SonicWALL VPN with Cisco PIX using IKE

Prepared by SonicWALL, Inc.

09/20/2001

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. Advanced setups are possible but are not covered in this document.

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.

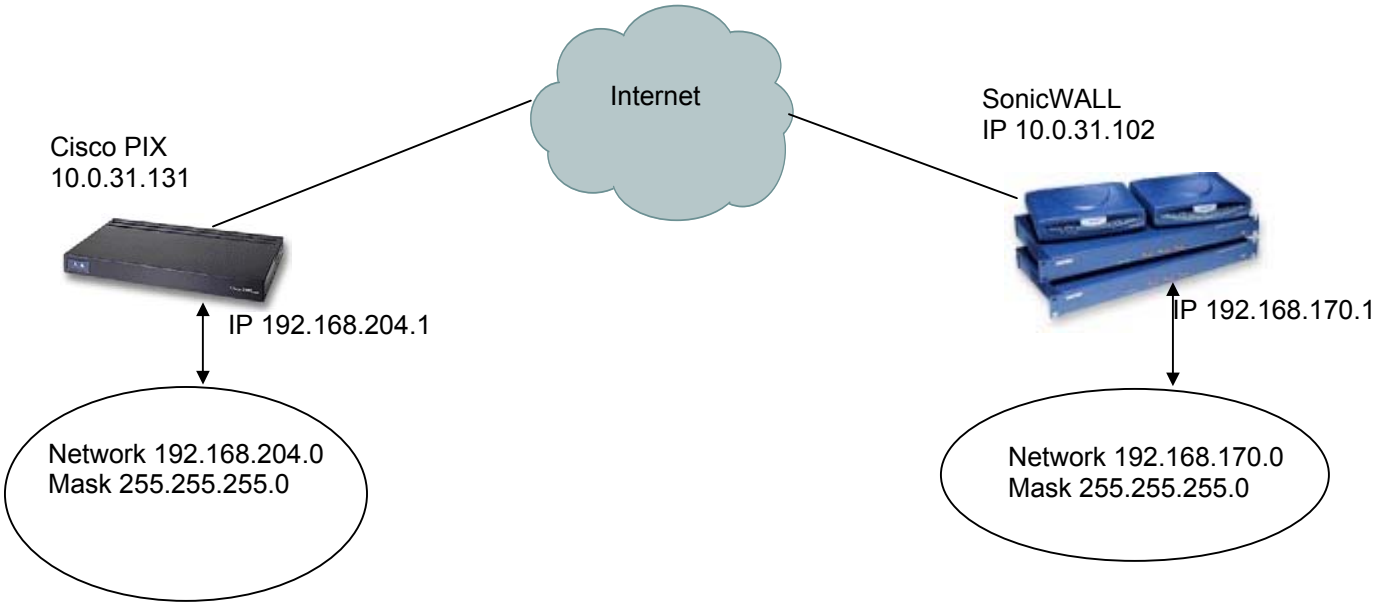
Technical Notes:

SonicWALL has tested VPN interoperability with Cisco PIX 506 version 5.1(3) and SonicWALL Pro 6.0.1.1 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 subnet
Encryption and Data Integrity:	ESP DES or ESP 3DES with MD5

EXAMPLE:

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.

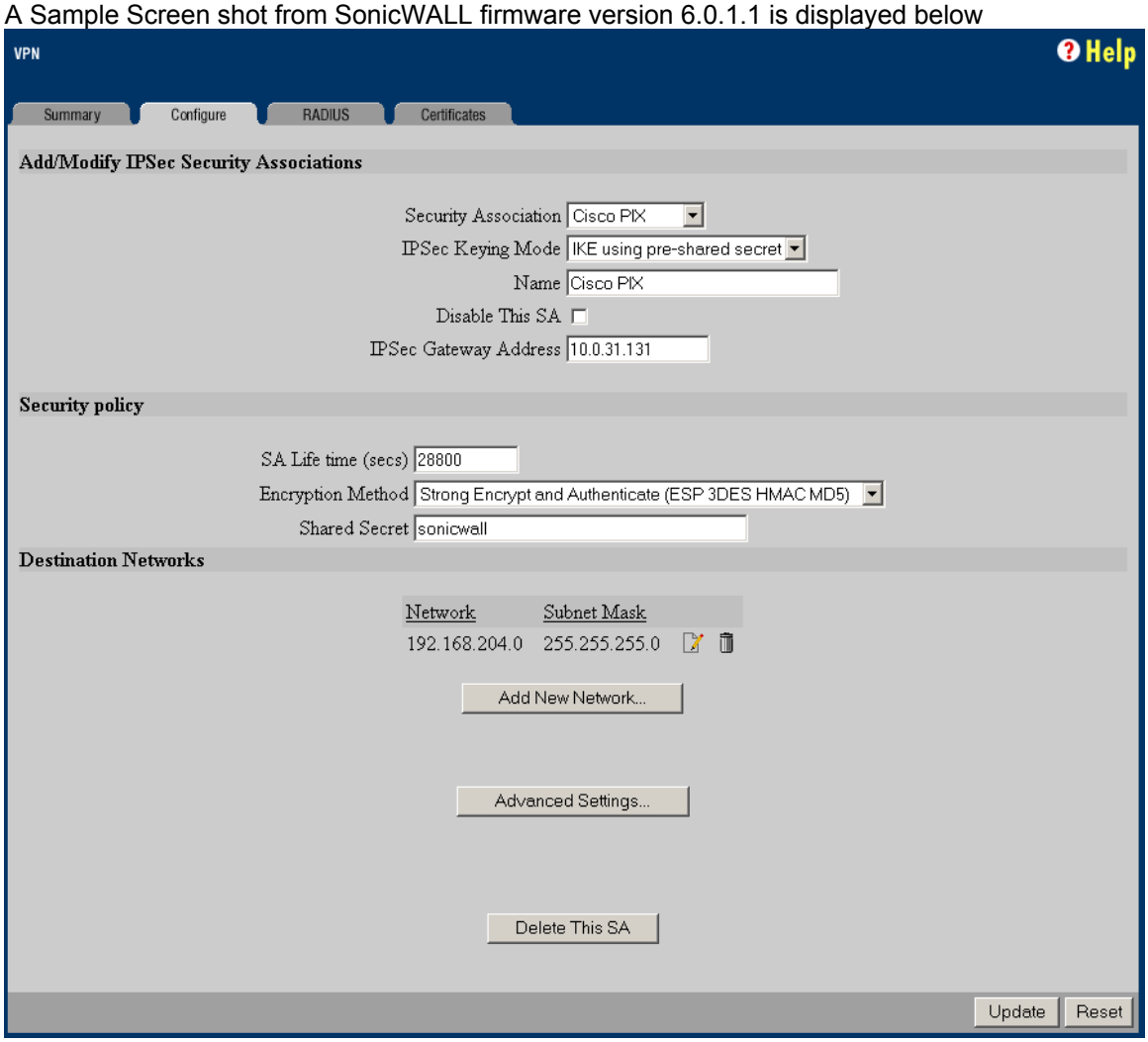


SonicWALL Configuration

On the SonicWALL, create an SA.

1. Change the IPSec Keying Mode to IKE using pre-shared secret.
2. Name your SA. (In this example Cisco)
3. Fill in the IPSec gateway (in this example 10.0.31.131)
4. Select ESP DES HMAC MD5 or ESP 3DES HMAC MD5 (in this example ESP 3DES HMAC MD5)
5. Enter your Shared Secret, (In this example sonicwall)
6. Fill in the appropriate Destination Network (in this example 192.168.204.0) and Subnet Mask (in this example 255.255.255.0)

A Sample Screen shot from SonicWALL firmware version 6.0.1.1 is displayed below



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 192.168.204.0 255.255.255.0 192.168.170.0 255.255.255.0	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 strong esp-3des esp-md5-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 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 10.0.31.102	To specify an IPSec peer in a crypto map entry,
crypto map tosonicwall 20 set transform-set strong	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 sonicwall address 10.0.31.102 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 “sonicwall”
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 md5	To specify the hash algorithm within an IKE policy
isakmp policy 20 group 1	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.

To Test the VPN tunnel:

From the PC behind the Cisco PIX firewall, try to ping 192.168.170.1
From the PC behind the SonicWALL, try to ping 192.168.204.1

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 in interface outside

From a machine behind the PIX, ping yahoo.com

Example PIX configuration File:

```
: Saved
:
PIX Version 5.3(1)
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password XXXXXXXXXXXXXXX encrypted
passwd XXXXXXXXXXXXXXX encrypted
hostname pixfirewall
fixup protocol ftp 21
fixup protocol http 80
fixup protocol h323 1720
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
names
access-list pixtosw permit ip 192.168.204.0 255.255.255.0 192.168.170.0 255.255.255.0
no pager
no logging on
interface ethernet0 10baset
interface ethernet1 10baset
mtu outside 1500
mtu inside 1500
ip address outside 10.0.31.131 255.255.0.0
ip address inside 192.168.204.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
arp timeout 14400
global (outside) 1 10.0.31.132
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 10.0.0.2 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
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
tftp-server outside 10.0.31.129 /
floodguard enable
sysopt connection permit-ipsec
no sysopt route dnat
crypto ipsec transform-set strong esp-3des esp-md5-hmac
crypto map tosonicwall 20 ipsec-isakmp
crypto map tosonicwall 20 match address pixtosw
crypto map tosonicwall 20 set peer 10.0.31.102
crypto map tosonicwall 20 set transform-set strong
crypto map tosonicwall interface outside
isakmp enable outside
isakmp key sonicwall address 10.0.31.102 netmask 255.255.255.255
isakmp identity address
isakmp policy 20 authentication pre-share
isakmp policy 20 encryption 3des
isakmp policy 20 hash md5
isakmp policy 20 group 1
isakmp policy 20 lifetime 28800
telnet 10.0.0.0 255.255.0.0 inside
telnet timeout 5
ssh timeout 5
terminal width 80
Cryptochecksum:43014c32dceffcb0d1ad55164ba95087
: end
```