ITCorporation

SONICWALL®

• SecureFirst •

Configuring a Tunnel Interface VPN with DHCP Relay using IP Helper

KNOWLEDGE

DATABASE

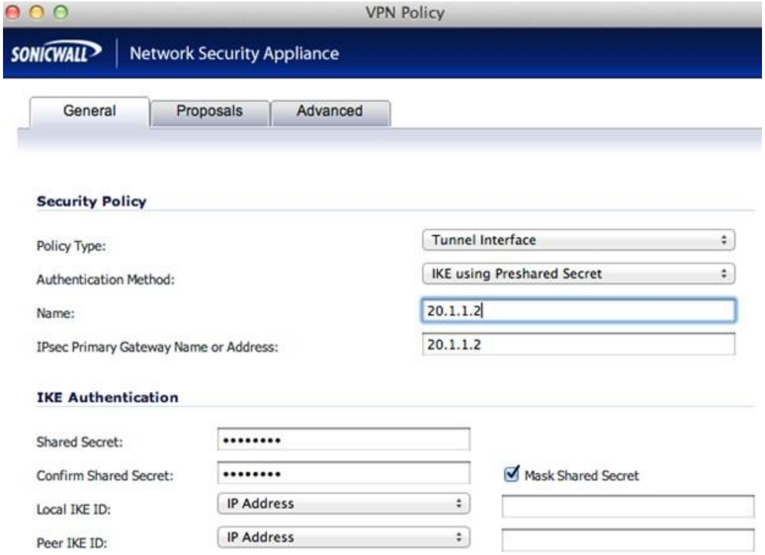
Configuring a Tunnel Interface VPN with DHCP Relay using IP Helper

Step 1: Configure the Tunnel Interface VPN Policy on each unit. This is done under VPN > Settings.

On the General tab of the new VPN Policy configuration window, configure the following settings.

- Policy Type: Tunnel Interface
- Authentication Method: IKE using Preshared Secret
- Name: Enter a desired policy name
- IPSec Primary Gateway Name/Address: Enter the remote unit's WAN IP.
- Enter a shared secret that will be used on each side of the tunnel.

General tab (Central site):



Security Policy

Policy Type: Tunnel Interface

Authentication Method: IKE using Preshared Secret

Name: 20.1.1.2

IPsec Primary Gateway Name or Address: 20.1.1.2

IKE Authentication

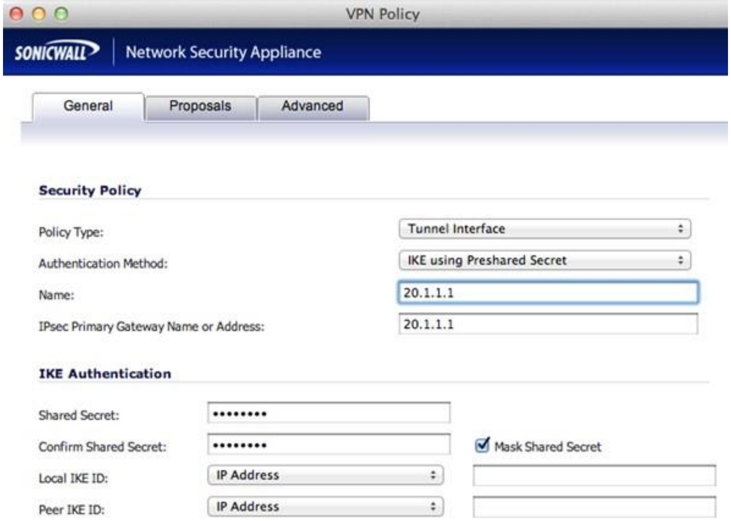
Shared Secret: ••••••••

Confirm Shared Secret: •••••••• ☑ Mask Shared Secret

Local IKE ID: IP Address

Peer IKE ID: IP Address

General tab (Remote site):



Security Policy

Policy Type: Tunnel Interface

Authentication Method: IKE using Preshared Secret

Name: 20.1.1.1

IPsec Primary Gateway Name or Address: 20.1.1.1

IKE Authentication

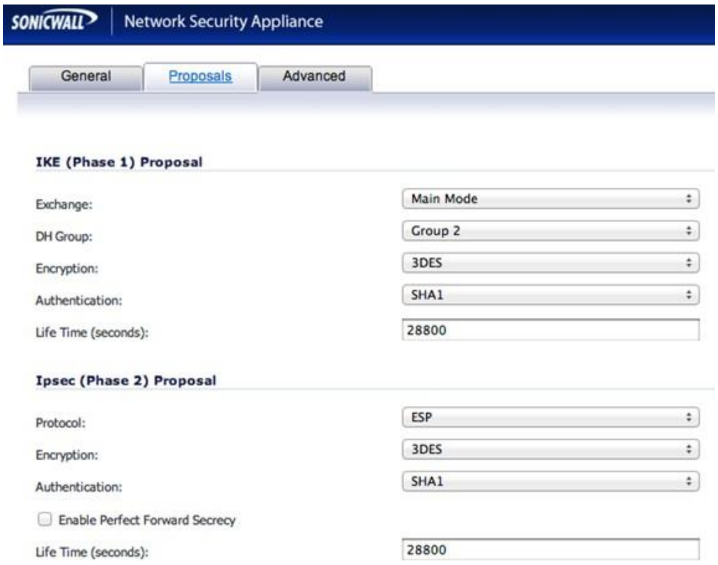
Shared Secret: ••••••••

Confirm Shared Secret: •••••••• ☑ Mask Shared Secret

Local IKE ID: IP Address

Peer IKE ID: IP Address

Enter your desired Proposal settings on each side of the tunnel. An example of the **Proposals** tab is shown below:



IKE (Phase 1) Proposal

Exchange: Main Mode

DH Group: Group 2

Encryption: 3DES

Authentication: SHA1

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP

Encryption: 3DES

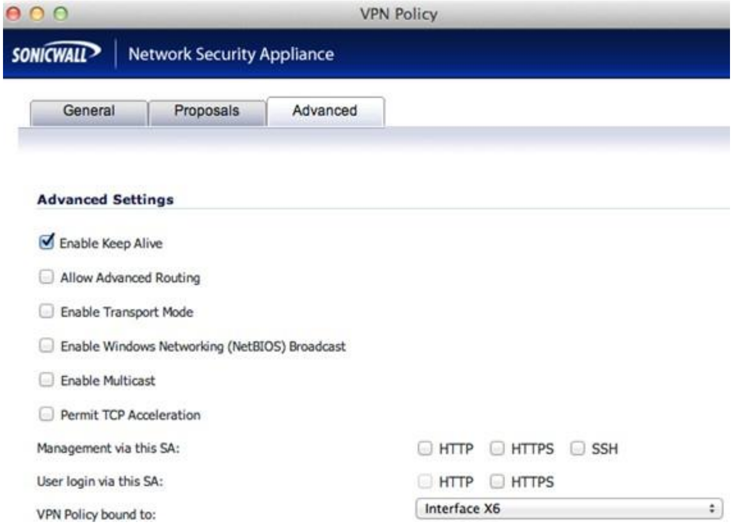
Authentication: SHA1

☐ Enable Perfect Forward Secrecy

Life Time (seconds): 28800

On the **Advanced** tab, configure Keep Alive, Management via this SA, and any other desired options. Ensure the **VPN Policy Bound To** dropdown menu is set to the WAN Interface that the tunnel will use to connect. In this example, the X6 WAN Interface is used on the Central site, while the Remote site uses X1 WAN.

Advanced tab (Central site):



VPN Policy

SONICWALL Network Security Appliance

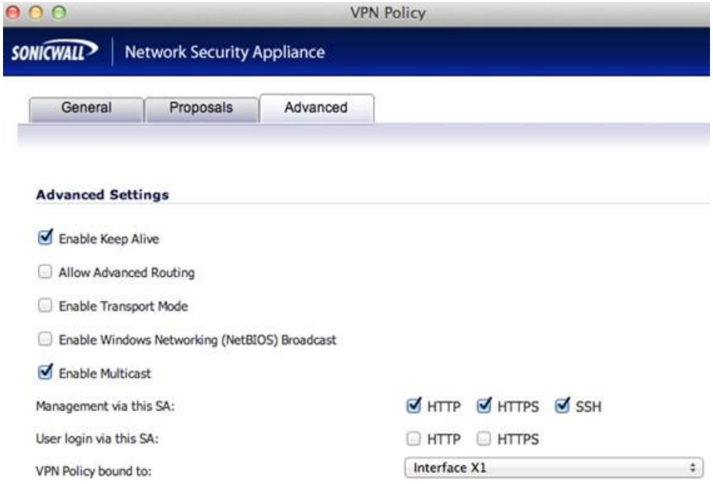
General | Proposals | Advanced

Advanced Settings

☑ Enable Keep Alive
□ Allow Advanced Routing
□ Enable Transport Mode
□ Enable Windows Networking (NetBIOS) Broadcast
□ Enable Multicast
□ Permit TCP Acceleration

Management via this SA: □ HTTP □ HTTPS □ SSH
User login via this SA: □ HTTP □ HTTPS
VPN Policy bound to: Interface X6

Advanced tab (Remote site):



VPN Policy

SONICWALL Network Security Appliance

General | Proposals | Advanced

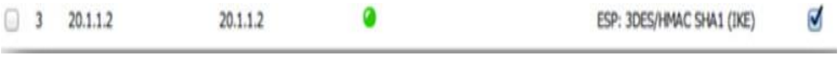
Advanced Settings

☑ Enable Keep Alive
□ Allow Advanced Routing
□ Enable Transport Mode
□ Enable Windows Networking (NetBIOS) Broadcast
☑ Enable Multicast

Management via this SA: ☑ HTTP ☑ HTTPS ☑ SSH
User login via this SA: □ HTTP □ HTTPS
VPN Policy bound to: Interface X1

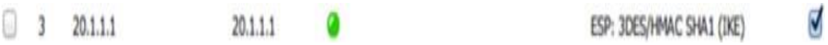
Once complete, the tunnel will be established, and will look like this:

Central:



□ 3 20.1.1.2 20.1.1.2 ● ESP: 3DES/HMAC SHA1 (IKE) ☑

Remote:

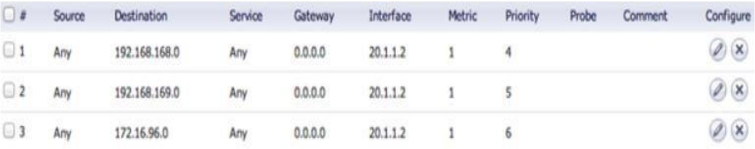


□ 3 20.1.1.1 20.1.1.1 ● ESP: 3DES/HMAC SHA1 (IKE) ☑

Step 2: Create routes on each unit. This can be done under Network > Routing. Options include Route-All VPN (all Internet traffic routes through the Central site over the tunnel) and the more traditional Split Tunnel VPN (only traffic destined for a remote subnet routes through the tunnel). Address Objects can be created while creating routes, or can be done before creating routes, under Network > Address Objects.

Step 2a – Central site routes:

In the example below, the Remote site has 3 networks: 2 LANs (X0 and X2), and 1 WLAN (W0). I have added one route per remote network.

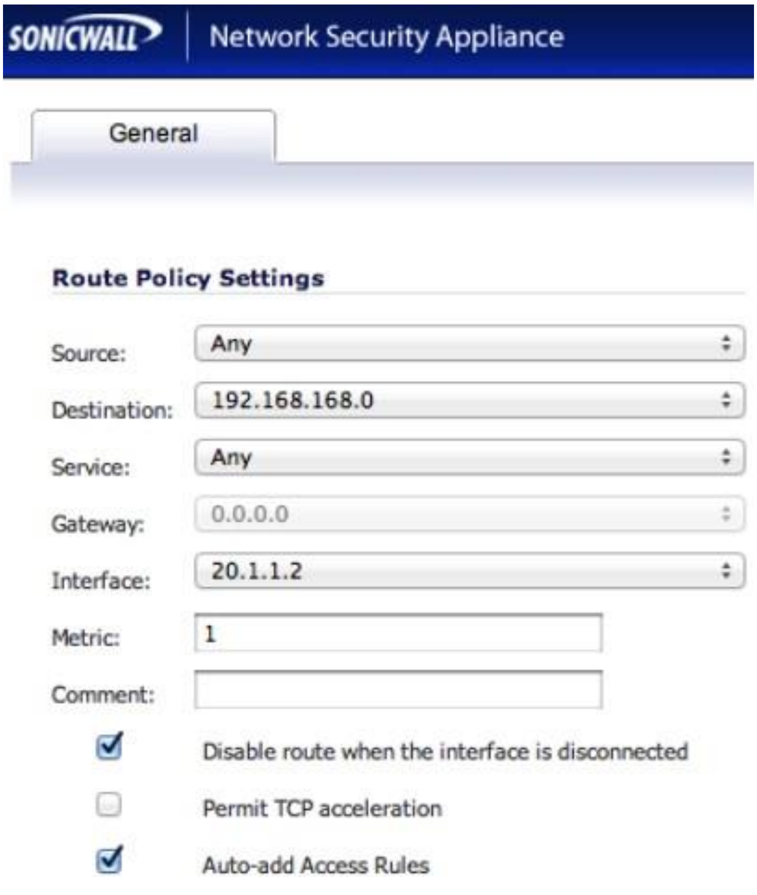


□ #	Source	Destination	Service	Gateway	Interface	Metric	Priority	Probe	Comment	Configure
□ 1	Any	192.168.168.0	Any	0.0.0.0	20.1.1.2	1	4			
□ 2	Any	192.168.169.0	Any	0.0.0.0	20.1.1.2	1	5			
□ 3	Any	172.16.96.0	Any	0.0.0.0	20.1.1.2	1	6			

Note: Create one route per remote network. The example below only shows one network route, but as shown above, three routes were created since three networks need to communicate over the tunnel.

Detailed route configuration:

- Source: Any
- Destination: Remote network Address Object. The Object should be assigned to the VPN Zone.
- Service: Any
- Interface: Select the Tunnel Interface name from the dropdown list.
- Allow Automatic Access Rule creation for simplicity, or disable it for granularity.



Route Policy Settings

Source:	Any
Destination:	192.168.168.0
Service:	Any
Gateway:	0.0.0.0
Interface:	20.1.1.2
Metric:	1
Comment:	

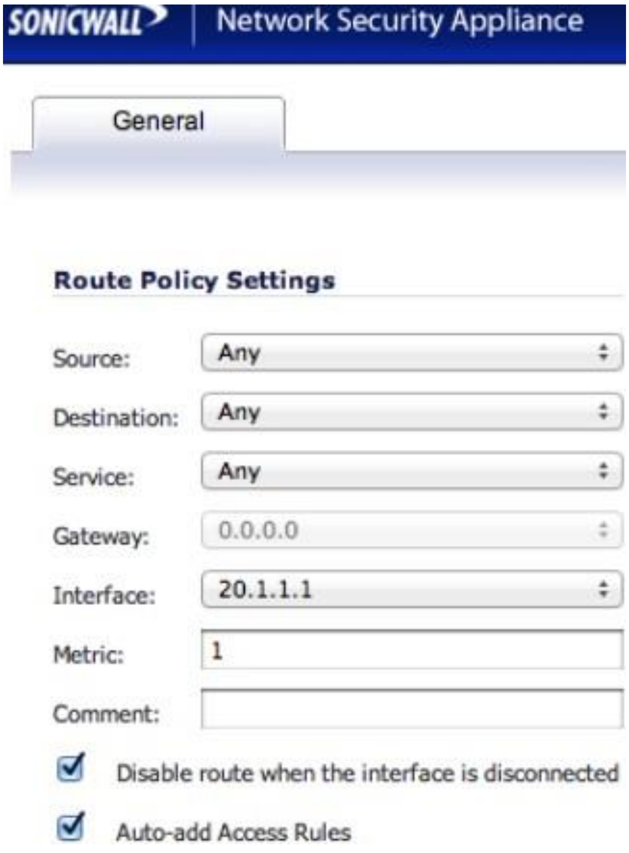
☑ Disable route when the interface is disconnected

☐ Permit TCP acceleration

☑ Auto-add Access Rules

Step 2b – Remote site routes:

Route-All Option:



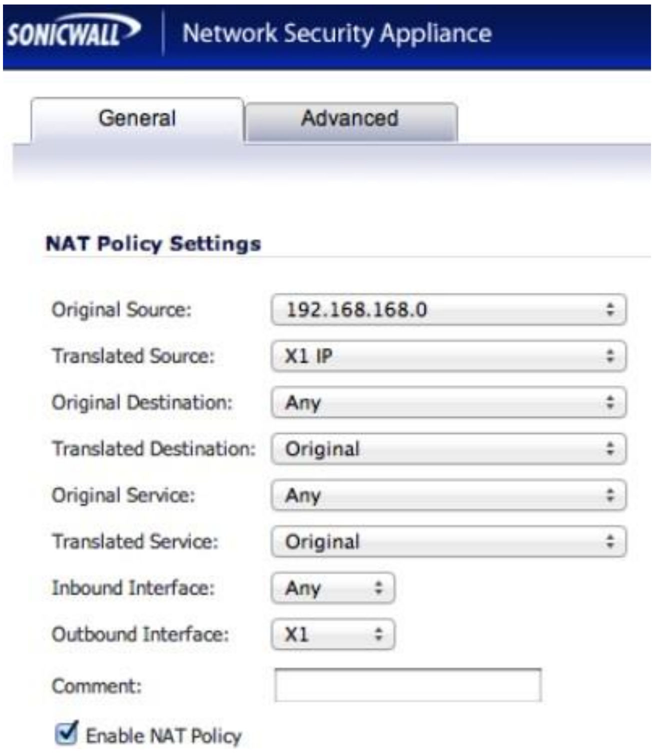
Route Policy Settings

Source:	Any
Destination:	Any
Service:	Any
Gateway:	0.0.0.0
Interface:	20.1.1.1
Metric:	1
Comment:	

☑ Disable route when the interface is disconnected

☑ Auto-add Access Rules

Note: If using the Route-All option, a NAT Policy must be created on the Central site for translation to the WAN IP. An example NAT Policy for the Remote site's X0 LAN can be found below.



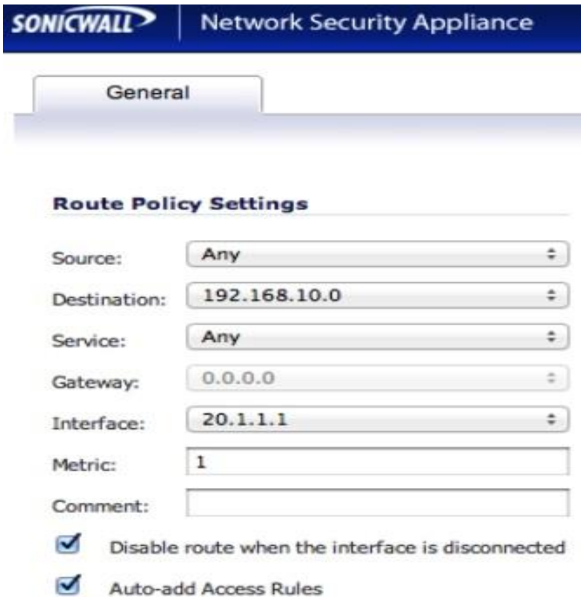
NAT Policy Settings

Original Source:	192.168.168.0
Translated Source:	X1 IP
Original Destination:	Any
Translated Destination:	Original
Original Service:	Any
Translated Service:	Original
Inbound Interface:	Any
Outbound Interface:	X1
Comment:	

☑ Enable NAT Policy

Split Tunnel Option:

In this example, only one network exists on the Central site, thus only one route is created.



Route Policy Settings

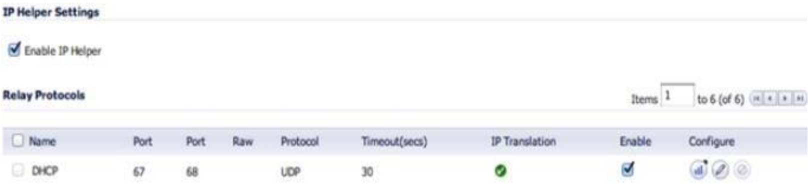
Source:	Any
Destination:	192.168.10.0
Service:	Any
Gateway:	0.0.0.0
Interface:	20.1.1.1
Metric:	1
Comment:	

☑ Disable route when the interface is disconnected

☑ Auto-add Access Rules

Step 3: On the Remote site, enable IP Helper and create IP Helper Policies for DHCP Relay. Options include DHCP Relay to the Central firewall's internal DHCP server and DHCP Relay to an external DHCP server behind the Central firewall.

Step 3a: Enable IP Helper and DHCP Protocol Support. An example is shown below.


IP Helper Settings

☑ Enable IP Helper

Relay Protocols

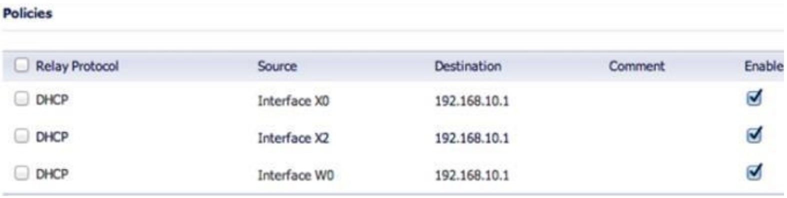
Items 1 to 6 (of 6)

□ Name	Port	Port	Raw	Protocol	Timeout(secs)	IP Translation	Enable	Configure
□ DHCP	67	68		UDP	30	●	☑	

Step 3b: Configure an IP Helper Policy for each network that requires remote DHCP.

Internal DHCP Option:

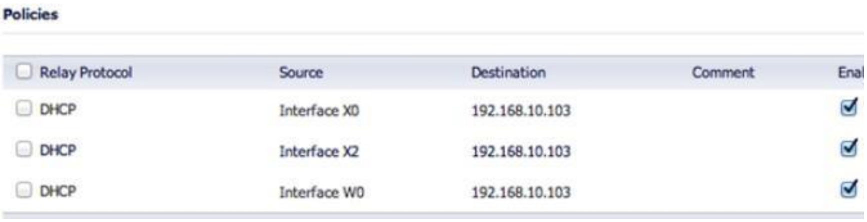
In this example, DHCP is relayed to the X0 LAN IP of the Central site. The Central firewall's internal DHCP server provides DHCP to remote VPN systems.


Policies

□ Relay Protocol	Source	Destination	Comment	Enable
□ DHCP	Interface X0	192.168.10.1		☑
□ DHCP	Interface X2	192.168.10.1		☑
□ DHCP	Interface W0	192.168.10.1		☑

External DHCP Option:

In this example, DHCP is relayed to the Central site's LAN DHCP server. The LAN server at the Central site provides DHCP to remote VPN systems.


Policies

□ Relay Protocol	Source	Destination	Comment	Enal
□ DHCP	Interface X0	192.168.10.103		☑
□ DHCP	Interface X2	192.168.10.103		☑
□ DHCP	Interface W0	192.168.10.103		☑

Step 4: Configure DHCP scopes for each remote network. Each network requires it's own DHCP scope on the DHCP server.

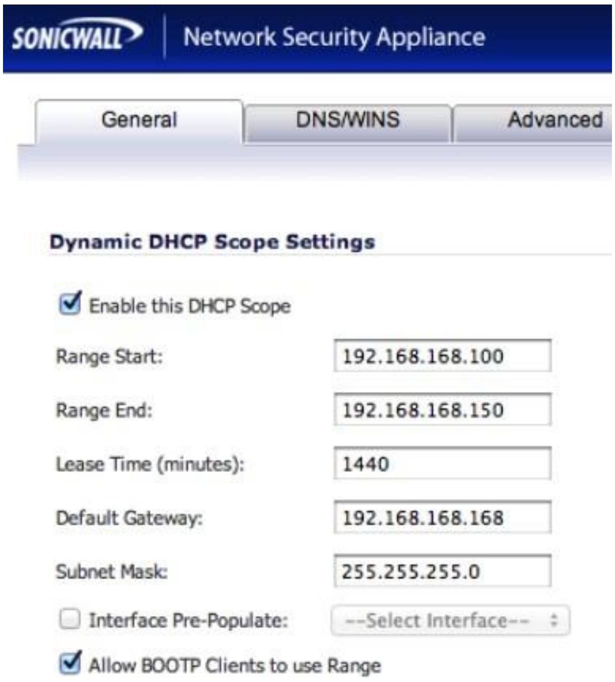
Note: DHCP Leases will be displayed on the Remote site firewall, on the Network > IP Helper page, as well as on the server which provided the lease.

Internal DHCP configuration:

If you plan to use the Central firewall's internal DHCP server, you will need to create a scope for each remote subnet, as shown below. This can be done on the Network > DHCP Server page. The scope must be large enough to support all of the DHCP clients on the remote network.

Note: Do not use the "Interface Pre-Populate" option. This will populate the DHCP scope configuration with information from the selected interface. Once the scope has been added, you will notice that the Interface reads "N/A".

Note: Leases can be found on the Network > DHCP Server page.



Dynamic DHCP Scope Settings

☑ Enable this DHCP Scope

Range Start: 192.168.168.100

Range End: 192.168.168.150

Lease Time (minutes): 1440

Default Gateway: 192.168.168.168

Subnet Mask: 255.255.255.0

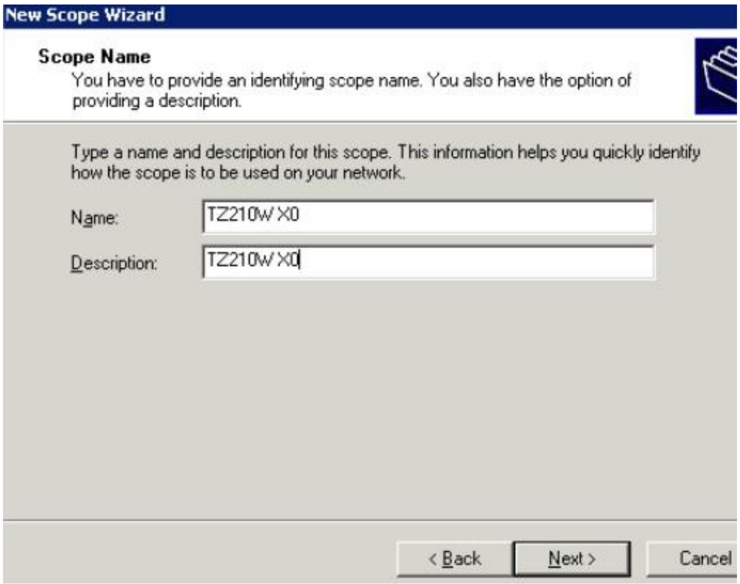
□ Interface Pre-Populate: --Select Interface--

☑ Allow BOOTP Clients to use Range

External DHCP configuration:

If you plan to use an external DHCP server, you will need to create a scope for each remote subnet on the DHCP server, as shown in the screenshots below. The screenshots are taken from Windows 2003Server.

Configure the Scope's name and description.


New Scope Wizard

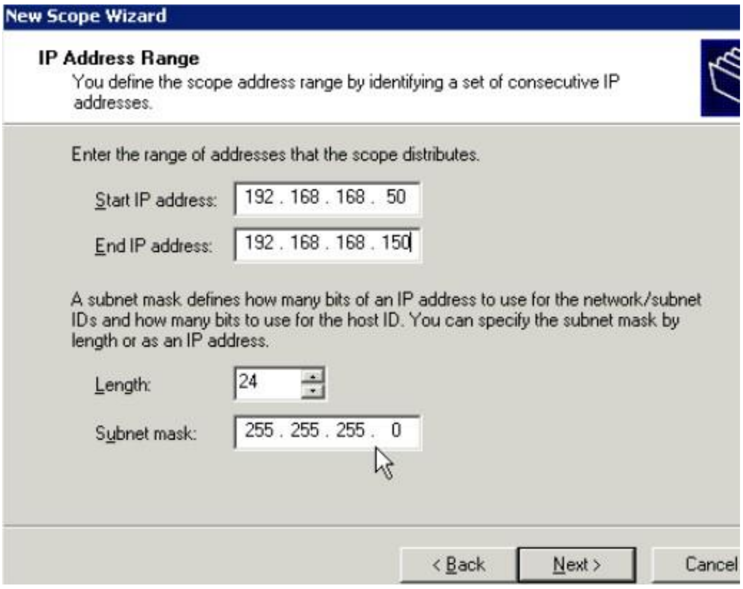
Scope Name
You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name: TZ210W X0

Description: TZ210W X0

Configure the desired IP Range. Set the appropriate Subnet Mask.


New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 168 . 50

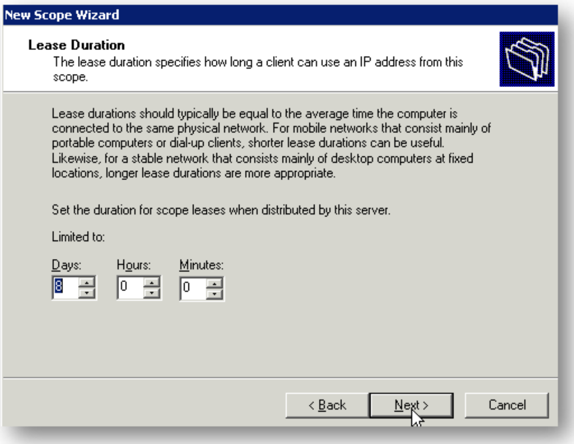
End IP address: 192 . 168 . 168 . 150

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 24

Subnet mask: 255 . 255 . 255 . 0

Set a DHCP Lease Duration.


New Scope Wizard

Lease Duration
The lease duration specifies how long a client can use an IP address from this scope.

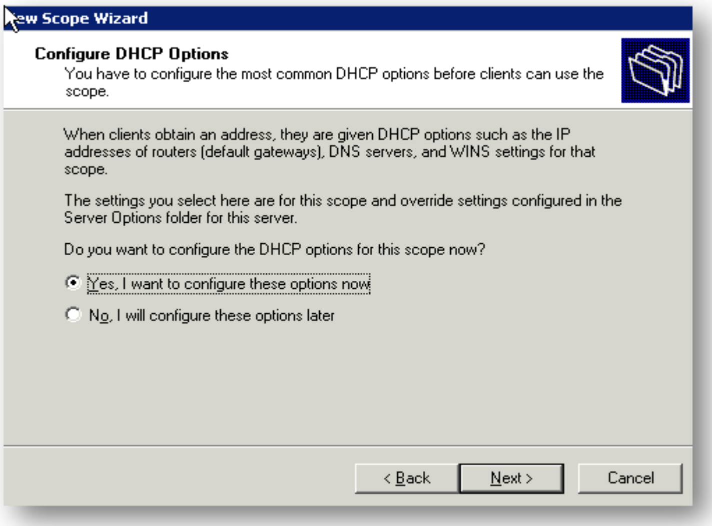
Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days: 8 Hours: 0 Minutes: 0

Configure the DHCP options.


New Scope Wizard

Configure DHCP Options
You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

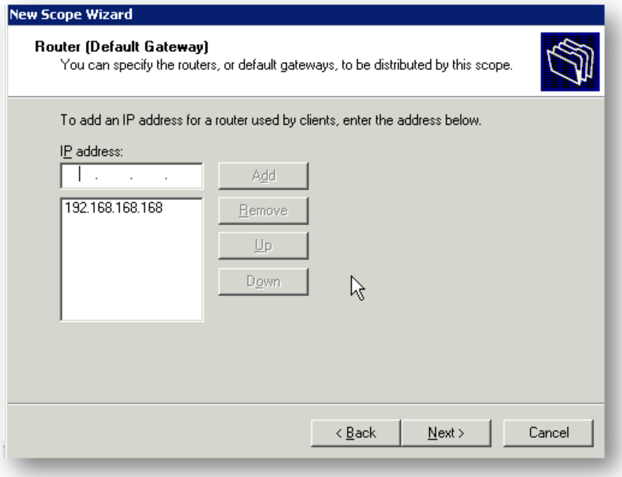
The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

● Yes, I want to configure these options now

○ No, I will configure these options later

Enter the Default Gateway IP that each DHCP client will use.


New Scope Wizard

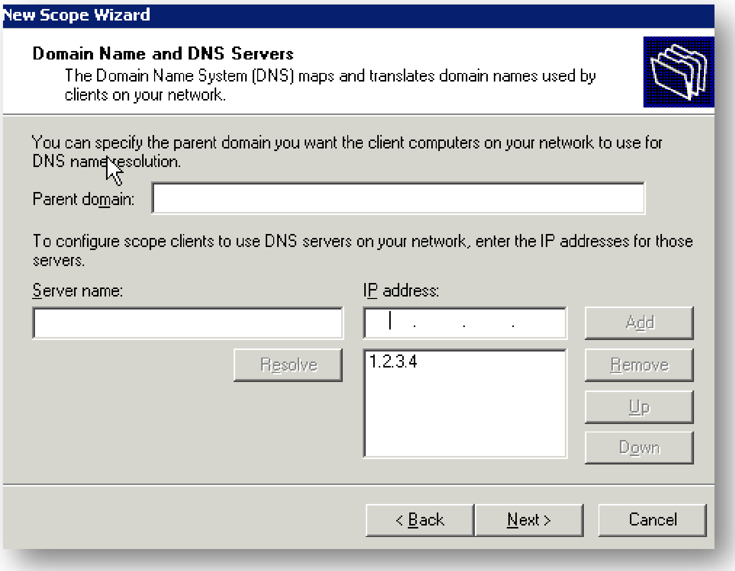
Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

192.168.168.168

Enter the IPs of any DNS servers you would like to use.



New Scope Wizard

Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

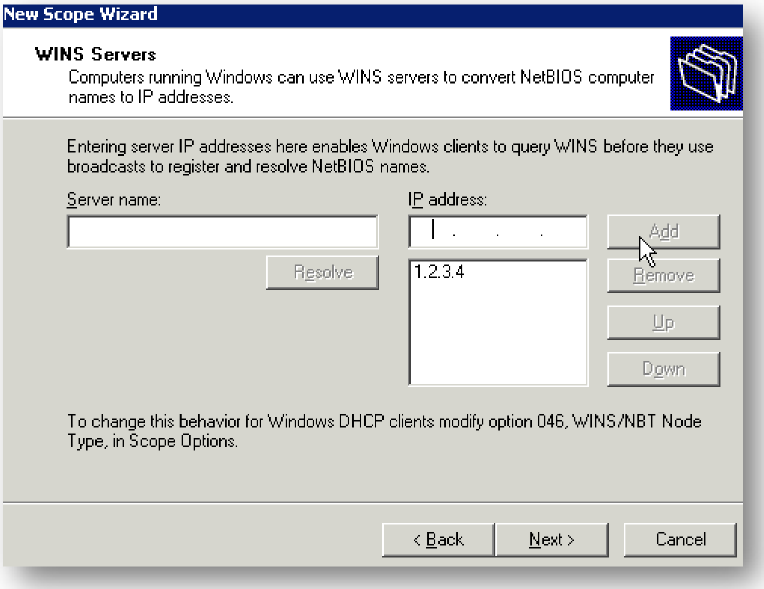
Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

IP address: 1.2.3.4

Enter the IPs of any WINS servers you would like to use.



New Scope Wizard

WINS Servers
Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.

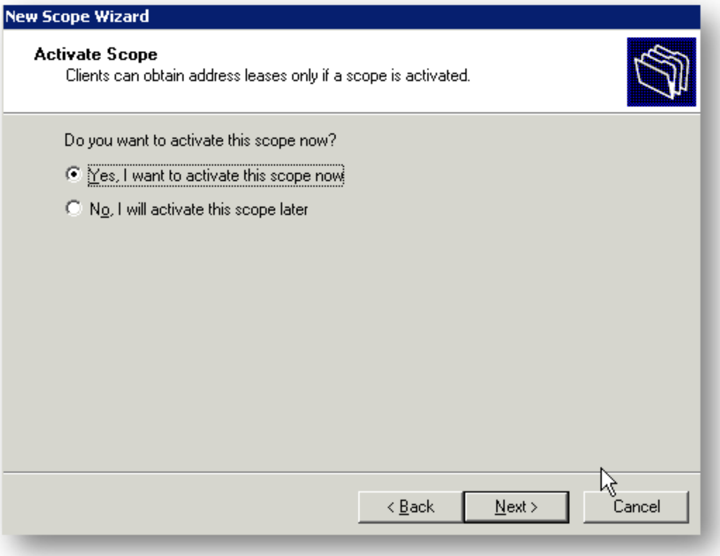
Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.

Server name:

IP address: 1.2.3.4

To change this behavior for Windows DHCP clients modify option 046, WINS/NBT Node Type, in Scope Options.

Activate the scope.



New Scope Wizard

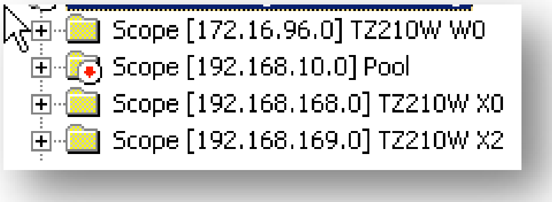
Activate Scope
Clients can obtain address leases only if a scope is activated.

Do you want to activate this scope now?

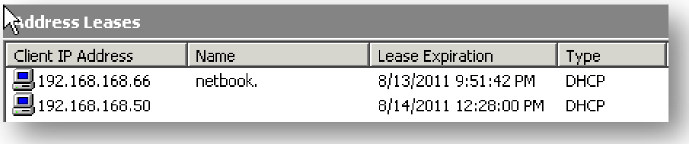
● Yes, I want to activate this scope now

○ No, I will activate this scope later

Below, the screenshots show the three configured (and active) scopes for the remote subnets, and two leases provided by the server to remote client systems.



Scope [172.16.96.0] TZ210W W0
Scope [192.168.10.0] Pool
Scope [192.168.168.0] TZ210W X0
Scope [192.168.169.0] TZ210W X2



Address Leases

Client IP Address	Name	Lease Expiration	Type
192.168.168.66	netbook.	8/13/2011 9:51:42 PM	DHCP
192.168.168.50		8/14/2011 12:28:00 PM	DHCP

RESOLUTION FOR SONICOS 6.5 AND LATER

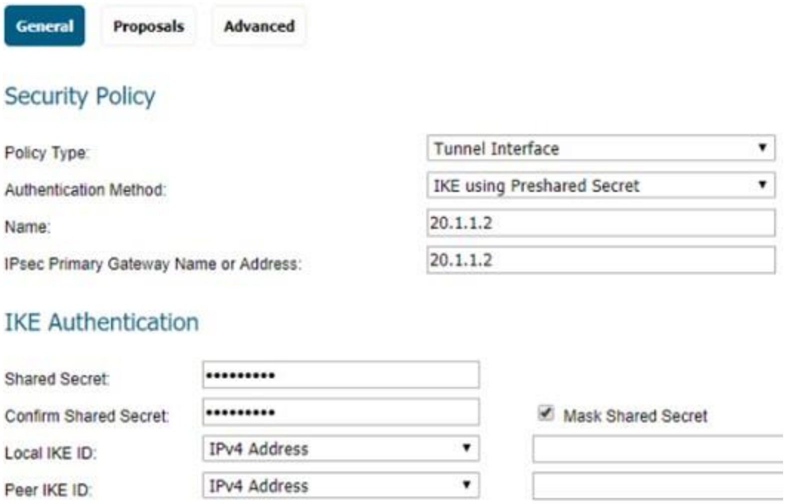
SonicOS 6.5 was released September 2017. This release includes significant user interface changes and many new features that are different from the SonicOS 6.2 and earlier firmware. The below resolution is for customers using SonicOS 6.5 and later firmware.

Step 1: Configure the Tunnel Interface VPN Policy on each unit. This is done under Manage |VPN | Base Settings.

On the General tab of the new VPN Policy configuration window, configure the following settings.

- Policy Type: Tunnel Interface
- Authentication Method: IKE using Preshared Secret
- Name: Enter a desired policy name
- IPSec Primary Gateway Name/Address: Enter the remote unit's WAN IP.
- Enter a shared secret that will be used on each side of the tunnel.

General tab (Central site):



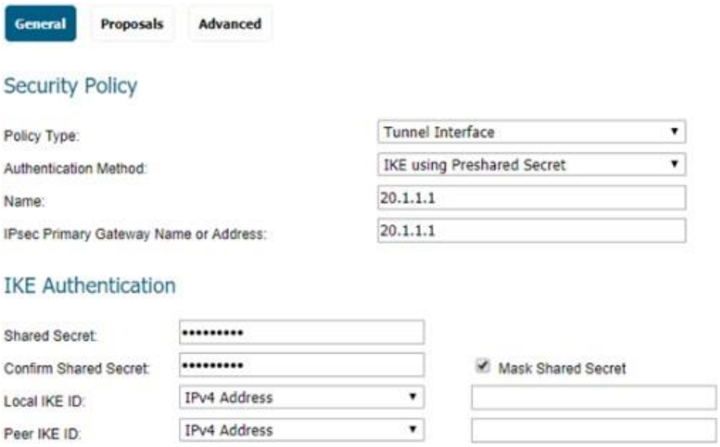
Security Policy

Policy Type: Tunnel Interface
Authentication Method: IKE using Preshared Secret
Name: 20.1.1.2
IPsec Primary Gateway Name or Address: 20.1.1.2

IKE Authentication

Shared Secret: •••••••••
Confirm Shared Secret: •••••••••
☑ Mask Shared Secret
Local IKE ID: IPv4 Address
Peer IKE ID: IPv4 Address

General tab (Remote site):



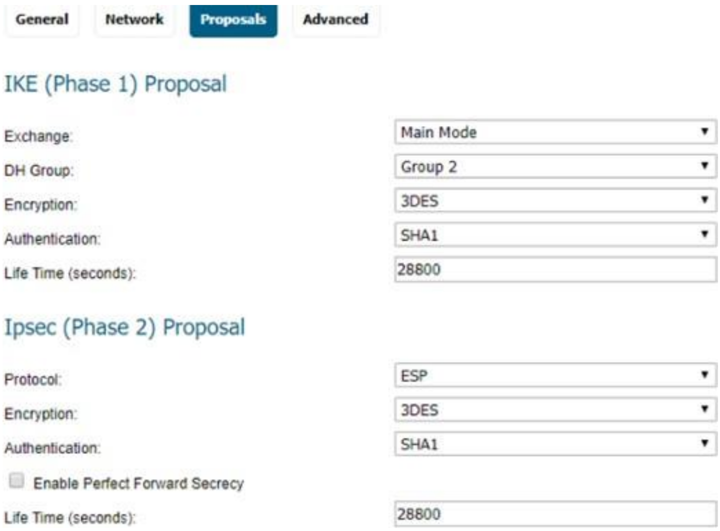
Security Policy

Policy Type: Tunnel Interface
Authentication Method: IKE using Preshared Secret
Name: 20.1.1.1
IPsec Primary Gateway Name or Address: 20.1.1.1

IKE Authentication

Shared Secret: •••••••••
Confirm Shared Secret: •••••••••
☑ Mask Shared Secret
Local IKE ID: IPv4 Address
Peer IKE ID: IPv4 Address

Enter your desired Proposal settings on each side of the tunnel. An example of the **Proposals** tab is shown below:



IKE (Phase 1) Proposal

Exchange: Main Mode
DH Group: Group 2
Encryption: 3DES
Authentication: SHA1
Life Time (seconds): 28800

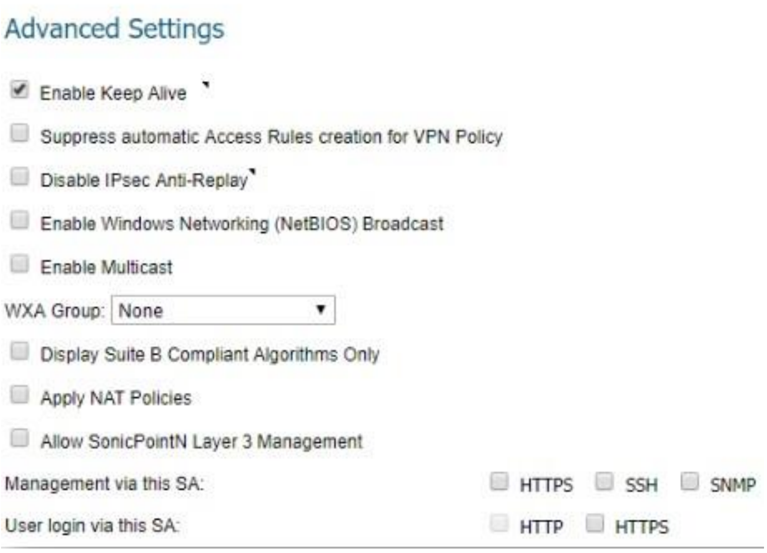
Ipsec (Phase 2) Proposal

Protocol: ESP
Encryption: 3DES
Authentication: SHA1
□ Enable Perfect Forward Secrecy
Life Time (seconds): 28800

On the **Advanced** tab, configure Keep Alive, Management via this SA, and any other desired options. Ensure the **VPN Policy Bound To** dropdown menu is set to the WAN Interface that the tunnel will use to connect. In this example, the X6 WAN Interface is used on the Central site, while the Remote site uses X1 WAN.

Advanced tab (Central site):

General | Network | Proposals | Advanced



Advanced Settings

☑ Enable Keep Alive

□ Suppress automatic Access Rules creation for VPN Policy

□ Disable IPsec Anti-Replay

□ Enable Windows Networking (NetBIOS) Broadcast

□ Enable Multicast

WXA Group: None

□ Display Suite B Compliant Algorithms Only

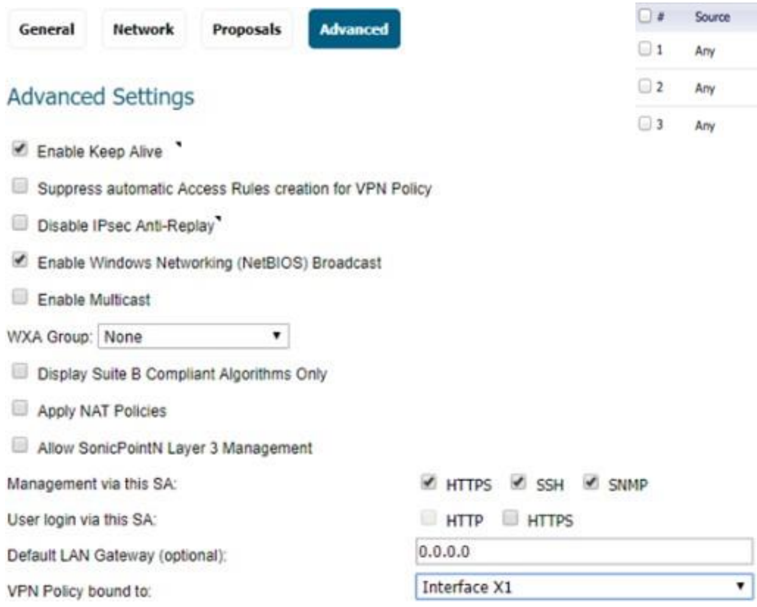
□ Apply NAT Policies

□ Allow SonicPointN Layer 3 Management

Management via this SA: □ HTTPS □ SSH □ SNMP

User login via this SA: □ HTTP □ HTTPS

Advanced tab (Remote site):



General | Network | Proposals | Advanced

Advanced Settings

☑ Enable Keep Alive

□ Suppress automatic Access Rules creation for VPN Policy

□ Disable IPsec Anti-Replay

☑ Enable Windows Networking (NetBIOS) Broadcast

□ Enable Multicast

WXA Group: None

□ Display Suite B Compliant Algorithms Only

□ Apply NAT Policies

□ Allow SonicPointN Layer 3 Management

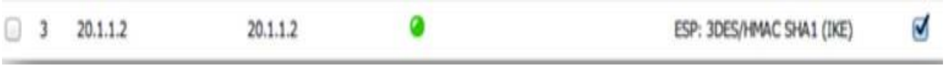
Management via this SA: ☑ HTTPS ☑ SSH ☑ SNMP

User login via this SA: □ HTTP □ HTTPS

Default LAN Gateway (optional): 0.0.0.0

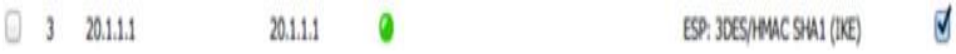
VPN Policy bound to: Interface X1

Once complete, the tunnel will be established, and will look like this:
Central:



□ 3 20.1.1.2 20.1.1.2 ● ESP: 3DES/HMAC SHA1 (IKE) ☑

Remote:

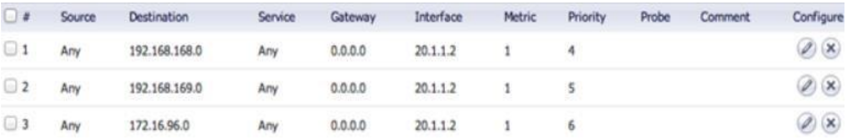


□ 3 20.1.1.1 20.1.1.1 ● ESP: 3DES/HMAC SHA1 (IKE) ☑

Step 2: Create routes on each unit. This can be done under Network | Routing. Options include Route-All VPN (all Internet traffic routes through the Central site over the tunnel) and the more traditional Split Tunnel VPN (only traffic destined for a remote subnet routes through the tunnel). Address Objects can be created while creating routes, or can be done before creating routes, under Network > Address Objects.

Step 2a – Central site routes:

In the example below, the Remote site has 3 networks: 2 LANs (X0 and X2), and 1 WLAN (W0). I have added one route per remote network.

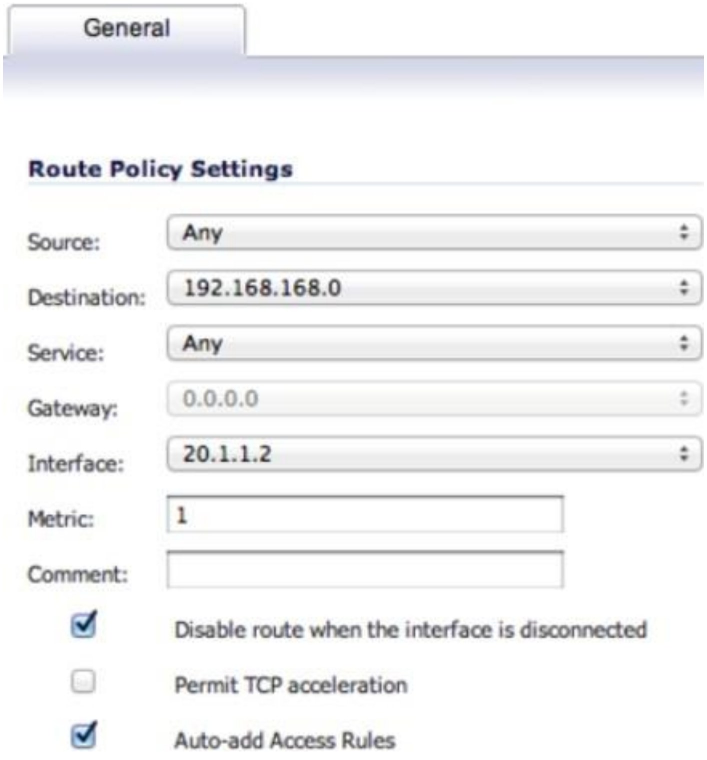


□ #	Source	Destination	Service	Gateway	Interface	Metric	Priority	Probe	Comment	Configure
□ 1	Any	192.168.168.0	Any	0.0.0.0	20.1.1.2	1	4			
□ 2	Any	192.168.169.0	Any	0.0.0.0	20.1.1.2	1	5			
□ 3	Any	172.16.96.0	Any	0.0.0.0	20.1.1.2	1	6			

Note: Create one route per remote network. The example below only shows one network route, but as shown above, three routes were created since three networks need to communicate over the tunnel.

Detailed route configuration:

- Source: Any
- Destination: Remote network Address Object. The Object should be assigned to the VPN Zone.
- Service: Any
- Interface: Select the Tunnel Interface name from the dropdown list.
- Allow Automatic Access Rule creation for simplicity, or disable it for granularity.



General

Route Policy Settings

Source: Any

Destination: 192.168.168.0

Service: Any

Gateway: 0.0.0.0

Interface: 20.1.1.2

Metric: 1

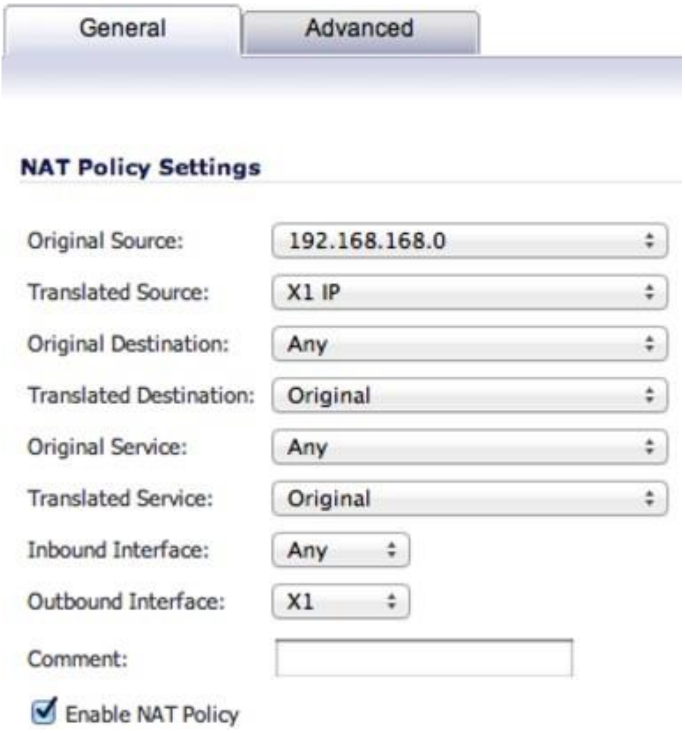
Comment:

☑ Disable route when the interface is disconnected

☐ Permit TCP acceleration

☑ Auto-add Access Rules

Note: If using the Route-All option, a NAT Policy must be created on the Central site for translation to the WAN IP. An example NAT Policy for the Remote site's X0 LAN can be found below.



NAT Policy Settings

Original Source: 192.168.168.0

Translated Source: X1 IP

Original Destination: Any

Translated Destination: Original

Original Service: Any

Translated Service: Original

Inbound Interface: Any

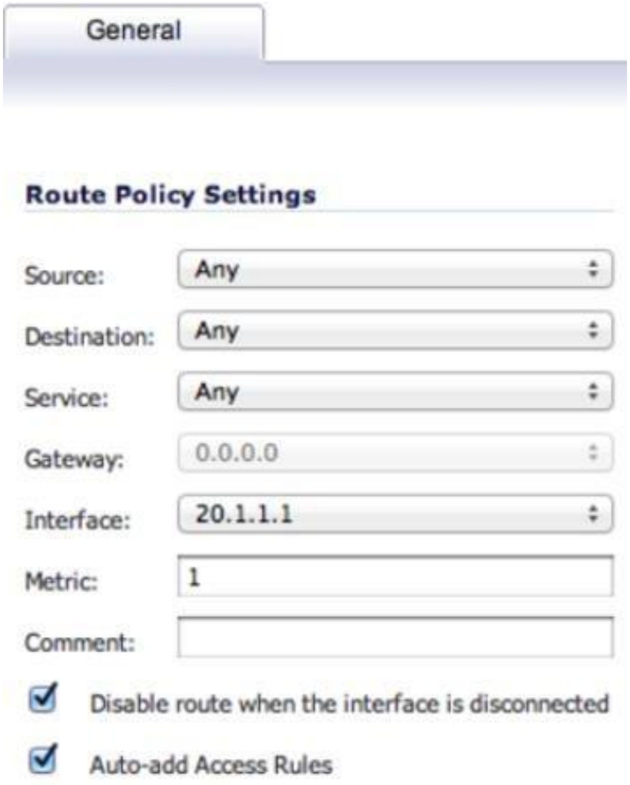
Outbound Interface: X1

Comment:

☑ Enable NAT Policy

Step 2b – Remote site routes:

Route-All Option:



General

Route Policy Settings

Source: Any

Destination: Any

Service: Any

Gateway: 0.0.0.0

Interface: 20.1.1.1

Metric: 1

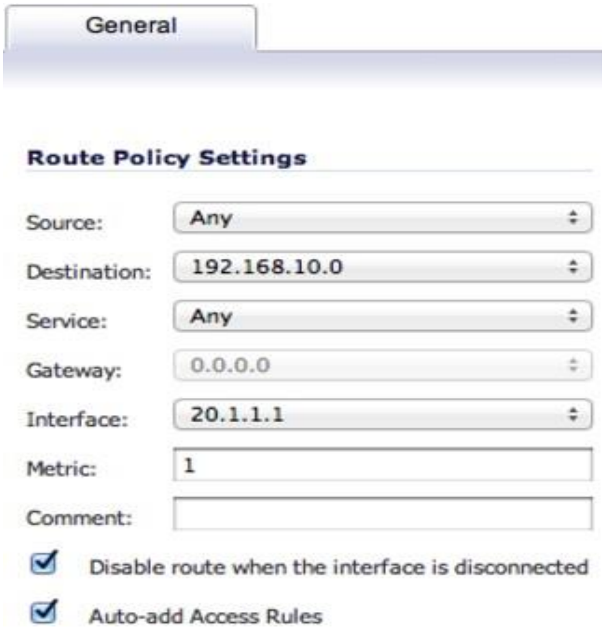
Comment:

☑ Disable route when the interface is disconnected

☑ Auto-add Access Rules

Split Tunnel Option:

In this example, only one network exists on the Central site, thus only one route is created.



General

Route Policy Settings

Source: Any

Destination: 192.168.10.0

Service: Any

Gateway: 0.0.0.0

Interface: 20.1.1.1

Metric: 1

Comment:

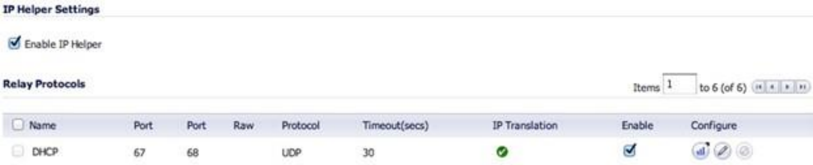
☑ Disable route when the interface is disconnected

☑ Auto-add Access Rules

Step 3: On the Remote site, enable IP Helper and create IP Helper Policies for DHCP Relay. Options include DHCP Relay to the Central firewall's internal DHCP server and DHCP Relay to an external DHCP server behind the Central firewall.

Step 3a: Enable IP Helper and DHCP Protocol Support. An example is shown below.

Under **Manage | Network | IP Helper**



IP Helper Settings

☑ Enable IP Helper

Relay Protocols

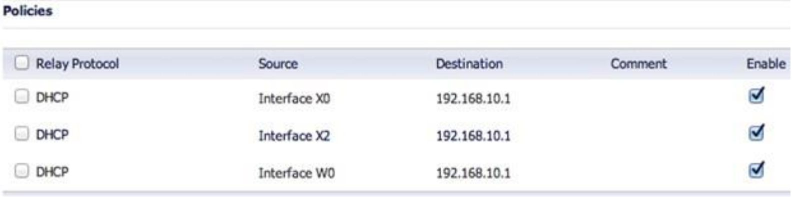
Items 1 to 6 (of 6)

☐ Name	Port	Port	Raw	Protocol	Timeout(secs)	IP Translation	Enable	Configure
☐ DHCP	67	68		UDP	30	✓	☑	

Step 3b: Configure an IP Helper Policy for each network that requires remote DHCP.

Internal DHCP Option:

In this example, DHCP is relayed to the X0 LAN IP of the Central site. The Central firewall's internal DHCP server provides DHCP to remote VPN systems.

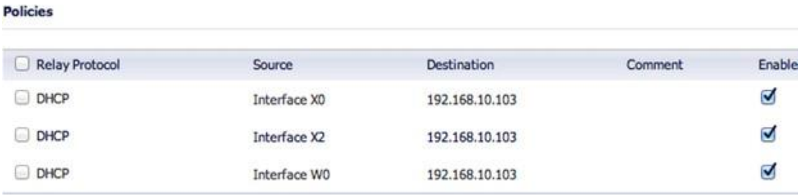


Policies

☐ Relay Protocol	Source	Destination	Comment	Enable
☐ DHCP	Interface X0	192.168.10.1		☑
☐ DHCP	Interface X2	192.168.10.1		☑
☐ DHCP	Interface W0	192.168.10.1		☑

External DHCP Option:

In this example, DHCP is relayed to the Central site's LAN DHCP server. The LAN server at the Central site provides DHCP to remote VPN systems.



Policies

☐ Relay Protocol	Source	Destination	Comment	Enable
☐ DHCP	Interface X0	192.168.10.103		☑
☐ DHCP	Interface X2	192.168.10.103		☑
☐ DHCP	Interface W0	192.168.10.103		☑

Step 4: Configure DHCP scopes for each remote network. Each network requires it's own DHCP scope on the DHCP server.

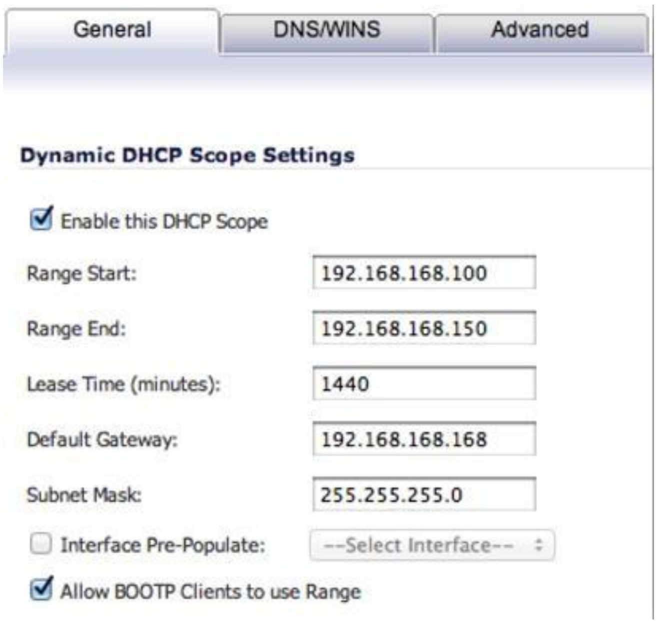
Note: DHCP Leases will be displayed on the Remote site firewall, on the Network > IP Helper page, as well as on the server which provided the lease.

Internal DHCP configuration:

If you plan to use the Central firewall's internal DHCP server, you will need to create a scope for each remote subnet, as shown below. This can be done on the Network > DHCP Server page. The scope must be large enough to support all of the DHCP clients on the remote network.

Note: Do not use the "Interface Pre-Populate" option. This will populate the DHCP scope configuration with information from the selected interface. Once the scope has been added, you will notice that the Interface reads "N/A".

Note: Leases can be found on the Network | DHCP Server page.



Dynamic DHCP Scope Settings

☑ Enable this DHCP Scope

Range Start: 192.168.168.100

Range End: 192.168.168.150

Lease Time (minutes): 1440

Default Gateway: 192.168.168.168

Subnet Mask: 255.255.255.0

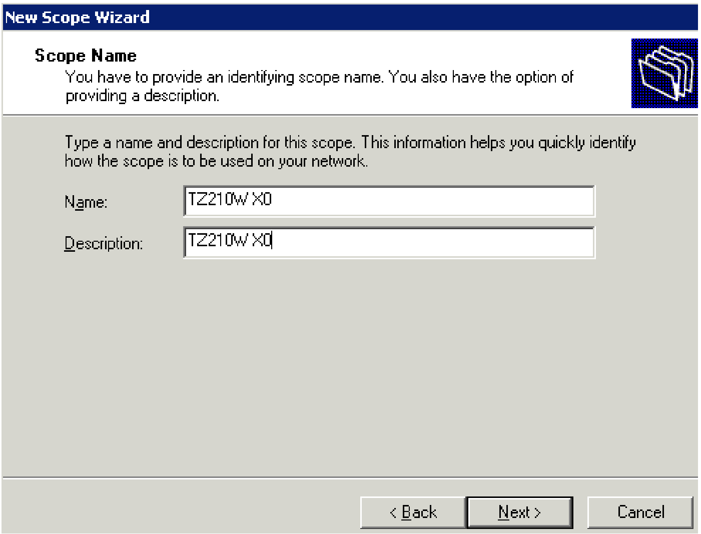
☐ Interface Pre-Populate: --Select Interface--

☑ Allow BOOTP Clients to use Range

External DHCP configuration:

If you plan to use an external DHCP server, you will need to create a scope for each remote subnet on the DHCP server, as shown in the screenshots below. The screenshots are taken from Windows 2003 Server.

Configure the Scope's name and description.



New Scope Wizard

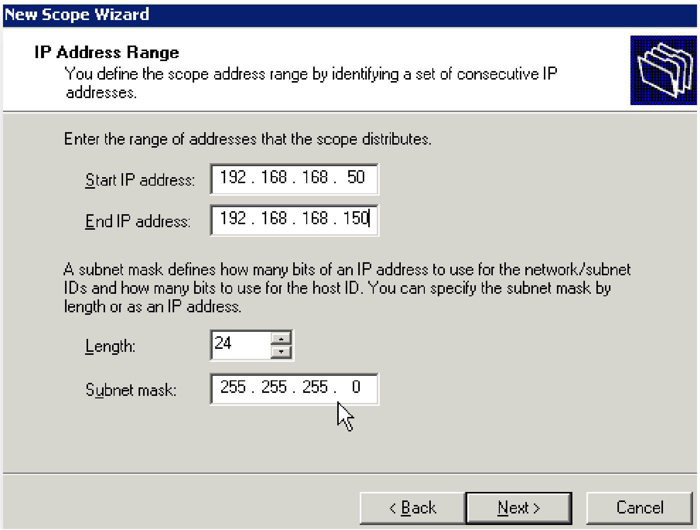
Scope Name
You have to provide an identifying scope name. You also have the option of providing a description.

Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name: TZ210W X0

Description: TZ210W X0

Configure the desired IP Range. Set the appropriate Subnet Mask.



New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 168 . 50

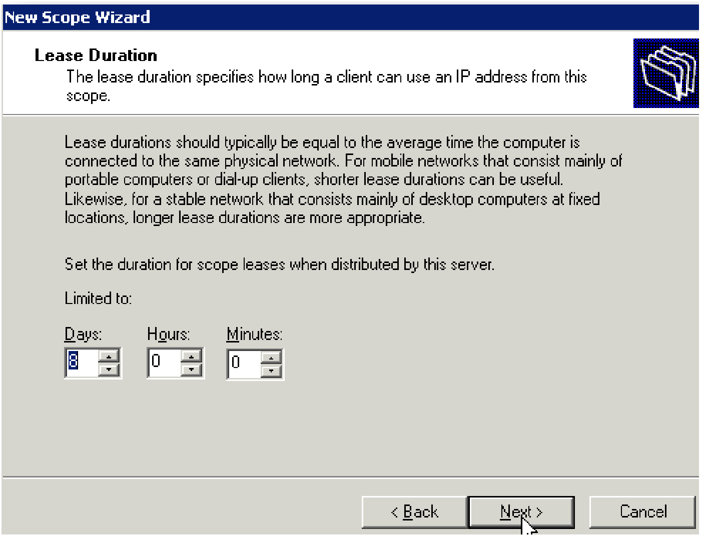
End IP address: 192 . 168 . 168 . 150

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 24

Subnet mask: 255 . 255 . 255 . 0

Set a DHCP Lease Duration.



New Scope Wizard

Lease Duration
The lease duration specifies how long a client can use an IP address from this scope.

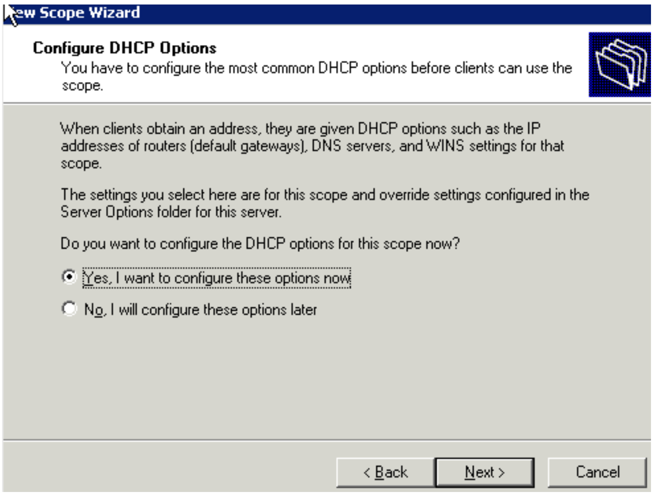
Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days: 8 Hours: 0 Minutes: 0

Configure the DHCP options.



New Scope Wizard

Configure DHCP Options
You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

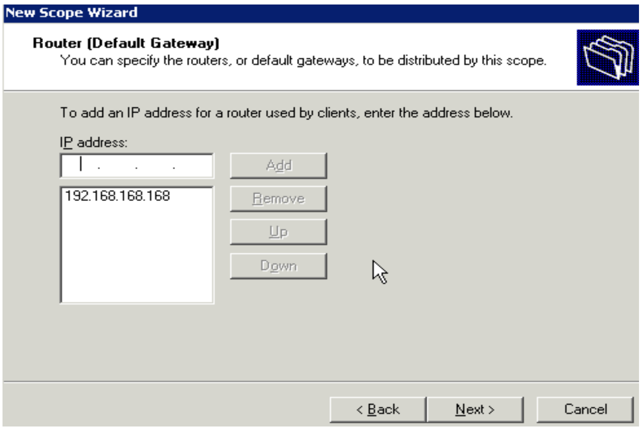
The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

● Yes, I want to configure these options now

○ No, I will configure these options later

Enter the Default Gateway IP that each DHCP client will use.



New Scope Wizard

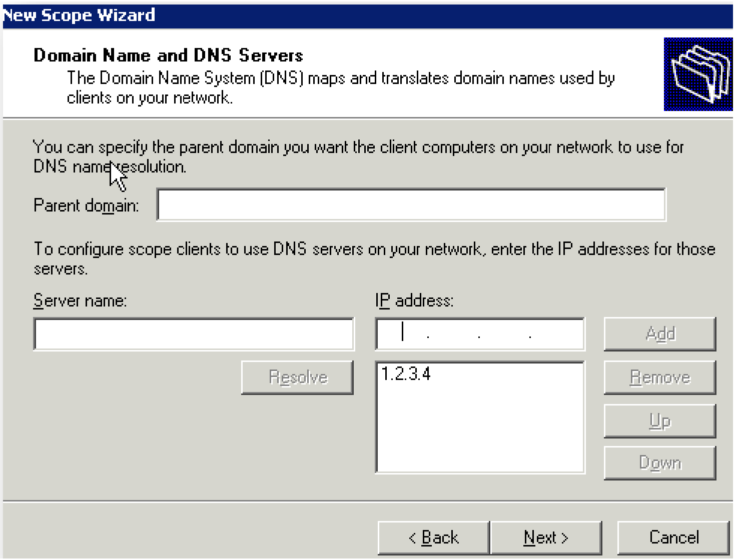
Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:

192.168.168.168

Enter the IPs of any DNS servers you would like to use.



New Scope Wizard

Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

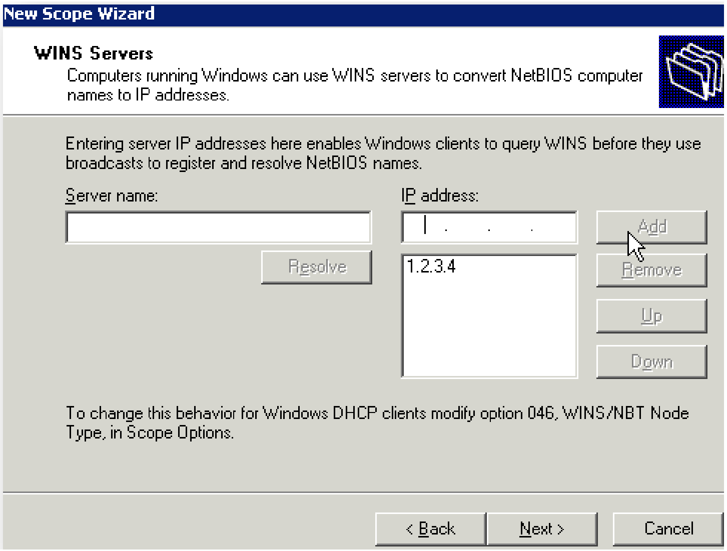
Parent domain:

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name:

IP address: 1.2.3.4

Enter the IPs of any WINS servers you would like to use.



New Scope Wizard

WINS Servers
Computers running Windows can use WINS servers to convert NetBIOS computer names to IP addresses.

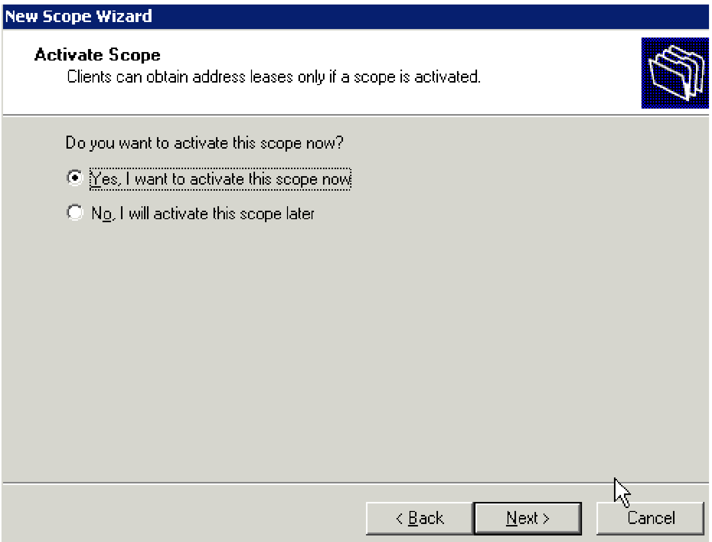
Entering server IP addresses here enables Windows clients to query WINS before they use broadcasts to register and resolve NetBIOS names.

Server name:

IP address: 1.2.3.4

To change this behavior for Windows DHCP clients modify option 046, WINS/NBT Node Type, in Scope Options.

Activate the scope.



New Scope Wizard

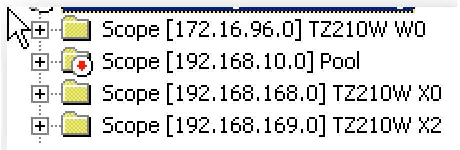
Activate Scope
Clients can obtain address leases only if a scope is activated.

Do you want to activate this scope now?

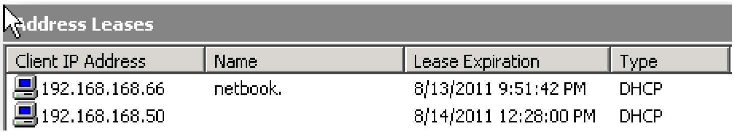
● Yes, I want to activate this scope now

○ No, I will activate this scope later

Below, the screenshots show the three configured (and active) scopes for the remote subnets, and two leases provided by the server to remote client systems.



Scope [172.16.96.0] TZ210W W0
Scope [192.168.10.0] Pool
Scope [192.168.168.0] TZ210W X0
Scope [192.168.169.0] TZ210W X2



Address Leases

Client IP Address	Name	Lease Expiration	Type
192.168.168.66	netbook.	8/13/2011 9:51:42 PM	DHCP
192.168.168.50		8/14/2011 12:28:00 PM	DHCP