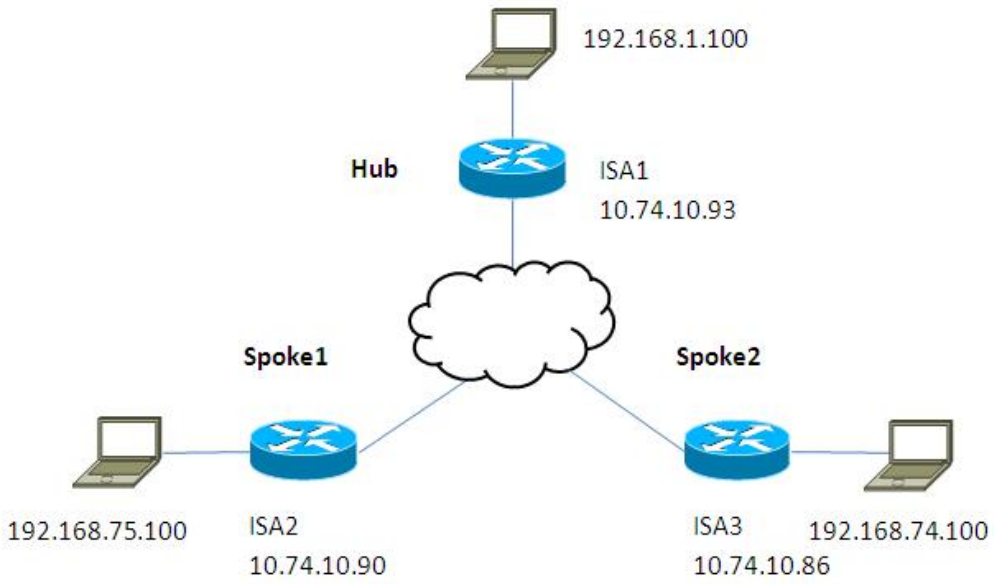
Configuring a Hub-and-Spoke Site-to-Site VPN with Cisco ISA500 Series Security Appliances

This application note explains how to set up a hub-and-spoke site-to-site VPN using Cisco ISA500 Series Security Appliances. In a VPN hub-and-spoke topology, multiple VPN routers (spokes) communicate securely with a central VPN router (hub). A separate, secured tunnel extends between each individual spoke and the hub.

This topology is a simple way to allow employees at remote sites to access your main network. It works well if most traffic is from the remote sites to the main network and there is little traffic between sites. Because inter-site traffic must pass through the hub first and then out to a spoke, too much inter-site traffic may create bottlenecks at the hub. An advantage of this topology is that it is much less complex than a full mesh topology.

In the following example, two spoke sites use VPN tunnels to access resources in the hub network.

Figure 1. Hub-and-Spoke Topology



Tip: You may find it helpful to create a worksheet listing the LAN IP address, “0” network address, and netmask for each site. When configuring the Cisco ISA500 at a spoke site, you will need the network addresses of the main site and all other spoke sites. When configuring the Cisco ISA500 at the hub site, you will need the network addresses of all of the spoke sites.

	Hub	Spoke1	Spoke2
LAN IP Address	192.168.1.100	192.168.75.100	192.168.74.100
“0” Network Address	192.168.1.0	192.168.75.0	192.168.74.0
Netmask	255.255.255.0	255.255.255.0	255.255.255.0

Configuring the Cisco ISA500 at a Spoke Site

Use this procedure to configure the VPN settings for each spoke site.

To support the multiple subnets in this topology, you will configure the following features:

- Multiple *Address Objects* to identify the hub and each spoke site. For the example in Figure 1, you would add two Address Objects: one for the hub site and one for the remote Spoke site.
- One *Address Group* to represent the complete hub-and-spoke Remote Network for the IPsec VPN policy.

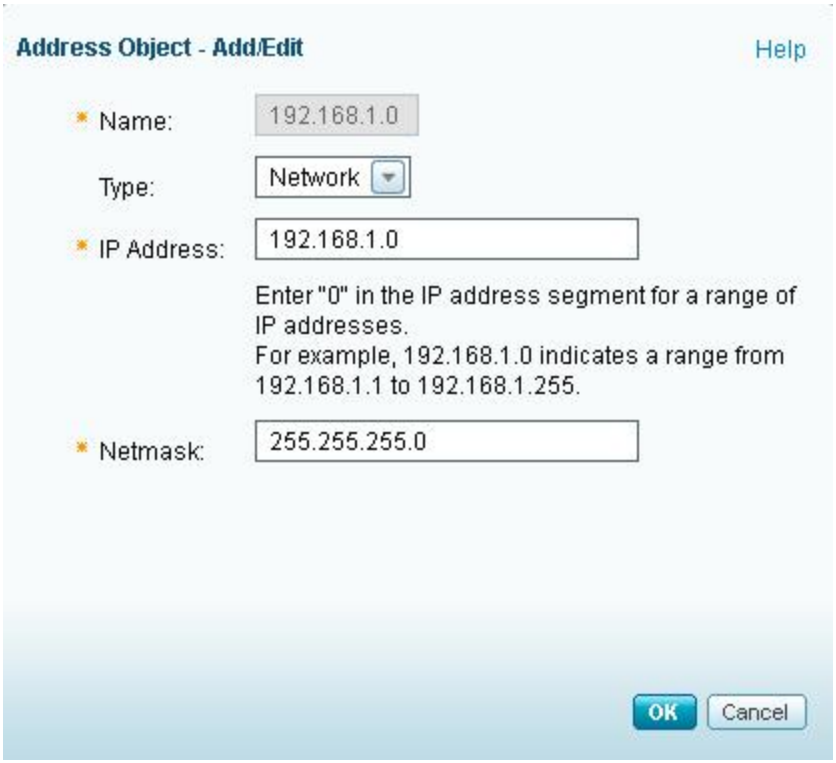
Step 1. Use a web browser to launch the configuration utility for the security appliance at the spoke site that you need to configure.

- If your computer is connected to the LAN, enter the LAN IP address of the security appliance.
- If you are accessing the device remotely, enter the protocol, the WAN IP address, and the port number, such as https://10.74.10.90:8080.

Step 2. In the navigation tree, click **Networking > Address Management**.

Step 3. In the **Address Objects** area, create an Address Object for the hub site and for each of the other spoke sites.

a. Click **Add Address**, and then enter the IP address and subnet mask for the LAN at the other site. Use the “0” notation to include the full range of IP addresses in the subnet.



b. Click **OK** to save your changes.

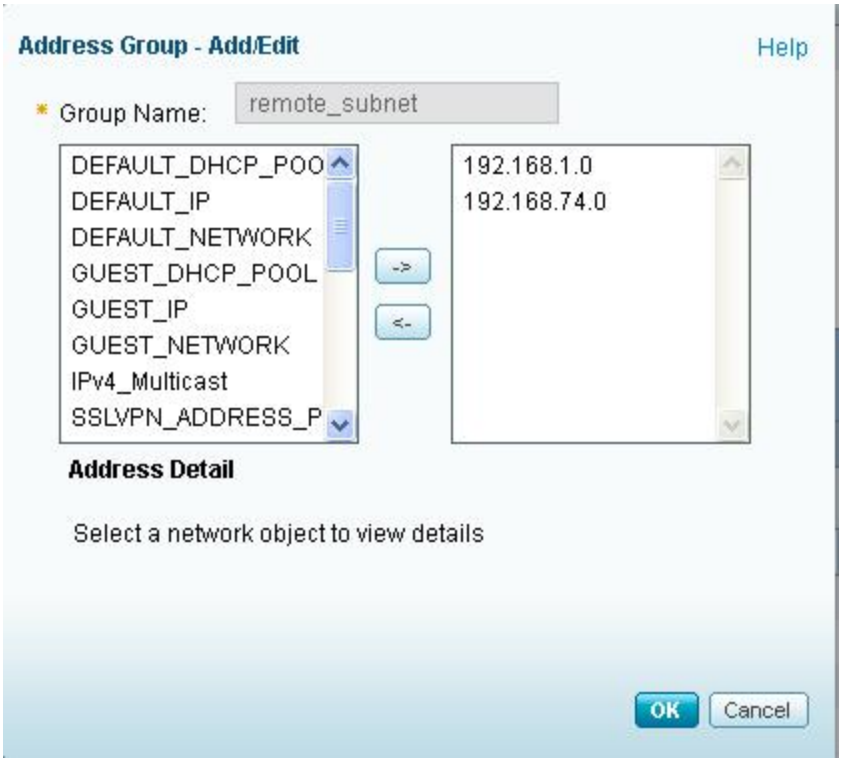
c. Repeat **Steps a-b** until you have identified the hub and all other spoke sites.

For example, to configure Spoke1 in Figure 1, you would create one Address Object for 192.168.1.0 (network address of the hub site) and one Address Object for 192.168.74.0 (network address of Spoke2).

Step 4. In the **Address Groups** area, create an address group that includes all of the new Address Objects that you created for this topology.

a. Click **Add Group**.

b. Enter a **Group Name**, such as *remote_subnet.*



c. In the list on the left side of the window, select each address that you created previously, and then click the right-arrow button to move it to the list on the right side of the window. Repeat until you have included all of the Address Objects for this topology.

d. Click **OK** to save the group.

Step 5. In the navigation tree, choose **VPN > Site-to-Site > IPsec Policies**.

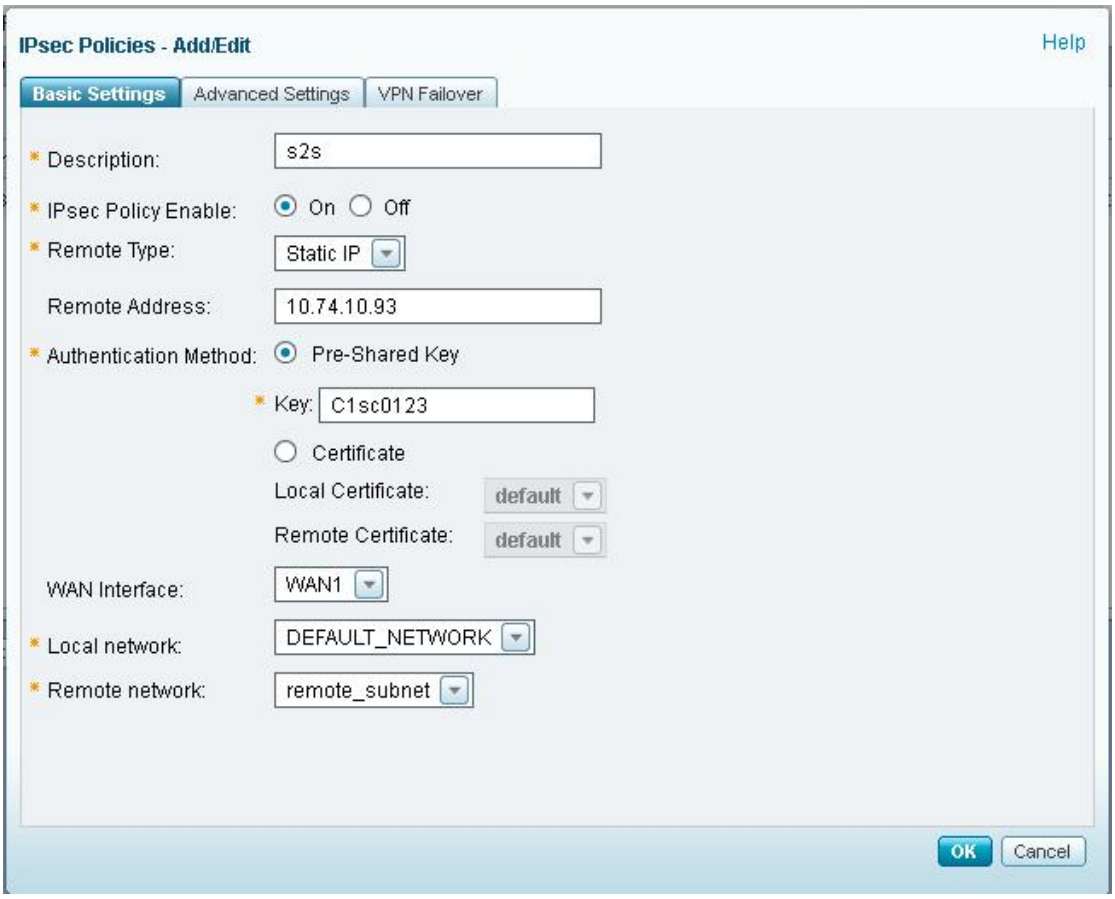
Step 6. If you have not previously enabled VPN on this security appliance, click **On**.

Step 7. Click **Add** to add a new VPN policy. This policy will be used to create a VPN tunnel from this spoke site to the hub.

a. In the pop-up window, enter the settings. For more information, you can click the **Help** link near the top right corner of the pop-up window.

For this scenario, only the Basic Settings tab is modified. The **Remote Address** is the WAN IP address of the hub site. The **Local Network** is the hub's DEFAULT_NETWORK. The Remote Network is the Address Group that was configured previously. The same Pre-Shared Key will be configured when setting up the IPsec policies for all security appliances in this scenario.

b. Click **OK**.



Step 8. On the IPsec Policies page, click **Save** to save the policy.

Step 9. Repeat **Steps 1-8** to configure the security appliance at each additional spoke site.

For example, to configure Spoke2 in Figure 1, you would create one Address Object for 192.168.1.0 (network address of the hub site) and one Address Object for 192.168.75.0 (network address of Spoke1). The IPsec policy would be identical. (You could enter different options for Description, Address Group name, WAN Interface, and Local Network.)

Configuring the Cisco ISA500 at the Hub Site

When configuring the hub site, you will create a separate VPN policy for each spoke site.

To support the multiple subnets in this topology, you will configure the following features:

- Multiple *Address Objects* to identify each spoke site. For the example in Figure 1, you would add two Address Objects: one for Spoke1 and one for Spoke2.
- Multiple *Address Groups* to represent each hub-to-spoke Local Network for each IPsec VPN policy.

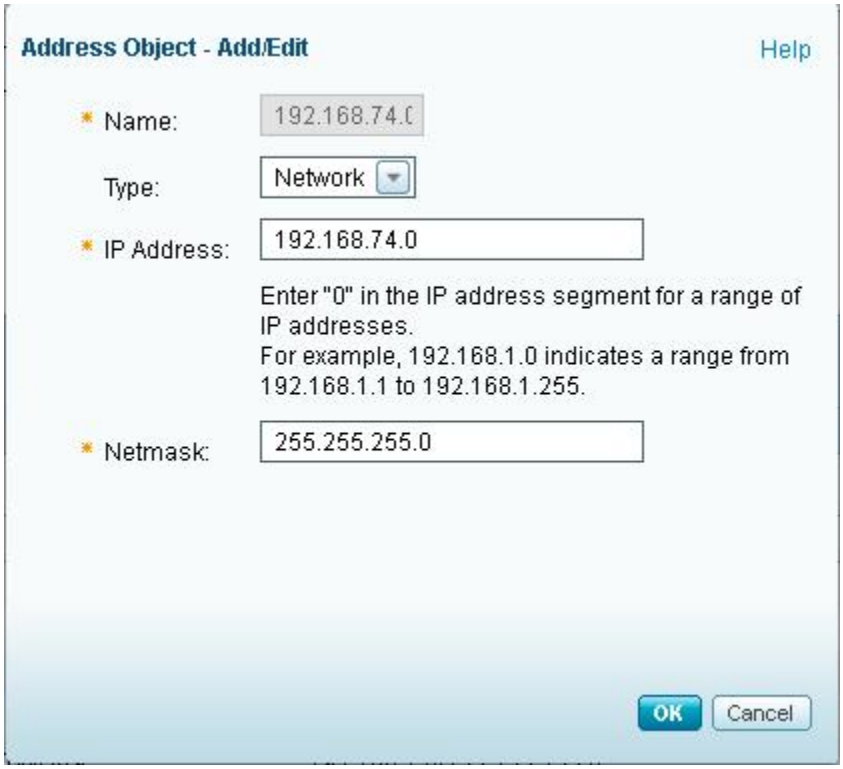
Step 1. Use a web browser to launch the configuration utility for the security appliance at the hub site.

- If your computer is connected to the LAN, enter the LAN IP address of the security appliance.
- If you are accessing the device remotely, enter the protocol, the WAN IP address, and the port number, such as https://10.74.10.90:8080.

Step 2. In the navigation tree, click **Networking > Address Management**.

Step 3. In the **Address Objects** area, create an Address Object for each spoke site.

a. Click **Add Address**, and then enter the IP address and subnet mask to identify the spoke site.



b. Click **OK** to save your changes.

c. Repeat **Steps a-b** until you have identified all of the spoke sites.

For example, to configure the hub site in Figure 1, you would create one Address Object for 192.168.75.0 (network address of Spoke1) and one Address Object for 192.168.74.0 (network address of Spoke2).

Step 4. In the **Address Groups** area, create a unique address group for each spoke site.

a. Click **Add Group**.

b. Enter a **Group Name** that identifies the spoke site.

c. In the list on the left side of the window, select the Address Object that you created for this spoke, and then click the right-arrow to move it to the right side of the window. Also move DEFAULT_NETWORK to the right side of the window.

For example, to configure Spoke1 in Figure 1, you could enter the group name *local_subnet_to_Spoke1* and add both 192.168.75.0 and DEFAULT_NETWORK to this group.

d. Click **OK** to save the group.

e. Repeat **Steps a-d** for each spoke site.

For example, to configure Spoke2 in Figure 1, you could enter the group name *local_subnet_to_Spoke2* and add both 192.168.74.0 and DEFAULT_NETWORK to this group.

Step 5. In the navigation tree, choose **VPN > Site-to-Site > IPsec Policies**.

Step 6. If you have not previously enabled VPN on this security appliance, click **On**.

Step 7. Create a VPN policy for each spoke site.

a. Click **Add** to add a new VPN policy. This policy will be used to create a VPN tunnel from the hub to the specified spoke site.

b. In the pop-up window, enter the settings. For more information, you can click the **Help** link near the top right corner of the pop-up window. Also see the example at the end of this procedure.

For this scenario, only the Basic Settings tab is modified. The **Remote Address** is the WAN IP address of the spoke site. The **Local Network** is the Address Group that was created previously for this spoke site. The **Remote Network** is the network address of the spoke site. The Pre-Shared Key is the same one that was configured when setting up the VPN policies on the security appliances at the spoke sites.

c. Click **OK**.

d. Repeat **Steps a-c** to add a policy for each spoke site.

The VPN policies will be similar, as shown in these examples.

	Policy for Spoke1	Policy for Spoke2
Description	vpn_to_Spoke1	vpn_to_Spoke2
IPsec Policy Enable	On	On
Remote Type	Static IP	Static IP
Remote Address	10.74.10.90	10.74.10.86
Authentication Method	Pre-Shared Key	Pre-Shared Key
Key	C1sc0123	C1sc0123
WAN Interface	WAN1	WAN1
Local Network	local_subnet_to_spoke1	local_subnet_to_spoke2
Remote Network	192.168.75.0	192.168.74.0

Verifying Connectivity

Step 1. Use a web browser to launch the configuration utility for the security appliance at a spoke site.

- If your computer is connected to the LAN, enter the LAN IP address of the security appliance.
- If you are accessing the device remotely, enter the protocol, the WAN IP address, and the port number, such as https://10.74.10.90:8080.

Step 2. In the navigation tree, choose **Device Management > Diagnostic Utilities > Ping**.

Step 3. Enter a valid IP address of a device at another spoke site. For example, from Spoke1, ping 192.168.74.100 for the Spoke2 computer illustrated in Figure 1.

Step 4. Click **Start**. If the ping succeeds, the VPN tunnel is connected.

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

78-21038-01