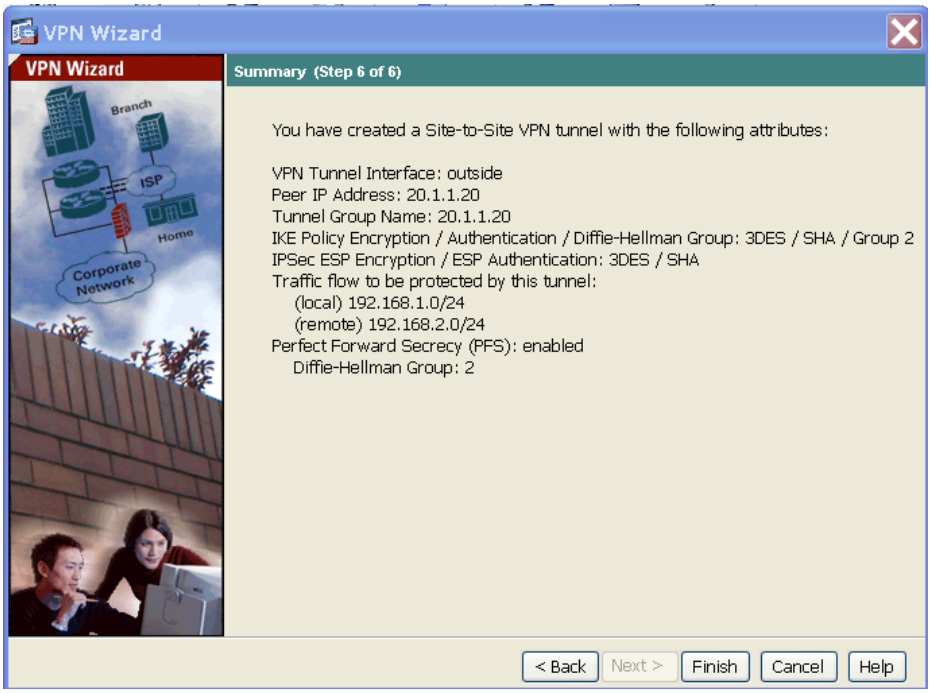
6. Specify 3DES for the Encryption, SHA for Authentication and DH Group 2 for the IPSec Policy. Perfect Forwarding Secrecy needs to be checked since we enabled this on the NETGEAR side.



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.