VPN Interoperability Between SonicOS Enhanced 3.0 and Cisco PIX Firewall

Introduction

This technote details the steps necessary to create a working IKE IPSec VPN tunnel between SonicOS Enhanced 3.0 and a Cisco PIX Firewall. This technote includes two scenarios for the SonicWALL security device:

- In the first scenario, both devices have static IP addresses (main mode IKE).
- In the second scenario, the SonicWALL has a dynamic IP address and the Cisco PIX has a static IP address (aggressive mode IKE).

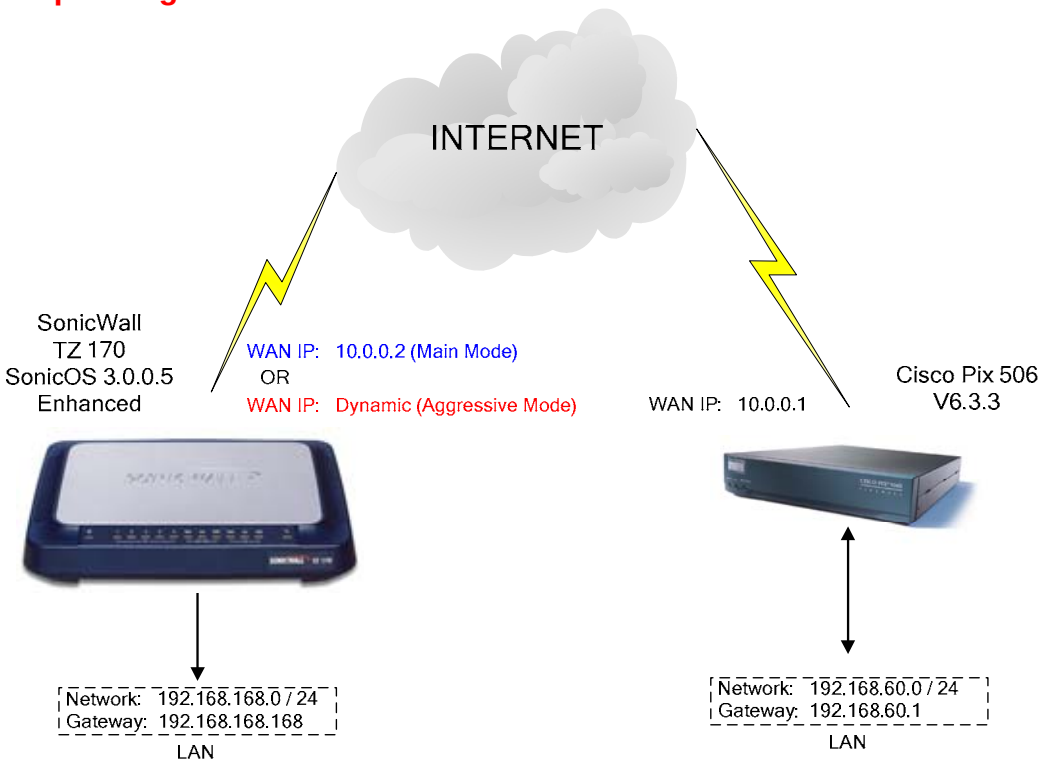
Recommended Versions

- SonicWALL security appliance running SonicOS Enhanced 3.0.0.5 (or greater)
- Cisco PIX Firewall Version 6.3(3)

Caveats

- This technote assumes good working knowledge of the Cisco PIX

Sample Diagram



Tasklist

Main Mode Example:

On the SonicWALL

- Create new network objects and groups
- Create new VPN Policy for the Cisco PIX
- Specify Destination Network, IKE Phase 1 and Phase 2 properties

On Cisco PIX

- Create access list
- Specify NAT
- Define IPSec parameters
- Define ISAKMP parameters

Aggressive Mode Example:

On the SonicWALL

- Create new network objects and groups
- Create new VPN Policy for the Cisco PIX
- Specify Destination Network, IKE Phase 1 and Phase 2 properties

On Cisco PIX

- Create access list
- Specify NAT
- Define IPSec parameters
- Define ISAKMP parameters

Testing:

- Verify that traffic flows through the tunnel.
- Verify that applications function properly through the tunnel.
- Verify that the tunnel can reestablish if either side is disconnected.
- Verify that the network map and documentation match the running configuration.

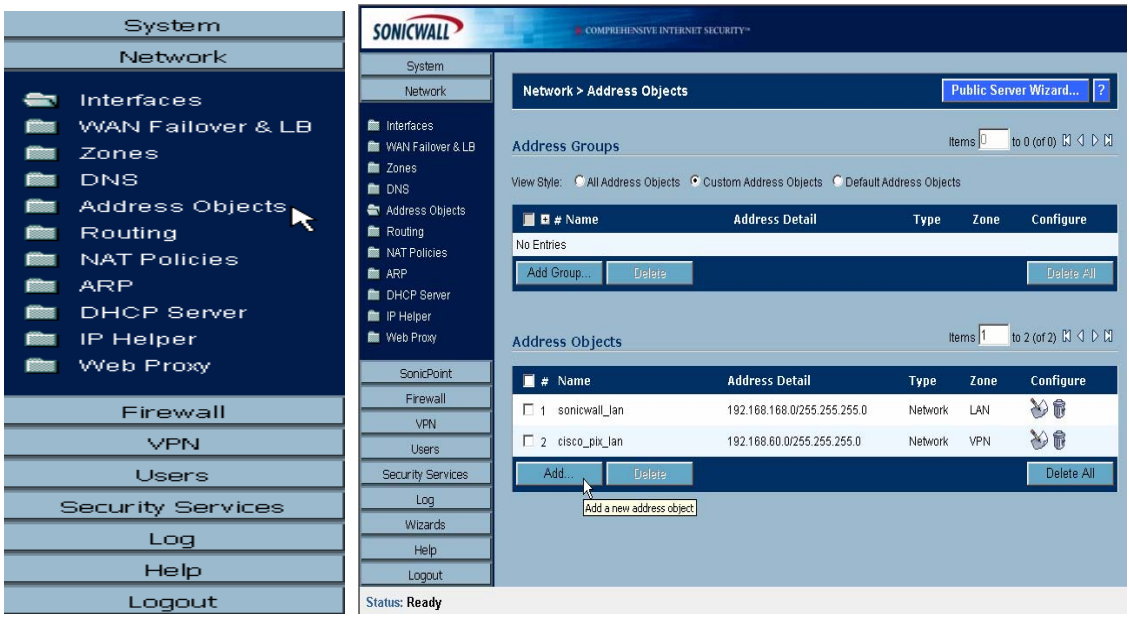
Before You Begin

If you have not already done so, set up a management system connecting to the SonicWALL's internal LAN interface. The SonicWALL should already be configured for Internet access; if not, do this before completing any further steps. The Cisco PIX is also assumed to be properly configured for internet access.

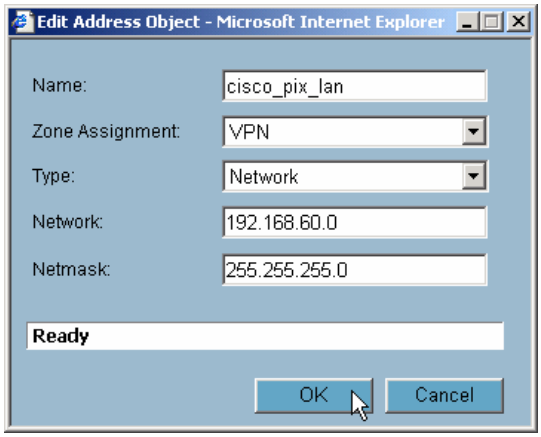
SonicWALL Setup (Main Mode)

Log into the SonicWALL's Management GUI using a current Web browser.

The address objects will be created first, and then a group will be created to contain the address objects. From the navigation bar on the left, click on 'Network' and then 'Address Objects', this will bring up the 'Network > Address Objects' page. In the 'Address Objects' section, click on 'Add' to create the address objects for the networks connected to the Cisco PIX and SonicWALL.



The first address object is for the LAN behind the Cisco PIX.



The **'Name:'** is **"cisco_pix_lan".**

The **'Zone Assignment:'** is **"VPN"**

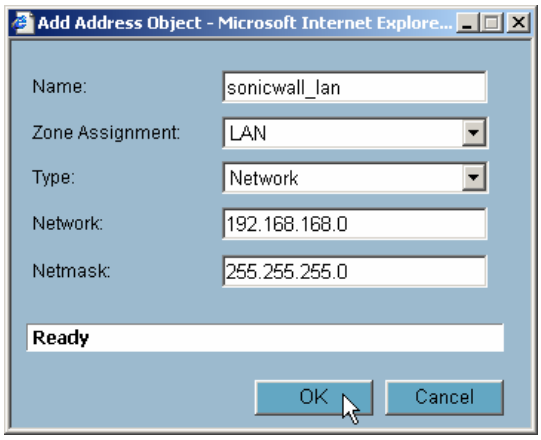
The **'Type:'** is **"Network"**

The **'Network:'** is **"192.168.60.0"**

The **'Netmask:'** is **"255.255.255.0"**

Click **'OK'** to finish.

Then create the address objects for the LAN behind the SonicWALL. Note: the 'sonicwall_lan' object is equivalent to the default "LAN Primary Subnet" object.



The **'Name:'** is **"sonicwall_lan"**

The **'Zone Assignment:'** is **"LAN"**

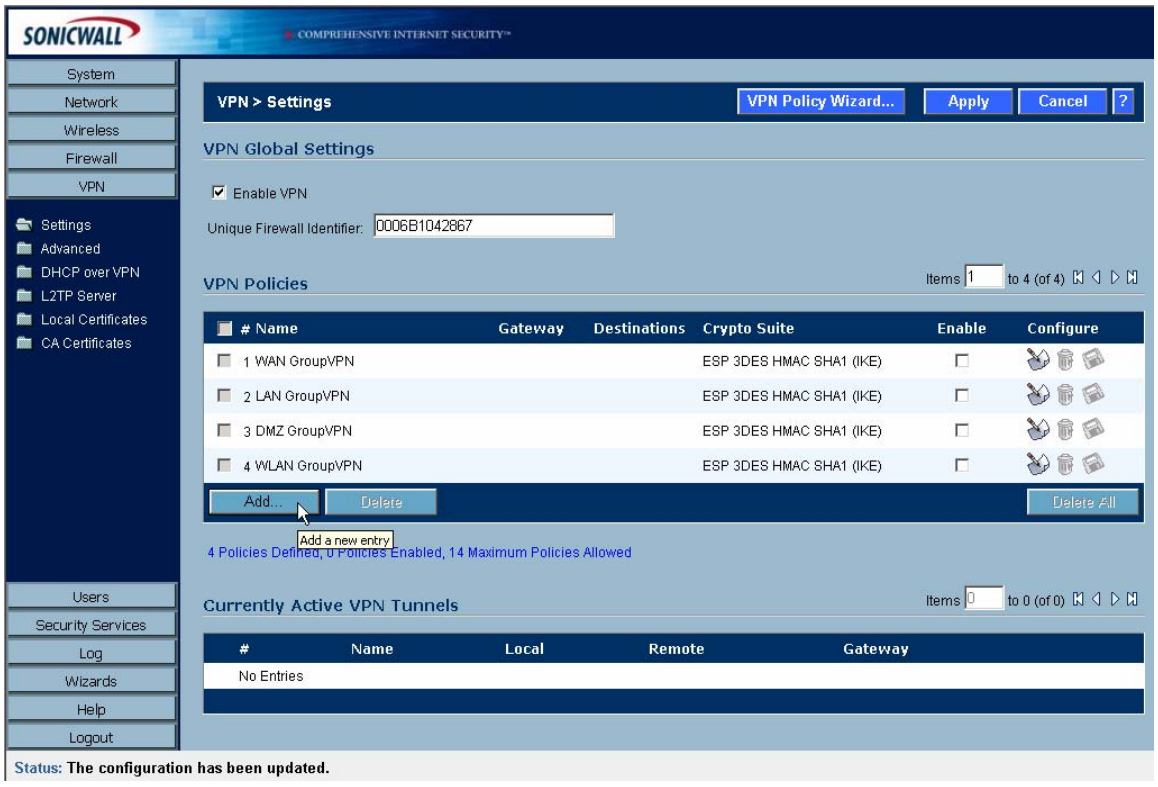
The **'Type:'** is **"Network"**

The **'Network:'** is **"192.168.168.0"**

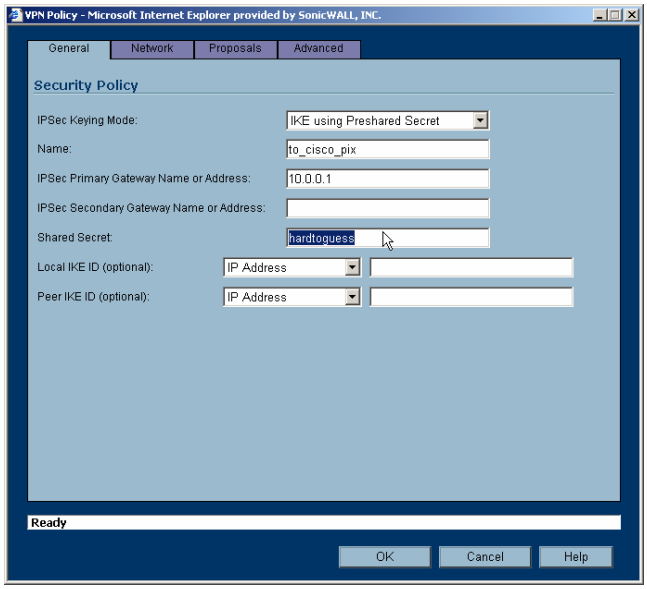
The **'Netmask:'** is **"255.255.255.0"**

Click **'OK'** to finish.

From the navigation bar on the left, click on 'VPN', this will bring up the 'VPN > Settings' page. In the 'VPN Global Settings' section, make sure the 'Enable VPN' radio button is selected. In the 'VPN Policies' section, click on 'Add' to create the new VPN policy for the Cisco PIX.



The ‘VPN Policy’ window will then appear. Go to the ‘General’ tab page, ‘Security Policy’ section.



The **‘IPSec Keying Mode:’** is **“IKE using Preshared Secret”**.

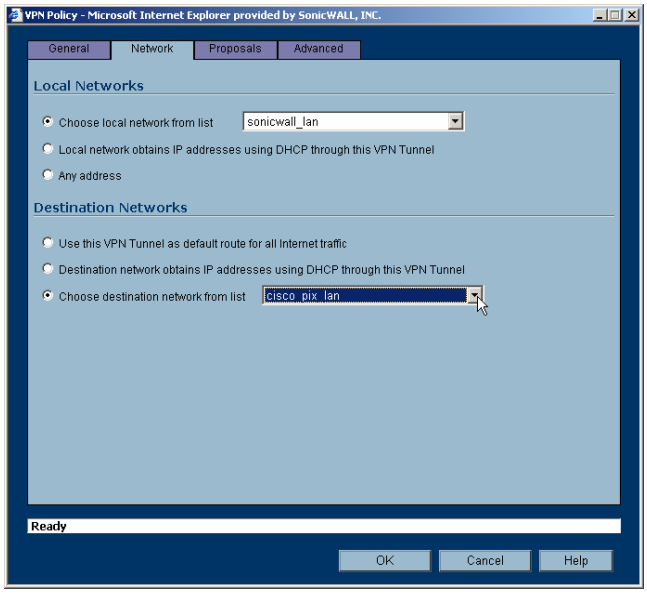
The **‘Name:’** for the VPN policy is **“to_cisco_pix”**.

Enter the IP address **“10.0.0.1”** of the Cisco PIX in the **‘IPSec Primary Gateway Name or Address:’** field.

The **‘Shared Secret:’** is **“hardtoguess”**.

Next select the **‘Network’** tab.

On the ‘Network’ tab,

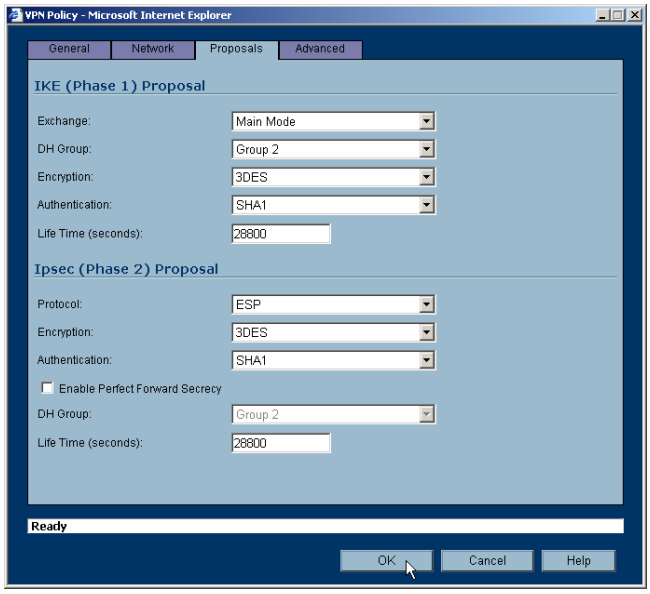


<u>Local Networks</u>
Select the radio button next to **‘Choose local network from list’** and select **“sonicwall_lan”** from the drop-down box.

<u>Destination Networks</u>
Select the radio button next to **‘Choose destination network from list’** and select **“cisco_pix_lan”** from the dropdown box.

Next select the **‘Proposals’** ta**b.**

On the ‘Proposals’ tab.



IKE (Phase 1) Proposal
‘Exchange:’ is **“Main Mode”**
‘DH Group’ is **“Group 2”**
‘Encryption’ is **“3DES”**
‘Authentication’ is **“SHA1”**
‘Life Time (seconds)’ is **“28800”**

Ipsec (Phase 2) Proposal
‘Protocol’ is **“ESP”**
‘Encryption’ is **“3DES”**
‘Authentication’ is **“SHA1”**
‘DH Group’ is **“Group 2”**
‘Life Time (seconds)’ is **“28800”**

Do not enable Perfect Forward Security.

Click **‘OK’** to finish.

This completes the setup on the SonicWALL.

Cisco PIX Setup (Main Mode)

In order to configure the SA on the PIX, you must be logged into the enable/configure terminal mode. For more details on logging into your Cisco Product and configuring settings, refer to the Cisco documentation available online at http://www.cisco.com

Once you are logged into the enable/configure terminal, use the commands below to setup a SA complimentary to the SA setup on the SonicWALL as shown in the sample diagram. The commands below are not a complete guide to configuring a Cisco PIX product, but are intended only to guide existing Cisco users. For more information regarding the commands below, refer to the Cisco PIX Firewall technical documentation: (http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_sw/index.htm).

COMMANDS FOR CISCO PIX

Command	Description
Set ACCESS LIST	
access-list pixtosnwl permit ip 192.168.60.0 255.255.255.0 192.168.168.0 255.255.255.0	Specifies the inside and destination networks
nat (inside) 0 access-list pixtosnwl	This turns NAT off for packets coming from the VPN tunnel
Define IPSec parameters	
sysopt connection permit-ipsec	Specifies that IPSec traffic be implicitly trusted (Allowed)
crypto ipsec transform-set ESP-3DES-SHA esp-des esp-des-hmac	A transform set is an acceptable combination of security protocols and algorithms Here you can specify if you want to use ESP with authentication and 3DES/SHA.
crypto ipsec security-association lifetime seconds 28800	Globally sets the lifetime for IPSec
crypto map tosonicwall 20 ipsec-isakmp	Indicates that IKE will be used to establish the IPSec security associations for protecting the traffic specified by this crypto map entry. 20 is the number assigned to the crypto map entry
crypto map tosonicwall 20 match address pixtosnwl	Specifies an extended access list for a crypto map entry
crypto map tosonicwall 20 set peer 10.0.0.2	Specifies an IPSec peer in a crypto map entry
crypto map tosonicwall 20 set transform-set ESP-3DES-SHA	Specifies which transform sets can be used with the crypto map entry
crypto map tosonicwall interface outside	Evaluates traffic going through the outside interface
Define ISAKMP parameters	
isakmp enable outside	
isakmp key HaRd!_to_Gue55 address 10.0.0.2 netmask 255.255.255.255	Configures a pre-shared authentication key, use the **isakmp key** global configuration command. In this case the pre-shared secret is “hardtoguess”
isakmp identity address	ISAKMP identity PIX uses when participating in IPSec

isakmp policy 20 authentication pre-share	Specifies the authentication method within an IKE policy, use the **authentication** (IKE policy) ISAKMP policy configuration command.
isakmp policy 20 encryption 3des	Specifies the encryption algorithm within an IKE policy
isakmp policy 20 hash sha	Specifies the hash algorithm within an IKE policy
isakmp policy 20 group 2	Specifies DH group 1
isakmp policy 20 lifetime 28800	Sets the life time intervals before IKE is renegotiated. The value 28800 can be changed.

Example #1 Sample Cisco PIX configuration file:

PIX Version 6.3(3)

interface ethernet0 10full
interface ethernet1 10full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pixfirewall
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list pixtosnwl permit ip 192.168.60.0 255.255.255.0 192.168.168.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside 10.0.0.1 255.255.255.0
ip address inside 192.168.60.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm logging informational 100
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list pixtosnwl
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 10.0.0.2 1
timeout xlate 0:05:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
http server enable
http 192.168.60.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec

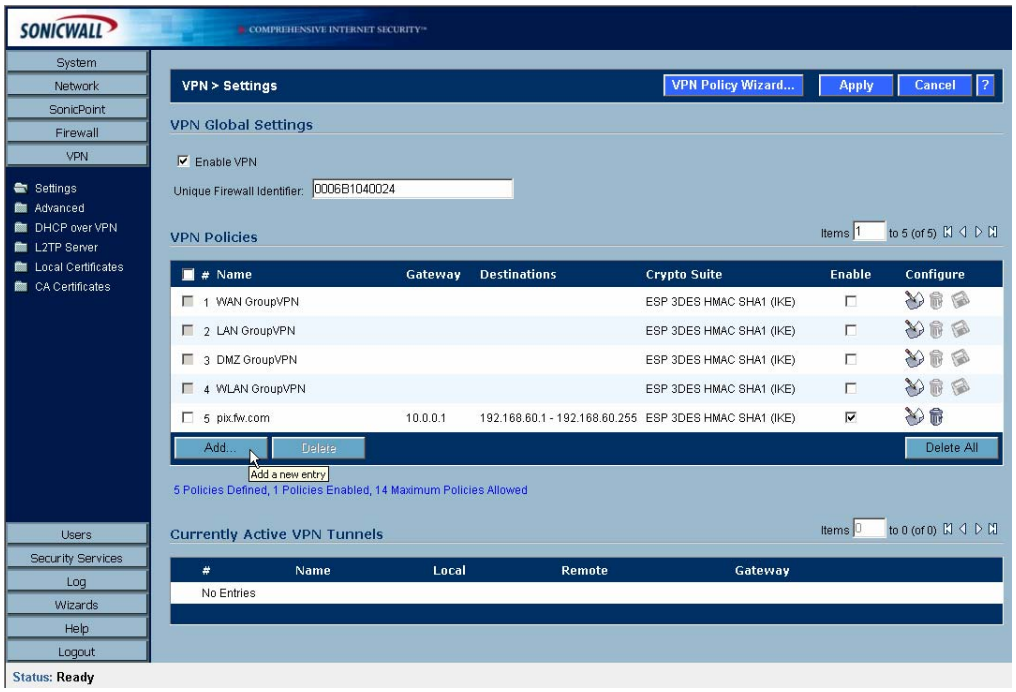
crypto ipsec transform-set strong esp-3des esp-sha-hmac
crypto map tosnwl 20 ipsec-isakmp
crypto map tosnwl 20 match address pixtosnwl
crypto map tosnwl 20 set peer 10.0.0.2
crypto map tosnwl 20 set transform-set strong
crypto map tosnwl interface outside
isakmp enable outside
isakmp key ****** address 10.0.0.2 netmask 255.255.255.255**
isakmp identity address
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption 3des
isakmp policy 20 hash sha
isakmp policy 20 group 2
isakmp policy 20 lifetime 28800
telnet timeout 5
ssh timeout 5
console timeout 0
dhcpd address 192.168.60.2-192.168.60.254 inside
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd auto_config outside
dhcpd enable inside
terminal width 80
Cryptochecksum:1ca7beb2e6b2d7c302085f4b14848d7a
: end

This completes the setup on the Cisco PIX and the main mode example.

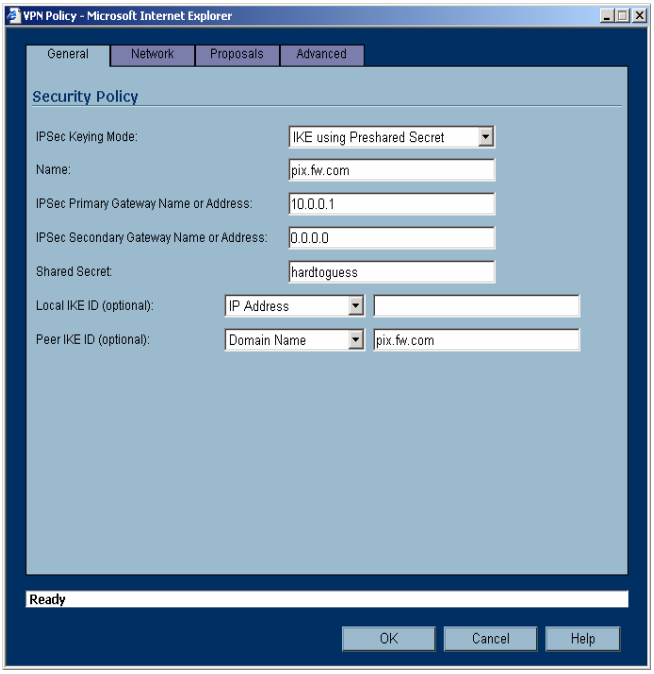
SonicWALL Setup (Aggressive Mode)

In this example the WAN IP address on the SonicWALL is dynamic while the WAN IP of the Cisco PIX is static. This scenario is typical of using a broadband connection such as DSL or cable modem. It is assumed that the WAN connection is setup and functional.

The first step is to create a new VPN Policy. Click on the '**Add**…' button to create a new entry.



Go to the 'General' tab page, 'Security Policy' section.



The **'IPSec Keying Mode:'** is **"IKE using Preshared Secret"**.

The **'Name:'** for the VPN policy has to match the FQDN of the Cisco PIX **"pix.fw.com"**.

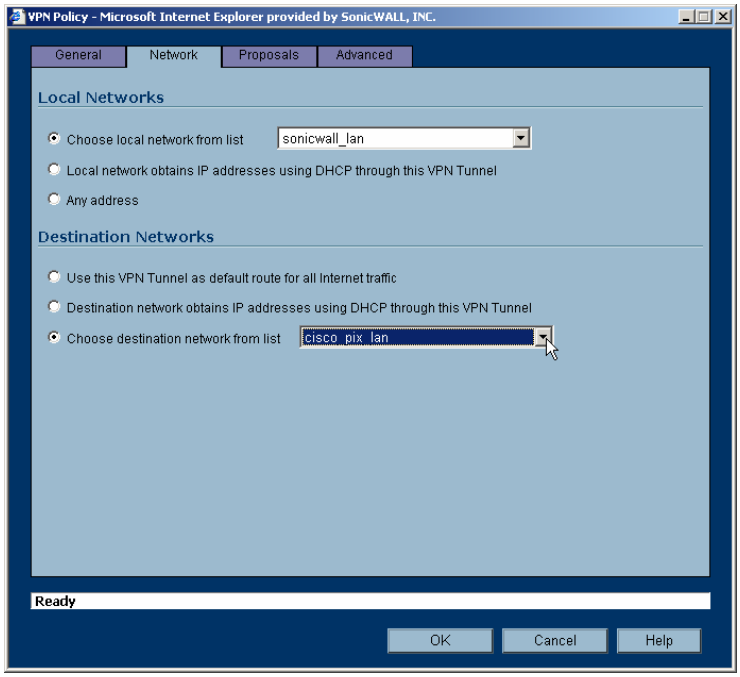
Enter the IP address **"10.0.0.1"** of the Cisco PIX in the **'IPSec Primary Gateway Name or Address:'** field.

The **'Shared Secret:'** is **"hardtoguess"**.

The **'Peer IKE ID (optional):'** should be **'Domain Name'** and the FQDN of the Cisco PIX **"pix.fw.com"**.

Next select the **'Network'** tab.

Go to the ‘Network’ tab page.

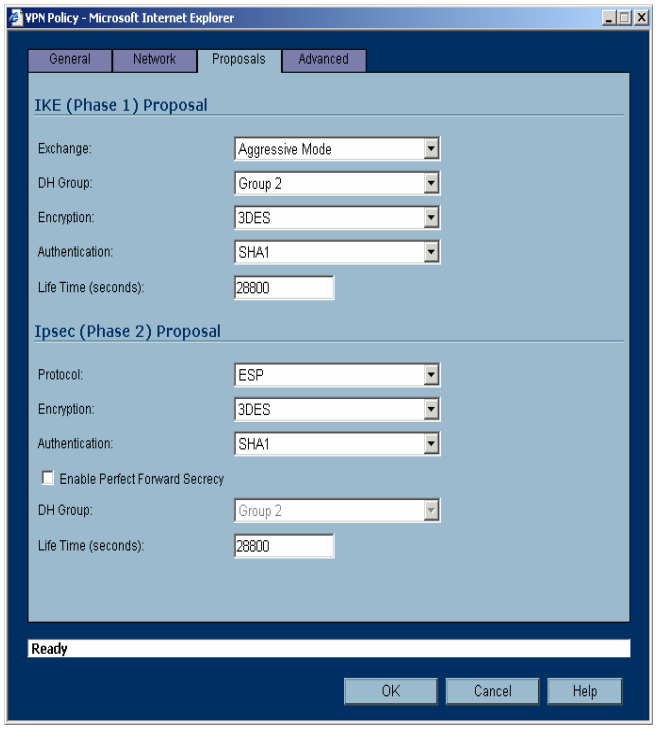


Local Networks
Select the radio button next to **‘Choose local network from list’** and select **“sonicwall_lan”** from the drop-down box.

Destination Networks
Select the radio button next to **‘Choose destination network from list’** and select **“cisco_pix_lan”** from the drop-down box.

Next select the **“Proposals”** tab.

On the “Proposals” tab.



IKE (Phase 1) Proposal
‘Exchange:’ is **“Aggressive Mode”**
‘DH Group’ is **“Group 2”**
‘Encryption’ is **“3DES”**
‘Authentication’ is **“SHA1”**
‘Life Time (seconds)’ is **“28800”**

Ipsec (Phase 2) Proposal
‘Protocol’ is **“ESP”**
‘Encryption’ is **“3DES”**
‘Authentication’ is **“SHA1”**
‘DH Group’ is **“Group 2”**
‘Life Time (seconds)’ is **“28800”**

Do not enable Perfect Forward Security.

Click **‘OK’** to finish.

Cisco PIX Setup (Aggressive Mode)

Command	Description
Set ACCESS LIST	
access-list pixtosnwl permit ip 192.168.60.0 255.255.255.0 192.168.168.0 255.255.255.0	Specifies the inside and destination networks
nat (inside) 0 access-list pixtosnwl	This turns NAT off for packets coming from the VPN tunnel
Define IPSec parameters	
sysopt connection permit-ipsec	Specifies that IPSec traffic be implicitly trusted (Allowed)
crypto ipsec transform-set strong esp-3des esp-sha-hmac	A transform set is an acceptable combination of security protocols and algorithms Here you can specify if you want to use ESP with authentication and 3DES/SHA.
crypto ipsec security-association lifetime seconds 28800	Globally sets the lifetime for IPSec
crypto dynamic-map cisco 1 set transform-set strong	The dynamic crypto map entry allows you to set up IPSec security associations with a previously unknown IPSec peer.
crypto map dyn-map 10 ipsec-isakmp dynamic cisco	Specifies an dynamic access list for a crypto map entry
crypto map dyn-map interface outside	Evaluates traffic going through the outside interface
Define ISAKMP parameters	
isakmp enable outside	
isakmp key hardtoguess address 0.0.0.0 netmask 0.0.0.0	Configures a pre-shared authentication key, use the **isakmp key** global configuration command. In this case the pre-shared secret is “hardtoguess”
isakmp identity hostname	ISAKMP identity PIX uses when participating in IPSec.
isakmp policy 20 authentication pre-share	Specifies the authentication method within an IKE policy, use the **authentication** (IKE policy) ISAKMP policy configuration command.
isakmp policy 20 encryption 3des	Specifies the encryption algorithm within an IKE policy
isakmp policy 20 hash sha	Specifies the hash algorithm within an IKE policy
isakmp policy 20 group 2	Specifies DH group 1
isakmp policy 20 lifetime 28800	Sets the life time intervals before IKE is renegotiated. The value 28800 can be changed.

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.

Agressive Mode Sample PIX configuration File:

```
:
PIX Version 6.3(3)
interface ethernet0 10full
interface ethernet1 10full
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix
domain-name fw.com
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
access-list pixtosnwl permit ip 192.168.60.0 255.255.255.0 192.168.168.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
ip address outside 10.0.0.1 255.255.255.0
ip address inside 192.168.60.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm logging informational 100
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list pixtosnwl
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 10.0.0.2 1
timeout xlate 0:05:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
http server enable
http 192.168.60.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
crypto ipsec transform-set strong esp-3des esp-sha-hmac
crypto dynamic-map cisco 1 set transform-set strong
crypto map dyn-map 10 ipsec-isakmp dynamic cisco
crypto map dyn-map interface outside
isakmp enable outside
isakmp key hardtoguess address 0.0.0.0 netmask 0.0.0.0
isakmp identity hostname
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption 3des
isakmp policy 20 hash sha
isakmp policy 20 group 2
isakmp policy 20 lifetime 28800
telnet timeout 5
```

```
ssh timeout 5
console timeout 0
dhcpd address 192.168.60.2-192.168.60.254 inside
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd auto_config outside
dhcpd enable inside
terminal width 80
Cryptochecksum:ca6aacd0a16d238a429397616b935c53
: end
```

Cisco PIX TESTING

show crypto isakmp sa – Displays all current IKE security associations (SAs) at a peer

show crypto ipsec sa – Displays the settings used by current [IPSEC] SAs.

This completes the setup on the Cisco PIX.

Testing

- From the management consoles of both the SonicWALL and Cisco verify the active VPN Tunnels.
- Pass traffic between all subnets to verify tunnel operation.
- Optional, if the environment allows downtime, reboot both the SonicWALL and Cisco and verify that the tunnels reestablish; verify again that traffic is again flowing.

Troubleshooting

- Create a diagram of the network. Include all network information and security association parameters. Include desired traffic flows. Be as specific as possible. When the diagram is complete, compare it with the configuration of each device. Verify that the configuration of each device is consistent with the diagram. This exercise should rule out most common configuration errors. The diagram is also good documentation.
- Verify all IPSec Security Association parameters match. Verify the Security policy parameters match. Verify that the VPN destination network parameters match. Verify the objects created match. This may sound repetitive, but one error can cause the configuration to not work.
- Verify the network routes. Verify the ARP tables on each device are correct.

Created: November 15, 2004
Updated: March 10, 2005
Version 1.2