

SonicWALL VPN with Cisco PIX using IKE

Prepared by SonicWALL, Inc.

7/15/2002

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 PIX using IKE as shown below.

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

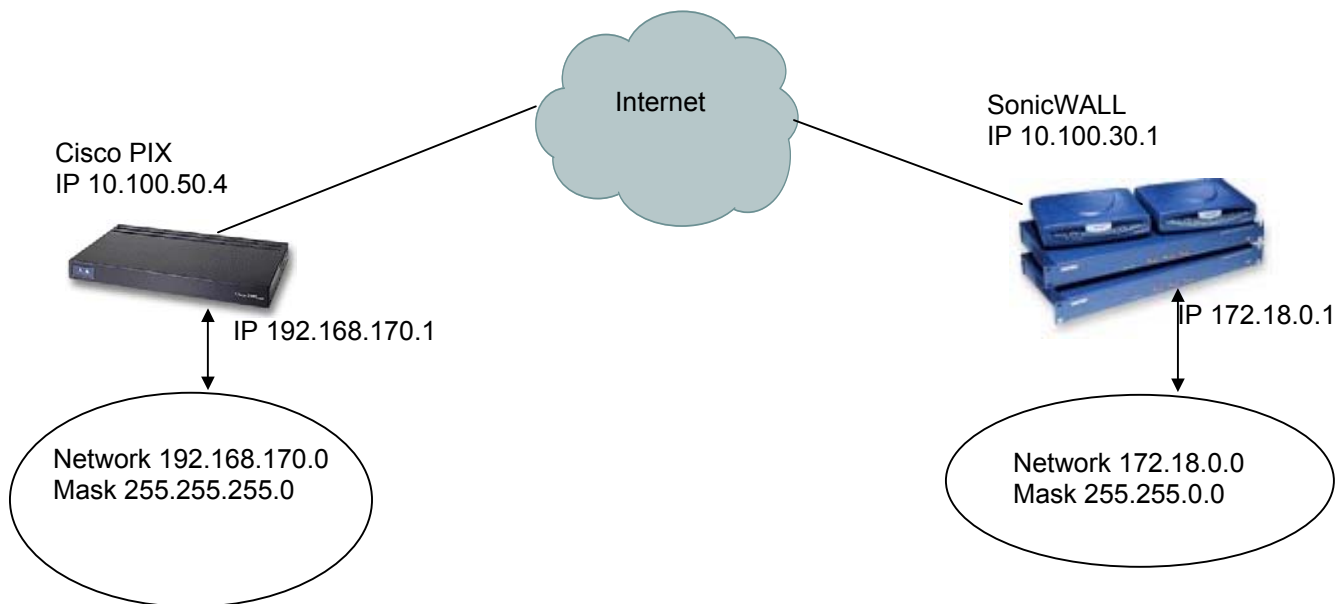
Technical Notes:

SonicWALL has tested VPN interoperability with Cisco PIX 506 version 6.2(1) and SonicWALL Pro 300 version 6.3.1.2 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

Change the IPsec Keying Mode to IKE using pre-shared secret

Name your SA. (In this example pix)

Fill in the IPsec gateway (in this example 10.100.50.4)

Select Group 2 for Phase 1 DH Group

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)

Fill in the appropriate Destination Network (in this example 192.168.170.0) and Subnet Mask (in this example 255.255.255.0)

A Sample Screen shot from SonicWALL firmware version 6.3.1.2 is displayed below

The screenshot shows the 'Add/Modify IPsec Security Associations' configuration page in the SonicWALL VPN management console. The interface includes a navigation bar with tabs for Summary, Configure, Authentication Service, Local Certificates, and CA Certificates. The main configuration area is divided into three sections: Security Association, Security policy, and Destination Networks.

Security Association:

- Security Association: pix
- IPsec Keying Mode: IKE using Preshared Secret
- Name: pix
- Disable This SA:
- IPsec Gateway Address: 10.100.50.4

Security policy:

- Phase 1 DH Group: Group 2
- SA Life time (secs): 28800
- Phase 1 Encryption/Authentication: 3DES & SHA1
- Phase 2 Encryption/Authentication: Strong Encrypt and Authenticate (ESP 3DES HMAC SHA1)
- Shared Secret: password

Destination Networks:

- Use this SA as default route for all Internet traffic:
- Destination network obtains IP addresses using DHCP through this SA:
- Specify destination networks below:

Network	Subnet Mask		
192.168.170.0	255.255.255.0		

Buttons: Add New Network..., Advanced Settings..., Delete This SA, Update, Reset

SonicWALL VPN with Cisco PIX using IKE

Click on Advanced Settings
Select Group 2 for Phase 2 DH Group
Click OK
Click Update

A sample screen shot from SonicWALL firmware version 6.3.1.2 is displayed below

Edit Advanced Settings

Use Aggressive Mode

Enable Keep Alive

Require authentication of local users

Require authentication of remote users

Remote users behind VPN gateway
 Remote VPN clients with XAUTH

Enable Windows Networking
(NetBIOS) broadcast

Apply NAT and firewall rules

Forward packets to remote VPNs

Enable Perfect Forward Secrecy

Phase 2 DH Group

Default LAN Gateway

VPN Terminated at LAN DMZ LAN/DMZ

Note that after clicking OK you must click Update on the main page to save changes made here.

CISCO PIX Configuration

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, please 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 above in the screen shot.

The commands below are not a complete guide to configuring a Cisco PIX 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 PIX

Command	Description
Set ACCESS LIST	
access-list pixtosw permit ip 192.168.170.0 255.255.255.0 172.18.0.0 255.255.0.0	Specifies the inside and destination networks
nat (inside) 0 access-list pixtosw	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 strongsha 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 DES or 3DES.
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 pixtosw	To specify an extended access list for a crypto map entry
crypto map tosonicwall 20 set peer 10.100.30.1	To specify an IPSec peer in a crypto map entry,
crypto map tosonicwall 20 set transform-set strongsha	To specify 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 password address 10.100.30.1 netmask 255.255.255.255	To configure a pre-shared authentication key, use the isakmp key global configuration command. In this case the pre-shared secret is "password"
isakmp identity address	ISAKMP identity PIX uses when participating in IPSec.
isakmp policy 20 authentication pre-share	To specify the authentication method within an IKE policy, use the authentication (IKE policy) ISAKMP policy configuration command.
isakmp policy 20 encryption 3des	To specify the encryption algorithm within an IKE policy
isakmp policy 20 hash sha	To specify the hash algorithm within an IKE policy
isakmp policy 20 group 2	This specifies DH group 1
isakmp policy 20 lifetime 28800	This commands sets the life time intervals before IKE is renegotiated. The value 28800 can be changed.

Example #1 PIX configuration File:

```
: Saved
: Written by enable_15 at 10:18:37.939 UTC Fri Jun 14 2002
PIX Version 6.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2Yjlyt7RRXU24 encrypted
passwd 2KFQnbNIdl.2KYOU encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list pixtosw permit ip 192.168.170.0 255.255.255.0 172.18.0.0 255.255.0.0
pager lines 24
interface ethernet0 10full
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 10.100.50.4 255.0.0.0
ip address inside 192.168.170.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 10.100.50.14
nat (inside) 0 access-list pixtosw
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
route outside 0.0.0.0 0.0.0.0 10.100.0.1 1
route inside 192.168.180.0 255.255.255.0 192.168.170.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 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
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
no floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set strongsha esp-3des esp-sha-hmac
crypto ipsec security-association lifetime seconds 28800
crypto map tosonicwall 20 ipsec-isakmp
crypto map tosonicwall 20 match address pixtosw
```

SonicWALL VPN with Cisco PIX using IKE

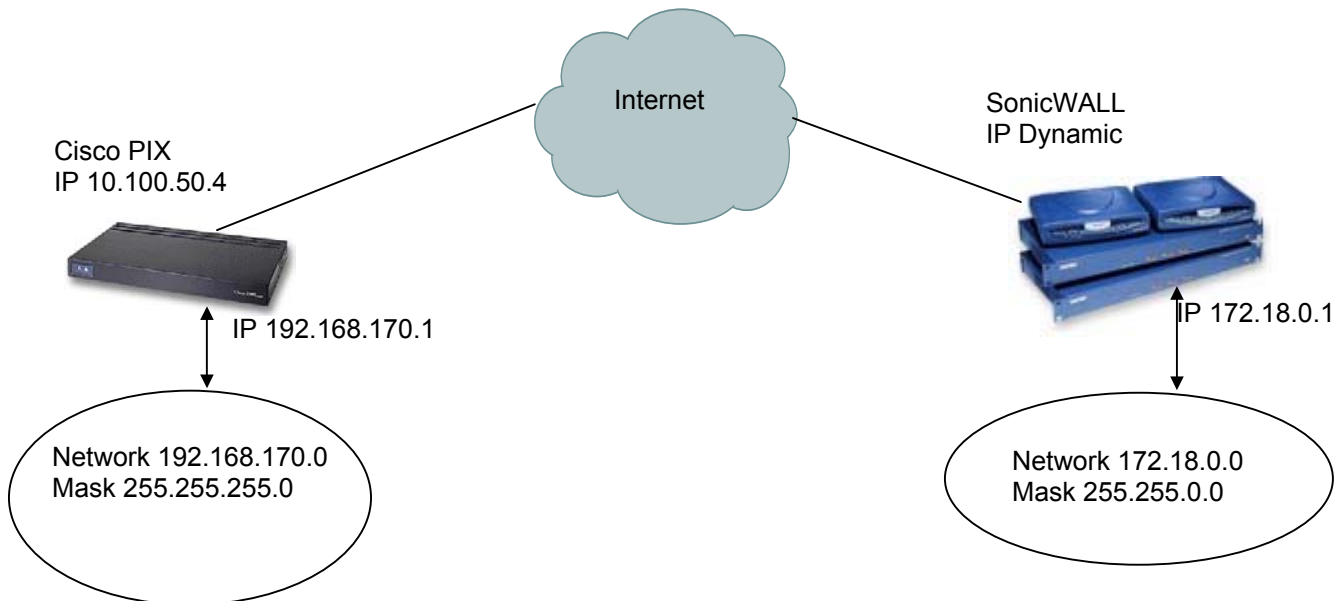
```

crypto map tosonicwall 20 set peer 10.100.30.1
crypto map tosonicwall 20 set transform-set strongsha
crypto map tosonicwall interface outside
isakmp enable outside
isakmp key password address 10.100.30.1 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
terminal width 80
Cryptochecksum:18e28ce2cb5056caa6d49014dadb1533
: 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

Change the IPsec Keying Mode to IKE using pre-shared secret

Name your SA. (In this example pix.interoplabs.com. **NOTE: this needs to be the same as the PIX's hostname.domain name**)

Fill in the IPsec gateway (in this example 10.100.50.4)

Select Group 2 for Phase 1 DH Group

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)

Fill in the appropriate Destination Network (in this example 192.168.170.0) and Subnet Mask (in this example 255.255.255.0)

A Sample Screen shot from SonicWALL firmware version 6.3.1.2 is displayed below

The screenshot shows the SonicWALL VPN configuration interface for adding or modifying an IPsec Security Association (SA). The interface is titled "VPN" and includes a "Help" icon. The configuration is organized into several sections:

- Add/Modify IPsec Security Associations:**
 - Security Association: pix.interoplabs.com
 - IPsec Keying Mode: IKE using Preshared Secret
 - Name: pix.interoplabs.com
 - Disable This SA:
 - IPsec Gateway Address: 10.100.50.4
- Security policy:**
 - Phase 1 DH Group: Group 2
 - SA Life time (secs): 28800
 - Phase 1 Encryption/Authentication: 3DES & SHA1
 - Phase 2 Encryption/Authentication: Strong Encrypt and Authenticate (ESP 3DES HMAC SHA1)
 - Shared Secret: password
- Destination Networks:**
 - Use this SA as default route for all Internet traffic:
 - Destination network obtains IP addresses using DHCP through this SA:
 - Specify destination networks below:

Network	Subnet Mask		
192.168.170.0	255.255.255.0		

Buttons: Add New Network..., Advanced Settings..., Delete This SA

At the bottom right, there are "Update" and "Reset" buttons.

Click on Advanced Settings
Select Group 2 for Phase 2 DH Group
Click OK
Click Update

A sample screen shot from SonicWALL firmware version 6.3.1.2 is displayed below

Edit Advanced Settings

Use Aggressive Mode

Enable Keep Alive

Require authentication of local users

Require authentication of remote users

Remote users behind VPN gateway
 Remote VPN clients with XAUTH

Enable Windows Networking (NetBIOS) broadcast

Apply NAT and firewall rules

Forward packets to remote VPNs

Enable Perfect Forward Secrecy

Phase 2 DH Group

Default LAN Gateway

VPN Terminated at LAN DMZ LAN/DMZ

Note that after clicking OK you must click Update on the main page to save changes made here.

CISCO PIX Configuration

Command	Description
Set ACCESS LIST/ NAT/ Host/Domain Name	
hostname pix	Set the hostname
domain-name interolab.com	Set the domain name
access-list 120 permit ip 192.168.170.0 255.255.255.0 172.18.0.0 255.255.0.0	Specifies the inside and destination networks
nat (inside) 0 access-list 120	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 strongsha 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 DES or 3DES.
crypto ipsec security-association lifetime seconds 28800	Globally sets the lifetime for IPSec
crypto dynamic-map pixtosw 10 match address 120	To specify an extended access list for a crypto map entry
crypto dynamic-map pixtosw 10 set transform-set strongsha	To specify which transform sets can be used with the crypto map entry
crypto map test 200 ipsec-isakmp dynamic pixtosw	Equates a dynamic map to a static map
crypto map test interface outside	Evaluates traffic going through the outside interface
Define ISAKMP parameters	
isakmp enable outside	
isakmp key password address 0.0.0.0 netmask 0.0.0.0	To configure a pre-shared authentication key, use the isakmp key global configuration command. In this case the pre-shared secret is "password"
isakmp identity hostname	ISAKMP identity PIX uses when participating in IPSec.
isakmp policy 20 authentication pre-share	To specify the authentication method within an IKE policy, use the authentication (IKE policy) ISAKMP policy configuration command.
isakmp policy 20 encryption 3des	To specify the encryption algorithm within an IKE policy
isakmp policy 20 hash sha	To specify the hash algorithm within an IKE policy
isakmp policy 20 group 2	This specifies DH group 1
isakmp policy 20 lifetime 28800	This commands sets the life time intervals before IKE is renegotiated. The value 28800 can be changed.

Example #2 PIX Configuration File

```
: Saved
: Written by enable_15 at 10:38:32.423 UTC Tue Jun 18 2002
PIX Version 6.2(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2Yjlyt7RRXU24 encrypted
passwd 2KFQnbNIdl.2KYOU encrypted
hostname pix
domain-name interoplabs.com
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list acl_out permit icmp any any
access-list 120 permit ip 192.168.170.0 255.255.255.0 172.18.0.0 255.255.0.0
pager lines 24
interface ethernet0 10full
interface ethernet1 auto
mtu outside 1500
mtu inside 1500
ip address outside 10.100.50.4 255.255.0.0
ip address inside 192.168.170.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
pdm history enable
arp timeout 14400
global (outside) 1 10.100.50.14
nat (inside) 0 access-list 120
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
access-group acl_out in interface outside
route outside 0.0.0.0 0.0.0.0 10.100.0.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 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
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnatt
crypto ipsec transform-set strongsha esp-3des esp-sha-hmac
Page 10 of 11
```

```
crypto ipsec security-association lifetime seconds 28800
crypto dynamic-map pxtosw 10 match address 120
crypto dynamic-map pxtosw 10 set transform-set strongsha
crypto map test 200 ipsec-isakmp dynamic pxtosw
crypto map test interface outside
isakmp enable outside
isakmp key password address 0.0.0.0 netmask 0.0.0.0
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
terminal width 80
Cryptochecksum:6833f0f0ae313529737322c815a7405c
: end
```

To Test the VPN tunnel:

From the PC behind the Cisco PIX 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 PIX and the SonicWALL to determine if IKE negotiation has started.

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

Test for connectivity to the Internet.
From a machine behind the SonicWALL, ping yahoo.com.

On the PIX, enter the following two commands. This will allow ping access from the LAN to the Internet.

```
Access-list acl_out permit icmp any any
Access-group acl_out in interface outside
```

From a machine behind the PIX, ping yahoo.com

Notes:

You can specify the lifetime for each crypto map instead using the global setting by entering the following commands.

Example#1: crypto map tosonicwall 20 set security-association lifetime seconds 28800

Example#2: crypto dynamic-map pxtosw 10 set security-association lifetime seconds 28800

For example two the isakmp identity hostname setting will not show up in the PIX config file, because it is the default.