Configuring VPN with Cisco ISA500 Series Security Appliances

This application note describes configurations of VPN on the Cisco ISA500 series security appliance. This document includes the following sections:

Supported VPN on the Cisco ISA500 Security Appliance

The Cisco ISA500 supports these VPNs:

- Remote access Easy Virtual Private Network (EzVPN)
- Secure Sockets Layer Virtual Private Network (SSLVPN)
- Site-to-site

  The site-to-site VPN does not support Dynamic Multipoint Virtual Private Network (DMVPN) and Generic Routing Encapsulation (GRE) tunnels.

Table 1 lists the clients that are supported on different operating systems.

Table 1 VPN Clients and Compatible Operating Systems

OS		Windows 7		Windows Vista		Windows XP		Linux		Mac	
		x86	x64	x86	x64	x86	x64	x86	x64	10.5	10.6
AnyConnect	2.x	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
	3.x	OK	OK	OK	OK	OK	OK	OK	OK	OK	OK
VPN client	4.x	OK	–[1]	OK	–	OK	–	OK	OK	OK	OK
	5.x	OK	OK	OK	OK	OK	–	[2]\	\	\	\

[1] “–” implies that the software can be installed on the OS but it will not work.

[2] “\” implies that there is no software.

Table 2 lists the versions of VPN tools compatible to the operating systems.

Table 2 OS-Compatible VPN Versions

OS	VPN Client Version	AnyConnect Version
Mac	4.9.01 (0080)	3.0.4235
iPad	5.0.1 (9A405)	5.0.1 (9A405)
Win x32	4.8.02.0010	3.0.2052
	5.0.07.0410	3.1.00495
	5.0.00.0340	
Win x64	4.8.02.0010	3.0.2052
	5.0.07.0410	3.1.00495
	5.0.00.0340	
Vista x32	5.0.00.0340	3.1.00495
Vista x64	5.0.070440	3.1.00495
Linux x32	4.8.02.0030	3.1.00495
Linux x64	4.8.02.0030	3.1.00495

Restricting Remote VPN Clients to Access Only Specific Networks and Servers

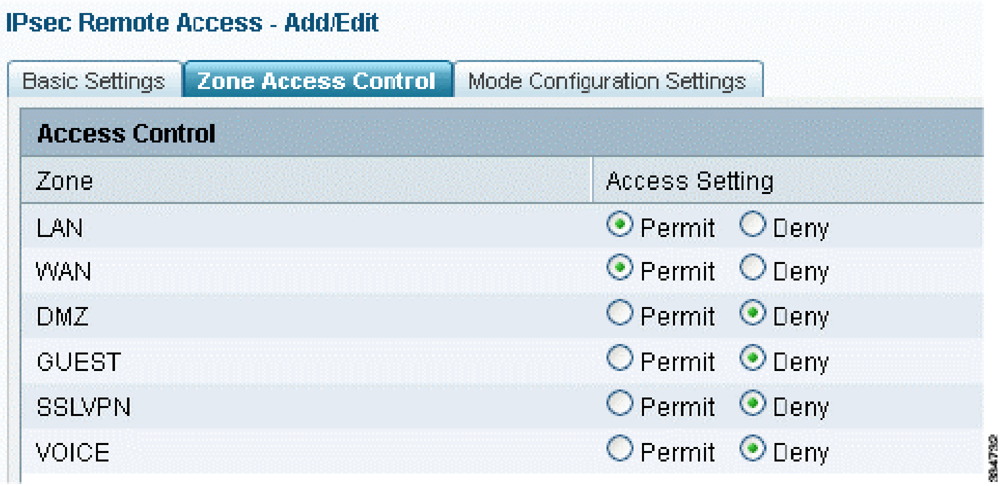
You can restrict remote VPN clients from accessing selective networks and servers at the zone level or at the IP address level.

Restricting Access at the Zone Level:

In the following

, the settings allow VPN clients to access only the LAN and WAN zones and deny access to other zones:

Figure 1 IPsec Remote Access - Add/Edit



IPsec Remote Access - Add/Edit

Access Control

Zone	Access Setting
LAN	● Permit ○ Deny
WAN	● Permit ○ Deny
DMZ	○ Permit ● Deny
GUEST	○ Permit ● Deny
SSLVPN	○ Permit ● Deny
VOICE	○ Permit ● Deny

To restrict access at the zone level, follow these steps:

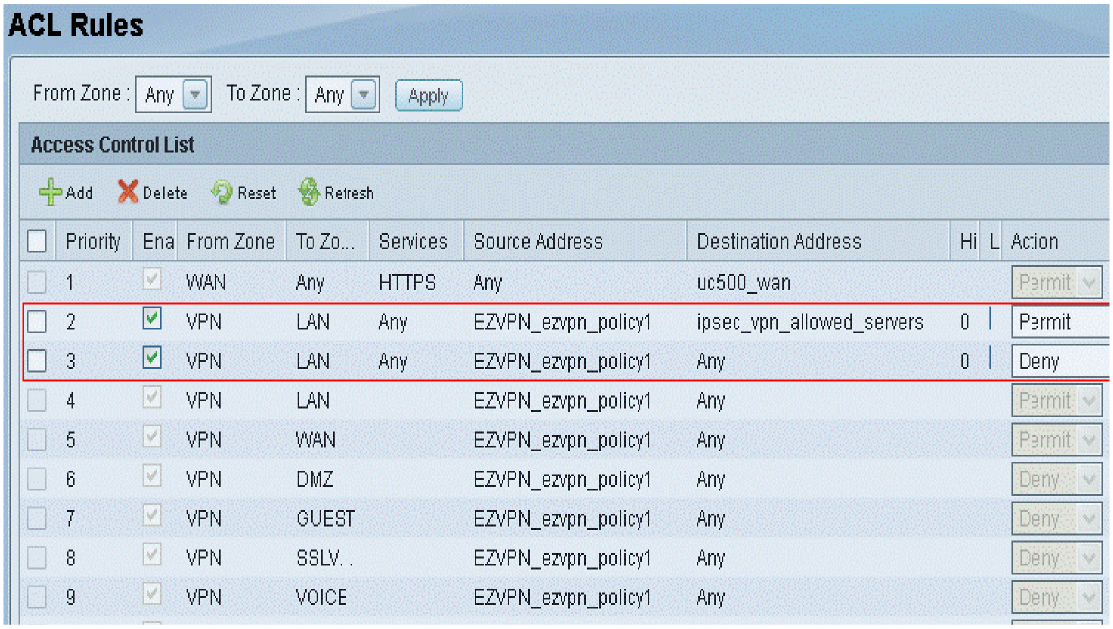
STEP 1 In the IPsec Remote Access - Add/Edit window, click the **Zone Access Control** tab.

STEP 2 To permit or deny access to a zone, click the **Access Setting** radio button for the zone.

Restricting Access at the IP Address Level:

In the following figure, the rule allows VPN clients to access only the IP address range defined in *ipsec_vpn_allowed_servers* in the LAN zone and to deny access to all other servers.

Figure 2 ACL Rules



ACL Rules

From Zone : Any ▾ To Zone : Any ▾ Apply

Access Control List

☐	Priority	Ena	From Zone	To Zo...	Services	Source Address	Destination Address	Hi	L	Action
☐	1	☑	WAN	Any	HTTPS	Any	uc500_wan			Permit
☐	2	☑	VPN	LAN	Any	EZVPN_ezvpn_policy1	ipsec_vpn_allowed_servers	0		Permit
☐	3	☑	VPN	LAN	Any	EZVPN_ezvpn_policy1	Any	0		Deny
☐	4	☑	VPN	LAN		EZVPN_ezvpn_policy1	Any			Permit
☐	5	☑	VPN	WAN		EZVPN_ezvpn_policy1	Any			Permit
☐	6	☑	VPN	DMZ		EZVPN_ezvpn_policy1	Any			Deny
☐	7	☑	VPN	GUEST		EZVPN_ezvpn_policy1	Any			Deny
☐	8	☑	VPN	SSLV. .		EZVPN_ezvpn_policy1	Any			Deny
☐	9	☑	VPN	VOICE		EZVPN_ezvpn_policy1	Any			Deny

To restrict access at the IP address level, follow these steps:

STEP 1 Click **Firewall** > **ACL Rules**

STEP 2 Click **Add** to create a new rule.

STEP 3 Check the **Enable** radio button for the rule.

STEP 4 From the **Action** drop-down list, click **Permit** to allow VPN clients access to the zone, or click **Deny** to deny VPN clients access to the zone.

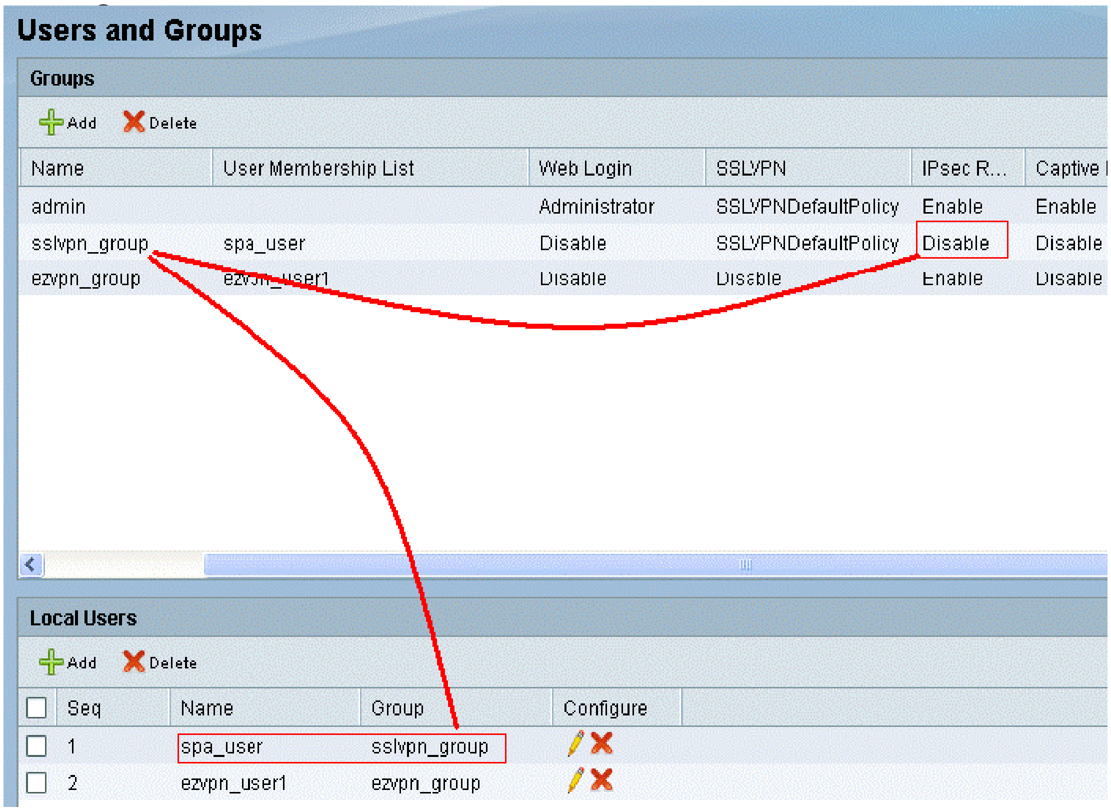
STEP 5 Click **OK** to create the rule.

Permitting Users to Remotely Connect to VPN

To permit users to connect to the IPsec VPN, you must add these users to a user group and then enable IPsec Remote Access for the group.

In the following figure, the user *spa_user* belongs to the *sslvpn_group*, which has IPsec Remote Access disabled for it. As a result, *spa_user* cannot use the IPsec VPN.

Figure 3 Users and Groups



Name	User Membership List	Web Login	SSLVPN	IPsec R...	Captive
admin		Administrator	SSLVPNDefaultPolicy	Enable	Enable
sslvpn_group	spa_user	Disable	SSLVPNDefaultPolicy	Disable	Disable
ezvpn_group	ezvpn_user1	Disable	Disable	Enable	Disable

□	Seq	Name	Group	Configure
□	1	spa_user	sslvpn_group	✎ ✖
□	2	ezvpn_user1	ezvpn_group	✎ ✖

Authenticating VPN Users Through RADIUS and Active Directory

For information on authenticating VPN users through RADIUS and Active Directory, see the *Configuring the Cisco ISA500 for Active Directory/LDAP and Radius Authentication Application Note* at www.cisco.com/en/US/products/ps11752/prod_technical_reference_list.html.

Setting Up Split Tunneling with EzVPN and SSLVPN

Split tunneling allows only traffic that is specified by the VPN client to reach the internal resources through the VPN tunnel.

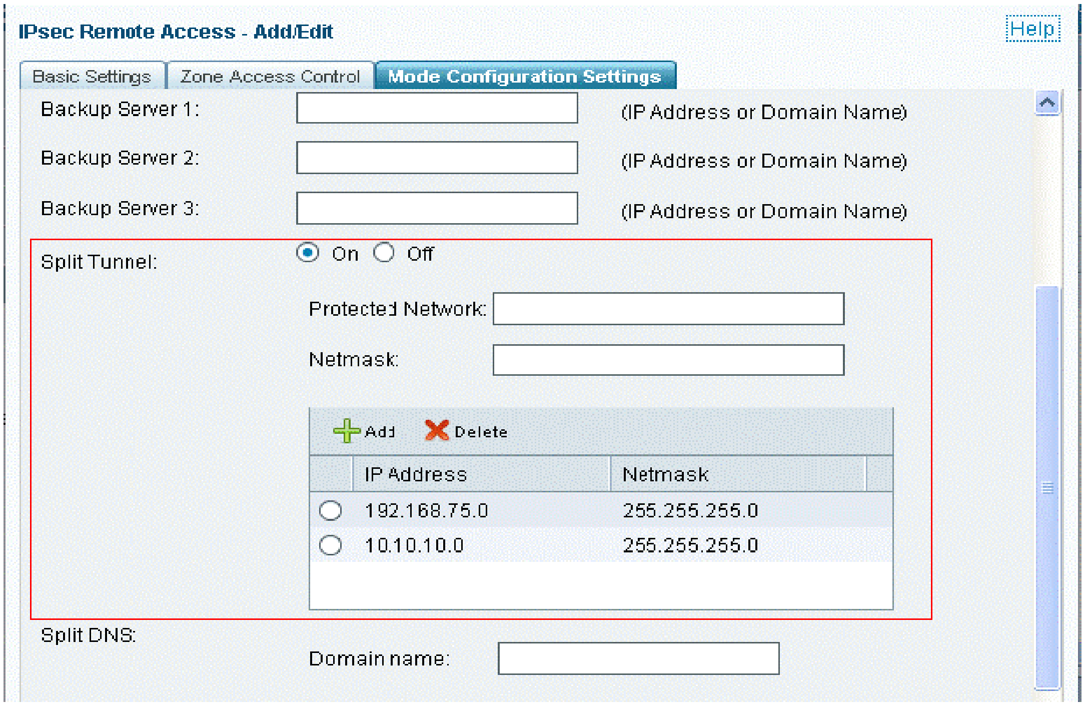
By default split tunneling is off, implying that all traffic from the VPN client is encrypted and sent to the security appliance irrespective of the destination IP address. As a result, the security appliance may consume too much bandwidth, especially when much of the traffic is destined for the Internet and does not need to pass through the Cisco ISA500.

Split tunneling resolves this issue by allowing the VPN client to send only the traffic that is destined for the internal network across the tunnel. All the other traffic is sent to the Internet directly from the client's local LAN.

Split Tunneling in EzVPN

In the following figure, the IP address 192.168.75.0/24 represents the LAN zone and the IP address 10.10.10.0/24 represents the DMZ zone. The split tunnel settings only allow traffic meant for the LAN and DMZ zones through the IPsec tunnel.

Figure 4 Split Tunneling in IPsec Remote Access



IPsec Remote Access - Add/Edit

Backup Server 1: (IP Address or Domain Name)

Backup Server 2: (IP Address or Domain Name)

Backup Server 3: (IP Address or Domain Name)

Split Tunnel: ● On ○ Off

Protected Network:

Netmask:

	IP Address	Netmask
○	192.168.75.0	255.255.255.0
○	10.10.10.0	255.255.255.0

Split DNS:

Domain name:

To configure IPsec VPN split tunneling, follow these steps:

STEP 1 From the Cisco ISA500 Configuration Utility, click **VPN** > **IPsec Remote Access**. The IPsec Remote Access window appears.

STEP 2 Click **On** to enable IPsec Remote Access, or click **Off** to disable it.

NOTE Enabling the IPsec Remote Access disables the Teleworker VPN Client feature.

STEP 3 Click **Add**. The IPsec Remote Access - Add/Edit window appears.

STEP 4 Click the **Mode Configuration Settings** tab.

STEP 5 To enable split tunnel, click **On**.

STEP 6 In the Protected Network field, enter the IP address.

STEP 7 In the Netmask field, enter the subnet mask.

STEP 8 Click **Add**.

STEP 9 Click **OK**.

STEP 10 Click **Save**.

Split Tunneling in SSLVPN

For information about split tunneling in SSL VPN, see the "Configuring SSL VPN Split Tunneling" section in the *Configuring SSL VPN on the Cisco ISA500 Security Appliance Application Note* at www.cisco.com/en/US/products/ps11752/prod_technical_reference_list.html.

Configuration Examples of EzVPN, SSLVPN and Site-to-Site Between Cisco ISA500 Appliances

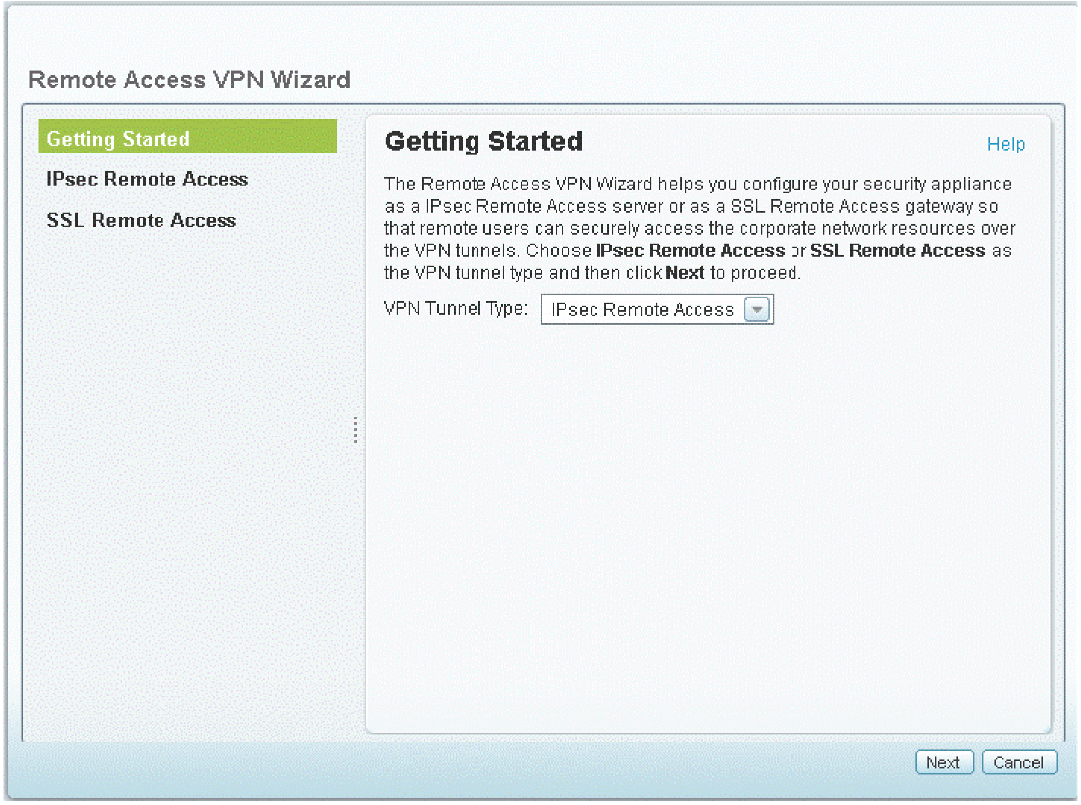
Configuring the Cisco ISA500 for IPsec VPN

You can configure the ISA500 for IPsec VPN using the Remote Access VPN Wizard. This feature allows remote users to establish the VPN tunnels to securely access the corporate network resource.

To configure the IPsec VPN, follow these steps:

STEP 1 From the ISA500 Configuration Utility, click **Configuration Wizards** > **Remote Access VPN Wizard**. The Remote Access VPN Wizard window appears.

Figure 5 Remote Access VPN Wizard - Getting Started



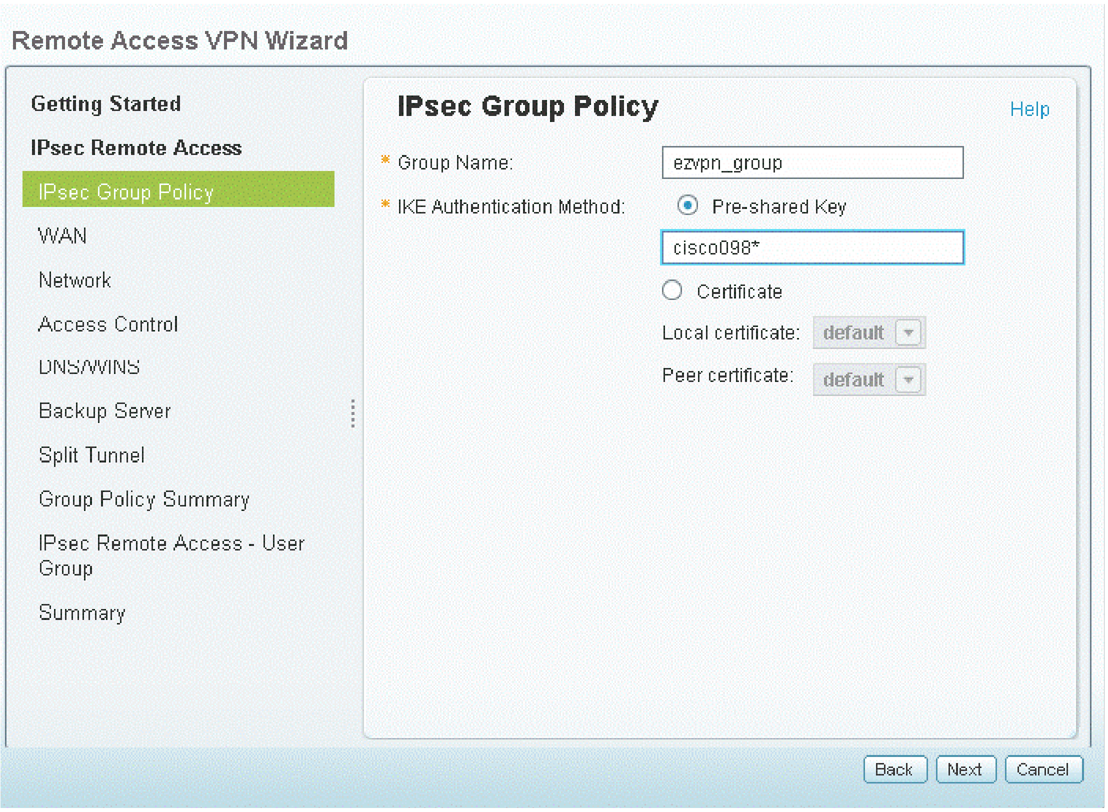
Getting Started

The Remote Access VPN Wizard helps you configure your security appliance as a IPsec Remote Access server or as a SSL Remote Access gateway so that remote users can securely access the corporate network resources over the VPN tunnels. Choose **IPsec Remote Access** or **SSL Remote Access** as the VPN tunnel type and then click **Next** to proceed.

VPN Tunnel Type: IPsec Remote Access

STEP 2 From the VPN Tunnel Type drop-down list, choose IPsec Remote Access and then click **Next**. The IPsec Group Policy page appears.

Figure 6 Remote Access VPN Wizard - IPsec Group Policy



IPsec Group Policy

* Group Name: ezvpn_group

* IKE Authentication Method: ● Pre-shared Key

cisco098*

○ Certificate

Local certificate: default

Peer certificate: default

STEP 3 In the Group Name field, enter the group for which you want to create the group policy.

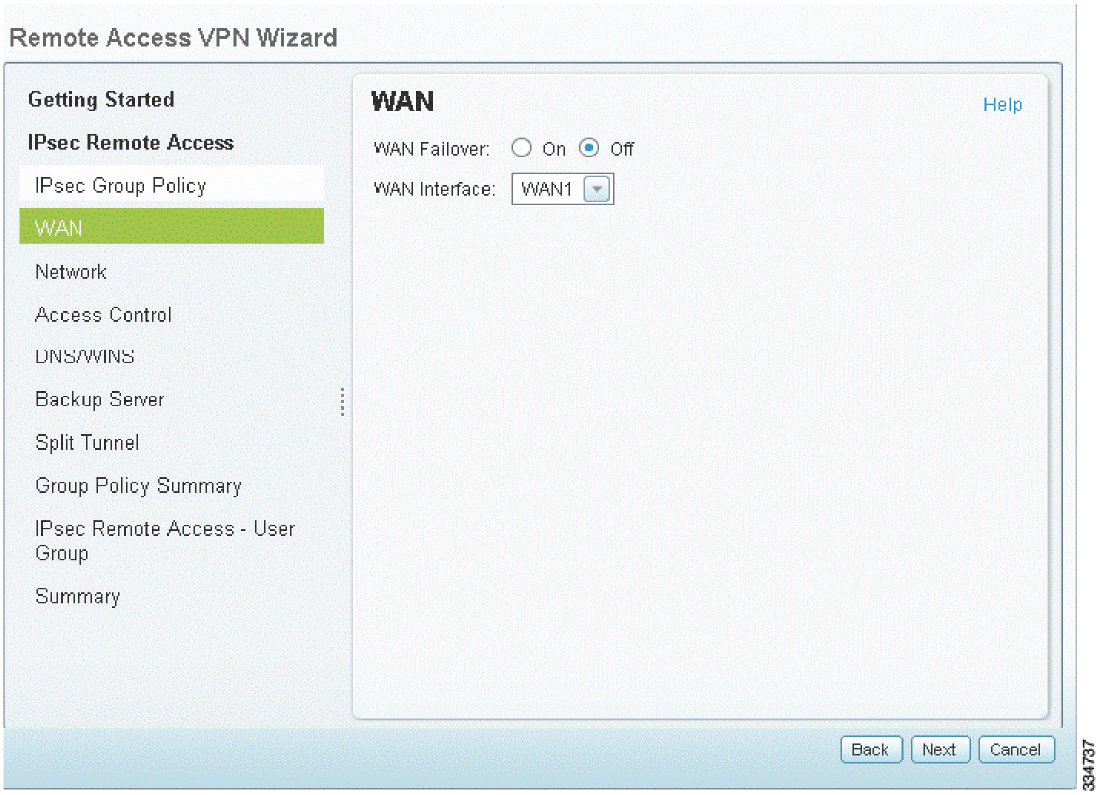
STEP 4 Choose the IKE Authentication Method.

a. If you choose Pre-shared Key as the authentication method, then enter the authentication key in the corresponding field.

b. If you choose Certificate as the authentication method, then you must select the Local certificate and Peer certificate from the drop-down lists for authentication. This example uses Pre-shared Key to authenticate the remote VPN clients.

STEP 5 Click **Next**. The WAN page appears.

Figure 7 Remote Access VPN Wizard - WAN

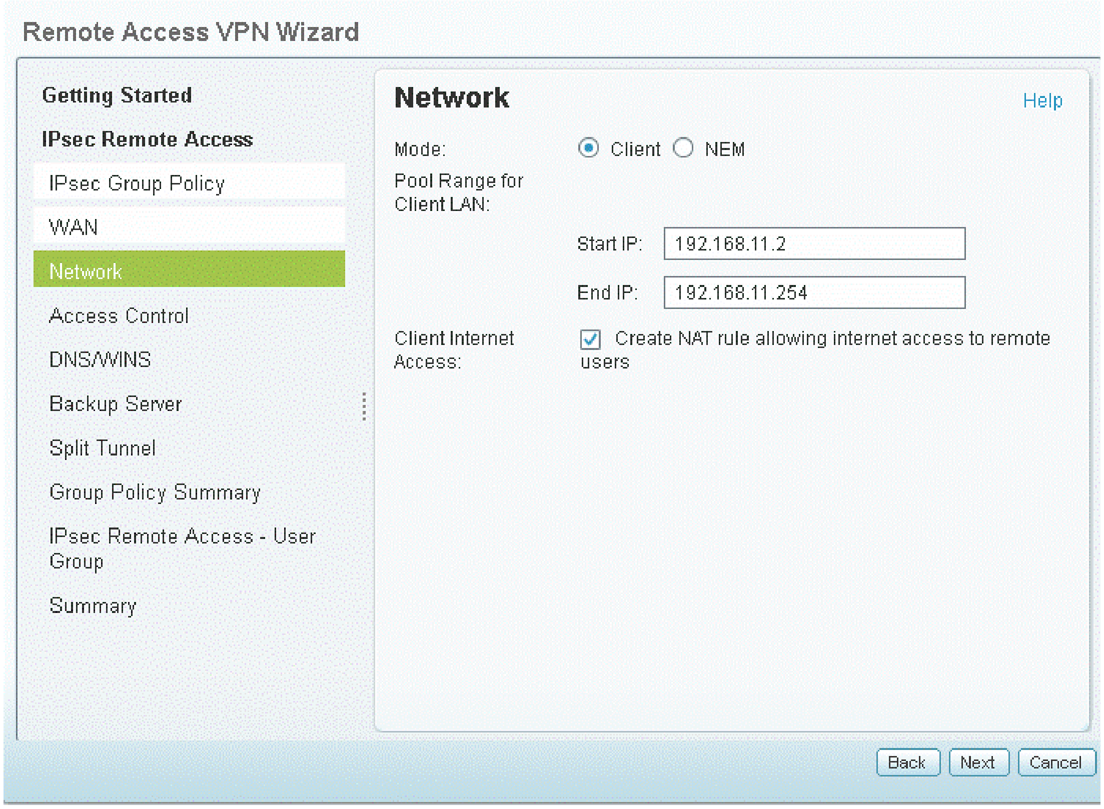


WAN Failover: ○ On ● Off

WAN Interface: WAN1

STEP 6 Choose the WAN Interface from the drop-down list and then click **Next**. The Network page appears.

Figure 8   Remote Access VPN Wizard - VPN



Network

Mode: ● Client ○ NEM

Pool Range for Client LAN:

Start IP: 192.168.11.2

End IP: 192.168.11.254

Client Internet Access: ☑ Create NAT rule allowing internet access to remote users

STEP 7 Choose the mode for the group policy.

In this example, the group policy is configured in the client mode. In client mode, the IPsec VPN server can assign the IP addresses to the outside interfaces of remote VPN clients. To define the pool range for remote VPN clients, enter the starting and ending IP addresses in the Start IP and End IP fields.

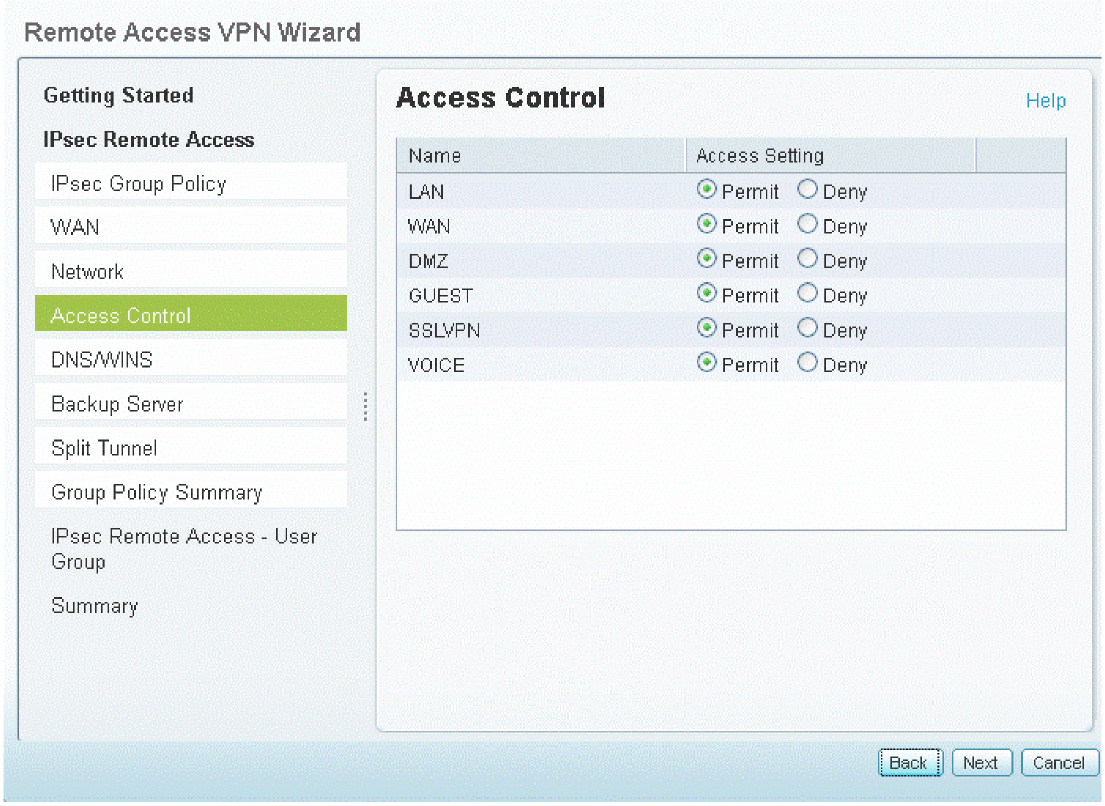
If you choose NEM mode for the group policy then it is only used for the Cisco device acting as a Cisco VPN hardware client in NEM mode.

STEP 8 Check the Client Internet Access check box to automatically create advanced NAT rules to allow remote VPN clients to access the Internet over the VPN tunnels.

If you uncheck this check box, you can manually create advanced NAT rules.

STEP 9 Click **Next**. The Access Control page appears.

Figure 9 Remote Access VPN Wizard - Access Control



Access Control

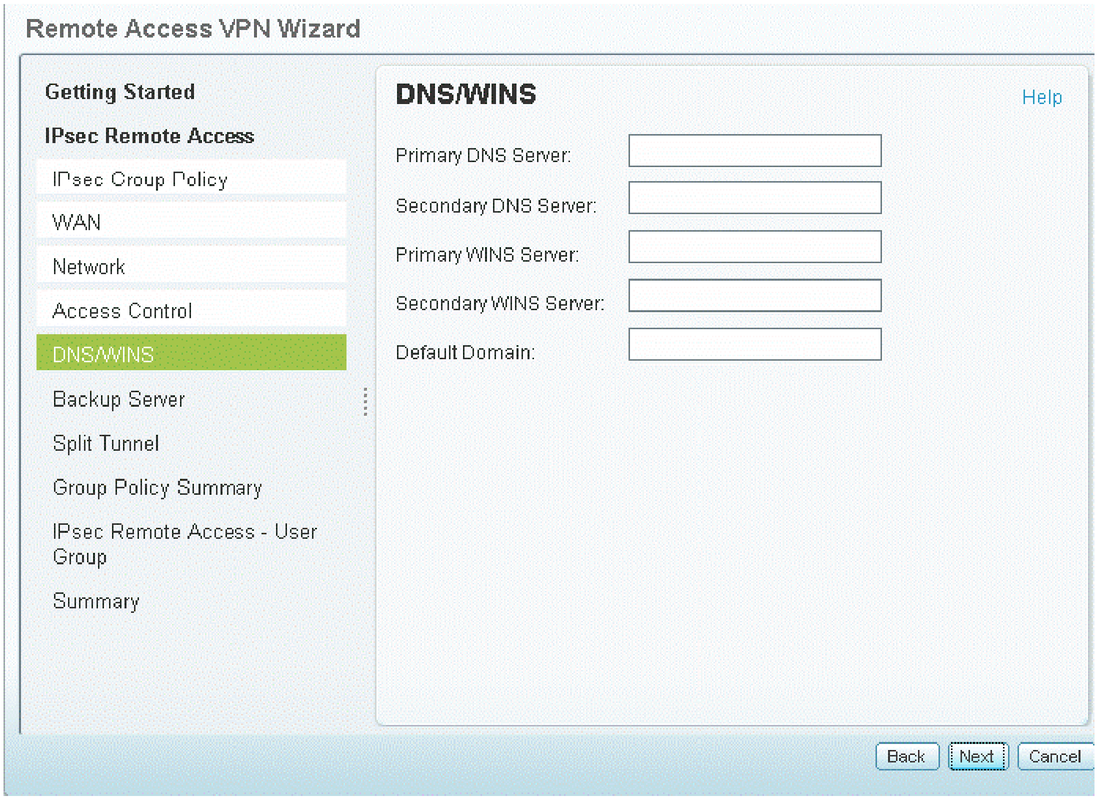
Name	Access Setting
LAN	● Permit ○ Deny
WAN	● Permit ○ Deny
DMZ	● Permit ○ Deny
GUEST	● Permit ○ Deny
SSLVPN	● Permit ○ Deny
VOICE	● Permit ○ Deny

STEP 10 Click the **Permit** or **Deny** radio button to set the access control for a zone.

By default, the remote clients can access all of the internal resources. You can control this access by changing the access control setting for the zone. In this example, the firewall is configured to the default settings.

STEP 11 Click **Next**. The DNS/WINS page appears.

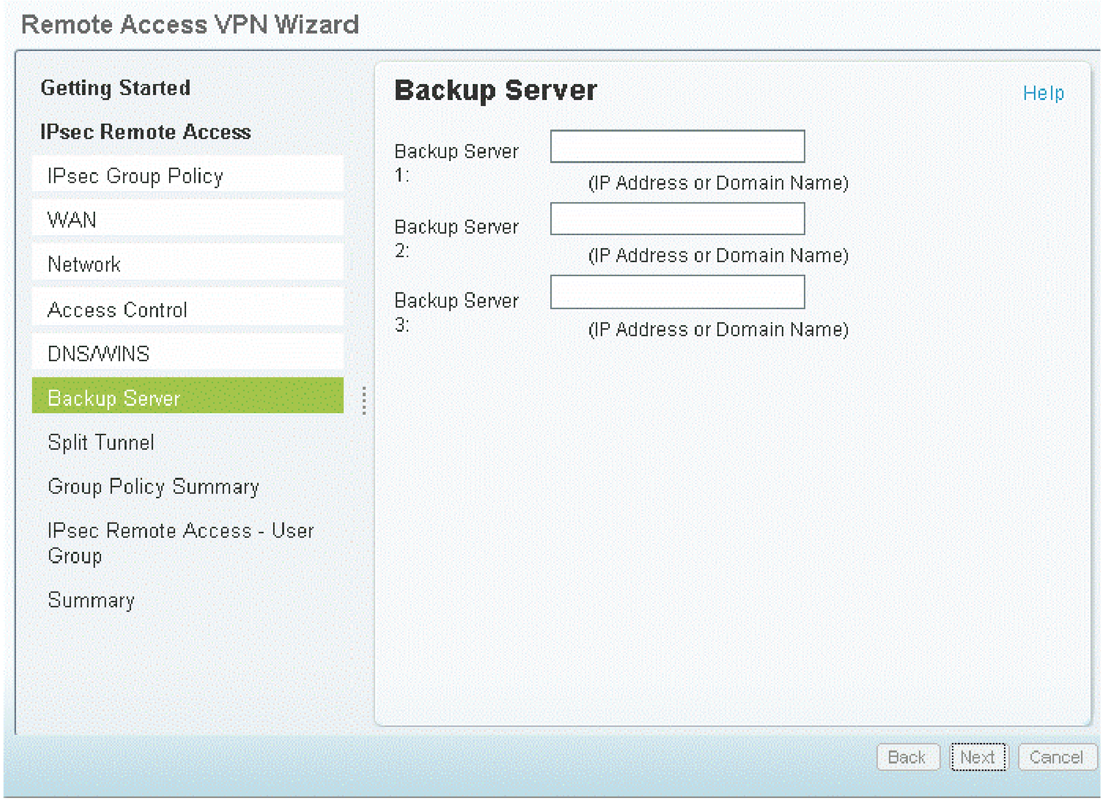
Figure 10 Remote Access VPN Wizard - DNS/WINS



STEP 12 Enter the DNS and WINS server addresses in the fields and then click **Next**.

NOTE Using this page to specify the DNS and domain settings is optional.

Figure 11   Remote Access VPN Wizard - Backup Server



Backup Server

Backup Server 1: ______ (IP Address or Domain Name)

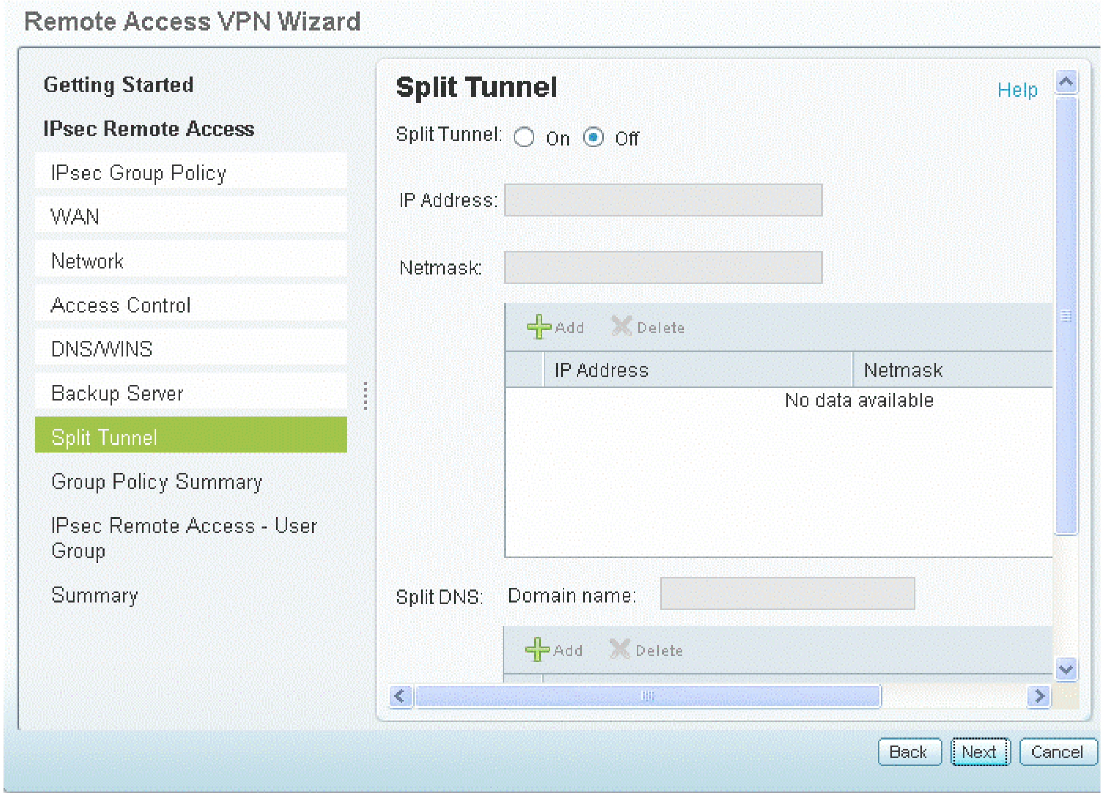
Backup Server 2: ______ (IP Address or Domain Name)

Backup Server 3: ______ (IP Address or Domain Name)

STEP 13 Enter the Backup Server IP addresses or domain names in the fields and then click **Next**.

NOTE Using this page to specify the backup server settings is optional.

Figure 12 Remote Access VPN Wizard - Split Tunnel



Split Tunnel

Split Tunnel: ○ On ● Off

IP Address:

Netmask:

IP Address	Netmask
No data available	

Split DNS: Domain name:

STEP 14 Click **On** to enable the split tunnel feature.

If you enable split tunneling, you need to define the split subnets. To add a subnet, enter the IP address and netmask in the IP Address and Netmask fields and click **Add**. To delete a subnet, select it from the list and click **Delete**.

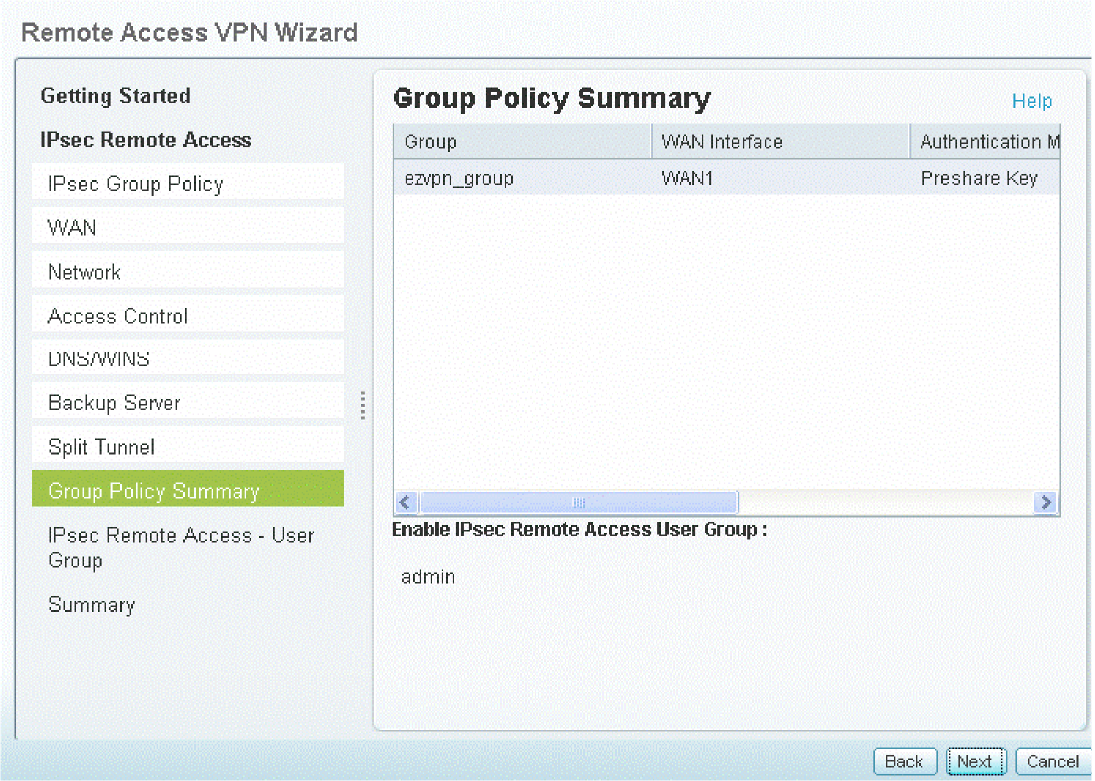
In this example, the split tunnel feature is disabled.

NOTE To use Split DNS, you must enable the split tunnel feature and specify the domains.

Split DNS directs DNS packets in clear text through the VPN tunnel to domains served by the corporate DNS. To add a domain, enter the Domain name that should be resolved by your network DNS server, and then click **Add**. To delete a domain, select it from the list and click **Delete**.

STEP 15 Click **Next**. The Group Policy Summary page appears.

Figure 13 Remote Access VPN Wizard - Group Policy Summary



Remote Access VPN Wizard

Group Policy Summary

Group	WAN Interface	Authentication M
ezvpn_group	WAN1	Preshare Key

Enable IPsec Remote Access User Group :

admin

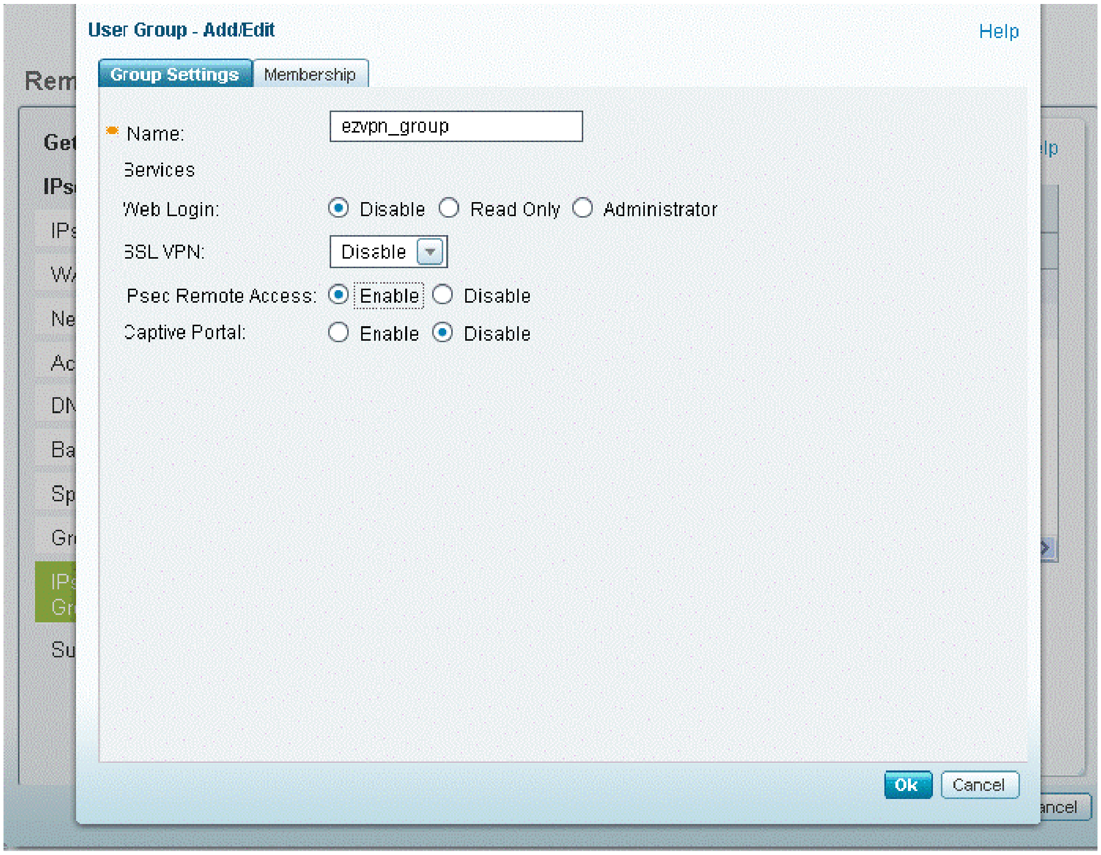
STEP 16 Use the Group Policy Summary page to view information for the group policy settings. The page displays all of the user groups that have IPsec Remote Access enabled for them. In this example, only the **admin** has the remote access enabled. You can add more user groups in the following step.

STEP 17 Click **Next**. The IPsec Remote Access - User Group page appears.

STEP 18 Click **Add**. The User Group - Add/Edit window appears.

Other options: To edit the configuration settings for a group, click **Edit** (pencil icon). To delete a group, check the **Sequence** check box and click **Delete** (cross icon).

Figure 14   Remote Access VPN Wizard - User Group Add/Edit



Name: ezvpn_group

Services

Web Login: ● Disable ○ Read Only ○ Administrator

SSL VPN: Disable

Psec Remote Access: ● Enable ○ Disable

Captive Portal: ○ Enable ● Disable

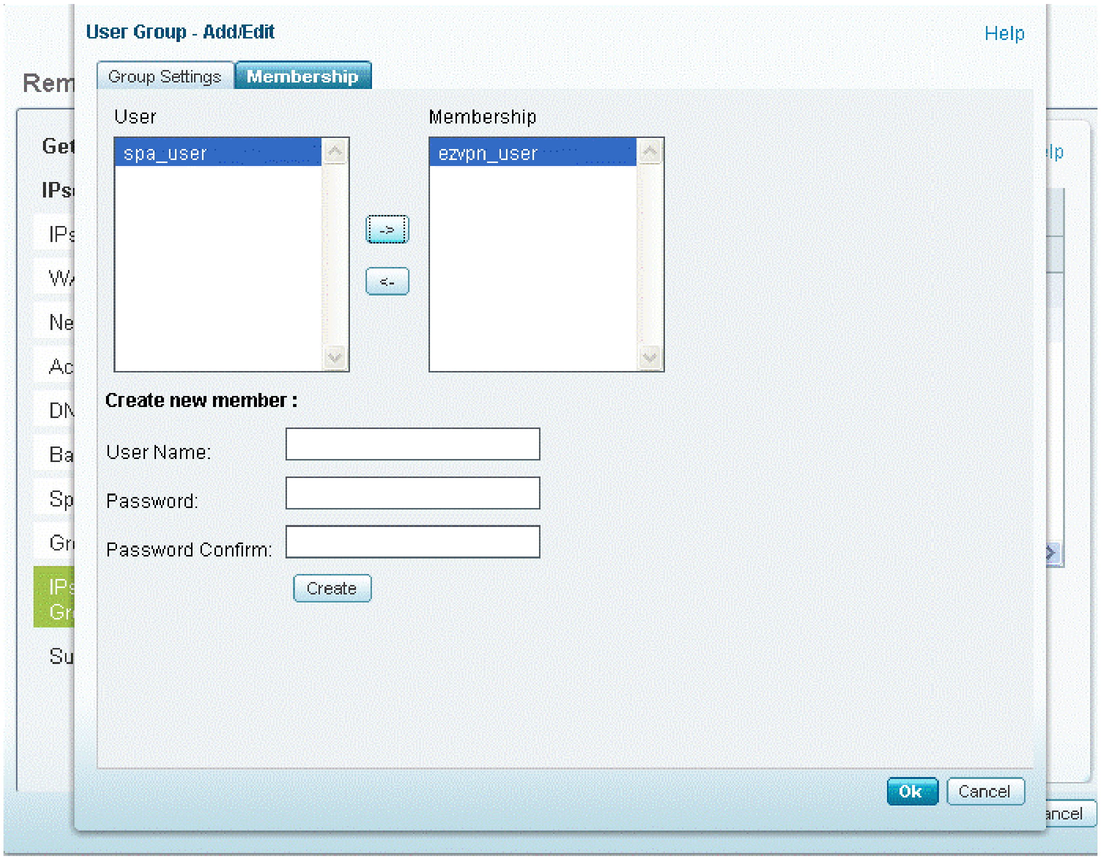
STEP 19 Click the **Group Settings** tab.

Enter the name of the user group in the **Name** field.

Specify the service policy for the user group. You must enable the IPsec Remote Access to allow members of the group can access the resources over the VPN tunnel. You must enable at least one service to create a user group.

STEP 20 Click the **Membership** tab.

Figure 15   Remote Access VPN Wizard - User Group Add/Edit Membership



User Group - Add/Edit

User

spa_user

Membership

ezvpn_user

Create new member :

User Name:

Password:

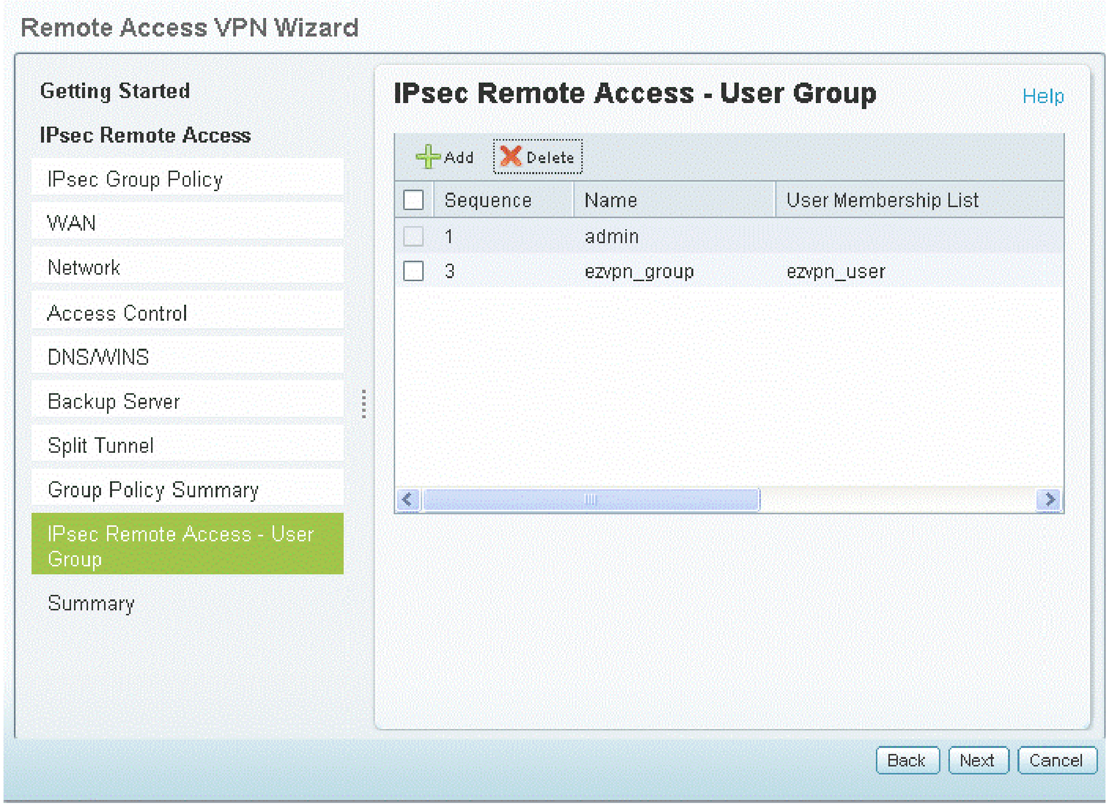
Password Confirm:

To add a member to the group, select a user from the **User** list and click the right arrow.

To create a new user, enter the username in the **User Name** field and the password in the **Password** field. Confirm the password in the **Password Confirm** field, and then click **Create**.

STEP 21 Click **OK**.

Figure 16 Remote Access VPN Wizard - IPsec Remote Access User Group

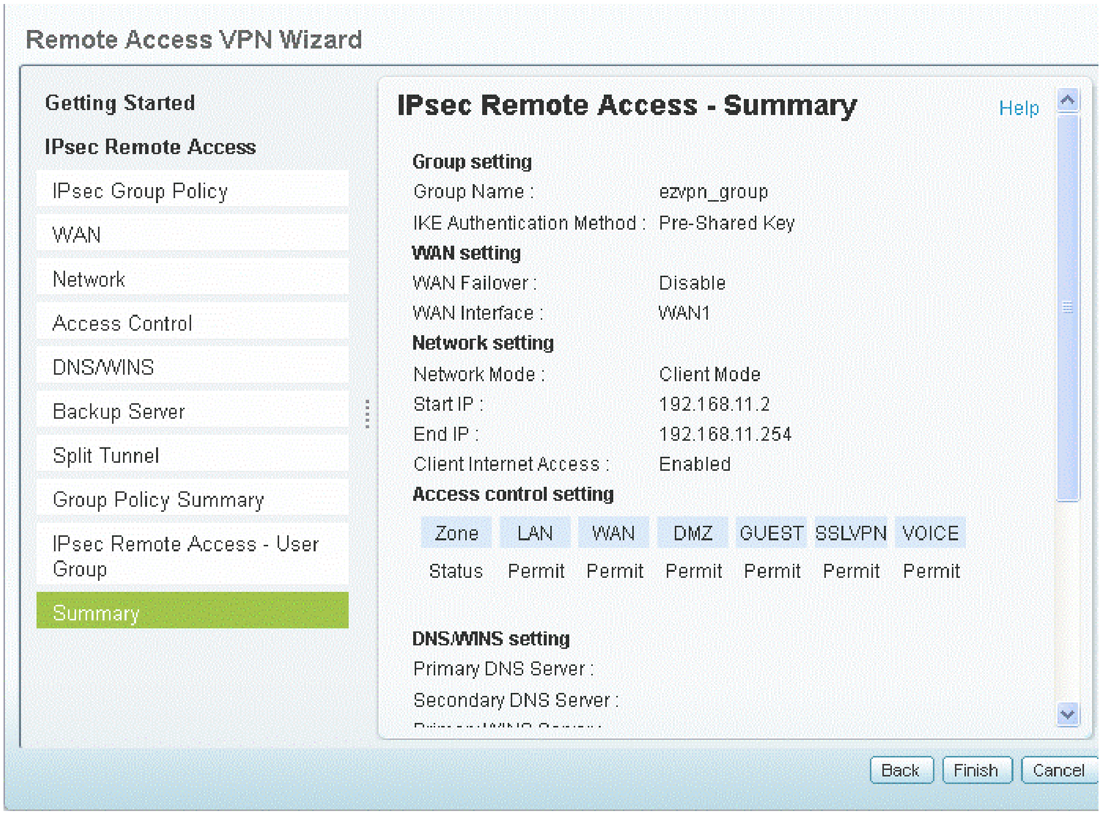


IPsec Remote Access - User Group

□	Sequence	Name	User Membership List
□	1	admin	
□	3	ezvpn_group	ezvpn_user

STEP 22 Click **Next**. The IPsec Remote Access - Summary page appears.

Figure 17 Remote Access VPN Wizard - IPsec Remote Access Summary



IPsec Remote Access - Summary

Group setting

Group Name : ezvpn_group

IKE Authentication Method : Pre-Shared Key

WAN setting

WAN Failover : Disable

WAN Interface : WAN1

Network setting

Network Mode : Client Mode

Start IP : 192.168.11.2

End IP : 192.168.11.254

Client Internet Access : Enabled

Access control setting

Zone	LAN	WAN	DMZ	GUEST	SSLVPN	VOICE
Status	Permit	Permit	Permit	Permit	Permit	Permit

DNS/WINS setting

Primary DNS Server :

Secondary DNS Server :

STEP 23 To modify the configuration settings, click **Back**. If the configuration is correct, click **Finish** to apply the settings.

Configuring the Cisco ISA500 for SSL VPN

For information about configuring the Cisco ISA500 for SSL VPN, see the *Configuring SSL VPN on the ISA500 Application Note* at www.cisco.com/en/US/products/ps11752/prod_technical_reference_list.html.

Configuring the Cisco ISA500 for Site-to-Site VPN

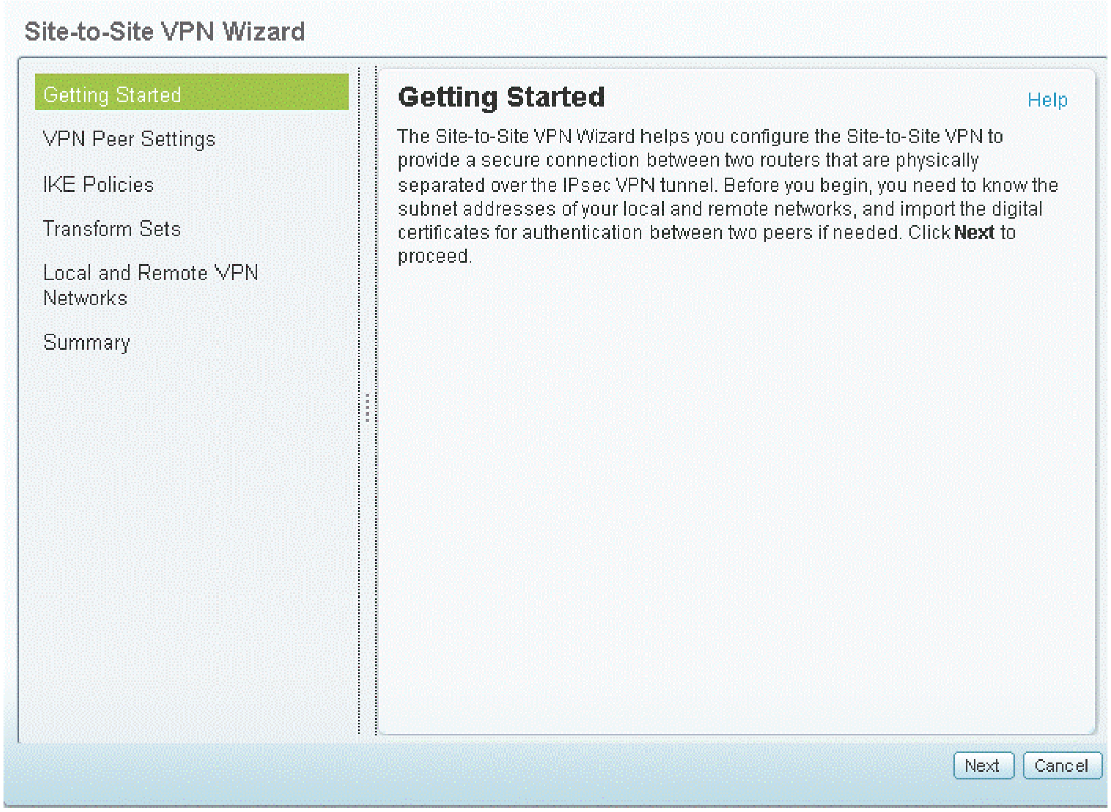
A site-to-site VPN tunnel connects two routers to secure traffic between two sites that are physically separated. The following example shows how to configure a VPN tunnel through a site-to-site VPN wizard for two sites, the *main office* and the *branch office*.

Cisco ISA500 Configuration for the Main Office

To configure site-to-site VPN policy using Site-to-Site VPN Wizard, follow these steps:

STEP 1 From the Cisco ISA500 Configuration Utility, click **Configuration Wizards > Site-to-Site VPN Wizard**.

Figure 18 Site-to-Site VPN Wizard



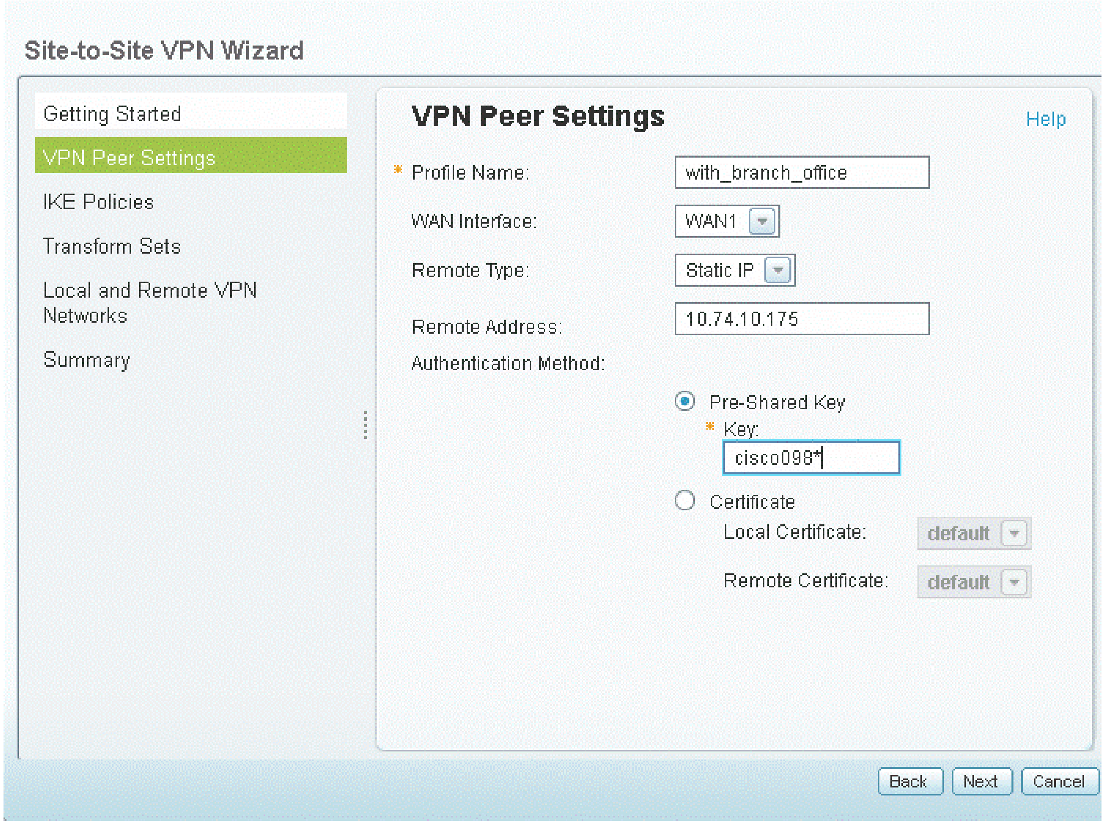
Site-to-Site VPN Wizard

Getting Started

The Site-to-Site VPN Wizard helps you configure the Site-to-Site VPN to provide a secure connection between two routers that are physically separated over the IPsec VPN tunnel. Before you begin, you need to know the subnet addresses of your local and remote networks, and import the digital certificates for authentication between two peers if needed. Click **Next** to proceed.

STEP 2 Click **Next**. The VPN Peer Settings page appears.

Figure 19 Site-to-Site VPN Wizard - VPN Peer Settings



Site-to-Site VPN Wizard

VPN Peer Settings

* Profile Name: with_branch_office

WAN Interface: WAN1

Remote Type: Static IP

Remote Address: 10.74.10.175

Authentication Method:

● Pre-Shared Key

* Key: cisco098*

○ Certificate

Local Certificate: default

Remote Certificate: default

STEP 3 Use the VPN Peer Settings page to configure an IPsec VPN policy for establishing the VPN connection with a remote router.

a. Enter the name of the VPN policy in the **Profile Name** field. In this example, for the main office the remote peer is the branch office.

b. Choose the WAN port from the **WAN Interface** drop-down list that traffic passes through over the VPN tunnel.

c. Choose one of the following remote peers from the **Remote Type** drop-down list:

- Choose Static IP if the remote peer uses a static IP address. Enter the IP address of the remote device in the **Remote Address** field. In this example, the remote peer in the branch office uses a static IP.

- Choose Dynamic IP if the remote peer uses a dynamic IP address.

- Choose FQDN (Fully Qualified Domain Name) if you want to use the domain name of the remote network, for example, *vpn.company.com*.

If you choose FQDN, then enter the domain name of the remote device in the **Remote Address** field.

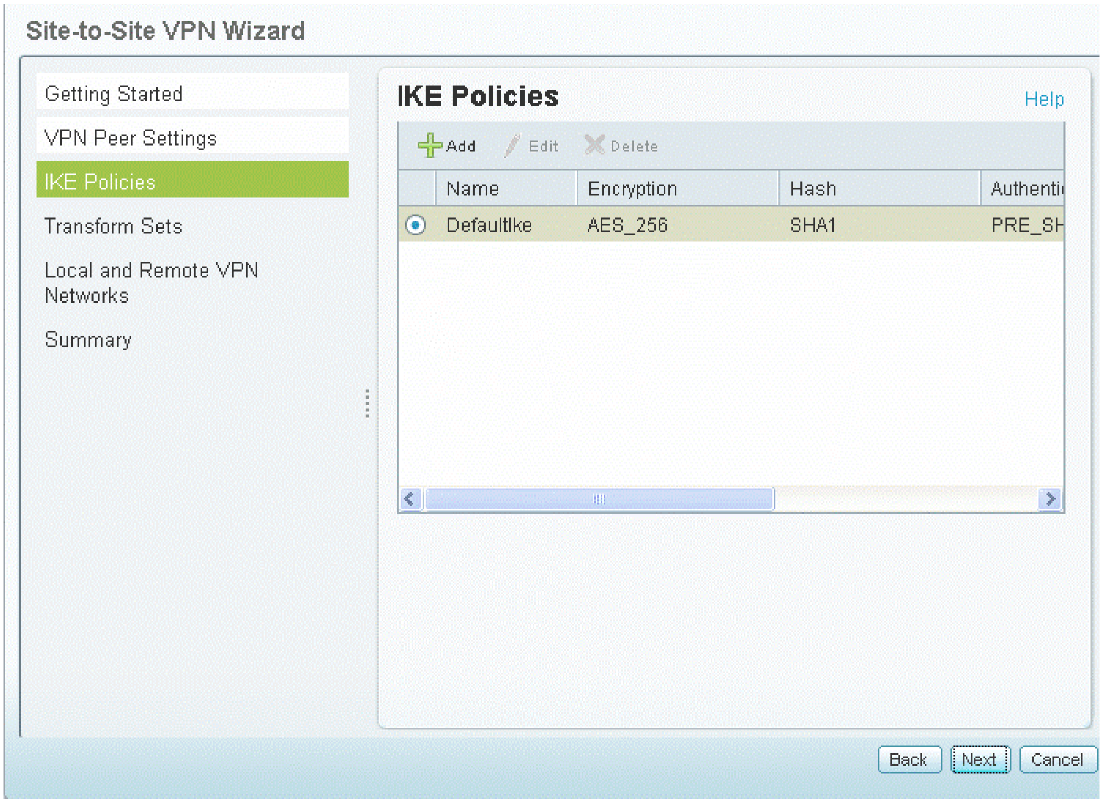
STEP 4 Choose the Authentication Method.

- If you choose Pre-shared Key as the authentication method, then enter the authentication key in the **Key** field.
- If you choose Certificate as the authentication method, then you must select the Local certificate and Peer certificate from the drop-down lists for authentication.

This example uses a pre-shared key for authentication.

STEP 5 Click **Next**. The IKE Policies page appears.

Figure 20 Site-to-Site VPN Wizard - IKE Policies



	Name	Encryption	Hash	Authenti
●	DefaultIke	AES_256	SHA1	PRE_SH

STEP 6 Choose the default IKE policy or create a new policy. This example uses the default IKE policy.

You can edit or delete a custom IKE policy. To edit a policy, click **Edit** (pencil icon). To delete a policy, select the policy from the list and click **Delete** (cross icon).

NOTE You cannot edit or delete the default IKE Policy **DefaultIke**.

STEP 7 Click **Add** to create a new IKE policy. The IKE Policy Add/Edit dialog box appears.

STEP 8 Enter the following information in the IKE Policy Add/Edit dialog box:

a. Enter the name of the policy in the **Name** field.

b. Choose the encryption algorithm from the Encryption drop-down list.

c. Choose the authentication algorithm for the VPN header. Ensure that the authentication algorithm is configured identically on both sides.

d. Choose the authentication method that the security appliance uses to establish the identity of each peer.

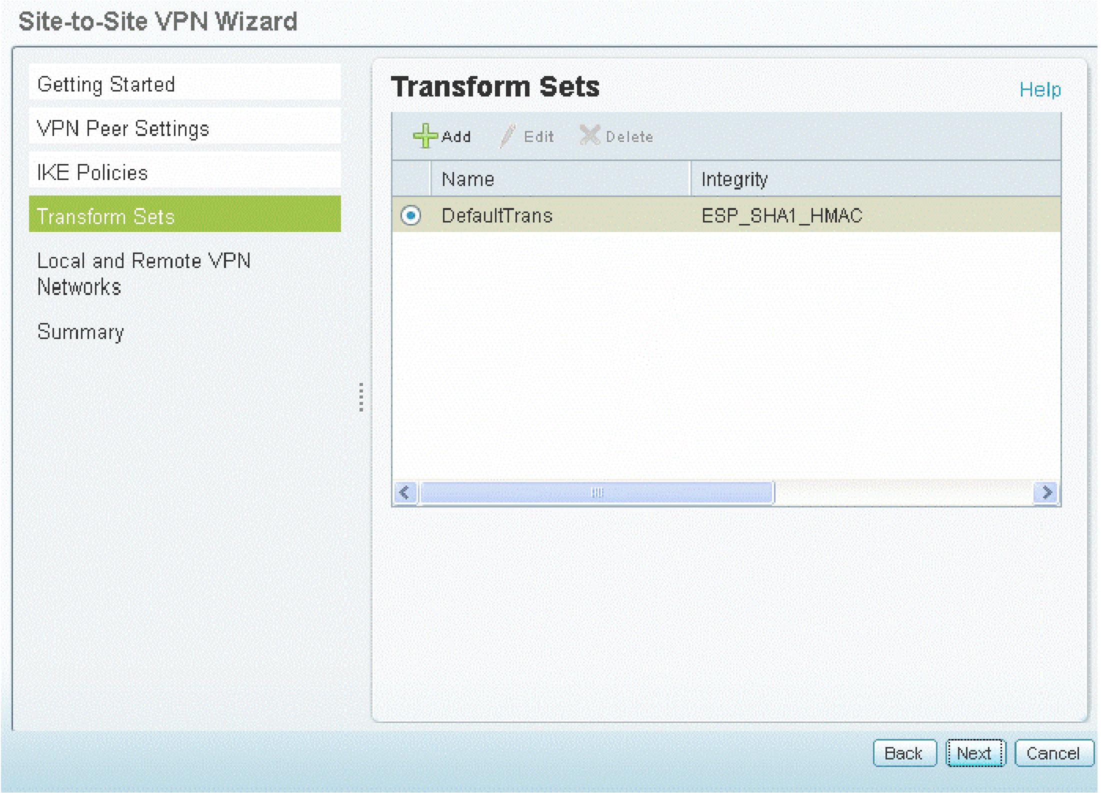
e. Choose the Diffie-Hellman group identifier from the D-H Group drop-down list. The identifier is used by two IPsec peers to derive a shared secret without transmitting it to each other. The D-H Group sets the strength of the algorithm in bits. The higher the D-H group number, the greater the security level.

f. Enter the number of seconds for the IKE Security Association (SA) to remain valid in the Lifetime fields. As a general rule, a shorter lifetime provides more secure ISAKMP negotiations. However, with shorter lifetimes, the security appliance sets up future IKE SAs more quickly.

STEP 9 Click **Next**. The Transform Sets page appears.

Figure 21 Site-to-Site VPN Wizard - Transform Set

s



	Name	Integrity
●	DefaultTrans	ESP_SHA1_HMAC

STEP 10 Choose the default transform set or create a new set. This example uses the default transform set.

You can edit or delete a custom transform set. To edit a policy, click **Edit** (pencil icon). To delete a policy, select the transform set from the list and click **Delete** (cross icon).

NOTE You cannot edit or delete the default transform set **DefaultTrans**.

STEP 11 Click **Add** to create a new transform set. The Transform Set - Add/Edit dialog box appears.

STEP 12 Enter the following information in the Transform Set - Add/Edit dialog box:

a. Enter the name of the transform set in the Name field.

b. Choose the Integrity option. This is the hash algorithm used to ensure data integrity.

c. Choose the encryption algorithm from the Encryption drop-down list. Ensure that the authentication algorithm is configured identically on both sides.

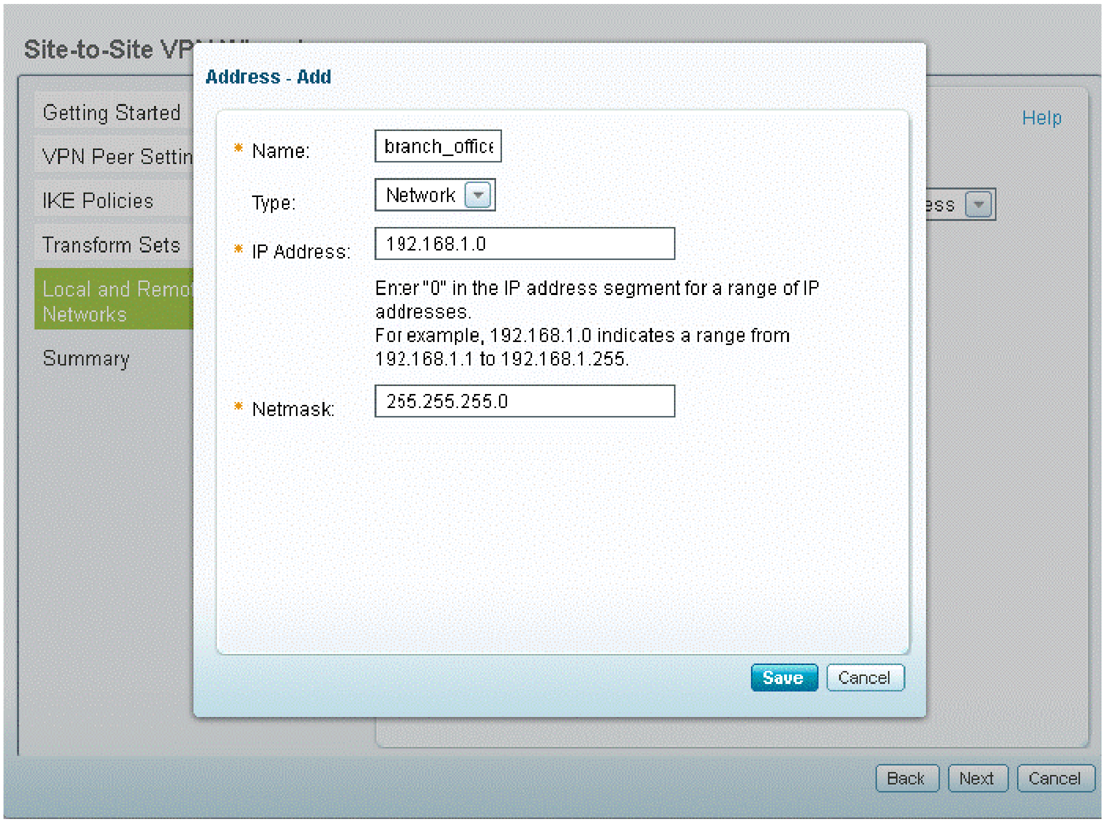
STEP 13 Click **OK**.

STEP 14 Click **Next**. The Local and Remote Networks page appears.

STEP 15 Choose the Local Subnet IP address from the drop-down list. In this example, Default_Network is chosen as the local subnet.

STEP 16 Choose the Remote Subnet IP address from the drop-down list. If the IP address is not present in the list, then choose **Create a New Address** option from the drop-down list.The Address - Add dialog box appears.

Figure 22 Site-to-Site VPN Wizard - Address - Add



Address - Add

* Name: branch_office

Type: Network

* IP Address: 192.168.1.0

Enter "0" in the IP address segment for a range of IP addresses.
For example, 192.168.1.0 indicates a range from 192.168.1.1 to 192.168.1.255.

* Netmask: 255.255.255.0

STEP 17 Enter the following information in the **Address - Add** dialog box:

a. Enter the name of the subnet in the **Name** field.

b. Select the Type from the **Network** drop-down list.

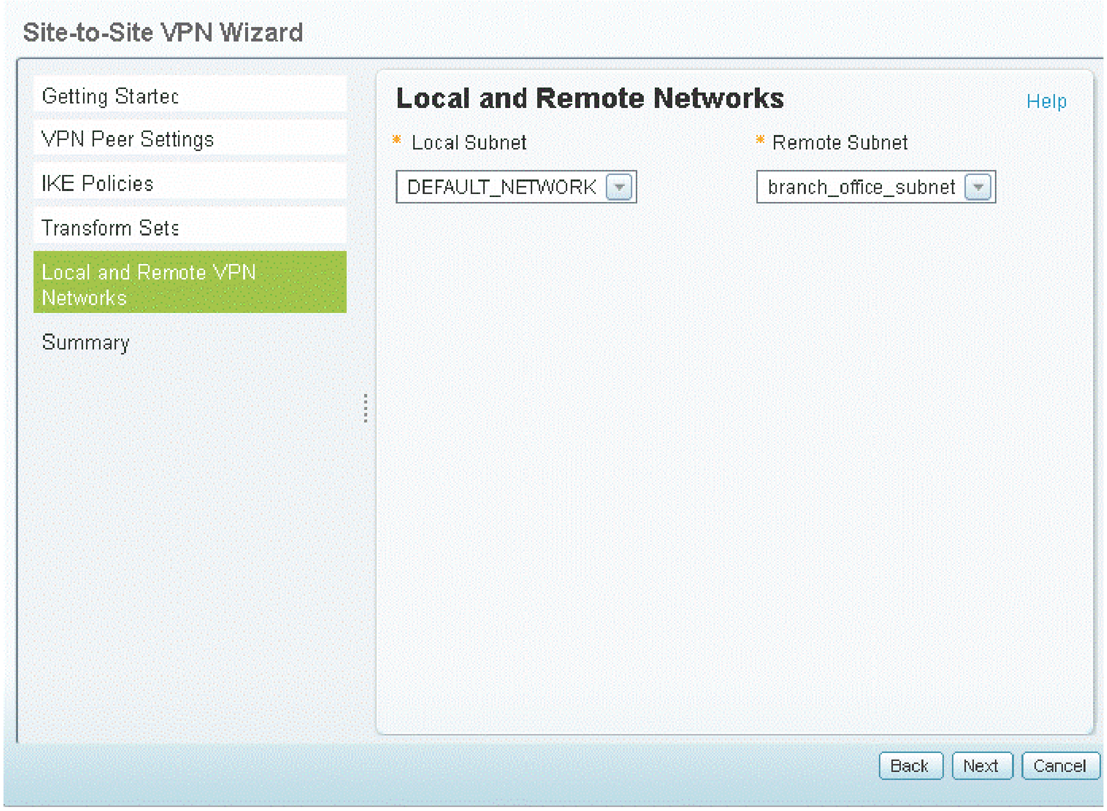
c. Enter the IP address in the **IP address** field.

NOTE In this example, the other peer is the branch office, which indicates that the remote IP address entered in the field is that of the branch office.

d. Enter the subnet mask in the **Netmask** field. In this example, the netmask is that of the branch office.

STEP 18 Click **Save**. The new subnet address is created for the network. In this example, the new remote subnet name is branch_office_subnet.

Figure 23 Site-to-Site VPN Wizard - Local and Remote Network



Site-to-Site VPN Wizard

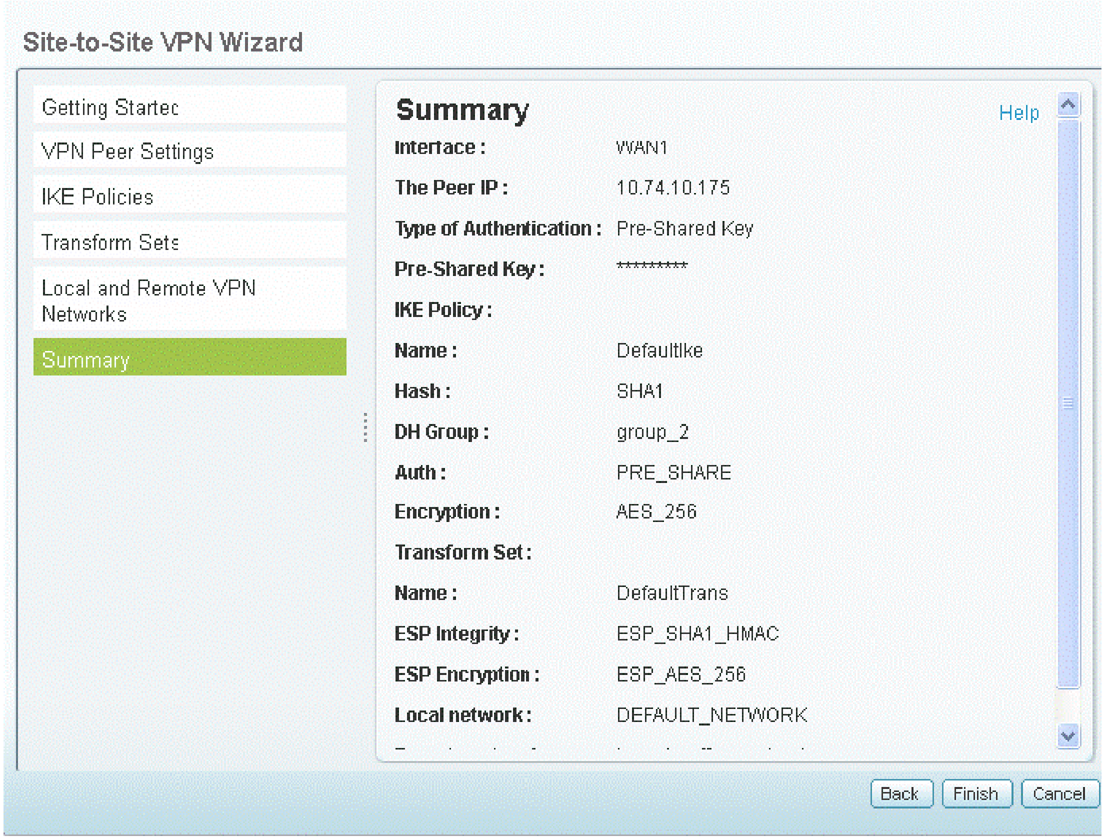
Local and Remote Networks

* Local Subnet: DEFAULT_NETWORK

* Remote Subnet: branch_office_subnet

STEP 19 Click **Next**. The Summary page appears.

Figure 24 Site-to-Site VPN Wizard - Summary



Summary

Interface :	WAN1
The Peer IP :	10.74.10.175
Type of Authentication :	Pre-Shared Key
Pre-Shared Key :	**********
IKE Policy :	
Name :	DefaultIke
Hash :	SHA1
DH Group :	group_2
Auth :	PRE_SHARE
Encryption :	AES_256
Transform Set :	
Name :	DefaultTrans
ESP Integrity :	ESP_SHA1_HMAC
ESP Encryption :	ESP_AES_256
Local network :	DEFAULT_NETWORK

STEP 20 To modify the configuration settings, click **Back**. If the configuration is correct, click **Finish** to apply the settings.

STEP 21 After you click **Finish**, this warning message appears, “Do you want to make this connection active when the settings are saved? (Only one connection can be active at a time.)”

- If you want to immediately activate the connection after the settings are saved, click Activate Connection. After you save your settings, the security appliance will immediately try to initiate the VPN connection.
- If you only want to create the IPsec VPN policy and do not want to immediately activate the connection after the settings are saved, click **Do Not Activate**. The connection will be triggered by any traffic that matches this Site-to-Site VPN policy and the VPN tunnel will be set up automatically. You can also go to the **VPN** > **Site-to-Site** > **IPsec Policies** page to manually establish the VPN connection by clicking the **Connect** icon.

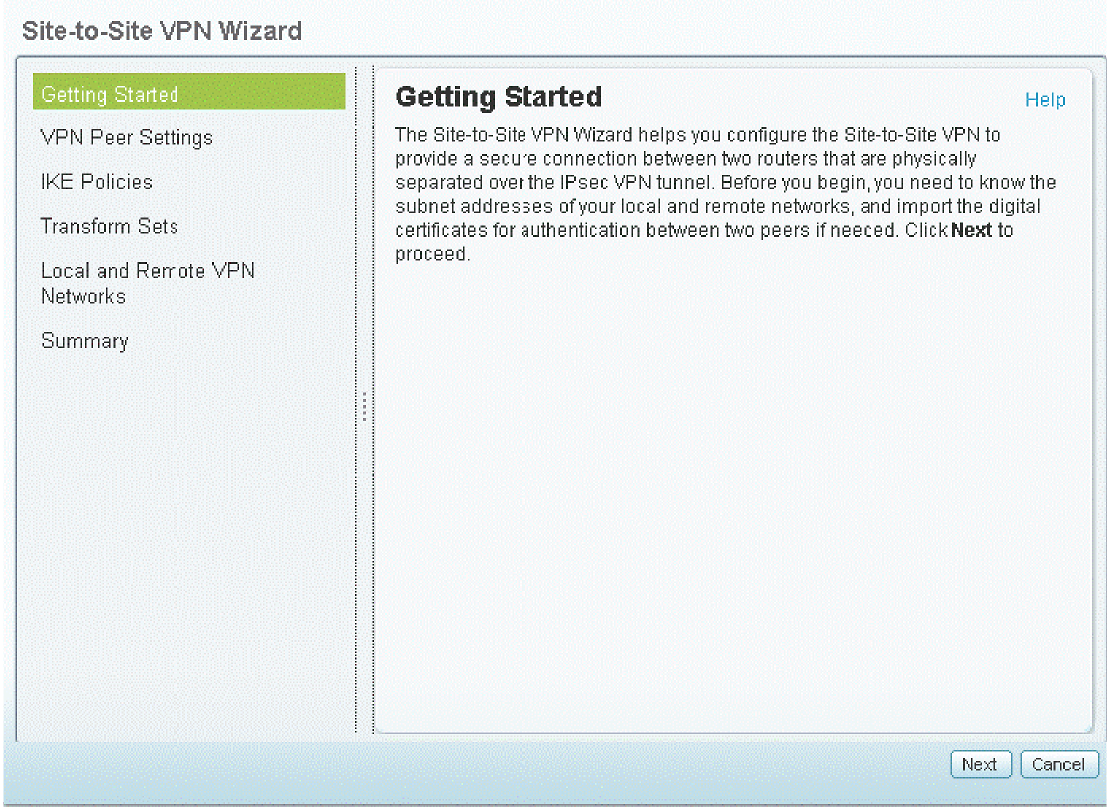
Cisco ISA500 Configuration for the Branch Office

After configuring the Site-to-Site VPN settings for the main office, you must also configure the VPN settings for the peer site. In this example the branch office acts as the peer site.

To configure the settings for the branch office, follow these steps:

STEP 1 From the ISA500 Configuration Utility, click **Configuration Wizards** > **Site-to-Site VPN Wizard**.

Figure 25 Site-to-Site VPN Wizard - Getting Started

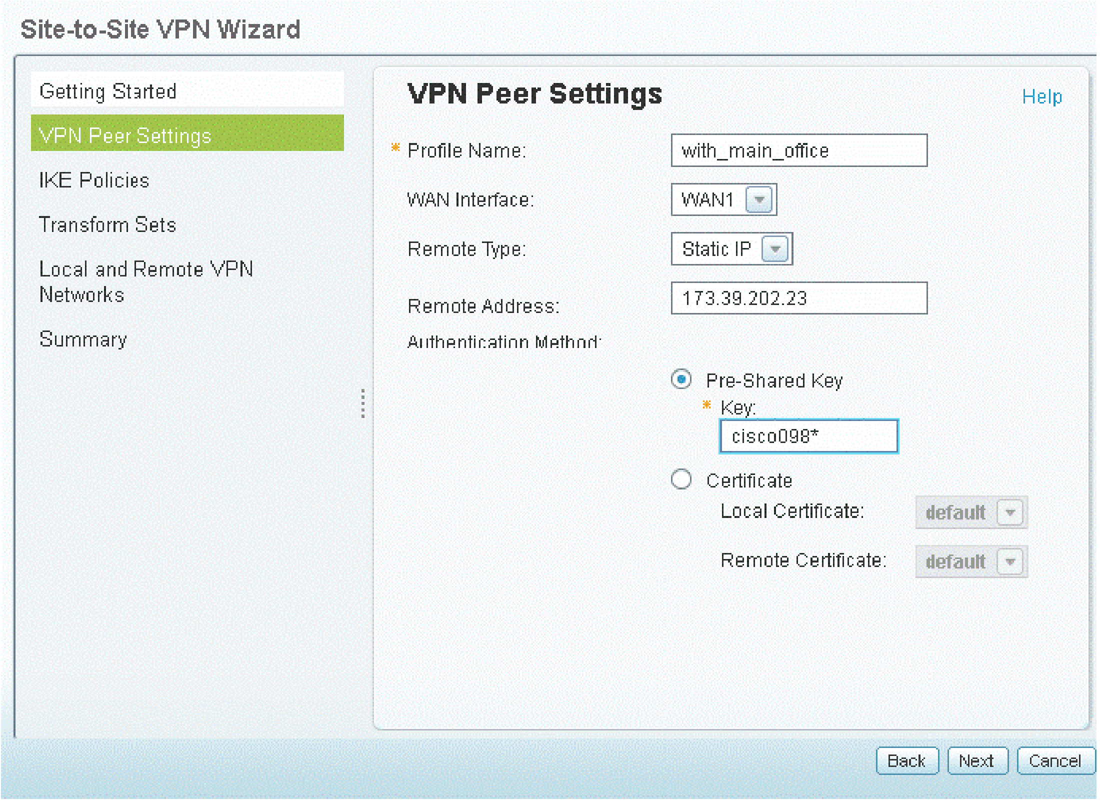


Getting Started

The Site-to-Site VPN Wizard helps you configure the Site-to-Site VPN to provide a secure connection between two routers that are physically separated over the IPsec VPN tunnel. Before you begin, you need to know the subnet addresses of your local and remote networks, and import the digital certificates for authentication between two peers if needed. Click **Next** to proceed.

STEP 2 Click **Next**. The VPN Peer Settings page appears.

Figure 26   Site-to-Site VPN Wizard - VPN Peer Settings



Site-to-Site VPN Wizard

VPN Peer Settings

* Profile Name:	with_main_office
WAN Interface:	WAN1
Remote Type:	Static IP
Remote Address:	173.39.202.23
Authentication Method:	

● Pre-Shared Key

* Key: cisco098*

○ Certificate

Local Certificate:	default
Remote Certificate:	default

STEP 3 Use the VPN Peer Settings page to configure an IPsec VPN policy for establishing the VPN connection with a remote router.

a. Enter the name of the VPN policy in the **Profile Name** field. In this example, the remote peer for the branch office is the main office.

b. Choose the WAN port from the **WAN Interface** drop-down list that traffic passes through the VPN tunnel.

c. Choose one of the following remote peers from the **Remote Type** drop-down list:

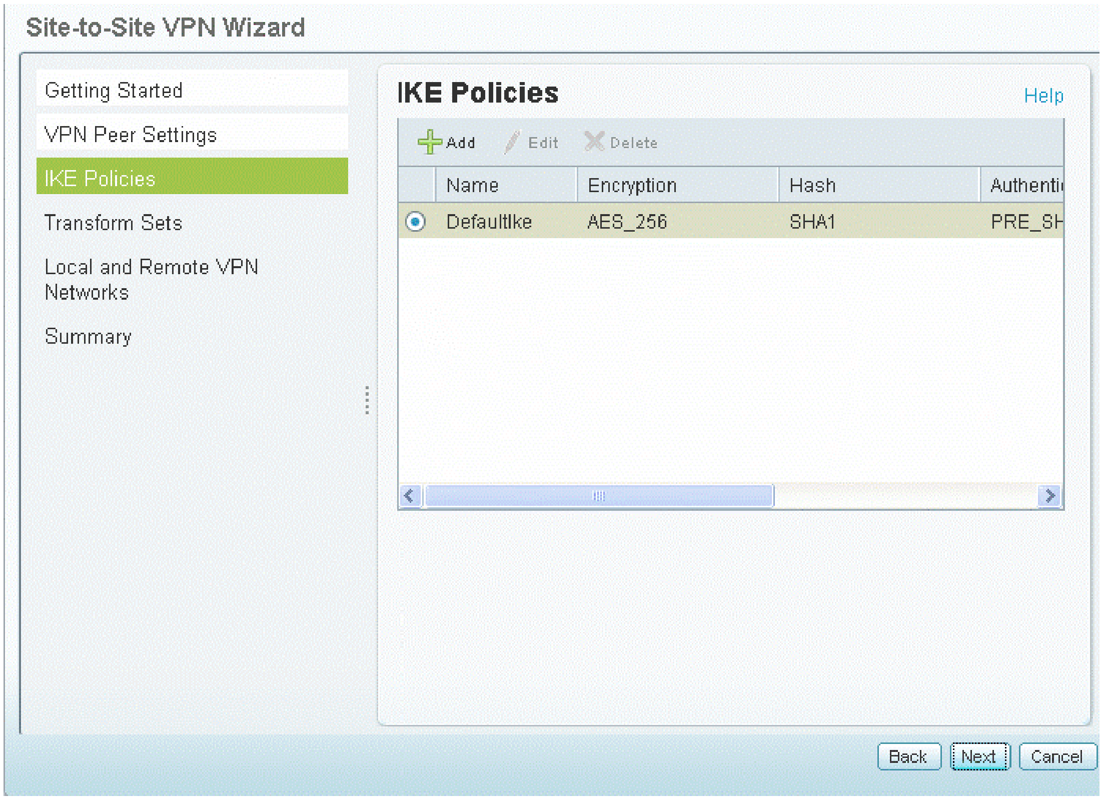
- Choose Static IP if the remote peer uses a static IP address. In this example, the remote peer in the main office uses a static IP.

- Enter the IP address of the remote device in the **Remote Address** field. In this example, the remote address is the IP address of the main office.

STEP 4 Choose the **Authentication Method**. This example uses pre-shared key for authentication.

STEP 5 Click **Next**. The IKE Policies page appears.

Figure 27 Site-to-Site VPN Wizard - IKE Policies



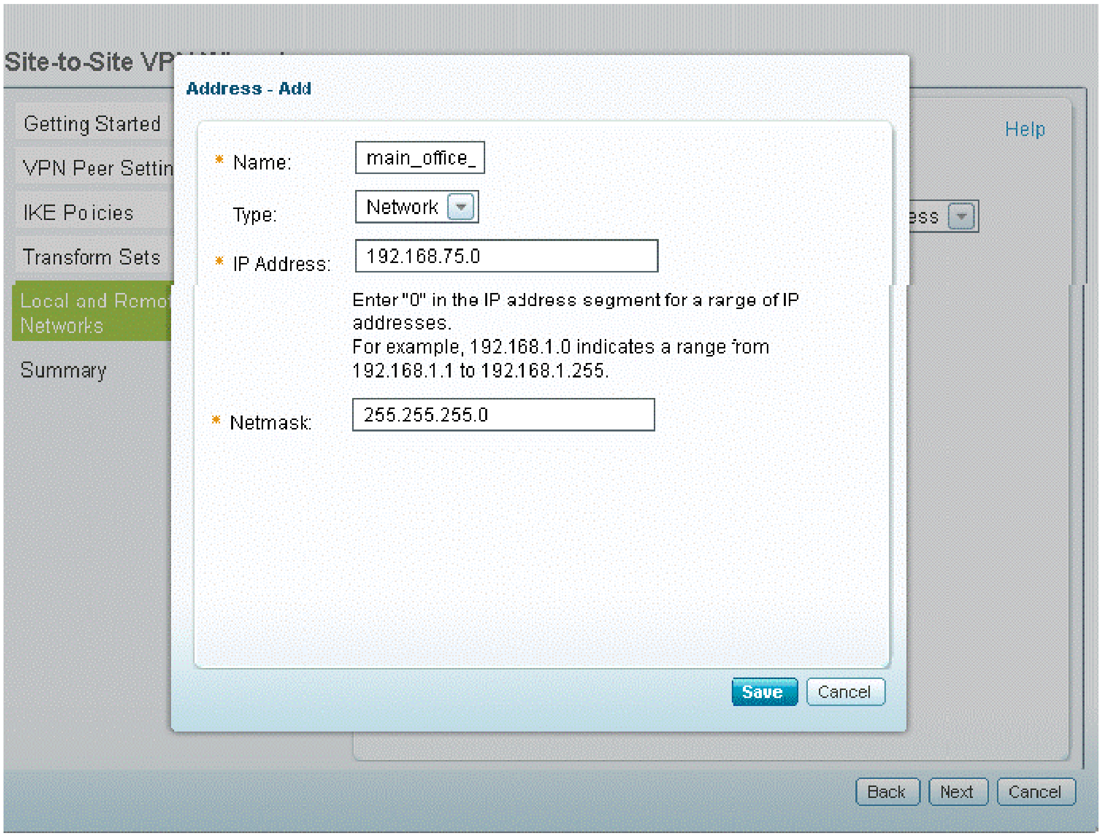
Site-to-Site VPN Wizard

IKE Policies

	Name	Encryption	Hash	Authenti
●	DefaultIke	AES_256	SHA1	PRE_SH

STEP 6 Follow Step 6 on page 24 to Step 16 on page 27 in the “Cisco ISA500 Configuration for the Main Office” section.

Figure 28   Site-to-Site VPN Wizard - Add



Address - Add

* Name: main_office_

Type: Network

* IP Address: 192.168.75.0

Enter "0" in the IP address segment for a range of IP addresses.
For example, 192.168.1.0 indicates a range from 192.168.1.1 to 192.168.1.255.

* Netmask: 255.255.255.0

STEP 7 Enter the following information in the **Address - Add** dialog box:

a. Enter the name of the subnet in the **Name** field.

b. Select the Type from the **Network** drop-down list.

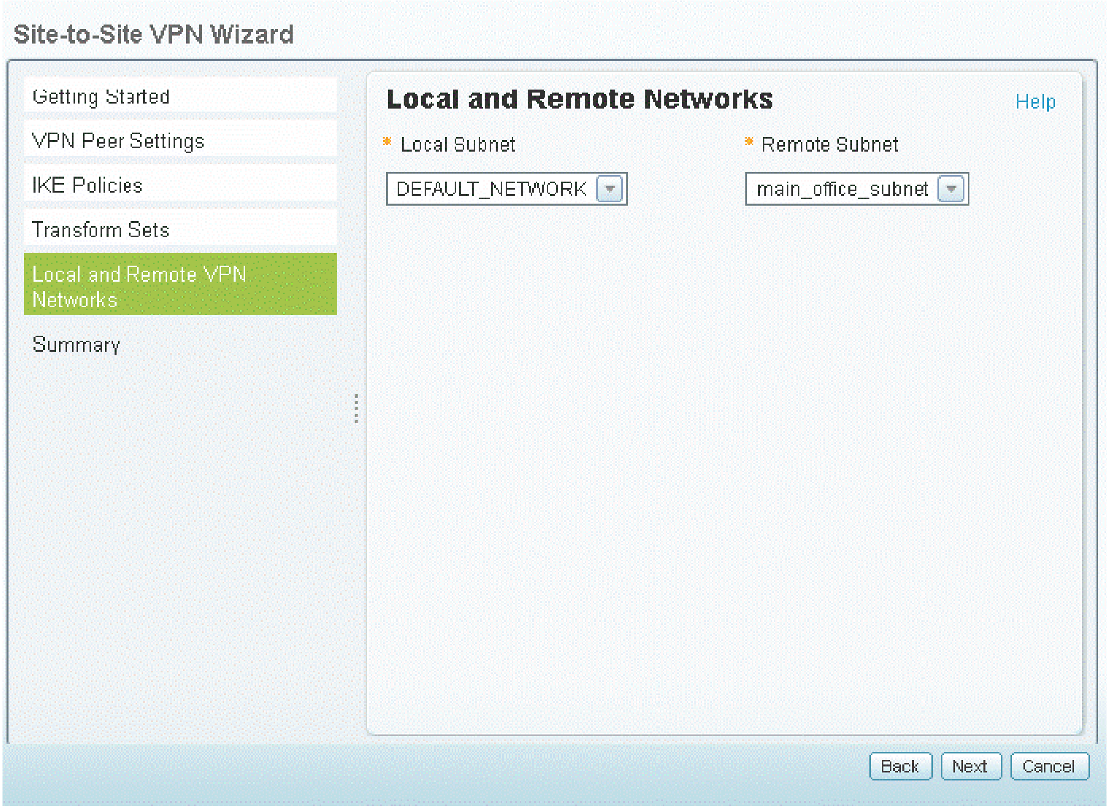
c. Enter the IP address in the **IP address** field.

NOTE In this example, the other peer is the main office; the remote IP address entered in the field is that of the main office.

d. Enter the subnet mask in the **Netmask** field. In this example, the netmask is that of the main office.

STEP 8 Click **Save**. The new subnet address is created for the network. In this example, the new remote subnet name is main_office_subnet.

Figure 29   Site-to-Site VPN Wizard - Local and Remote Networks


Site-to-Site VPN Wizard

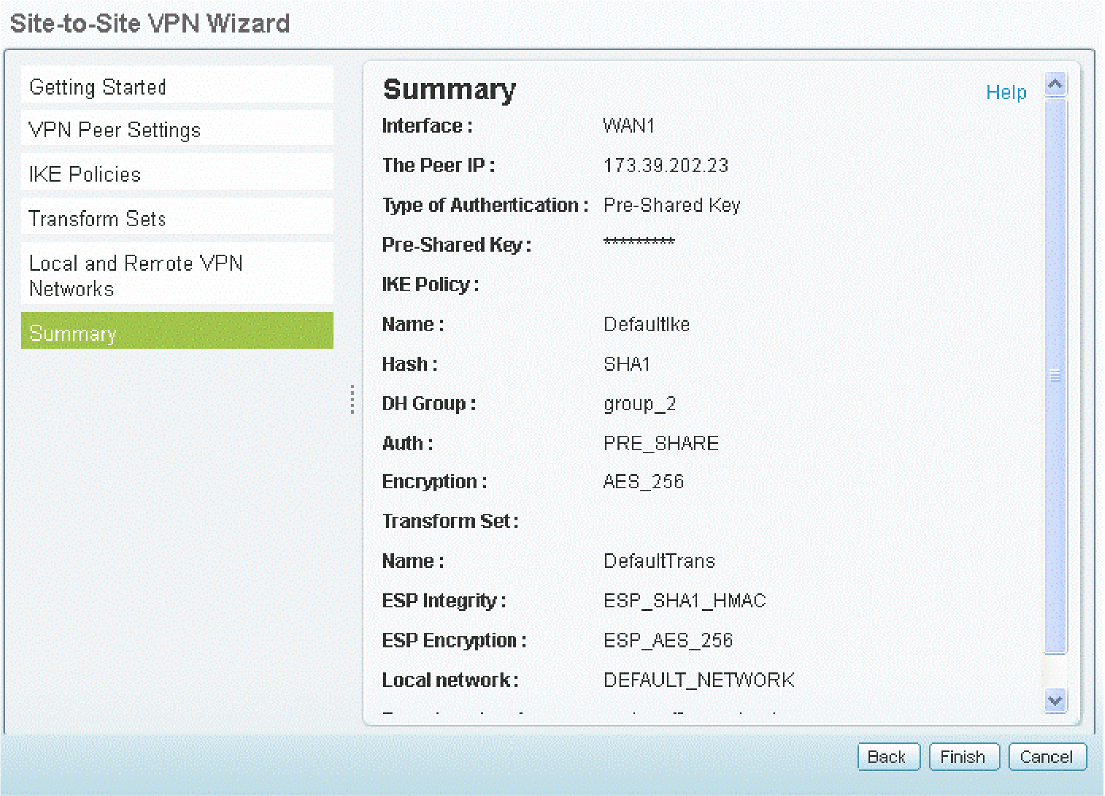
Local and Remote Networks

* Local Subnet: DEFAULT_NETWORK

* Remote Subnet: main_office_subnet

STEP 9 Click **Next**. The Summary page appears.

Figure 30 Site-to-Site VPN Wizard - Summary


Site-to-Site VPN Wizard

Summary

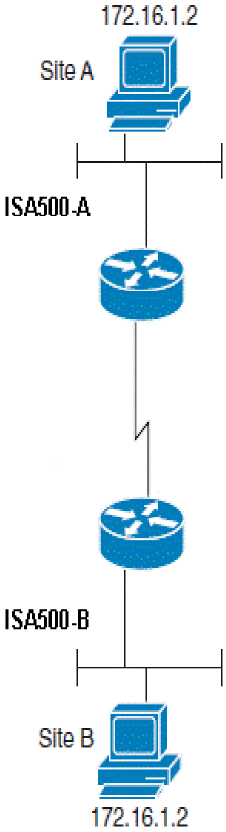
Interface :	WAN1
The Peer IP :	173.39.202.23
Type of Authentication :	Pre-Shared Key
Pre-Shared Key :	*********
IKE Policy :	
Name :	DefaultIke
Hash :	SHA1
DH Group :	group_2
Auth :	PRE_SHARE
Encryption :	AES_256
Transform Set :	
Name :	DefaultTrans
ESP Integrity :	ESP_SHA1_HMAC
ESP Encryption :	ESP_AES_256
Local network :	DEFAULT_NETWORK

This completes the site-to-site configuration settings in the example using the Site-to-Site VPN Wizard for two sites, the main office, and the branch office.

Configuring the Cisco ISA500 Security Appliance for Site-to-Site When the Networks Overlap

In this example, Site A and Site B both have same IP addresses assigned to them. For a site-to-site configuration, the ISA500-A and ISA500-B security appliances must be configured to different subnets at both ends.

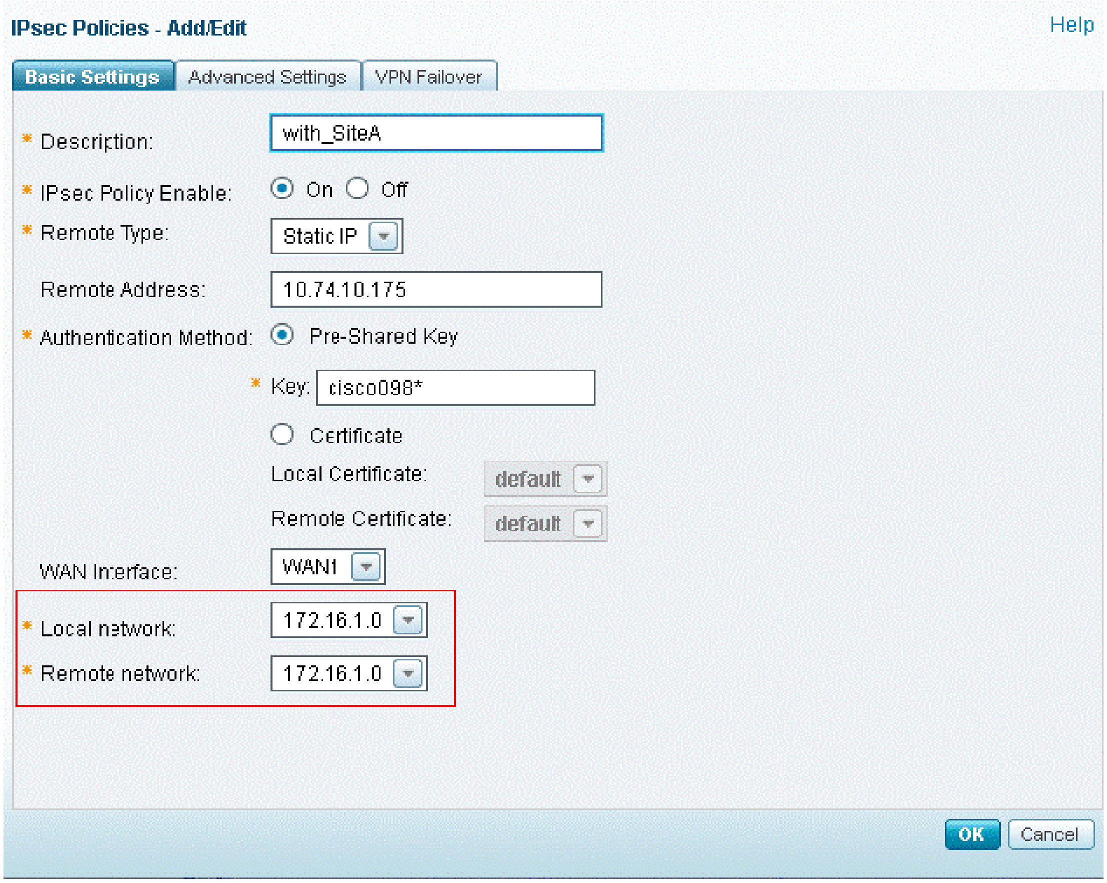
Figure 31 Network Overlap Configuration Example



Cisco ISA500-B Configuration

The following example shows the IPsec policy settings at Site B where both local networks and remote networks are set to the IP address 172.16.1.0/24.

Figure 32   IPsec Policies - Add/Edit



IPsec Policies - Add/Edit

* Description: with_SiteA

* IPsec Policy Enable: ● On ○ Off

* Remote Type: Static IP

Remote Address: 10.74.10.175

* Authentication Method: ● Pre-Shared Key

* Key: cisco098*

○ Certificate

Local Certificate: default

Remote Certificate: default

WAN Interface: WAN1

* Local network: 172.16.1.0

* Remote network: 172.16.1.0

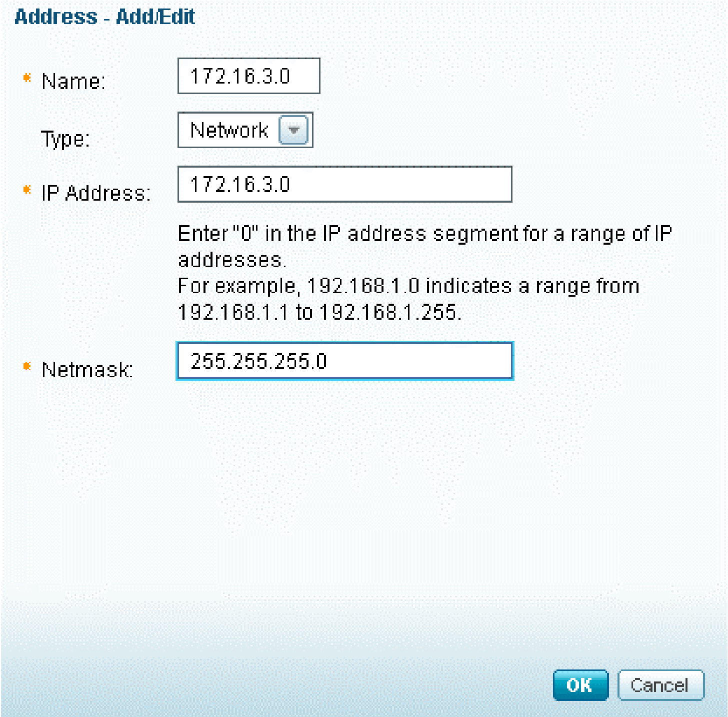
To configure different subnets for local and remote networks at Site B, follow these steps:

STEP 1 Click the **Advance Settings** tab.

STEP 2 Click **On** for Apply NAT Policies.

STEP 3 Click **Create a new address** to add a new address. The Address-Add/Edit window opens.

Figure 33 Address - Add/Edit



Address - Add/Edit

* Name: 172.16.3.0

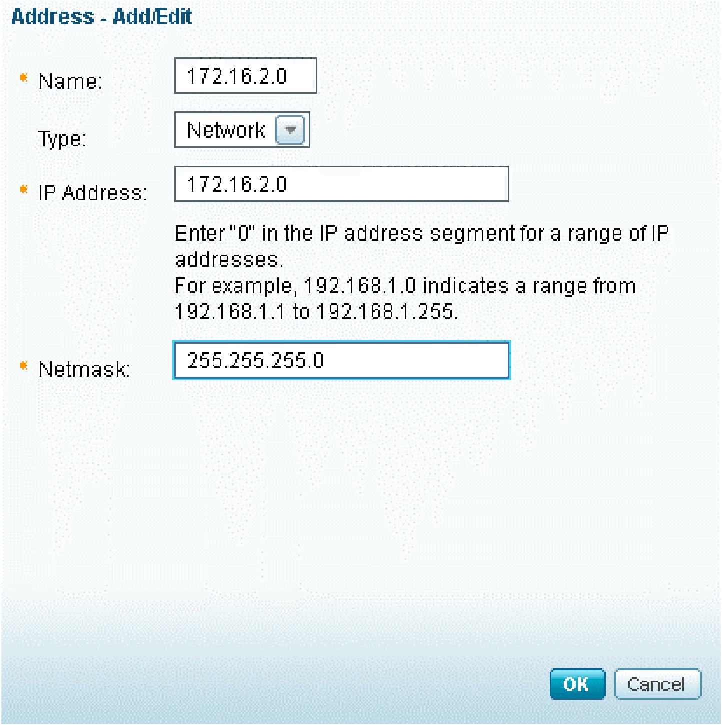
Type: Network

* IP Address: 172.16.3.0

Enter "0" in the IP address segment for a range of IP addresses.
For example, 192.168.1.0 indicates a range from 192.168.1.1 to 192.168.1.255.

* Netmask: 255.255.255.0

Figure 34 Address - Add/Edit



Address - Add/Edit

* Name: 172.16.2.0

Type: Network

* IP Address: 172.16.2.0

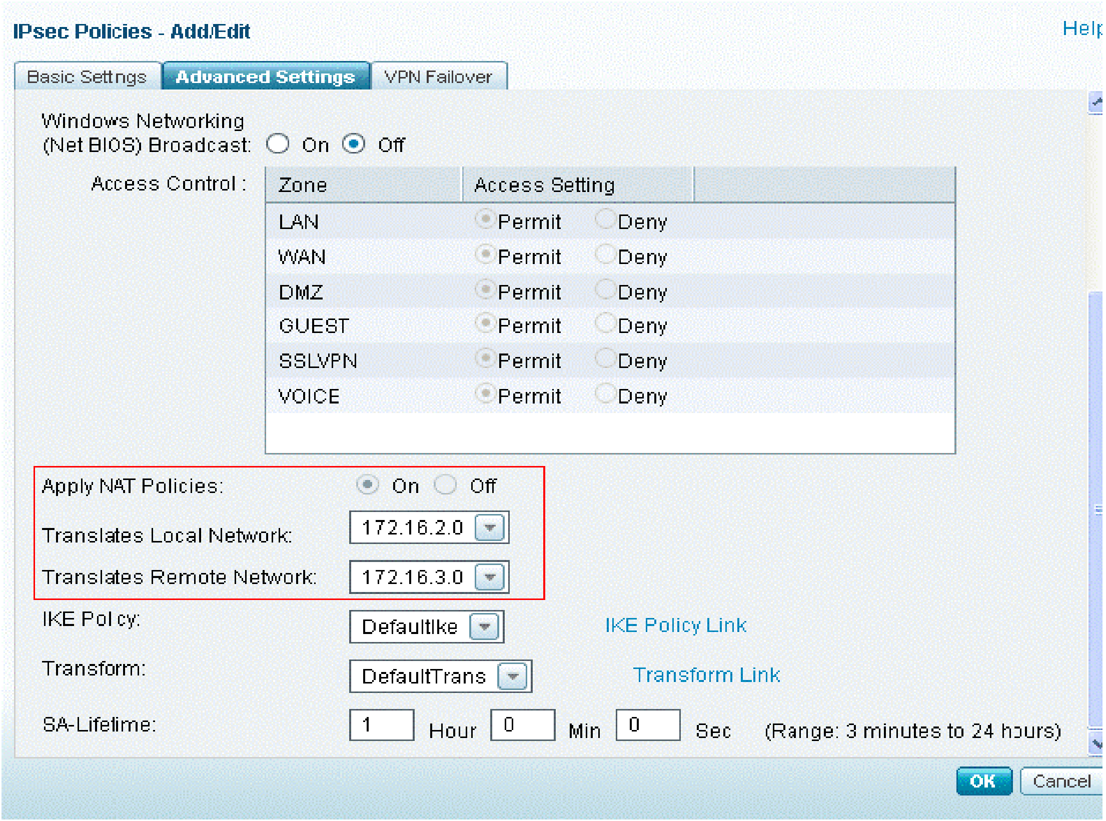
Enter "0" in the IP address segment for a range of IP addresses.
For example, 192.168.1.0 indicates a range from 192.168.1.1 to 192.168.1.255.

* Netmask: 255.255.255.0

STEP 4 Add the IP address for the local and remote networks. In this example, the IP addresses added are 172.16.2.0/24 and 172.16.3.0/24.

STEP 5 Click **OK**.

Figure 35 IPsec Policies - Add/Edit



Windows Networking (Net BIOS) Broadcast: ○ On ● Off

Access Control :

Zone	Access Setting	
LAN	● Permit	○ Deny
WAN	● Permit	○ Deny
DMZ	● Permit	○ Deny
GUEST	● Permit	○ Deny
SSLVPN	● Permit	○ Deny
VOICE	● Permit	○ Deny

Apply NAT Policies: ● On ○ Off

Translates Local Network: 172.16.2.0

Translates Remote Network: 172.16.3.0

IKE Policy: DefaultIke IKE Policy Link

Transform: DefaultTrans Transform Link

SA-Lifetime: 1 Hour 0 Min 0 Sec (Range: 3 minutes to 24 hours)

STEP 6 Choose the IP address that you want to assign, from the **Translates Local Network** drop-down list. In this example, 172.16.2.0 is set as the translated address.

STEP 7 Choose the IP address that you want to assign, from the **Translates Remote Network** drop-down list. In this example, 172.16.3.0 is set as the translated address.

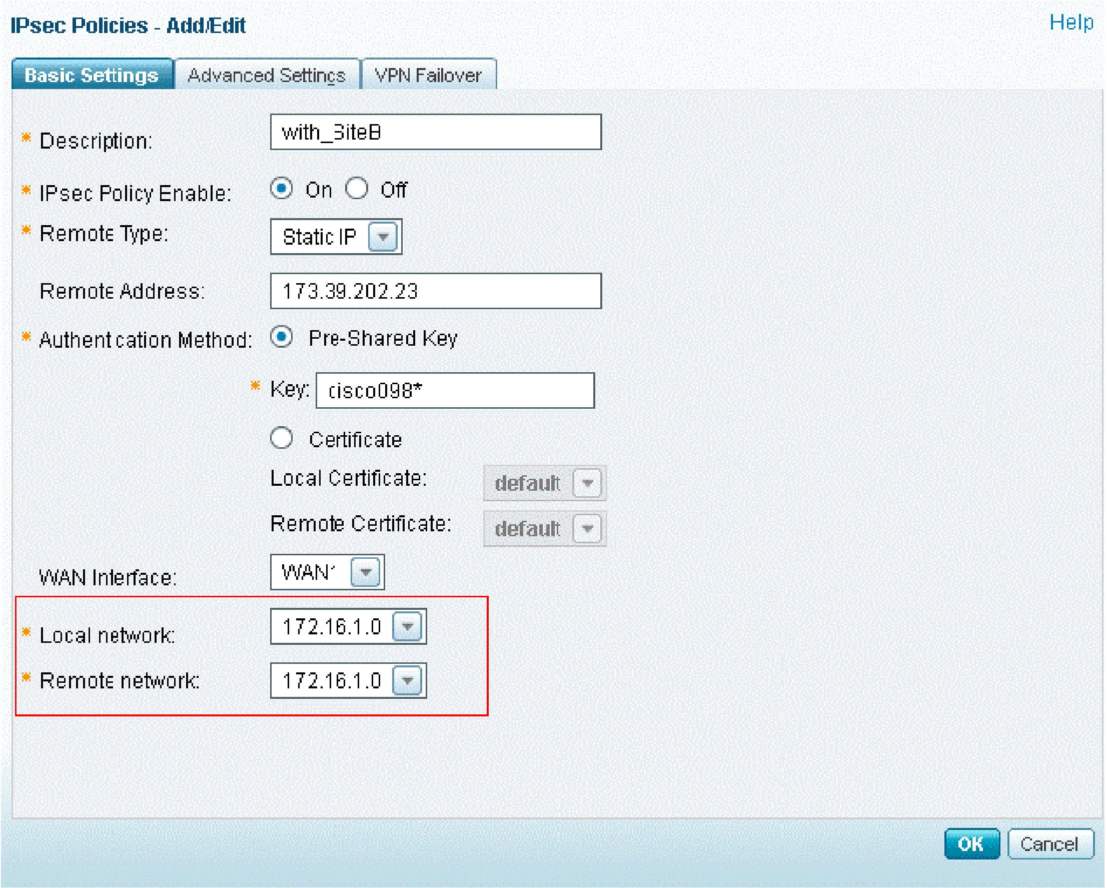
STEP 8 Click **OK**.

You must now configure the local and remote subnets for the peer site which is Site A in this example.

Cisco ISA500-A Configuration

The following example shows the IPsec policy settings at Site A where both local networks and remote networks are set to the IP address 172.16.1.0/24.

Figure 36 IPsec Policies - Add/Edit



IPsec Policies - Add/Edit

* Description: with_SiteB

* IPsec Policy Enable: ● On ○ Off

* Remote Type: Static IP

Remote Address: 173.39.202.23

* Authentication Method: ● Pre-Shared Key

* Key: cisco098*

○ Certificate

Local Certificate: default

Remote Certificate: default

WAN Interface: WAN1

* Local network: 172.16.1.0

* Remote network: 172.16.1.0

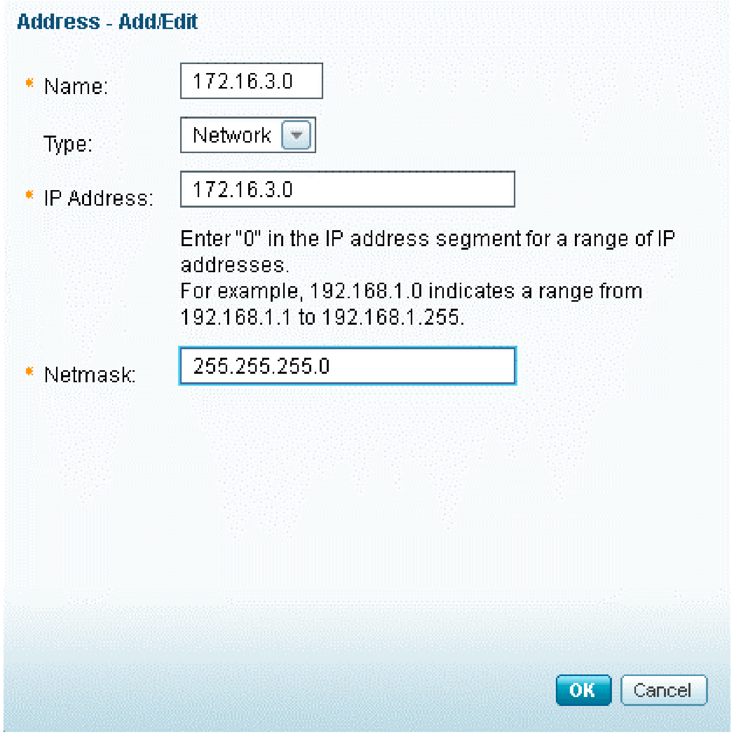
To configure different subnets for local and remote networks at Site B, follow these steps:

STEP 1 Click the **Advance Settings** tab.

STEP 2 Click **On** for Apply NAT Policies.

STEP 3 Click **Create a new address** to add a new address. The Address-Add/Edit window opens.

Figure 37 Address - Add/Edit



Address - Add/Edit

* Name: 172.16.3.0

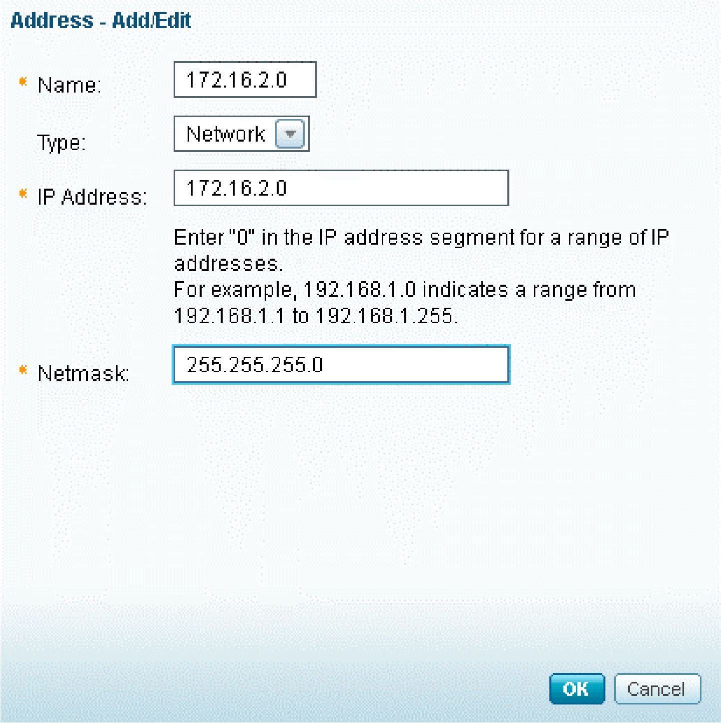
Type: Network

* IP Address: 172.16.3.0

Enter "0" in the IP address segment for a range of IP addresses.
For example, 192.168.1.0 indicates a range from 192.168.1.1 to 192.168.1.255.

* Netmask: 255.255.255.0

Figure 38 Address - Add/Edit



Address - Add/Edit

* Name: 172.16.2.0

Type: Network

* IP Address: 172.16.2.0

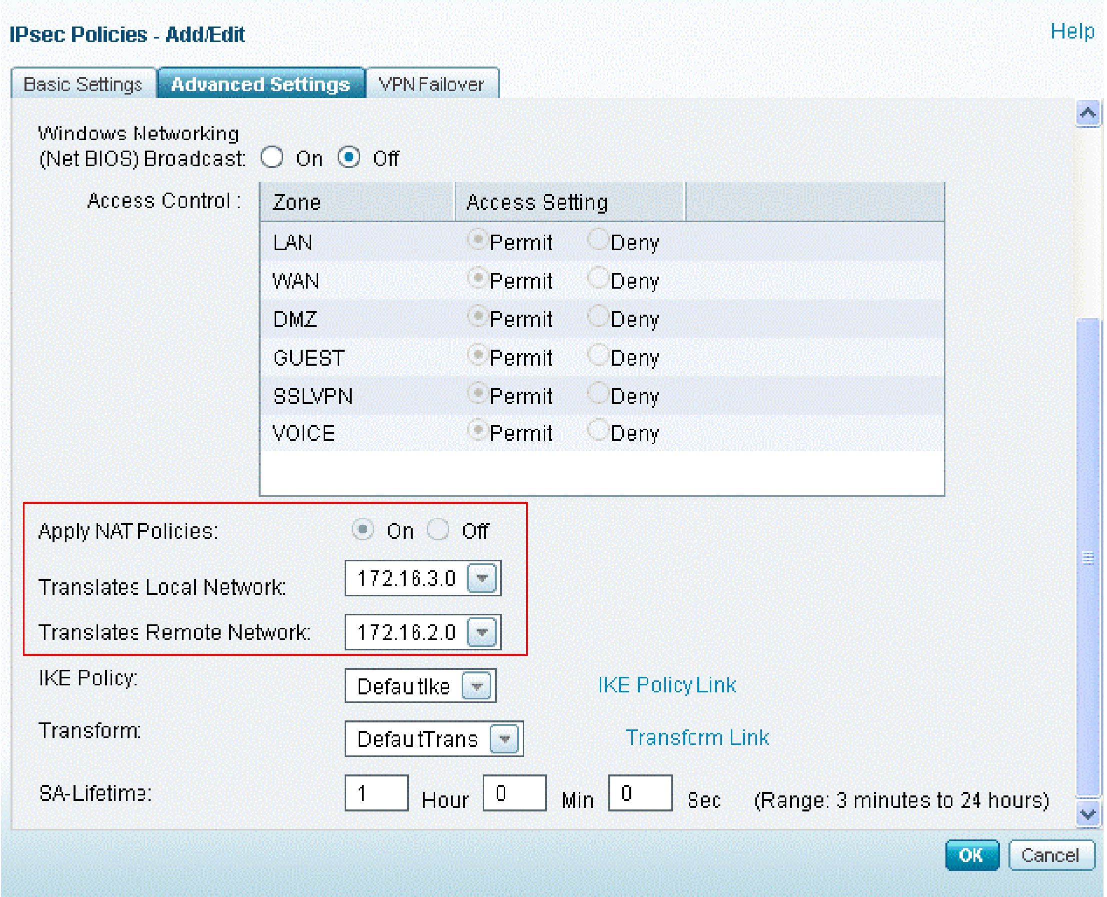
Enter "0" in the IP address segment for a range of IP addresses.
For example, 192.168.1.0 indicates a range from 192.168.1.1 to 192.168.1.255.

* Netmask: 255.255.255.0

STEP 4 Add the IP address for the local and remote networks.In this example, the IP addresses added are 172.16.2.0/24 and 172.16.3.0/24.

STEP 5 Click **OK**.

Figure 39 IPsec Policies - Add/Edit



IPsec Policies - Add/Edit

Windows Networking (Net BIOS) Broadcast: ○ On ● Off

Access Control :

Zone	Access Setting	
LAN	● Permit	○ Deny
WAN	● Permit	○ Deny
DMZ	● Permit	○ Deny
GUEST	● Permit	○ Deny
SSLVPN	● Permit	○ Deny
VOICE	● Permit	○ Deny

Apply NAT Policies: ● On ○ Off

Translates Local Network: 172.16.3.0

Translates Remote Network: 172.16.2.0

IKE Policy: Defau tIke

Transform: Defau tTrans

SA-Lifetime: 1 Hour 0 Min 0 Sec (Range: 3 minutes to 24 hours)

STEP 6 Choose the IP address that you want to assign, from the **Translates Local Network** drop-down list. In this example, 172.16.3.0 is set as the translated address.

STEP 7 Choose the IP address that you want to assign, from the **Translates Remote Network** drop-down list. In this example, 172.16.2.0 is set as the translated address.

NOTE Make sure that the local network subnet for Site B is the same as the remote network subnet in Site A. In this example, 172.16.3.0 is chosen as the remote network translated subnet for Site B and translated local network subnet for Site A.

STEP 8 Click **OK**.

Based on the modified site-to-site configuration of ISA500 in Site A and Site B, if Site B host 172.16.1.2 wants to access Site A host 172.16.1.2, it uses the destination IP address 172.16.3.2. Similarly, if Site A host 172.16.1.2 wants to access Site B host 172.16.1.2, it uses destination IP address 172.16.2.2.

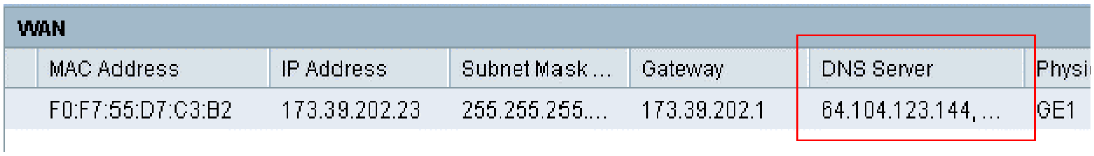
Configuring Split DNS

Split DNS directs DNS queries through the VPN tunnel for domains served by the internal DNS servers. These specific domains must be defined in the IPsec remote access policy. All other DNS queries are sent to the ISP DNS servers configured on the WAN interface. The Split DNS feature is available only when a split tunnel is enabled for the policy.

The following example explains the function of Split DNS:

In this example, Cisco ISA500 utility has the IP address 64.104.123.144 assigned as the DNS server from ISP on WAN1.

Figure 40 WAN Settings

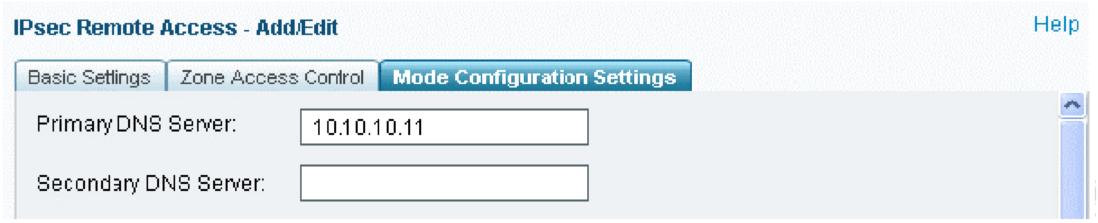


WAN

MAC Address	IP Address	Subnet Mask ...	Gateway	DNS Server	Physi
F0:F7:55:D7:C3:B2	173.39.202.23	255.255.255....	173.39.202.1	64.104.123.144, ...	GE1

The DNS server 10.10.10.11 is specified as the Primary DNS in the IPsec remote access group policy.

Figure 41 Mode Configuration Settings - Primary DNS Server



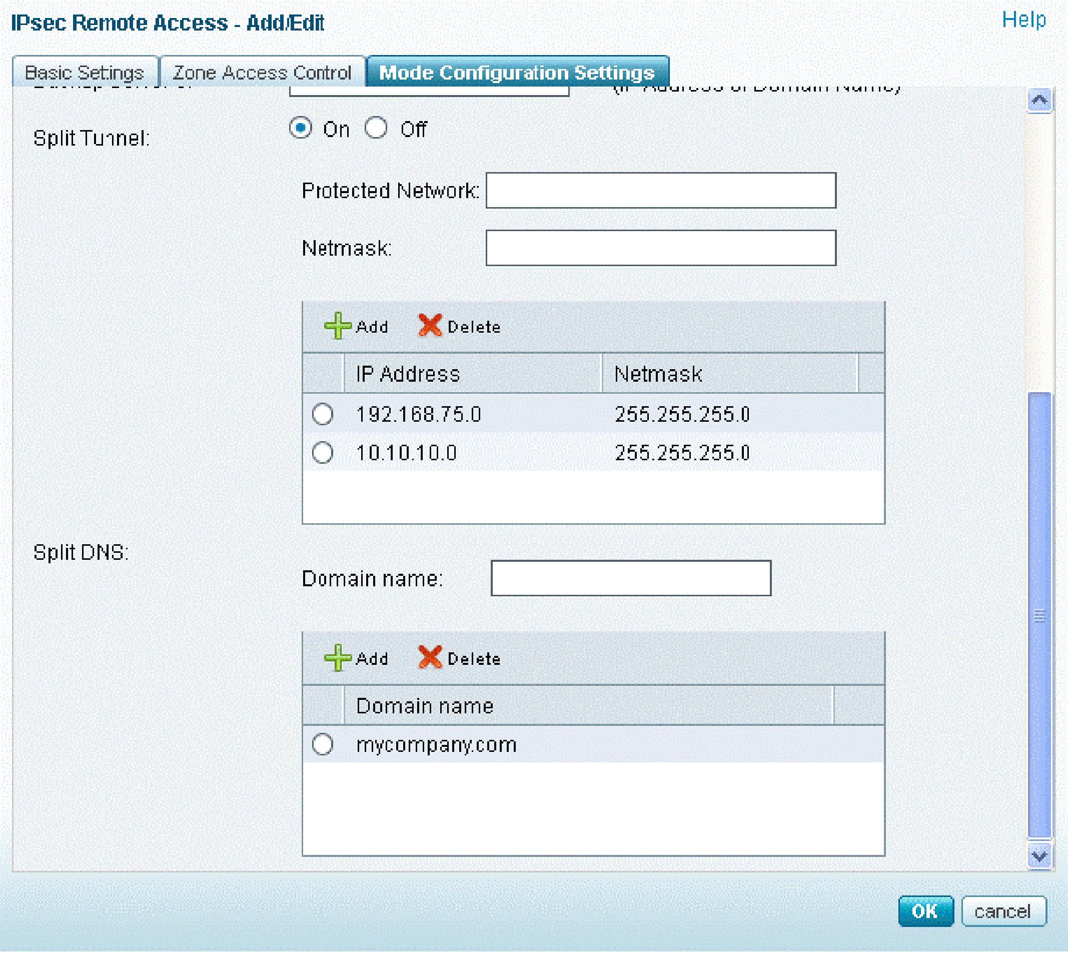
IPsec Remote Access - Add/Edit

Primary DNS Server: 10.10.10.11

Secondary DNS Server:

The domain name mycompany.com is added to the Split DNS settings. Because this domain is not a public domain name the DNS server 64.104.123.144 cannot resolve it. As per the settings, the IPsec VPN client thus sends DNS queries for mycompany.com to 10.10.10.11 (which is the Primary DNS server), and all the other DNS queries to 64.104.123.144 (DNS server from the ISP).

Figure 42 IPsec Remote Access - Add/Edit



Split Tunnel: ● On ○ Off

Protected Network:

Netmask:

Add Delete

	IP Address	Netmask
○	192.168.75.0	255.255.255.0
○	10.10.10.0	255.255.255.0

Split DNS:

Domain name:

Add Delete

	Domain name
○	mycompany.com

To configure Split DNS for an IPsec remote access policy, follow these steps:

STEP 1 On the ISA500 utility page, click **VPN** > **IPSec Remote Access**.

STEP 2 To add an IPsec Remote Access policy, click **Add**.

Other options: To edit the configuration settings for a policy, click **Edit** (pencil icon). To delete a policy, click **Delete** (cross icon).

STEP 3 Enter the information in the **Basic Settings** tab.

STEP 4 Enter the information in the **Zone Access Control** tab.

STEP 5 In the **Mode Configuration Settings** tab:

a. Enter the IP addresses of the DNS Server, WNS Server, and Backup Server. In this example, 10.10.10.11 is the Primary DNS configured for the policy.

b. Click **On** to enable the split tunneling feature.

c. To add the split subnets, enter the IP address and netmask in the **Protected Network** and **Netmask** fields.

NOTE You must enable the split tunnel feature and add the subnets to configure Split DNS.

d. In the Split DNS section, specify the domain that should be resolved by your network DNS server. Enter the domain name in the **Domain Name** field and click **Add**. In this example, mycompany.com is the domain name that must be resolved by the Primary DNS Server 10.10.10.11.

e. Click **OK**.

f. Click **Save**.

Configuring Split DNS in a Site-to-Site Setup

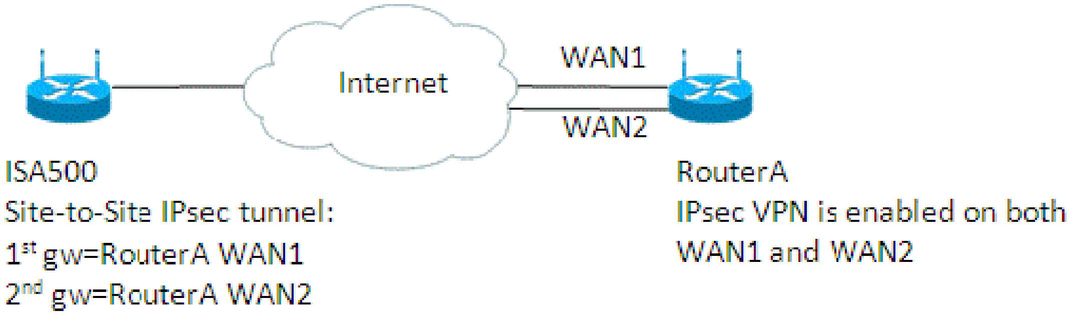
Split DNS feature is not supported in a site-to-site setup.

Configuring Redundant VPN

Redundant VPN allows Cisco ISA500 to establish another tunnel if the default tunnel is down.

In the following example, the Cisco ISA500 initially establishes a tunnel with RouterA WAN1. At some point, if RouterA WAN 1 stops working, then the tunnel also goes down. To create another tunnel, the Cisco ISA500 now tries to establish the tunnel with RouterA WAN2.

Figure 43 Redundant VPN Configuration



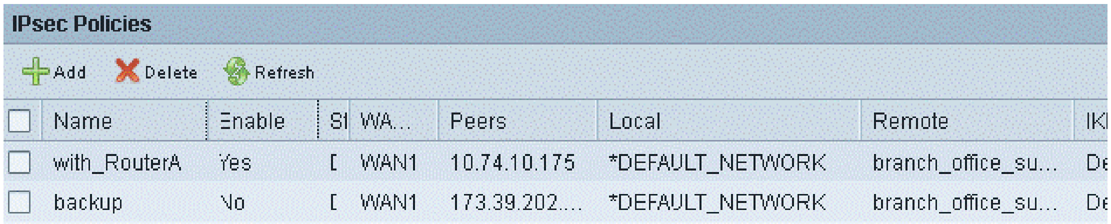
To configure the redundant VPN policy, follow these steps:

STEP 1 Create two IPsec policies with two different peers.

In this example in Figure 44, the two policies created are with_RouterA and backup. Note that the peers for the two policies are different. The first policy uses the IP address for RouterA WAN1 while the second policy uses the IP address for RouterA WAN2 as peers.

NOTE You can enable only one policy at a time.

Figure 44 IPsec Policies

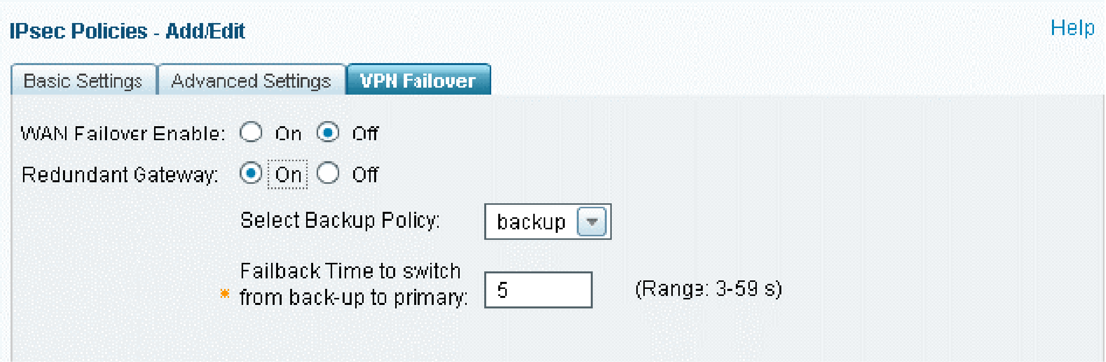


□	Name	Enable	St	WA...	Peers	Local	Remote	IK
□	with_RouterA	Yes	[	WAN1	10.74.10.175	*DEFAULT_NETWORK	branch_office_su...	De
□	backup	No	[	WAN1	173.39.202....	*DEFAULT_NETWORK	branch_office_su...	De

STEP 2 Select the backup policy. To select the backup policy:

a. Choose the policy for which you want to select the backup policy and click **Edit** (pencil icon). In the example in Figure 44, you click **Edit** for the policy with_RouterA. The IPsec Policies - Add/Edit window appears.

Figure 45 IPsec Policies - Add/Edit



WAN Failover Enable: ○ On ● Off

Redundant Gateway: ● On ○ Off

Select Backup Policy: backup

* Failback Time to switch from back-up to primary: 5 (Range: 3-59 s)

b. Click **On** to enable the Redundant Gateway.

c. Choose the policy that you want to set as the backup from the **Select Backup Policy** drop-down list. In this example, backup is chosen from the drop-down list.

Checking the Status of VPN Tunnels

To check the status of VPN tunnels, follow this step:

On the ISA500 utility, click **VPN** > **VPN Status** > **IPSec VPN Status**.

Using the VPN Passthrough Feature

The VPN Passthrough feature allows or denies traffic from internal hosts to pass through your security appliance and initiate VPN connections. You can specify the following types of traffic that can pass through your security appliance:

- Layer-2 Tunneling Protocol (L2TP)
- Point-to-Point Tunneling Protocol (PPTP)
- Internal Protocol Security (IPsec)

The VPN Passthrough feature is enabled by default.

Setting Up Firewall Policies for VPN Zones

For default firewall rules, see the “Default Firewall Settings” section in the *Configuring a Zone-Based Firewall on the Cisco ISA500 Security Appliance Application Note* at www.cisco.com/en/US/products/ps11752/prod_technical_reference_list.html

To set up firewall policies for a VPN zone, see Restricting Remote VPN Clients to Access Only Specific Networks and Servers, page 4.

Troubleshooting IPsec Tunnel Setup

- If tunnel does not come up, what do you look for in the logs?

  To troubleshoot IPsec tunnel setup:

  - Check log facility for Site-to-Site IPsec VPN.
  - Check log facility for IPsec Remote Access.
  - Check log facility for User if connection fails due to authentication failure.

  See the following sample error syslog from IPsec VPN:

  Term definitions in example:

  tunnelname: name of policy.

  netA, netB: subnet of the policy.

  Num: a number.

  FName: FQDN.

```
"tunnelname" received and failed on unknown informational message
Informational Exchange is for an unknown (expired?)
encrypted Informational Exchange message is invalid, key is unknown?
Informational Exchange message is invalid, unknown Message
Informational Exchange message is invalid, previously used Message
Informational Exchange message must be encrypted
Quick Mode message is invalid, unknown Initiator Cookie
Quick Mode message is invalid, unknown Responder Cookie
Quick Mode message is invalid, unknown Message
Quick Mode message is for a non-existent (expired?)
Quick Mode message is unacceptable, incomplete ISAKMP SA
Quick Mode I1 message is unacceptable, perhaps this is a duplicated
packet
"tunnelname" unable to locate private key for RSA Signature
"tunnelname" failed to build notification in send_notification
"tunnelname" failed to build notification
Cannot respond to IPsec SA request because no connection is known
"tunnelname":No acceptable response, possible authentication failure
"tunnelname":No response (or no acceptable response) to our first IKE
message
"tunnelname": No acceptable response, peer's network (local:netA,
remote:netB) mismatch with remote site
Max number of retransmissions (Num) reached
Failed to convert 'FName' at load time
Certificate rejected
Error in certificate crl
No crl from issuer
DPD: There is no response from peer
```

- When a tunnel comes up successfully, what do you see in the logs?

  See the following sample syslog for Site-to-Site IPsec VPN:

```
2000-01-03 00:50:27 - Info - Site-to-Site VPN: msg=with_RouterA IPsec SA
established tunnel mode; (pluto)
2000-01-03 00:50:27 - Info - Site-to-Site VPN: msg=with_RouterA tunnel
up; (vpn-up)
2000-01-03 00:50:27 - Info - Site-to-Site VPN: msg=Dead Peer Detection
enabled; (pluto)
2000-01-03 00:50:27 - Info - Site-to-Site VPN: msg=with_RouterA Respond
to Quick Mode proposal; (pluto)
2000-01-03 00:50:27 - Debug - Site-to-Site VPN: msg=the peer proposed:
192.168.75.0/24 -> 192.168.1.0/24; (pluto)
2000-01-03 00:50:26 - Info - Site-to-Site VPN: msg=Dead Peer Detection
enabled; (pluto)
2000-01-03 00:50:26 - Info - Site-to-Site VPN: msg=with_RouterA
responding to Main Mode; (pluto)
2000-01-03 00:50:26 - Info - Site-to-Site VPN: msg=Tunnel with_RouterA
initiate attempt; (vpn-down)
2000-01-03 00:50:26 - Debug - Site-to-Site VPN: msg=find_host_connection
returns Tunnel0; (pluto)
2000-01-03 00:47:25 - Debug - Site-to-Site VPN: msg=Set all policies with
NetBIOS done; (rcConfd)
2000-01-03 00:47:25 - Debug - Site-to-Site VPN: msg=Set all policies with
overlap ip done; (rcConfd)
```

  See the following sample syslog for IPsec Remote Access VPN:

```
2000-01-03 00:56:09 - Info - IPsec Remote Access: msg=[IPsec Remote
Access][pluto]  IPsec SA established tunnel mode; (pluto)
2000-01-03 00:56:09 - Info - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] Dead Peer Detection enabled; (pluto)
2000-01-03 00:56:08 - Info - IPsec Remote Access: msg=[IPsec Remote
Access][pluto]  Respond to Quick Mode proposal; (pluto)
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] the peer proposed: 0.0.0.0/0 -> 192.168.11.2/32; (pluto)
2000-01-03 00:56:08 - Info - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] Dead Peer Detection enabled; (pluto)
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] modecfg_inR0(STF_OK); (pluto)
2000-01-03 00:56:08 - Info - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] Assign a virtual IP address (192.168.11.2); (pluto)
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] Unsupported MODECFG attribute CISCO_DDNS_HOSTNAME
received.; (pluto)
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] Unsupported MODECFG attribute CISCO_FW_TYPE received.;
(pluto)
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] Unsupported MODECFG attribute APPLICATION_VERSION
received.; (pluto)
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] Unsupported MODECFG attribute 28684?? received.; (pluto)
```

```
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] MODECFG attribute 'CISCO_BACKUP_SERVER' received.;
(pluto)
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] Unsupported MODECFG attribute 28683?? received.; (pluto)
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] Unsupported MODECFG attribute CISCO_DO_PFS received.;
(pluto)
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] MODECFG attribute 'CISCO_SPLIT_DNS' received.; (pluto)
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] MODECFG attribute 'CISCO_SPLIT_INC' received.; (pluto)
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] MODECFG attribute 'CISCO_DEF_DOMAIN' received.; (pluto)
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] MODECFG attribute 'CISCO_SAVE_PW' received.; (pluto)
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] Unsupported MODECFG attribute CISCO_BANNER received.;
(pluto)
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] Unsupported MODECFG attribute INTERNAL_ADDRESS_EXPIRY
received.; (pluto)
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] MODECFG attribute 'INTERNAL_IP4_NBNS' received.; (pluto)
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] MODECFG attribute 'INTERNAL_IP4_DNS' received.; (pluto)
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] MODECFG attribute 'INTERNAL_IP4_NETMASK' received.;
(pluto)
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] MODECFG attribute 'INTERNAL_IP4_ADDRESS' received.;
(pluto)
2000-01-03 00:56:08 - Debug - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] modecfg_inR0; (pluto)
2000-01-03 00:56:07 - Info - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] Dead Peer Detection enabled; (pluto)
2000-01-03 00:56:07 - Info - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] User ezvpn_user: Authentication Successful; (pluto)
2000-01-03 00:56:07 - Info - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] User ezvpn_user: Attempting to login; (pluto)
2000-01-03 00:55:57 - Info - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] Sending Username/Password request; (pluto)
2000-01-03 00:55:57 - Info - IPsec Remote Access: msg=[IPsec Remote
Access][pluto] Dead Peer Detection enabled; (pluto)
```

- See the following sample syslog for user authentication:

```
2000-01-03 00:56:07 - Info - User:
user=ezvpn_user;from=ezvpn;result=success (pluto)
```

For More Information

Product Resources	
Product Documentation	www.cisco.com/en/US/products/ps11752/prod_technical_reference_list.html
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
Cisco Small Business Firmware Downloads	www.cisco.com/go/software
Cisco Partner Central for Small Business (Partner Login Required)	www.cisco.com/web/partners/sell/smb
Cisco Small Business Home	www.cisco.com/smb

OL-28506-01