SonicWALL VPN with Cisco IOS using IKE

Prepared by SonicWALL, Inc.
6/19/2003

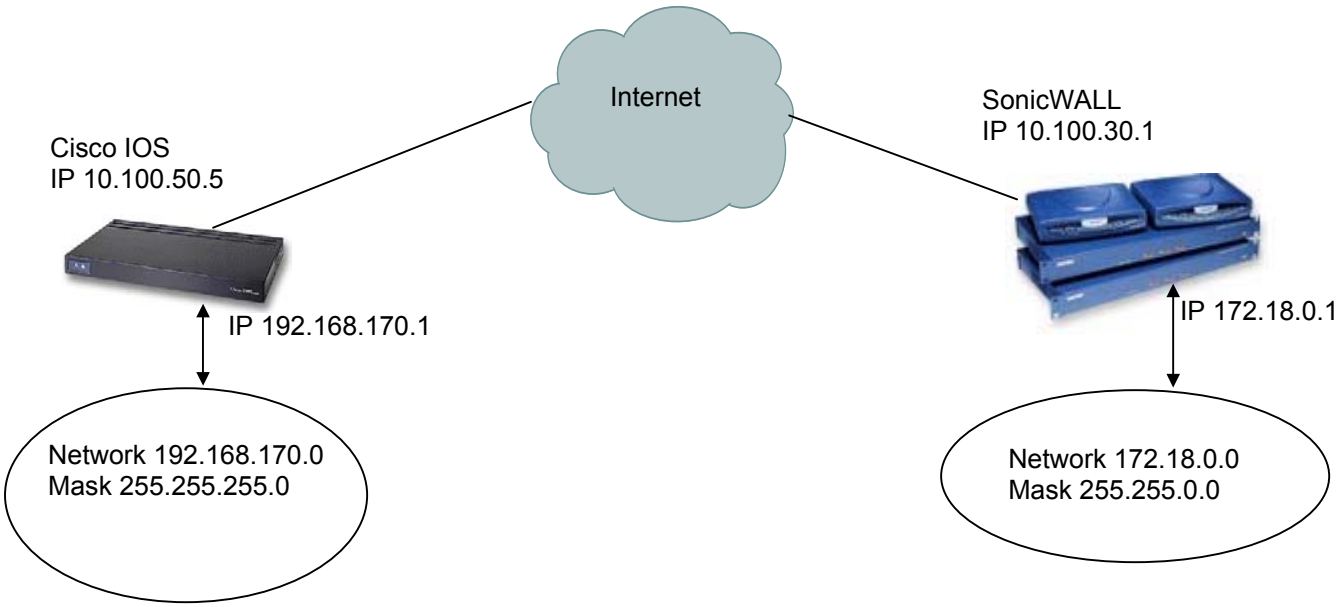
Introduction:
VPN standards are still evolving and interoperability between products is a continued effort. SonicWALL has made progress in this area and is interoperable with Cisco IOS using IKE as shown below. Advanced setups are possible but are not covered in this document.

This tech-note assumes the reader has a working knowledge of Cisco IOS management tools and SonicWALL appliance configuration. This tech-note describes the required steps to set-up a compatible Security Association on both Cisco IOS and SonicWALL products.

Technical Notes:
SonicWALL has tested VPN interoperability with Cisco 2621 version 12.2 and SonicWALL Pro 300 version 6.4.0.0 using the following VPN Security Association information:

Keying Mode:	IKE
IKE Mode:	Main Mode with No PFS (perfect forward secrecy) Example #1 Aggressive Mode with no PFS Example #2
SA Authentication Method:	Pre-Shared key
Keying Group:	DH (Diffie Hellman) – Group 2
Encryption and Data Integrity:	ESP 3DES with SHA1

EXAMPLE #1:
The network configuration shown below is used in the example VPN configuration. The example will configure a VPN using 3DES encryption with SHA1 and without PFS.

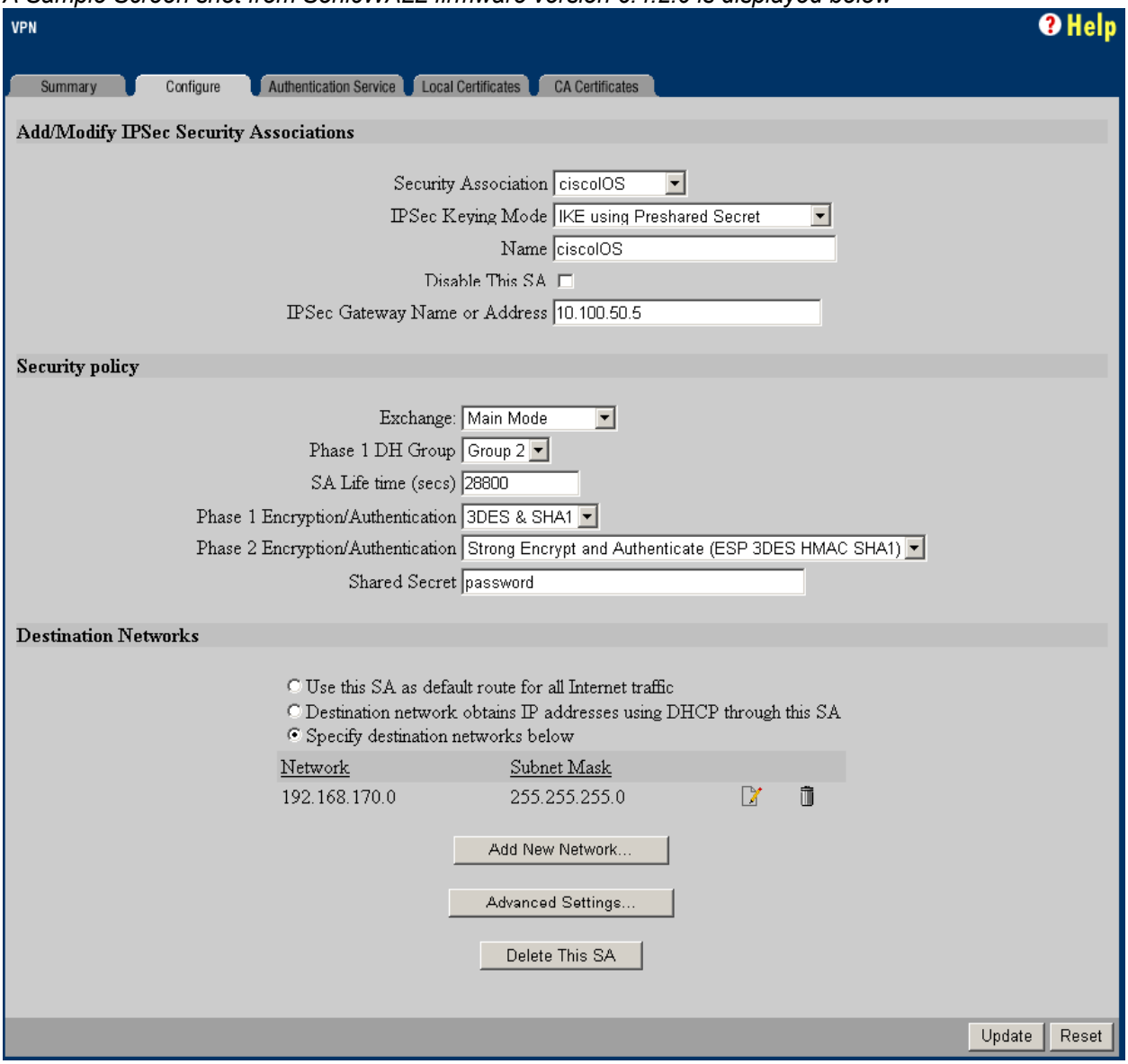


SonicWALL Configuration

On the SonicWALL, create an SA

Select IPSec Keying Mode (In this example, IKE using pre-shared secret)
Name your SA (In this example, ciscoIOS)
Fill in the IPSec gateway (In this example, 10.100.50.5)
Select Main Mode for the Exchange
Select Group 2 for Phase 1 DH Group
Enter Lifetime (In this example, 28800)
Select 3DES & SHA1 for Phase 1 Encryption/Authentication
Select ESP 3DES HMAC SHA1 for Phase 2 Encryption/Authentication
Enter your Shared Secret (In this example, password)
Click Add New Network. Enter Destination Network (In this example, 192.168.170.0). Enter Subnet Mask (In this example, 255.255.255.0). Click Update

A Sample Screen shot from SonicWALL firmware version 6.4.2.0 is displayed below



CISCO IOS Configuration

The Cisco IOS system has a very rich and complex instruction set. Before you proceed to enter commands on the Cisco Product, you must be logged into the enable/configure terminal mode. The commands below are not a complete guide to configuring a Cisco IOS product, but are intended only to guide existing Cisco users. Refer to the Cisco documentation (www.cisco.com) for more information regarding the commands below.

COMMANDS FOR CISCO IOS

Command	Description
Set ACCESS LIST	
access-list 115 permit ip 192.168.170.0 0.0.0.255 172.18.0.0 0.0.255.255	Specify the inside and destination networks. This permits the IP network traffic you want to protect to pass through the router.
Define IKE parameters	
crypto isakmp policy 15	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.)
encryption 3des	To specify the encryption algorithm
hash sha	To specify the hash algorithm
authentication pre-share	To specify the authentication
group 2	To specify the Diffe-Hellman group identifier
lifetime 28800	Specify the security association's lifetime
exit	To exit the config-isakmp command mode
crypto isakmp key password address 10.100.30.1	To configure a pre-shared authentication key. In this case the pre-shared secret is "password"
crypto isakmp identity address	Set the identity type to address
Define IPSEC parameters	
crypto ipsec transform-set strongsha esp-3des esp-sha-hmac	Configure a transform-set. This identifies the encryption and authentication methods you want to use.
crypto ipsec security-association lifetime seconds 28800	Globally sets the IPSec lifetime. Note this will not show in the config file if it is the same as the isakmp lifetime.
crypto map tosonicwall 15 ipsec-isakmp	Create a crypto map that binds together elements of the IPSec configuration. (This command puts you into the crypto map command mode.)
match address 115	To specify an extended access list for a crypto map entry
set transform-set strongsha	To specify which transform sets can be used with the crypto map entry
set peer 10.100.30.1	To specify an IPSec peer in a crypto map entry
exit	To exit the crypto map command mode
Apply Crypto Map to an Interface	
interface fastethernet0/1	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).
crypto map tosonicwall	Apply the previously defined crypto map set to an interface
exit	Exit the interface command mode
exit	Exit the global configuration mode

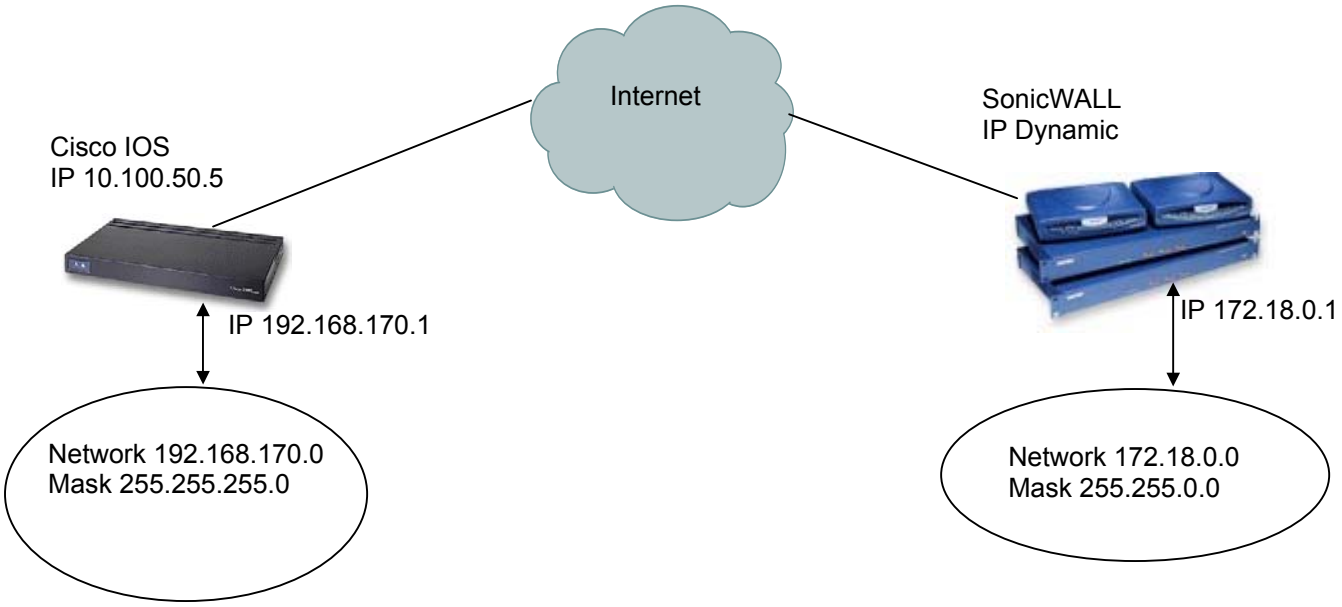
Example #1 IOS Configuration file

```
!
version 12.2
service config
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ios
!
enable secret 5 $1$MVPd$dl6l9A13yQmkfPx465teY0
enable password passwd
!
ip subnet-zero
!
!
!
ip audit notify log
ip audit po max-events 100
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 15
 encr 3des
 authentication pre-share
 group 2
 lifetime 28800
!

crypto isakmp key password address 10.100.30.1
!
!
crypto ipsec security-association lifetime seconds 28800
crypto ipsec transform-set strongsha esp-3des esp-sha-hmac
!
crypto map tosonicwall 15 ipsec-isakmp
 set peer 10.100.30.1
 set transform-set strongsha
 match address 115
!
call rsvp-sync
!
!
!
!
!
!
!
!
interface FastEthernet0/0
 ip address 192.168.170.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1
```

```
 ip address 10.100.50.5 255.255.0.0
 ip nat outside
 speed auto
 half-duplex
 crypto map tosonicwall
!
ip nat inside source route-map nonat interface FastEthernet0/1 overload
ip classless
ip route 0.0.0.0 0.0.0.0 10.100.0.1
no ip http server
ip pim bidir-enable
!
access-list 110 deny   ip 192.168.170.0 0.0.0.255 172.18.0.0 0.0.255.255
access-list 110 permit ip 192.168.170.0 0.0.0.255 any
access-list 115 permit ip 192.168.170.0 0.0.0.255 172.18.0.0 0.0.255.255
route-map nonat permit 10
 match ip address 110
!
!
dial-peer cor custom
!
!
!
!
!
line con 0
line aux 0
line vty 0 4
 password pass
 login
!
end
```

EXAMPLE #2:
The network configuration shown below is used in the example VPN configuration. The example will configure a VPN using 3DES encryption with SHA1, without PFS, and the SonicWALL is getting a dynamic WAN IP address. This means the SonicWALL is using one of the following network modes NAT with DHCP Client, NAT with PPPOE Client, or NAT with L2TP Client.

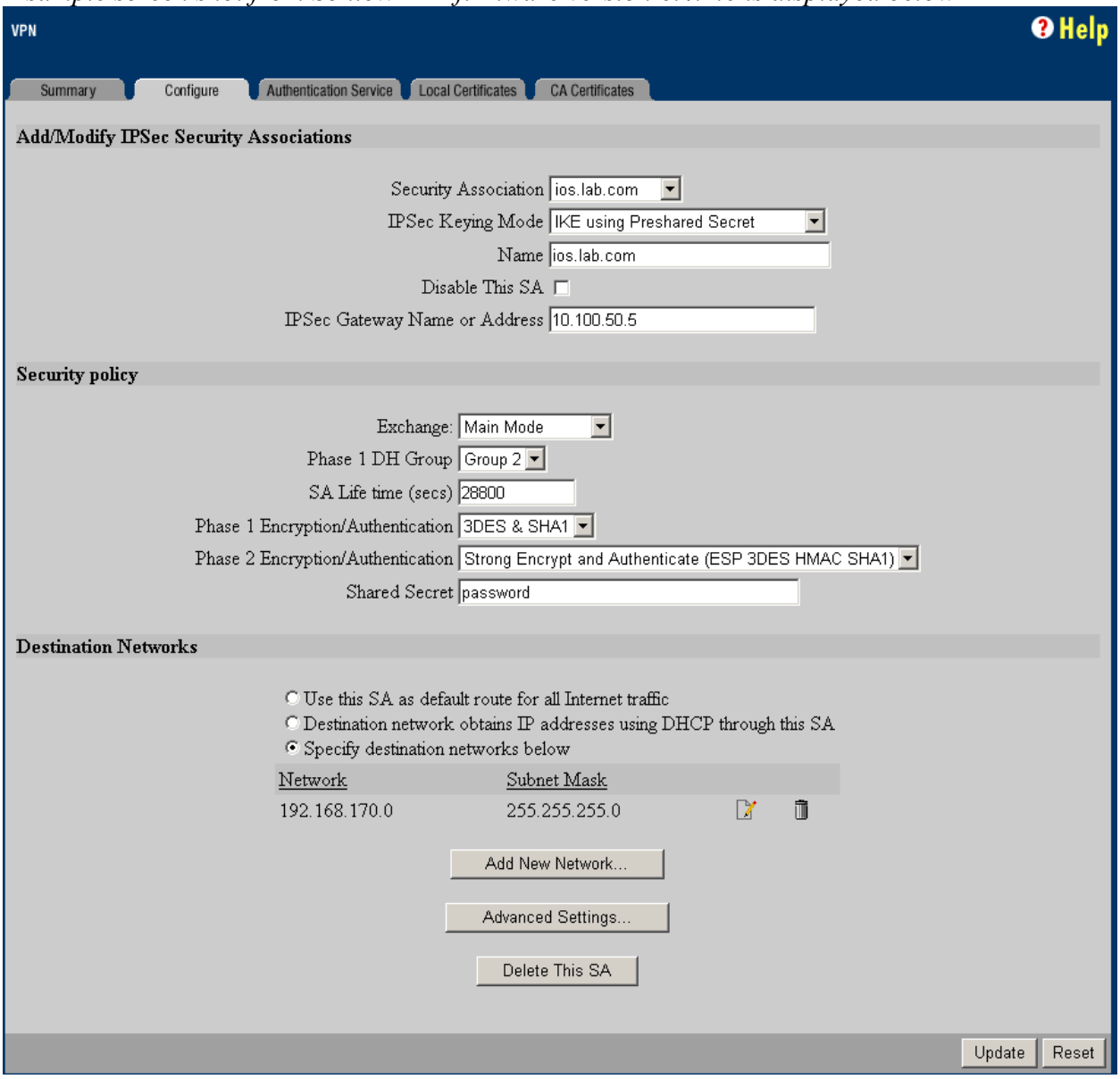


SonicWALL Configuration

On the SonicWALL, create an SA

Select IPSec Keying Mode (In this example, IKE using pre-shared secret)
Name your SA (In this example ios.lab.com. **Note: this needs to be the same as the hostname.domain name on IOS**)
Fill in the IPSec gateway (In this example, 10.100.50.5)
Select Group 2 for Phase 1 DH Group
Enter SA Life time (In this example, 28800)
Select 3DES & SHA1 for Phase 1 Encryption/Authentication
Select ESP 3DES HMAC SHA1 for Phase 2 Encryption/Authentication
Enter your Shared Secret (In this example password)
Click Add New Network. Enter Destination Network (In this example, 192.168.170.0). Enter Subnet Mask (In this example, 255.255.255.0). Click Update

A sample screen shot from SonicWALL firmware version 6.4.2.0 is displayed below



CISCO IOS Configuration

Command	Description
Set ACCESS LIST	
access-list 120 permit ip 192.168.170.0 0.0.0.255 172.18.0.0 0.0.255.255	Specify the inside and destination networks. This permits the IP network traffic you want to protect to pass through the router.
Define IKE parameters	
crypto isakmp policy 20	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.)
encryption 3des	To specify the encryption algorithm
hash sha	To specify the hash algorithm
authentication pre-share	To specify the authentication
group 2	To specify the Diffe-Hellman group identifier
lifetime 28800	Specify the security association's lifetime
exit	To exit the config-isakmp command mode
crypto isakmp key password address 0.0.0.0 0.0.0.0	To configure a pre-shared authentication key. In this case the pre-shared secret is "password"
crypto isakmp identity hostname	Set the identity type to hostname
Define IPSEC parameters	
crypto ipsec transform-set strongsha esp-3des esp-sha-hmac	Configure a transform-set. This identifies the encryption and authentication methods you want to use.
crypto ipsec security-association lifetime seconds 28800	Globally sets the IPSec lifetime. Note this will not show in the config file if it is the same as the isakmp lifetime.
crypto dynamic-map sonicwall 10	Create a crypto map that binds together elements of the IPSec configuration. (This command puts you into the crypto map command mode.)
match address 120	To specify an extended access list for a crypto map entry
set transform-set strongsha	To specify which transform sets can be used with the crypto map entry
exit	To exit the crypto map command mode
crypto map tosonicwall 10 ipsec-isakmp dynamic sonicwall	Associate a dynamic map with a static map
Apply Crypto Map to an Interface	
interface fastethernet0/1	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).
crypto map tosonicwall	Apply the previously defined crypto map set to an interface
exit	Exit the interface command mode
exit	Exit the global configuration mode

Example #2 IOS Configuration File

```
!
version 12.2
service config
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname ios
!
enable secret 5 $1$8HEg$z./a6ojQvLRo002TggotF1
enable password passwd
!
ip subnet-zero
!
!
ip domain-name lab.com
!
ip audit notify log
ip audit po max-events 100
ip ssh time-out 120
ip ssh authentication-retries 3
!
crypto isakmp policy 20
 encr 3des
 authentication pre-share
 group 2
 lifetime 28800
crypto isakmp key password address 0.0.0.0 0.0.0.0
crypto isakmp identity hostname
!
!
crypto ipsec security-association lifetime seconds 28800
crypto ipsec transform-set strongsha esp-3des esp-sha-hmac
!
crypto dynamic-map sonicwall 10
 set transform-set strongsha
 match address 120
!
!
crypto map tosonicwall 10 ipsec-isakmp dynamic sonicwall
!
call rsvp-sync
!
interface FastEthernet0/0
 ip address 192.168.170.1 255.255.255.0
 ip nat inside
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 10.100.50.5 255.255.0.0
 ip nat outside
 speed auto
 half-duplex
 crypto map tosonicwall
```

```
!
ip nat pool INTERNET 10.100.50.15 10.100.50.15 prefix-length 16
ip nat inside source route-map nonat pool INTERNET
ip classless
ip route 0.0.0.0 0.0.0.0 10.100.0.1
no ip http server
ip pim bidir-enable
!
access-list 110 deny   ip 192.168.170.0 0.0.0.255 172.18.0.0 0.0.255.255
access-list 110 permit ip 192.168.170.0 0.0.0.255 any
access-list 120 permit ip 192.168.170.0 0.0.0.255 172.18.0.0 0.0.255.255
dialer-list 1 protocol ip permit
dialer-list 1 protocol ipx permit
route-map nonat permit 10
 match ip address 110
!
!
dial-peer cor custom
!
!
line con 0
line aux 0
line vty 0 4
 password pass
 login
!
end
```

To Test the VPN tunnel:

From the PC behind the Cisco IOS firewall, try to ping 172.18.0.1
From the PC behind the SonicWALL, try to ping 192.168.170.2

Trouble Shooting Tips:

Use the Log Viewer on the Cisco IOS and the SonicWALL to determine if IKE negotiation has started.

If IKE negotiation is complete but pings timeout, the Cisco IOS host computer may need route configuration.

Notes:
You can specify the lifetime for each crypto map instead of using the global setting by entering the following commands.
Example #1:
crypto map tosonicwall 15 ipsec-isakmp
set security-association lifetime seconds 28800
exit
Example #2:
crypto dynamic-map sonicwall 10
set security-association lifetime seconds 28800
exit