Site to Site VPN between a SonicWall firewall and a Cisco IOS device

KNOWLEDGE DATABASE

SONICWALL
Knowledge Database

Site to Site VPN between a SonicWall firewall and a Cisco IOS device

Technical Notes:

SonicWall has tested VPN interoperability with Cisco IOS SonicOS Standard and Enhanced using the following VPN Security Association information:
Keying Mode: IKE
IKE Mode: Main Mode with No PFS (perfect forward secrecy)
SA Authentication Method: Pre-Shared key
Keying Group: DH (Diffie Hellman) – Group 1
ID_Type: IP
Encryption and Data Integrity: ESP DES with MD5
ESP 3DES with MD5
ESP DES with SHA1
ESP 3DES with SHA1

EXAMPLE setup:

The network configuration shown below is used in the example VPN configuration. The example will configure a VPN using 3DES encryption with MD5 and without PFS.

SonicWall
WAN: IP 10.0.31.102
LAN: 192.168.170.1/24

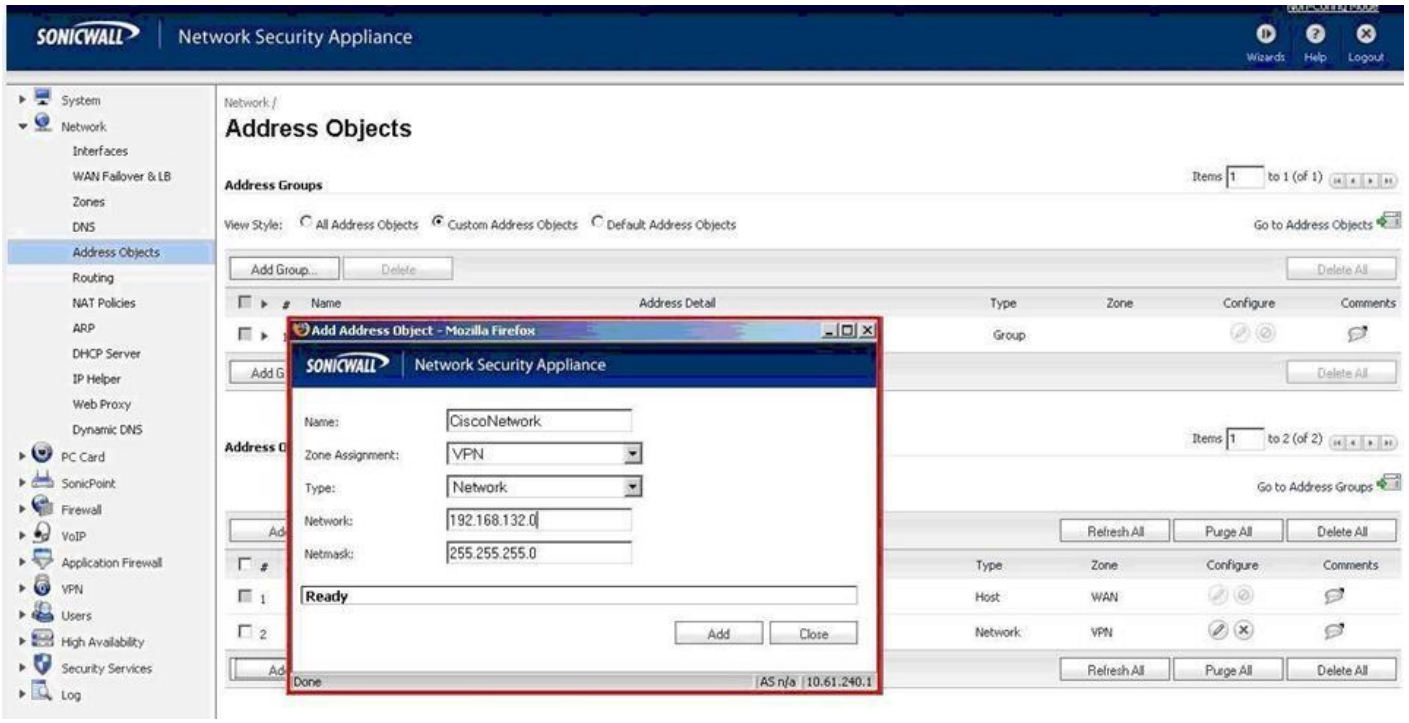
Cisco IOS
WAN: 10.0.31.132
LAN: IP 192.168.132.1/24

SonicWall Configuration

First, on the SonicWall, you must create an address object for the remote network.

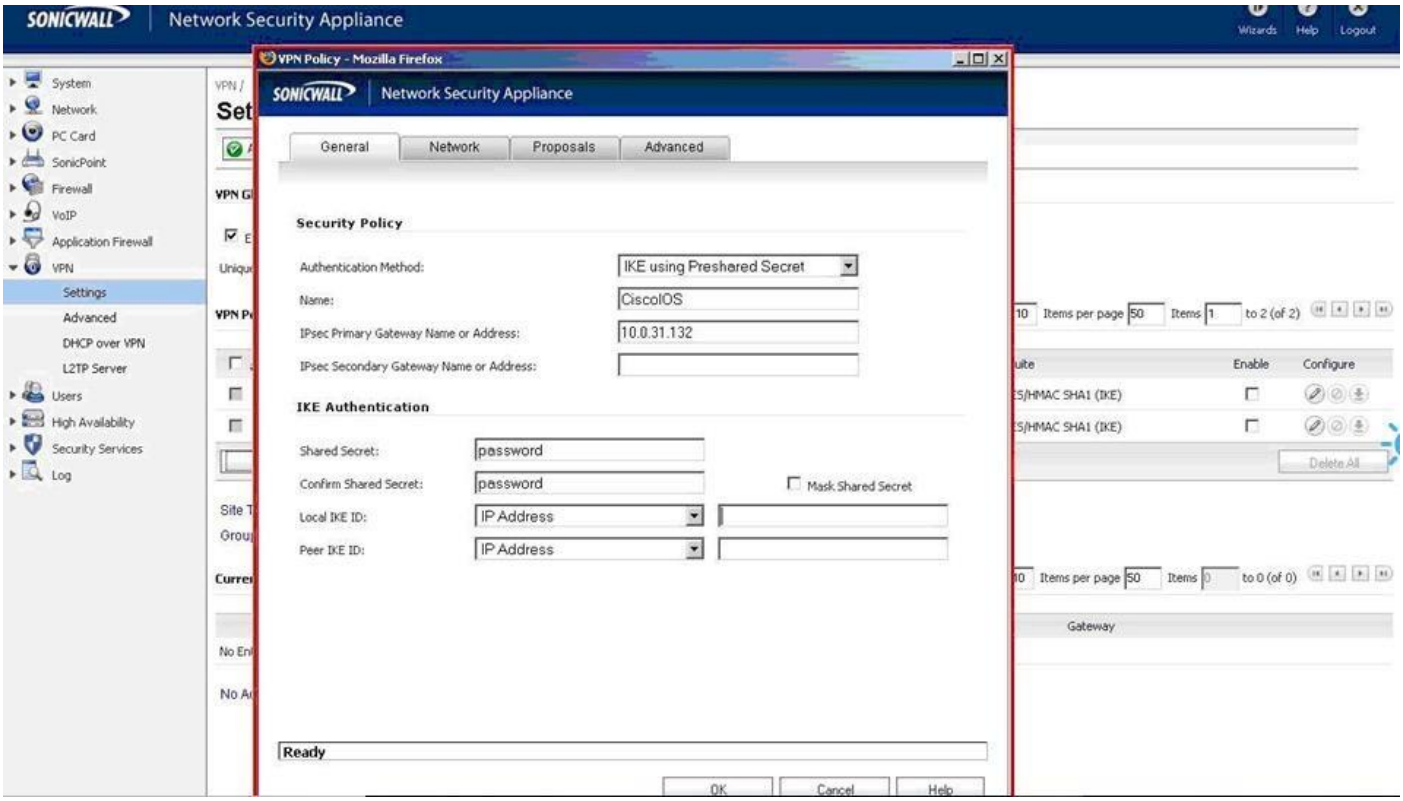
1. Log into the SonicWall.
2. Browse to Network, then Address Objects
3. Create a new Address Object for the network on the Cisco end you wish to reach (Cisco LAN).

Calle 140 #11-45. Bogotá D.C. Colombia
+57 1 3680290 / +57 318 4914652
sales@itclatam.com / tss@itclatam.com

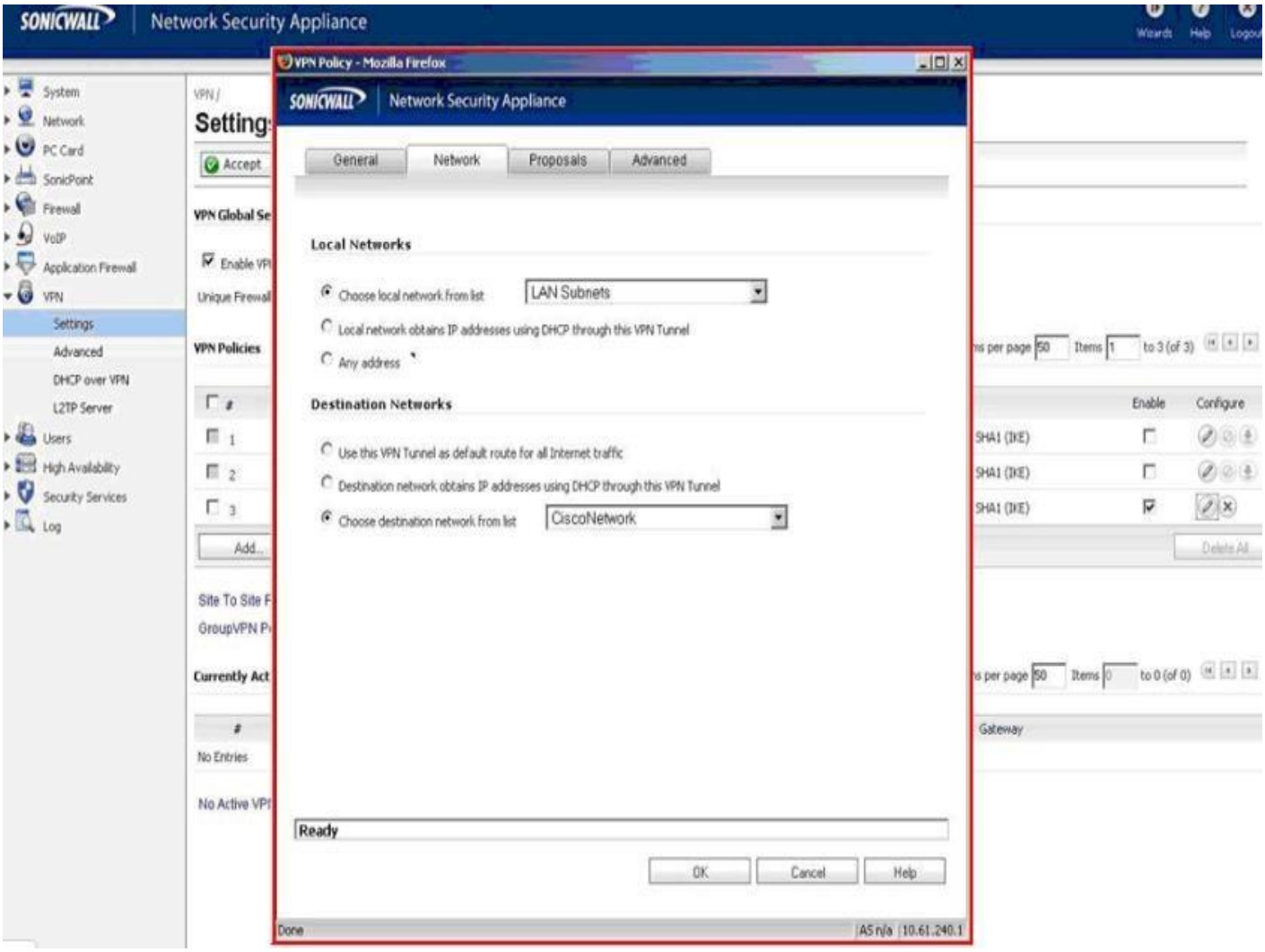


Next, on the SonicWall you must create an SA.

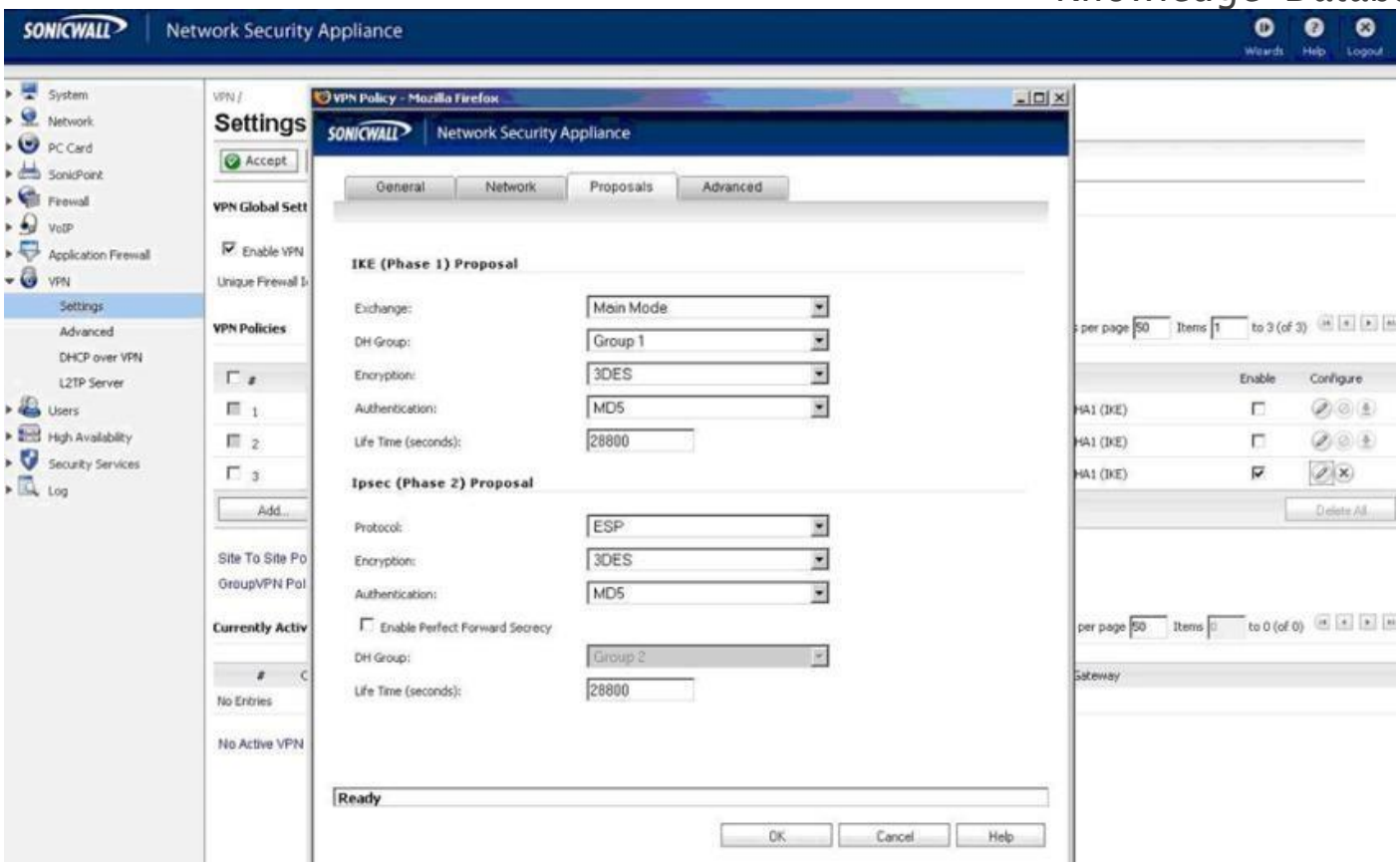
1) Browse to VPN, then Settings (default view for VPN).
2) Ensure that “Enable VPN” is selected.
3) Click Add.
4) Change the Authentication Method to “IKE using pre-shared secret”.
5) Name the SA, in this example “CiscoIOS”.
6) Enter the WAN IP of the Cisco for “IPSec Primary Gateway Name or Address:”.
7) Enter your shared secret, in this example “password”



1) Select the “Network”tab.
2) Select “Lan Subnets” for Local Networks from the drop down box.
   Select the address object previously created for the destination network.



1) Select the “Proposals”tab.
2) Change DH group under IKE Phase 1 to “Group 1”.
3) Change authentication for IKE Phase 1 to “MD5”.
4) Change the authentication for IPSec Phase 2 to “MD5”
5) Do not enable Perfect Forward Secrecy.



1) Select "Advanced" tab.
2) Ensure that keep alive is enabled on only one end of the tunnel.
3) Select "Enable Windows Networking (NetBIOS) Broadcast" if you would like to pass NetBIOS across the VPN.

COMMANDS FOR CISCO IOS

Do not forget to issue the command "write memory" or "copy running-config startup-config" when configuration is complete.

Task: Set ACCESS LIST

Command:

Access-list 101 permit ip 192.168.132.0 0.0.0.255 192.168.170.0 0.0.0.255

Description:

Specify the inside and destination networks. This permits the IP network traffic you want to protect to pass through the router.

Task: Define IKE parameters

Command:

crypto isakmp policy 15

Description:

Identify the policy to create. (Each policy is uniquely identified by the priority number you assign.) (This command puts you into the config-isakmp command mode.)

Calle 140 #11-45. Bogotá D.C. Colombia
+57 1 3680290 / +57 318 4914652
sales@itclatam.com / tss@itclatam.com

Command:
encryption 3des
Description:
To specify the encryption algorithm

Command:
hash md5
Description:
To specify the hash algorithm

Command:
authentication pre-share
Description:
To specify theauthentication

Command:
group 1
Description:
To specify the Diffe-Hellman group identifier

Command:
lifetime 3600
Description:
Specify the security association's lifetime

Command:
exit
Description:
To exit the config-isakmp command mode

Command:
crypto isakmp key password address 10.0.31.102
Description:
To configure a pre-shared authentication key. In this case the pre-shared secret is "password"

Task: Define IPSEC parameters

Command:
crypto ipsec transform-set strong esp-3des esp-md5-hmac
Description:
Configure a transform-set. This identifies the encryption and authentication methods you want to use.

Command:
crypto map tosonicwall 15 ipsec-isakmp
Description:
Create a crypto map that binds together elements of the IPSec configuration. (This command puts you into the crypto map command mode.)

Command:
match address 101
Description:
To specify an extended access list for a crypto map entry

Command:
set transform-set strong
Description:
To specify which transform sets can be used with the crypto map entry

Command:
set peer 10.0.31.102
Description:
To specify an IPSec peer in a crypto map entry

Command:
exit
Description:
To exit the crypto map command mode

Task: Apply Crypto Map to an Interface

Command:
interface fastethernet0/1
Description:
Specify an interface on which to apply the crypto map. (This command puts you into the interface command mode). Please note, you need to specify the interface that you have defined as external (your WAN interface).

Command:
crypto map tosonicwall
Description:
Apply the previously defined crypto map set to an interface

Command:
exit
Description:
Exit the interface command mode

Command:
exit
Description:
Exit the global configuration mode

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.

Technical Notes:

SonicWall has tested VPN interoperability with Cisco IOS SonicOS Standard and Enhanced using the following VPN Security Association information:

Keying Mode: IKE

IKE Mode: Main Mode with No PFS (perfect forward secrecy)

SA Authentication Method: Pre-Shared key

Keying Group: DH (Diffie Hellman) – Group 1

ID_Type: IP

Encryption and Data Integrity: ESP DES with MD5

ESP 3DES with MD5

ESP DES with SHA1

ESP 3DES with SHA1

EXAMPLE setup:

The network configuration shown below is used in the example VPN configuration. The example will configure a VPN using 3DES encryption with MD5 and without PFS.

SonicWall

WAN: IP 10.0.31.102

LAN: 192.168.170.1/24

Cisco IOS

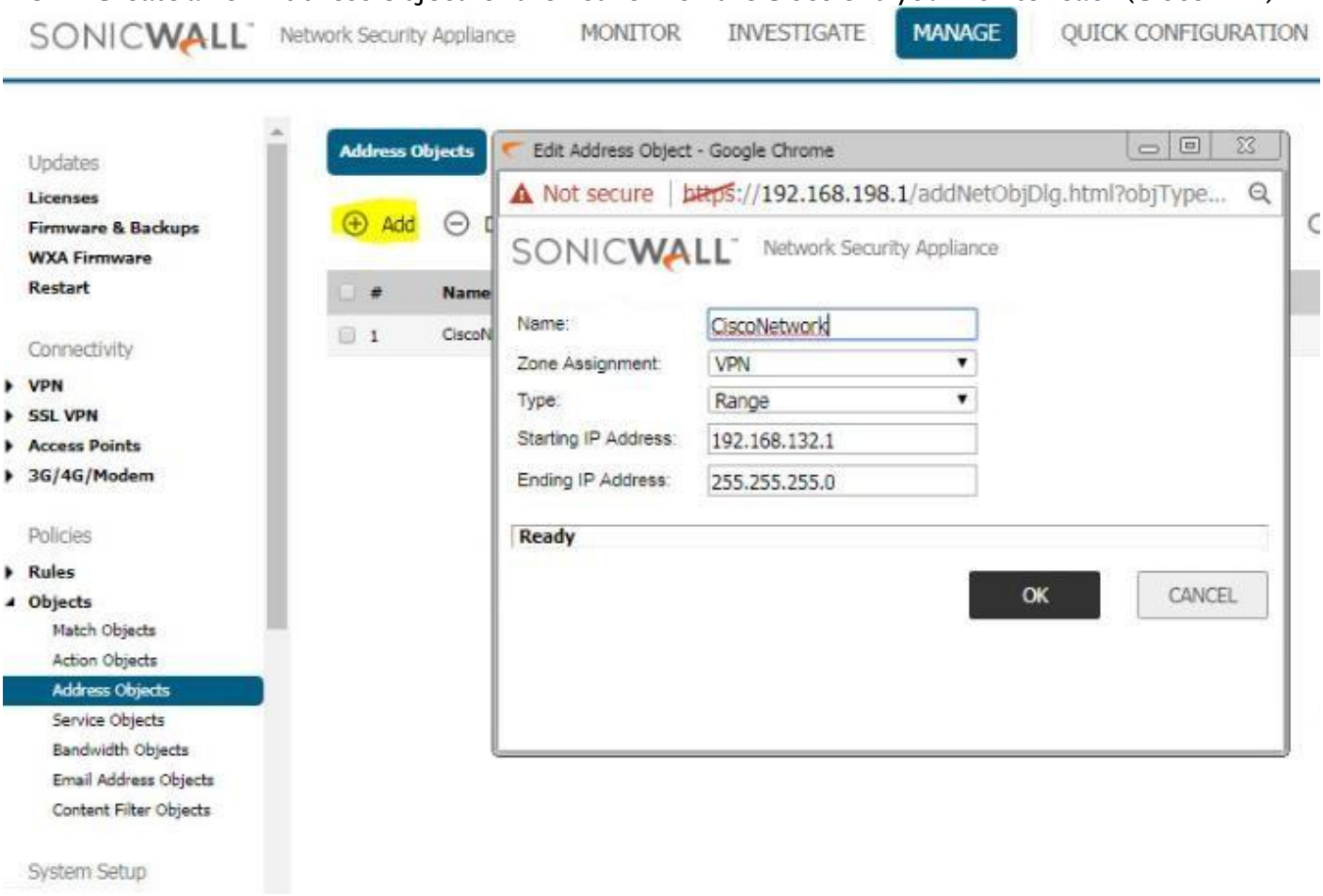
WAN: 10.0.31.132

LAN: IP 192.168.132.1/24

SonicWall Configuration

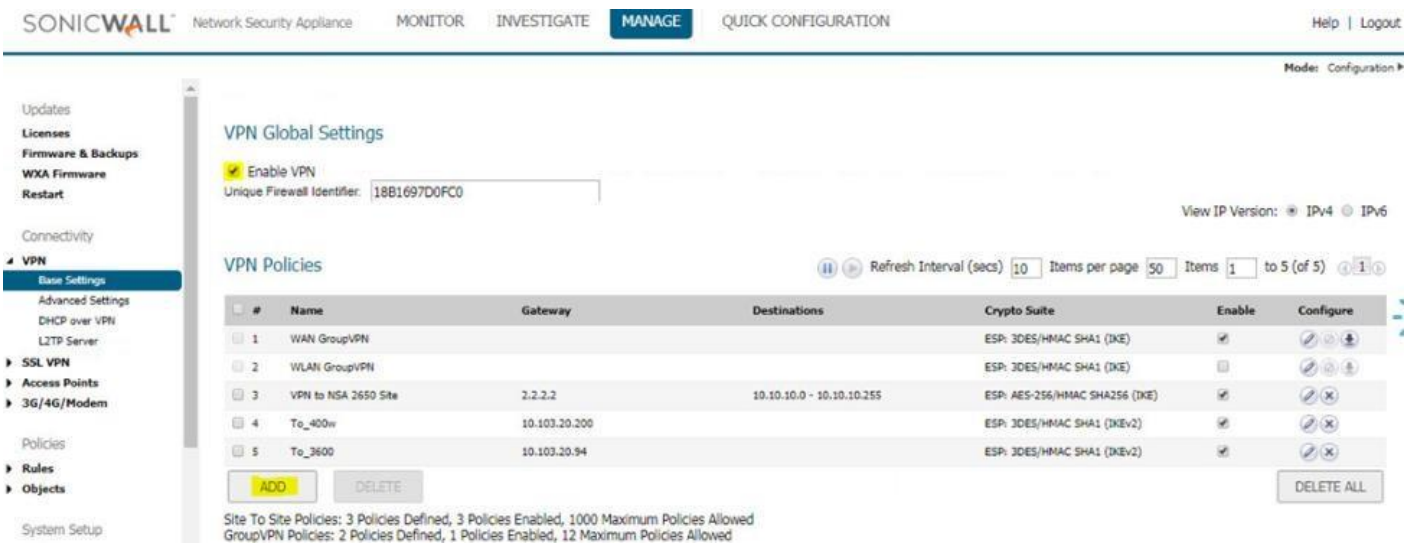
First, on the SonicWall, you must create an address object for the remote network.

1. Log into theSonicWall.
2. Browse to **Manage > Objects > Address Objects**
3. Create a new Address Object for the network on the Cisco end you wish to reach (Cisco LAN).

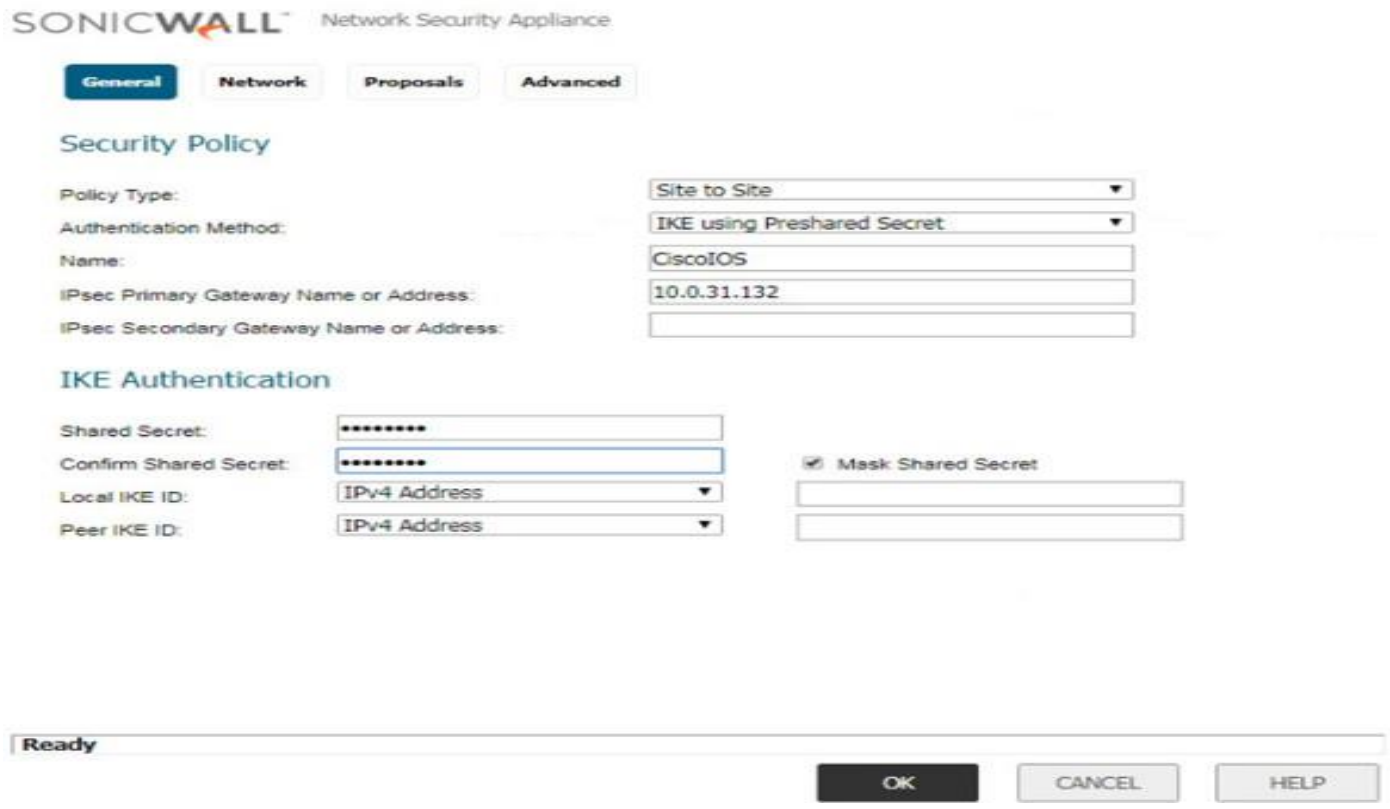


Next, on the SonicWall you must create an SA.

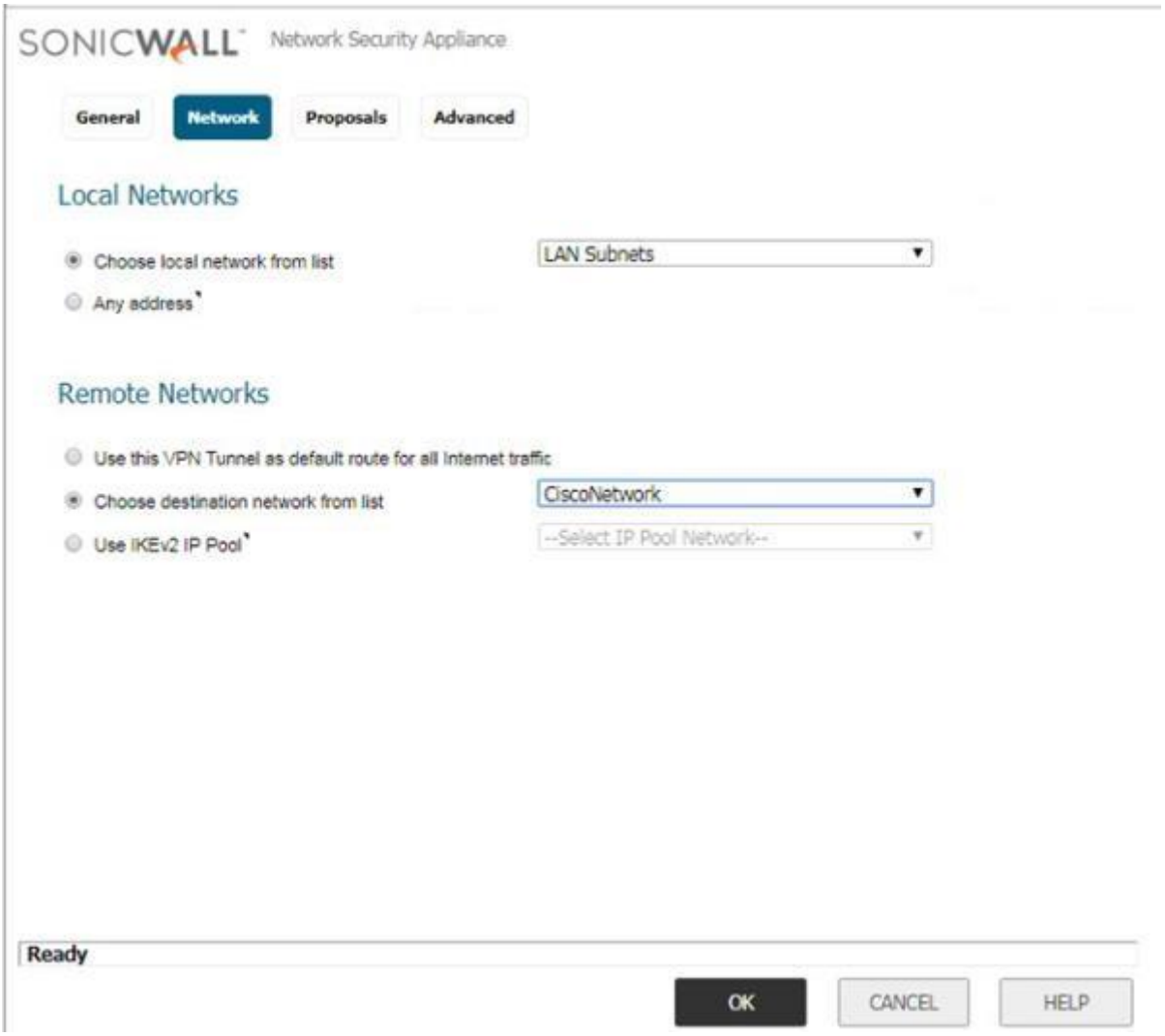
1) Browse to **Manage > VPN > Base Settings.**
2) Ensure that "Enable VPN" is selected.
3) Click Add.



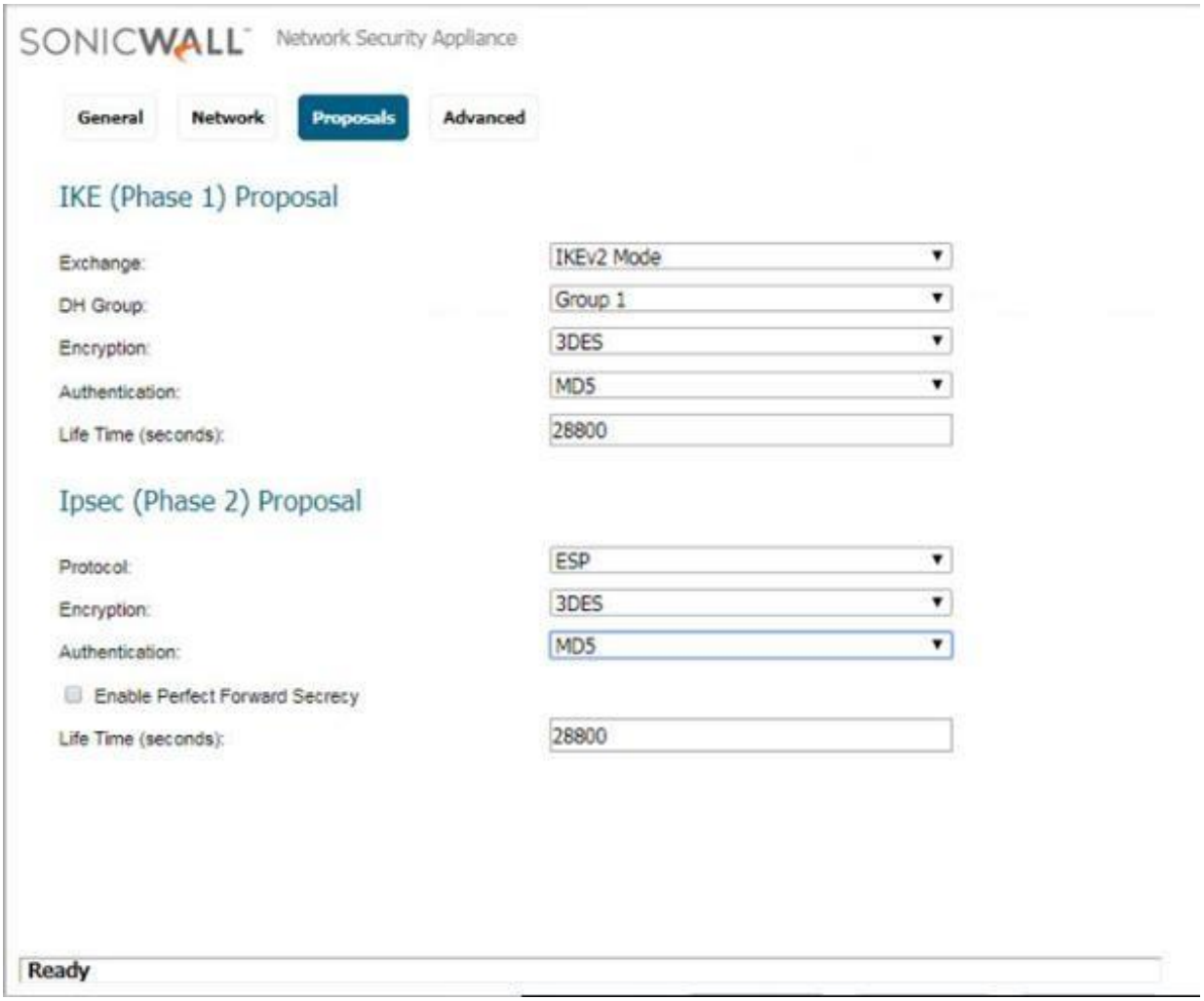
4) Select Authentication Method to “IKE using pre-shared secret”.
5) Name the SA, in this example “CiscoIOS”.
6) Enter the WAN IP of the Cisco for “IPSec Primary Gateway Name or Address:”.
7) Enter your shared secret, in this example “password”



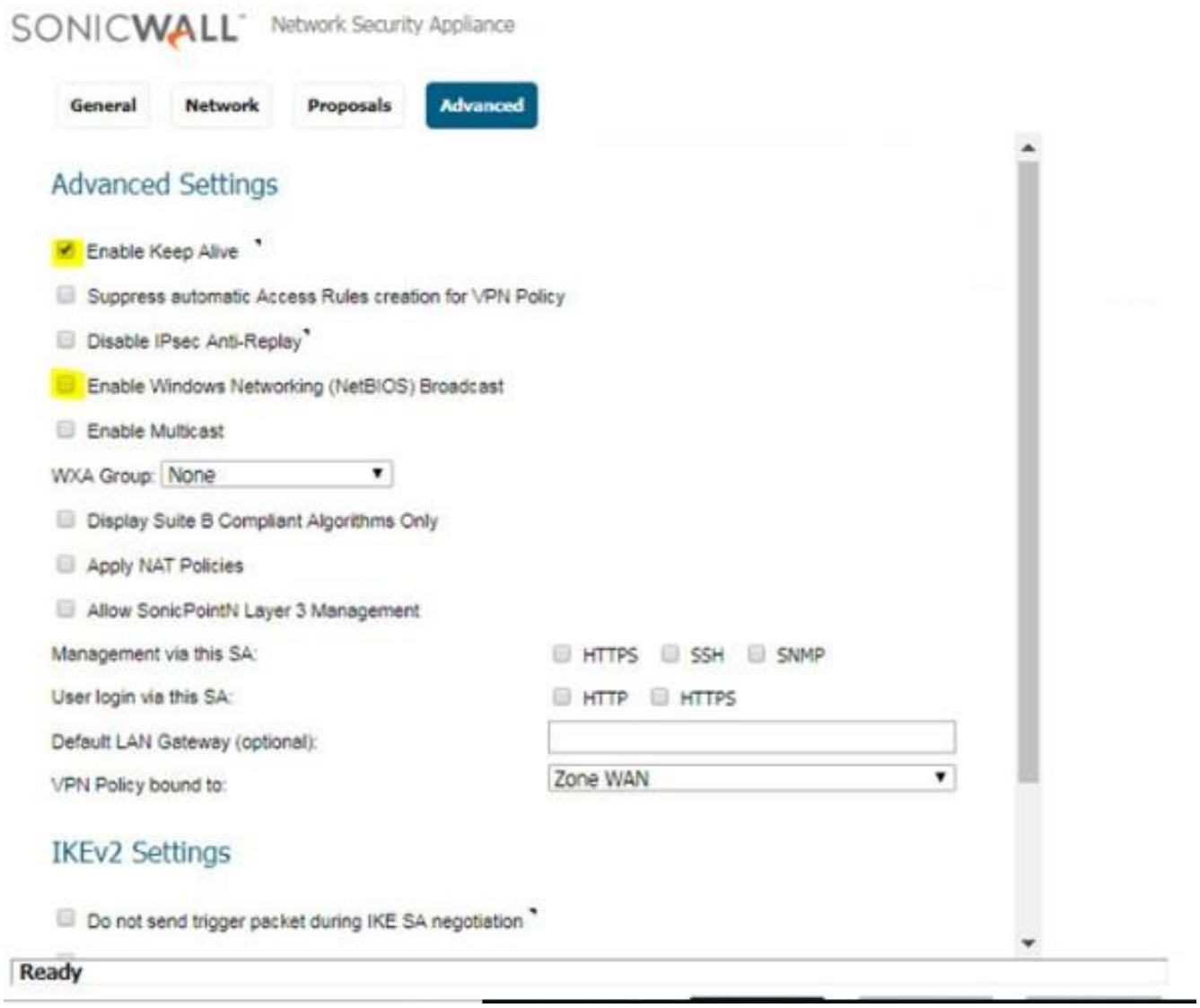
1) Select the “Network”tab.
2) Select “Lan Subnets” for Local Networks from the drop down box.
   Select the address object previously created for the destination network (CiscoNetwork).



1) Select the “Proposals”tab.
2) Change DH group under IKE Phase 1 to “Group 1”.
3) Change authentication for IKE Phase 1 to “MD5”.
4) Change the authentication for IPSec Phase 2 to “MD5”
5) Do not enable Perfect Forward Secrecy.



1) Select "Advanced" tab.
2) Ensure that keep alive is enabled on only one end of the tunnel.
3) Select "Enable Windows Networking (NetBIOS) Broadcast" if you would like to pass NetBIOS across the VPN.



COMMANDS FOR CISCO IOS

Do not forget to issue the command “write memory” or “copy running-config startup-config” when configuration is complete.

Task: Set ACCESS LIST

Command:
Access-list 101 permit ip 192.168.132.0 0.0.0.255 192.168.170.0 0.0.0.255
Description:
Specify the inside and destination networks. This permits the IP network traffic you want to protect to pass through the router.

Task: Define IKE parameters

Command:
crypto isakmp policy15
Description:
Identify the policy to create. (Each policy is uniquely identified by the priority number you assign.) (This command puts you into the config-isakmp command mode.)

Command:
encryption 3des
Description:
To specify the encryption algorithm

Command:
hash md5
Description:
To specify the hash algorithm

Command:
authentication pre-share
Description:
To specify theauthentication

Command:
group 1
Description:
To specify the Diffe-Hellman group identifier

Command:
lifetime 3600
Description:
Specify the security association's lifetime

Command:
exit
Description:
To exit the config-isakmp command mode

Command:
crypto isakmp key password address 10.0.31.102
Description:
To configure a pre-shared authentication key. In this case the pre-shared secret is "password"

Task: Define IPSEC parameters

Command:
crypto ipsec transform-set strong esp-3des esp-md5-hmac
Description:
Configure a transform-set. This identifies the encryption and authentication methods you want to use.

Command:
crypto map tosonicwall 15 ipsec-isakmp
Description:
Create a crypto map that binds together elements of the IPSec configuration. (This command puts you into the crypto map command mode.)

Command:
match address 101
Description:
To specify an extended access list for a crypto map entry

Command:
set transform-set strong
Description:
To specify which transform sets can be used with the crypto map entry

Command:
set peer 10.0.31.102
Description:
To specify an IPSec peer in a crypto map entry

Command:
exit
Description:
To exit the crypto map command mode

Task: Apply Crypto Map to an Interface

Command:
interface fastethernet0/1
Description:
Specify an interface on which to apply the crypto map. (This command puts you into the interface command mode). Please note, you need to specify the interface that you have defined as external (your WAN interface).

Command:
crypto map tosonicwall
Description:
Apply the previously defined crypto map set to an interface

Command:
exit
Description:
Exit the interface command mode

Command:
exit
Description:
Exit the global configuration mode.