Ejemplo de Configuración de VPN entre Productos Sonicwall y Cisco Security Appliance

Contenido

Introducción

Este documento demuestra cómo configurar un túnel IPsec con claves previamente compartidas para comunicar entre dos redes privadas usando el modo agresivo y el principal. En este ejemplo, las redes de comunicación son la red privada 192.168.1.x interna de Cisco Security Appliance (PIX/ASA) y la red privada 172.22.1.x interna del firewall SonicwallTM TZ170.

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- El tráfico desde dentro del dispositivo de seguridad de Cisco y dentro del Sonicwall TZ170 debe fluir a Internet (representado aquí por las redes 10.x.x.x) antes de iniciar esta configuración.
- Los usuarios deben conocer el IPSec Negotiation. Este proceso se puede dividir en cinco pasos que incluyen dos fases de intercambio de claves de Internet (IKE).Un túnel IPSec es iniciado por un tráfico interesado. Se considera que el tráfico es interesante cuando se transmite entre los pares IPSec.En la Fase 1 IKE, las entidades pares IPSec negocian la política establecida de la Asociación de seguridad (SA) IKE. Una vez que se autentican los

pares, se crea un túnel seguro por medio de la Asociación de Seguridad en Internet y del Protocolo de administración de clave (ISAKMP).En la fase 2 de IKE, los pares IPSec usan el túnel autenticado y seguro para negociar las transformaciones de IPSec SA. La negociación de la política compartida determina el modo en que se establece el túnel IPSec.Se crea el túnel IPSec y los datos se transfieren entre los pares IPSec según los parámetros IPSec configurados en los conjuntos de transformaciones de IPSec.El túnel IPSec termina cuando los IPSec SAs son borrados o cuando caduca su vigencia.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco PIX 515E versión 6.3(5)
- Cisco PIX 515 versión 7.0(2)
- Sonicwall TZ170, SonicOS Standard 2.2.0.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Productos Relacionados

Esta configuración también se puede utilizar con las siguientes versiones de hardware y software:

- La configuración PIX 6.3(5) se puede utilizar con todos los demás productos de firewall Cisco PIX que ejecutan esa versión de software (PIX 501, 506, etc.)
- La configuración de PIX/ASA 7.0(2) sólo se puede utilizar en dispositivos que ejecutan la serie PIX 7.0 de software (no incluye los 501, 506 y posiblemente algunos 515 antiguos), así como Cisco 5500 Series ASA.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

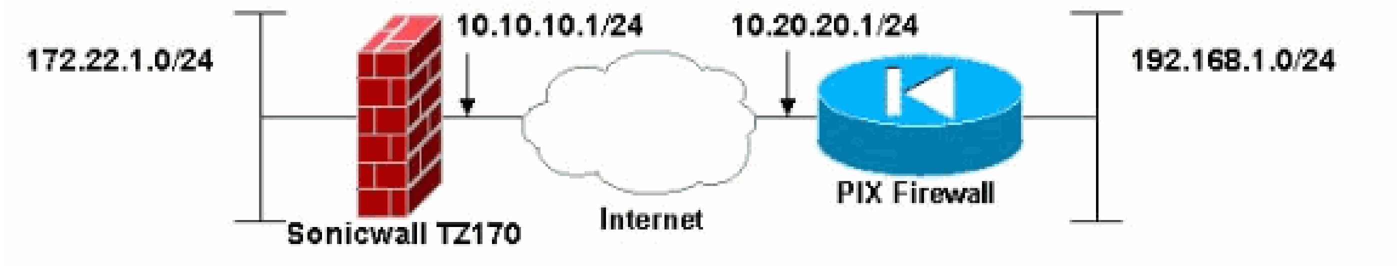
En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta Command Lookup (sólo para clientes registrados) para obtener más información sobre los comandos utilizados en esta sección.

Nota: En el Modo Agresivo IPSec, es necesario que Sonicwall inicie el túnel IPsec al PIX. Puede ver esto cuando analice las depuraciones para esta configuración. Esto es inherente a la forma en que funciona el Modo Agresivo IPSec.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

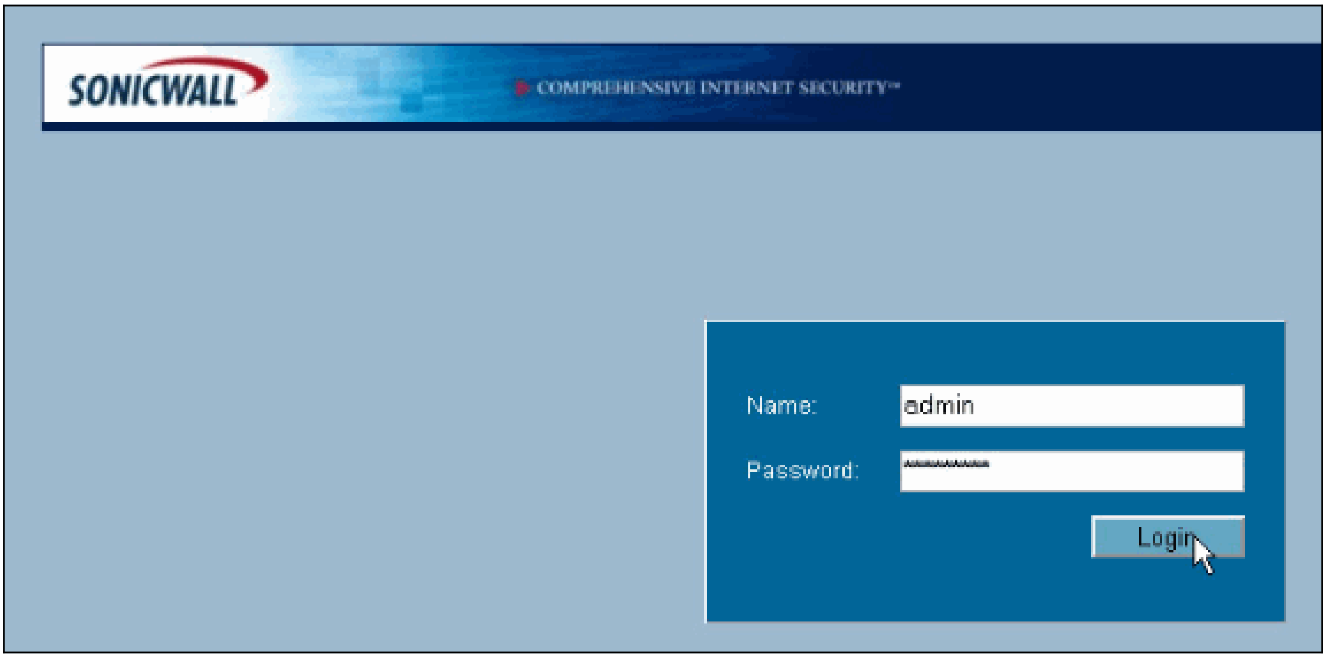


Configuración de Sonicwall

La configuración del Sonicwall TZ170 se realiza a través de una interfaz basada en web.

Complete estos pasos:

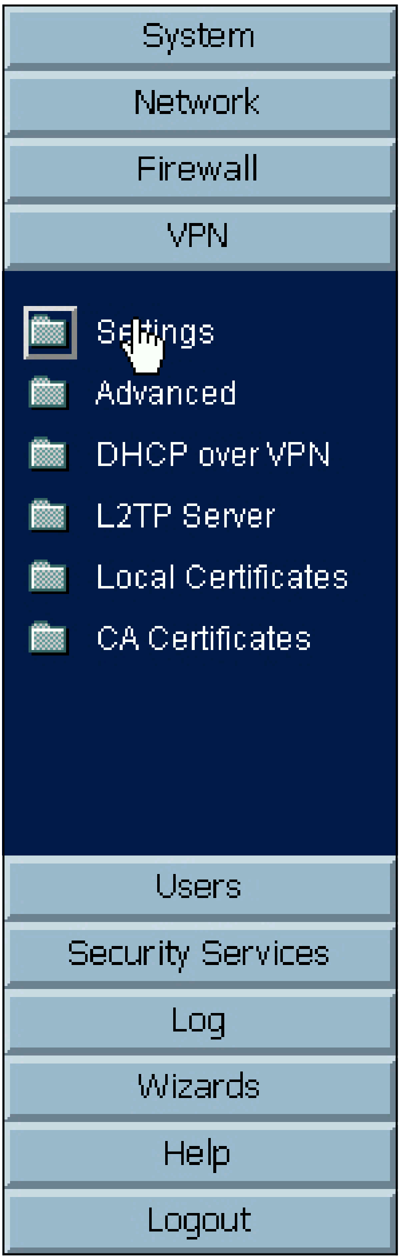
1. Conéctese a la dirección IP del router en una de las interfaces internas mediante un navegador web estándar.Esto abre la ventana de inicio de sesión.



Name: admin

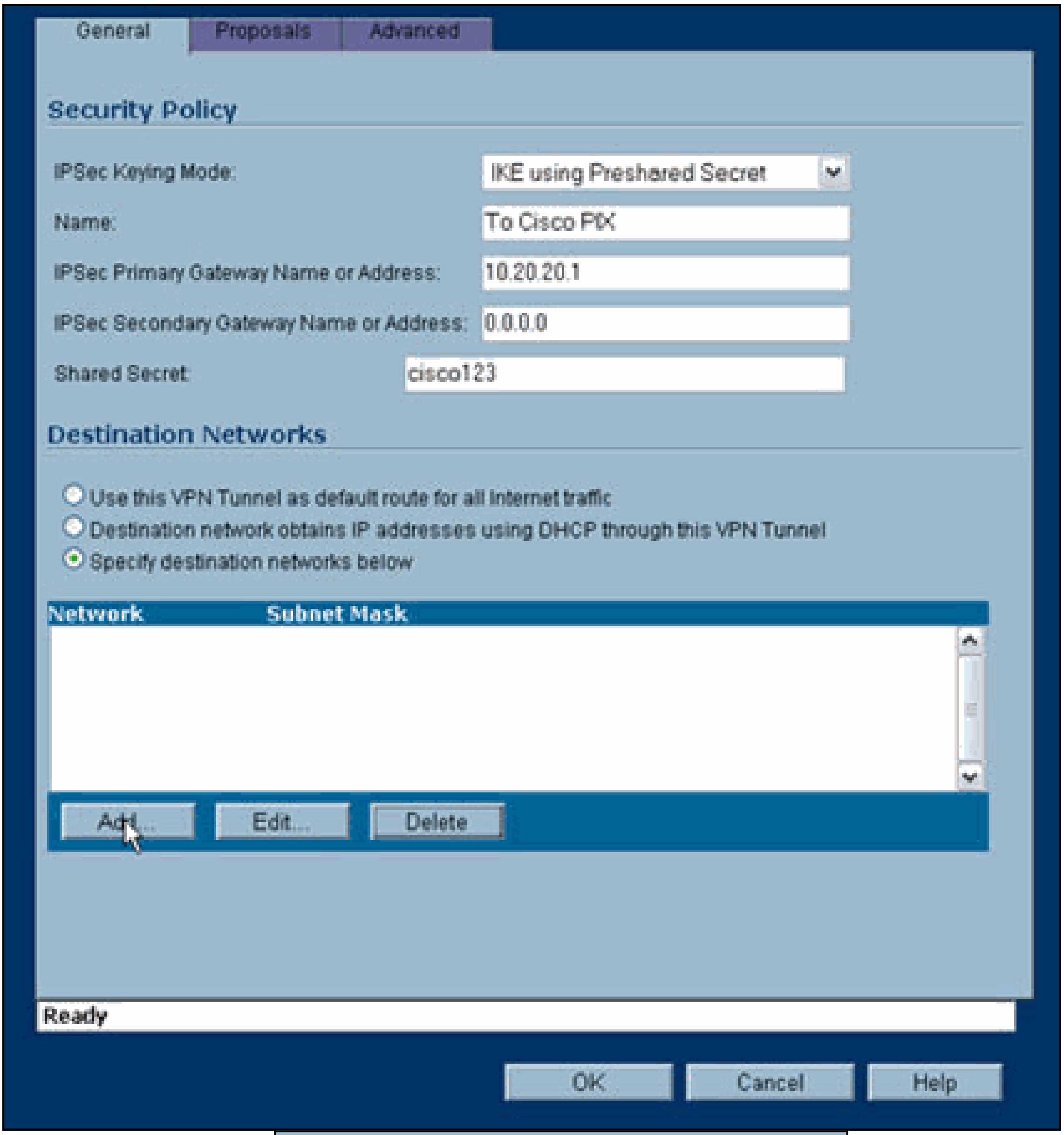
Password: **********

2. Inicie sesión en el dispositivo Sonicwall y seleccione **VPN >**



Settings.

3. Introduzca la dirección IP del par VPN y el secreto precompartido que se utilizará. Haga clic en **Agregar** en Redes de

destino.

Security Policy

IPSec Keying Mode: IKE using Preshared Secret

Name: To Cisco PIX

IPSec Primary Gateway Name or Address: 10.20.20.1

IPSec Secondary Gateway Name or Address: 0.0.0.0

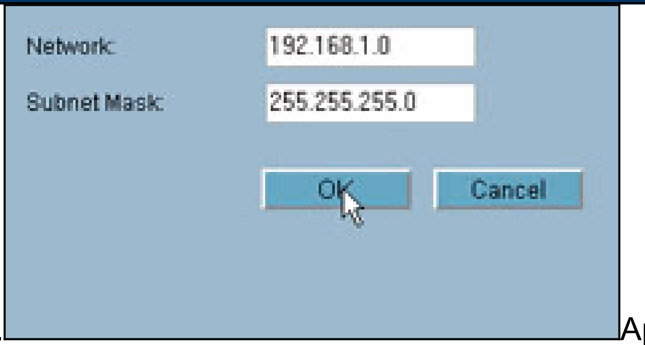
Shared Secret: cisco123

Destination Networks

○ Use this VPN Tunnel as default route for all Internet traffic
○ Destination network obtains IP addresses using DHCP through this VPN Tunnel
● Specify destination networks below

Network	Subnet Mask

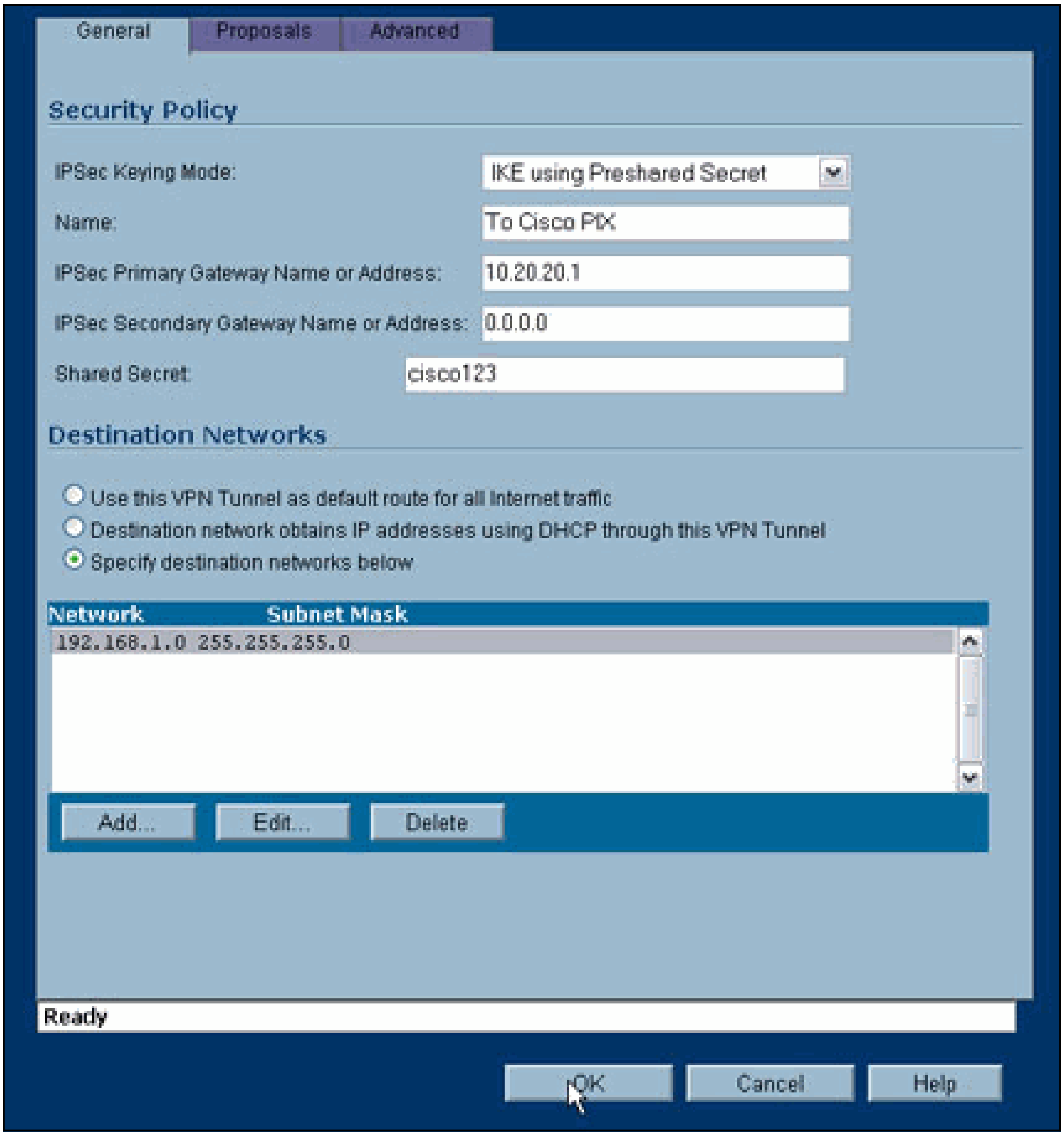
Ready

4. Introduzca la red de destino.

Network: 192.168.1.0

Subnet Mask: 255.255.255.0

Aparece la ventana Settings (Configuración).



Security Policy

IPSec Keying Mode: IKE using Preshared Secret

Name: To Cisco PIX

IPSec Primary Gateway Name or Address: 10.20.20.1

IPSec Secondary Gateway Name or Address: 0.0.0.0

Shared Secret: cisco123

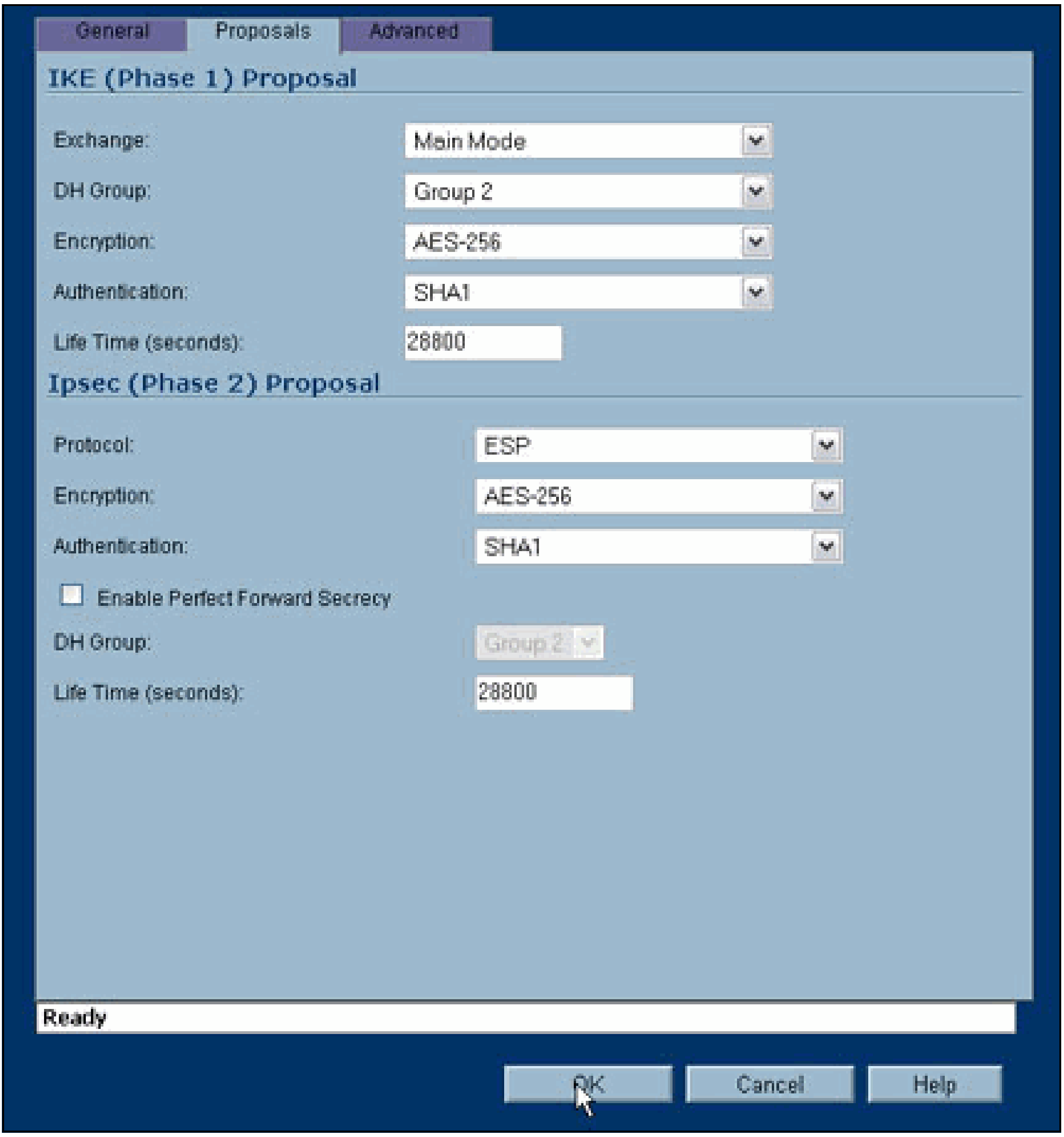
Destination Networks

○ Use this VPN Tunnel as default route for all Internet traffic
○ Destination network obtains IP addresses using DHCP through this VPN Tunnel
● Specify destination networks below

Network	Subnet Mask
192.168.1.0	255.255.255.0

Ready

5. Haga clic en la ficha Propuestas de la parte superior de la ventana Configuración.
6. Seleccione el intercambio que planea utilizar para esta configuración (Modo principal o Modo agresivo) junto con el resto de los parámetros de fase 1 y fase 2.Este ejemplo de configuración utiliza el cifrado AES-256 para ambas fases con el algoritmo hash SHA1 para la autenticación y el grupo Diffie-Hellman de 1024 bits 2 para la política



IKE (Phase 1) Proposal

Exchange: Main Mode

DH Group: Group 2

Encryption: AES-256

Authentication: SHA1

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP

Encryption: AES-256

Authentication: SHA1

□ Enable Perfect Forward Secrecy

DH Group: Group 2

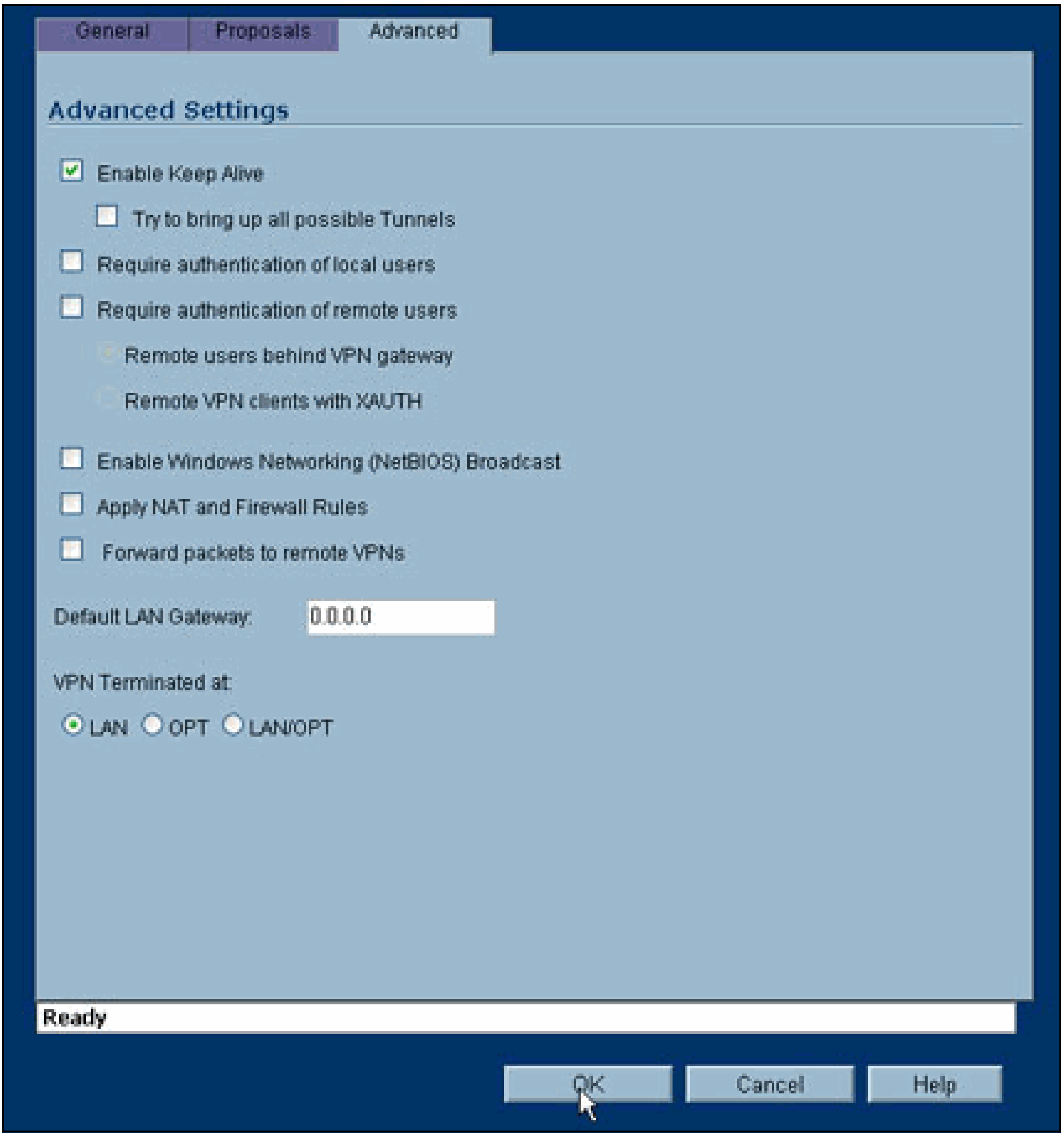
Life Time (seconds): 28800

Ready

IKE.

7. Haga clic en la ficha Advanced (Opciones avanzadas).Hay opciones adicionales que puede que desee configurar en esta ficha. Estos son los ajustes utilizados para esta configuración

de ejemplo.



Advanced Settings

☑ Enable Keep Alive

□ Try to bring up all possible Tunnels

□ 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

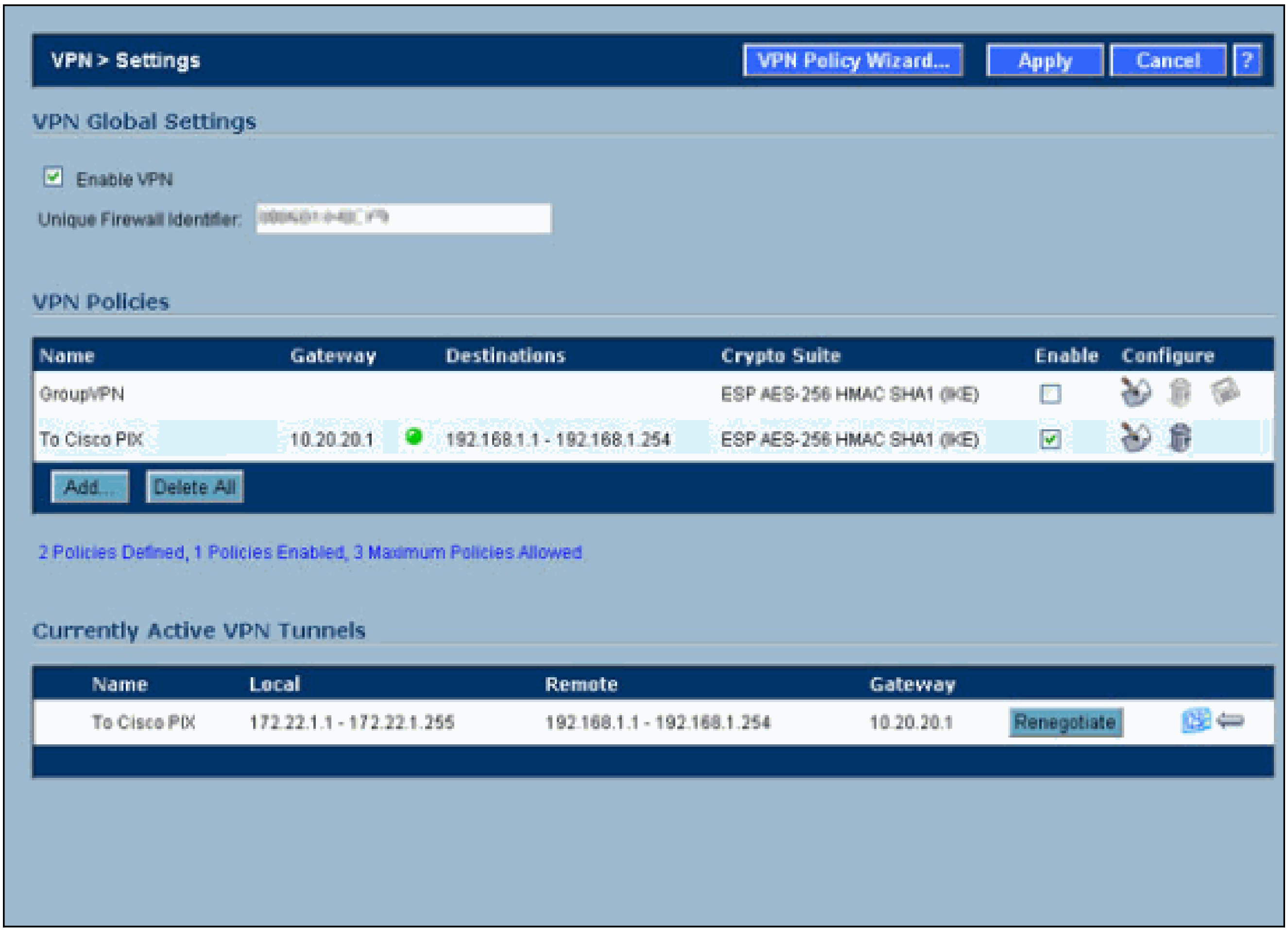
Default LAN Gateway: 0.0.0.0

VPN Terminated at:

● LAN ○ OPT ○ LAN/OPT

Ready

8. Click OK.Una vez que complete esta configuración y la configuración en el PIX remoto, la ventana Settings debe ser similar a esta ventana de ejemplo
   Settings.



VPN Global Settings

☑ Enable VPN

Unique Firewall Identifier: [redacted]

VPN Policies

Name	Gateway	Destinations	Crypto Suite	Enable	Configure
GroupVPN			ESP AES-256 HMAC SHA1 (IKE)	□	
To Cisco PIX	10.20.20.1	● 192.168.1.1 - 192.168.1.254	ESP AES-256 HMAC SHA1 (IKE)	☑	

2 Policies Defined, 1 Policies Enabled, 3 Maximum Policies Allowed

Currently Active VPN Tunnels

Name	Local	Remote	Gateway		
To Cisco PIX	172.22.1.1 - 172.22.1.255	192.168.1.1 - 192.168.1.254	10.20.20.1	Renegotiate	

Configuración del Modo Principal IPsec

Esta sección usa estas configuraciones:

- Cisco PIX 515e versión 6.3(5)
- Cisco PIX 515 versión 7.0(2)

Cisco PIX 515e versión 6.3(5)

```
pix515e-635#show running-config
: Saved
:
PIX Version 6.3(5)
!--- Sets the hardware speed to auto on both interfaces.
interface ethernet0 auto interface ethernet1 auto !---
Specifies the inside and outside interfaces. nameif
ethernet0 outside security0 nameif ethernet1 inside
security100 enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted hostname pix515e-635
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 !--- Specifies the traffic that
can pass through the IPsec tunnel. access-list pixtosw
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu outside 1500 mtu inside
1500 !--- Sets the inside and outside IP addresses and
```

```
subnet masks. ip address outside 10.20.20.1
255.255.255.0 ip address inside 192.168.1.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm pdm history enable arp timeout 14400 !---
Instructs PIX to perform PAT on the IP address on the
outside interface. global (outside) 1 interface !---
Specifies addresses to be exempt from NAT (traffic to be
tunneled). nat (inside) 0 access-list pixtosw !---
Specifies which addresses should use NAT (all except
those exempted). nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !---
Specifies the default route on the outside interface.
route outside 0.0.0.0 0.0.0.0 10.20.20.2 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 rpc 0:10:00 h225 1:00:00 timeout h323 0:05:00
mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout sip-
disconnect 0:02:00 sip-invite 0:03:00 timeout uauth
0:05:00 absolute aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3 aaa-server
TACACS+ deadtime 10 aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3 aaa-server
RADIUS deadtime 10 aaa-server LOCAL protocol local no
snmp-server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable !--- Implicit permit for all packets that come
from IPsec tunnels. sysopt connection permit-ipsec !---
PHASE 2 CONFIGURATION: !--- Defines the transform set
for Phase 2 encryption and authentication. !---
Austinlab is the name of the transform set that uses
aes-256 encryption !--- as well as the SHA1 hash
algorithm for authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Specifies IKE is used to establish the IPsec SAs
for the map "maptosw". crypto map maptosw 67 ipsec-
isakmp !--- Specifies the ACL "pixtosw" to use with this
map . crypto map maptosw 67 match address pixtosw !---
Specifies the IPsec peer for this map. crypto map
maptosw 67 set peer 10.10.10.1 !--- Specifies the
transform set to use. crypto map maptosw 67 set
transform-set austinlab !--- Specifies the interface to
use with this map. crypto map maptosw interface outside
!--- PHASE 1 CONFIGURATION !--- Specifies the interface
to use for the IPsec tunnel.

isakmp enable outside

!--- Specifies the preshared key and the addresses to
use with that key. !--- In this case only one address is
used with the preshared key cisco123. isakmp key
******** address 10.10.10.1 netmask 255.255.255.255 !---
Defines how the PIX identifies itself in !--- IKE
negotiations (IP address in this case). isakmp identity
address !--- These five commands specify the Phase 1
configuration settings !--- specific to this sample
configuration. isakmp policy 13 authentication pre-share
isakmp policy 13 encryption aes-256 isakmp policy 13
hash sha isakmp policy 13 group 2 isakmp policy 13
lifetime 28800 telnet timeout 5 ssh timeout 5 console
timeout 0 terminal width 80
Cryptochecksum:07a3815d59db9965b72c7d8a7aaf7f5f : end
pix515e-635#
```

Cisco PIX 515 versión 7.0(2)

```
pix515-702#show running-config
: Saved
:
PIX Version 7.0(2)
names
!

!--- PIX 7 uses an interface configuration mode similar
to Cisco IOS®. !--- This output configures the IP
address, interface name, !--- and security level for
interfaces Ethernet0 and Ethernet1. interface Ethernet0
nameif outside security-level 0 ip address 10.20.20.1
255.255.255.0 ! interface Ethernet1 nameif inside
security-level 100 ip address 192.168.1.1 255.255.255.0
! interface Ethernet2 shutdown no nameif no security-
level no ip address ! interface Ethernet3 shutdown no
nameif no security-level no ip address ! interface
Ethernet4 shutdown no nameif no security-level no ip
address ! interface Ethernet5 shutdown no nameif no
security-level no ip address ! enable password
8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname pix515-702 domain-name cisco.com ftp
mode passive !--- Specifies the traffic that can pass
through the IPsec tunnel. access-list pixtosw extended
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu inside 1500 mtu outside
1500 no failover monitor-interface inside monitor-
interface outside no asdm history enable arp timeout
14400 !--- Instructs PIX to perform PAT on the IP
address on the outside interface. global (outside) 1
interface !--- Specifies addresses to be exempt from NAT
(traffic to be tunneled). nat (inside) 0 access-list
pixtosw !--- Specifies which addresses should use NAT
(all except those exempted). nat (inside) 1 0.0.0.0
0.0.0.0 !--- Specifies the default route on the outside
interface. route outside 0.0.0.0 0.0.0.0 10.20.20.2 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat
0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth
0:05:00 absolute no snmp-server location no snmp-server
contact snmp-server enable traps snmp !--- Implicit
permit for all packets that come from IPsec tunnels.
sysopt connection permit-ipsec !--- PHASE 2
CONFIGURATION !--- Defines the transform set for Phase 2
encryption and authentication. !--- Austinlab is the
name of the transform set that uses aes-256 encryption
!--- as well as the SHA1 hash algorithm for
authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Specifies the ACL pixtosw to use with this map.
crypto map maptosw 67 match address pixtosw !---
Specifies the IPsec peer for this map. crypto map
maptosw 67 set peer 10.10.10.1 !--- Specifies the
transform set to use. crypto map maptosw 67 set
transform-set austinlab !--- Specifies the interface to
use with this map . crypto map maptosw interface outside
!--- PHASE 1 CONFIGURATION !--- Defines how the PIX
```

```
identifies itself in !--- IKE negotiations (IP address
in this case).

isakmp identity address

!--- Specifies the interface to use for the IPsec
tunnel. isakmp enable outside !--- These five commands
specify the Phase 1 configuration !--- settings specific
to this sample configuration. isakmp policy 13
authentication pre-share isakmp policy 13 encryption
aes-256 isakmp policy 13 hash sha isakmp policy 13 group
2 isakmp policy 13 lifetime 28800 telnet timeout 5 ssh
timeout 5 console timeout 0 !--- These three lines set
the IPsec attributes for the tunnel to the !--- remote
peer. This is where the preshared key is defined for
Phase 1 and the !--- IPsec tunnel type is set to site-
to-site. tunnel-group 10.10.10.1 type ipsec-l2l tunnel-
group 10.10.10.1 ipsec-attributes pre-shared-key *
Cryptochecksum:092b6fc5370e2ef0cf07c2bc10f1d44a : end
pix515-702#
```

Configuración del Modo Agresivo IPsec

Esta sección usa estas configuraciones:

- Cisco PIX 515e versión 6.3(5)
- Cisco PIX 515 versión 7.0(2)

Cisco PIX 515e versión 6.3(5)

```

pix515e-635#show running-config
: Saved
:
PIX Version 6.3(5)
!--- Sets the hardware speed to auto on both interfaces.
interface ethernet0 auto interface ethernet1 auto !---
Specifies the inside and outside interfaces. nameif
ethernet0 outside security0 nameif ethernet1 inside
security100 enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted hostname pix515e-635
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 !--- Specifies the traffic that
can pass through the IPsec tunnel. access-list pixtosw
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu outside 1500 mtu inside
1500 !--- Sets the inside and outside IP addresses and
subnet masks. ip address outside 10.20.20.1
255.255.255.0 ip address inside 192.168.1.1
255.255.255.0 ip audit info action alarm ip audit attack
action alarm pdm history enable arp timeout 14400 !---
Instructs PIX to perform PAT on the IP address on the
outside interface. global (outside) 1 interface !---
Specifies addresses to be exempt from NAT (traffic to be
tunneled). nat (inside) 0 access-list pixtosw !---
Specifies which addresses should use NAT (all except
those exempted). nat (inside) 1 0.0.0.0 0.0.0.0 0 0 !---
Specifies the default route on the outside interface.
route outside 0.0.0.0 0.0.0.0 10.20.20.2 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 rpc 0:10:00 h225 1:00:00 timeout h323 0:05:00
mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout sip-
disconnect 0:02:00 sip-invite 0:03:00 timeout uauth
0:05:00 absolute aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3 aaa-server
TACACS+ deadtime 10 aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3 aaa-server
RADIUS deadtime 10 aaa-server LOCAL protocol local no
snmp-server location no snmp-server contact snmp-server
community public no snmp-server enable traps floodguard
enable !--- Implicit permit for all packets that come
from IPsec tunnels. sysopt connection permit-ipsec !---
PHASE 2 CONFIGURATION !--- Defines the transform set for
Phase 2 encryption and authentication. !--- Austinlab is
the name of the transform set that uses aes-256
encryption !--- as well as the SHA1 hash algorithm for
authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Creates the dynamic map ciscopix for the transform
set. crypto dynamic-map ciscopix 1 set transform-set
austinlab !--- Specifies the IKE that should be used to
establish SAs !--- for the dynamic map. crypto map
dynmaptosw 66 ipsec-isakmp dynamic ciscopix !--- Applies
the settings above to the outside interface. crypto map
dynmaptosw interface outside !--- PHASE 1 CONFIGURATION
!--- Specifies the interface to use for the IPsec tunnel
.
isakmp enable outside

!--- Specifies the preshared key and the addresses to
use with that key. !--- In this case only one address is
used as the preshared key "cisco123". isakmp key
******** address 10.10.10.1 netmask 255.255.255.255 !---
Defines how the PIX identifies itself in !--- IKE
negotiations (IP address in this case). isakmp identity
address !--- These five commands specify the Phase 1
configuration settings !--- specific to this sample
configuration. isakmp policy 13 authentication pre-share
isakmp policy 13 encryption aes-256 isakmp policy 13
hash sha isakmp policy 13 group 2 isakmp policy 13
lifetime 28800 telnet timeout 5 ssh timeout 5 console
timeout 0 terminal width 80
Cryptochecksum:07a3815d59db9965b72c7d8a7aaf7f5f : end
pix515e-635#
```

Cisco PIX 515 versión 7.0(2)

```
pix515-702#show running-config
: Saved
:
PIX Version 7.0(2)
names
!

!--- PIX 7 uses an interface configuration mode similar
to Cisco IOS. !--- This output configures the IP
```

```
address, interface name, and security level for !---
interfaces Ethernet0 and Ethernet1. interface Ethernet0
nameif outside security-level 0 ip address 10.20.20.1
255.255.255.0 ! interface Ethernet1 nameif inside
security-level 100 ip address 192.168.1.1 255.255.255.0
! interface Ethernet2 shutdown no nameif no security-
level no ip address ! interface Ethernet3 shutdown no
nameif no security-level no ip address ! interface
Ethernet4 shutdown no nameif no security-level no ip
address ! interface Ethernet5 shutdown no nameif no
security-level no ip address ! enable password
8Ry2YjIyt7RRXU24 encrypted passwd 2KFQnbNIdI.2KYOU
encrypted hostname pix515-702 domain-name cisco.com ftp
mode passive !--- Specifies the traffic that can pass
through the IPsec tunnel. access-list pixtosw extended
permit ip 192.168.1.0 255.255.255.0 172.22.1.0
255.255.255.0 pager lines 24 mtu inside 1500 mtu outside
1500 no failover monitor-interface inside monitor-
interface outside no asdm history enable arp timeout
14400 !--- Instructs PIX to perform PAT on the IP
address on the outside interface. global (outside) 1
interface !--- Specifies addresses to be exempt from NAT
(traffic to be tunneled). nat (inside) 0 access-list
pixtosw !--- Specifies which addresses should use NAT
(all except those exempted). nat (inside) 1 0.0.0.0
0.0.0.0 !--- Specifies the default route on the outside
interface. route outside 0.0.0.0 0.0.0.0 10.20.20.2 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat
0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth
0:05:00 absolute no snmp-server location no snmp-server
contact snmp-server enable traps snmp !--- Implicit
permit for all packets that come from IPsec tunnels.
sysopt connection permit-ipsec !--- PHASE 2
CONFIGURATION !--- Defines the transform set for Phase 2
encryption and authentication. !--- Austinlab is the
name of the transform set that uses aes-256 encryption
!--- as well as the SHA1 hash algorithm for
authentication.

crypto ipsec transform-set austinlab esp-aes-256 esp-
sha-hmac

!--- Creates the dynamic map "ciscopix" for the defined
transform set. crypto dynamic-map ciscopix 1 set
transform-set austinlab !--- Specifies that IKE should
be used to establish SAs !--- for the defined dynamic
map. crypto map dynmaptosw 66 ipsec-isakmp dynamic
ciscopix !--- Applies the settings to the outside
interface. crypto map dynmaptosw interface outside !---
PHASE 1 CONFIGURATION !--- Defines how the PIX
identifies itself in !--- IKE negotiations (IP address
in this case).

isakmp identity address

!--- Specifies the interface to use for the IPsec
tunnel. isakmp enable outside !--- These five commands
specify the Phase 1 configuration settings !--- specific
to this sample configuration. isakmp policy 13
authentication pre-share isakmp policy 13 encryption
aes-256 isakmp policy 13 hash sha isakmp policy 13 group
2 isakmp policy 13 lifetime 28800 telnet timeout 5 ssh
```

```
timeout 5 console timeout 0 !--- These three lines set
the IPsec attributes for the tunnel to the !--- remote
peer. This is where the preshared key is defined for
Phase 1 and the !--- IPsec tunnel type is set to site-
to-site. tunnel-group 10.10.10.1 type ipsec-l2l tunnel-
group 10.10.10.1 ipsec-attributes pre-shared-key *
Cryptochecksum:092b6fc5370e2ef0cf07c2bc10f1d44a : end
pix515-702#
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **show crypto isakmp sa — Muestra todas las asociaciones actuales de seguridad (SA) IKE de un par.**
- **show crypto ipsec sa — Muestra la configuración actual utilizada por las SA actuales**

Estas tablas muestran las salidas de algunos debugs para el modo principal y agresivo tanto en PIX 6.3(5) como en PIX 7.0(2) después de que el túnel esté completamente establecido.

Nota: Esta información debe ser suficiente para establecer un túnel IPsec entre estos dos tipos de hardware. Si tiene algún comentario, utilice el formulario de comentarios del lado izquierdo de este documento.

- Cisco PIX 515e versión 6.3(5) - Modo principal
- Cisco PIX 515 versión 7.0(2) - Modo principal
- Cisco PIX 515e versión 6.3(5) - Modo agresivo
- Cisco PIX 515 versión 7.0(2) - Modo agresivo

Cisco PIX 515e versión 6.3(5) - Modo principal

```

pix515e-635#show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst               src        state     pending
created
      10.10.10.1       10.20.20.1    QM_IDLE         0
1
pix515e-635#



pix515e-635#show crypto ipsec sa



           interface: outside
           Crypto map tag: maptosw, local addr.
10.20.20.1

 local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
           remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
           current_peer: 10.10.10.1:500
           PERMIT, flags={origin_is_acl,}
           #pkts encaps: 4, #pkts encrypt: 4, #pkts
digest 4
           #pkts decaps: 4, #pkts decrypt: 4, #pkts
verify 4
           #pkts compressed: 0, #pkts decompressed: 0
           #pkts not compressed: 0, #pkts compr. failed:
0, #pkts decompress failed: 0
           #send errors 1, #recv errors 0

 local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1
           path mtu 1500, ipsec overhead 72, media mtu
1500
           current outbound spi: ed0afa33

 inbound esp sas:
           spi: 0xac624692(2892121746)
           transform: esp-aes-256 esp-sha-hmac ,
           in use settings ={Tunnel, }
           slot: 0, conn id: 1, crypto map: maptosw
           sa timing: remaining key lifetime (k/sec):
(4607999/28718)
           IV size: 16 bytes
           replay detection support: Y


           inbound ah sas:


           inbound pcp sas:


           outbound esp sas:
           spi: 0xed0afa33(3976919603)
           transform: esp-aes-256 esp-sha-hmac ,
           in use settings ={Tunnel, }
           slot: 0, conn id: 2, crypto map: maptosw
           sa timing: remaining key lifetime (k/sec):
(4607999/28718)
           IV size: 16 bytes
           replay detection support: Y


           outbound ah sas:


           outbound pcp sas:

pix515e-635#
```

Cisco PIX 515 versión 7.0(2) - Modo principal

```

pix515-702#show crypto isakmp sa

 Active SA: 1
           Rekey SA: 0 (A tunnel will report 1 Active
and 1 Rekey SA during rekey)
           Total IKE SA: 1

1 IKE Peer: 10.10.10.1
           Type : L2L Role : initiator
           Rekey : no State : MM_ACTIVE
           pix515-702#

pix515-702#show crypto ipsec sa
interface: outside
    Crypto map tag: maptosw, local addr: 10.20.20.1

 local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
           remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
           current_peer: 10.10.10.1

 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
           #pkts decaps: 5, #pkts decrypt: 5, #pkts
verify: 5
           #pkts compressed: 0, #pkts decompressed: 0
           #pkts not compressed: 5, #pkts comp failed:
0, #pkts decomp failed: 0
           #send errors: 0, #recv errors: 0

 local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1

 path mtu 1500, ipsec overhead 76, media mtu 1500
           current outbound spi: 2D006547

 inbound esp sas:
           spi: 0x309F7A33 (815757875)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: maptosw
           sa timing: remaining key lifetime (kB/sec):
(4274999/28739)
           IV size: 16 bytes
           replay detection support: Y
           outbound esp sas:
           spi: 0x2D006547 (755000647)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: maptosw
           sa timing: remaining key lifetime (kB/sec):
(4274999/28737)
           IV size: 16 bytes
           replay detection support: Y

pix515-702#
```

Cisco PIX 515e versión 6.3(5) - Modo agresivo

```
pix515e-635#show crypto isakmp sa
Total     : 1
Embryonic : 0
        dst               src        state     pending
created
      10.20.20.1       10.10.10.1    QM_IDLE         0
1

pix515e-635#show crypto ipsec sa



           interface: outside
           Crypto map tag: dynmaptosw, local addr.
10.20.20.1
```

```
 local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
           remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
           current_peer: 10.10.10.1:500
           PERMIT, flags={}
           #pkts encaps: 0, #pkts encrypt: 0, #pkts
digest 0
           #pkts decaps: 0, #pkts decrypt: 0, #pkts
verify 0
           #pkts compressed: 0, #pkts decompressed: 0
           #pkts not compressed: 0, #pkts compr. failed:
0, #pkts decompress failed: 0
           #send errors 0, #recv errors 0

 local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1
           path mtu 1500, ipsec overhead 72, media mtu
1500
           current outbound spi: efb1149d

 inbound esp sas:
           spi: 0x2ad2c13c(718455100)
           transform: esp-aes-256 esp-sha-hmac ,
           in use settings ={Tunnel, }
           slot: 0, conn id: 2, crypto map: dynmaptosw
           sa timing: remaining key lifetime (k/sec):
(4608000/28736)
           IV size: 16 bytes
           replay detection support: Y


           inbound ah sas:


           inbound pcp sas:


           outbound esp sas:
           spi: 0xefb1149d(4021359773)
           transform: esp-aes-256 esp-sha-hmac ,
           in use settings ={Tunnel, }
           slot: 0, conn id: 1, crypto map: dynmaptosw
           sa timing: remaining key lifetime (k/sec):
(4608000/28727)
           IV size: 16 bytes
           replay detection support: Y


           outbound ah sas:


           outbound pcp sas:

pix515e-635#
```

Cisco PIX 515 versión 7.0(2) - Modo agresivo

```
pix515-702#show crypto isakmp sa

 Active SA: 1
           Rekey SA: 0 (A tunnel will report 1 Active
and 1 Rekey SA during rekey)
           Total IKE SA: 1

1 IKE Peer: 10.10.10.1
           Type : L2L Role : responder
           Rekey : no State : AM_ACTIVE
           pix515-702#

pix515-702#show crypto ipsec sa
           interface: outside
           Crypto map tag: ciscopix, local addr:
10.20.20.1

 local ident (addr/mask/prot/port):
(192.168.1.0/255.255.255.0/0/0)
           remote ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
           current_peer: 10.10.10.1

 #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
           #pkts decaps: 5, #pkts decrypt: 5, #pkts
verify: 5
           #pkts compressed: 0, #pkts decompressed: 0
           #pkts not compressed: 5, #pkts comp failed:
0, #pkts decomp failed: 0
           #send errors: 0, #recv errors: 0

 local crypto endpt.: 10.20.20.1, remote crypto endpt.:
10.10.10.1

 path mtu 1500, ipsec overhead 76, media mtu 1500
           current outbound spi: D7E2F5FD

 inbound esp sas:
           spi: 0xDCBF6AD3 (3703532243)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: ciscopix
           sa timing: remaining key lifetime (sec):
28703
           IV size: 16 bytes
           replay detection support: Y
           outbound esp sas:
           spi: 0xD7E2F5FD (3621975549)
           transform: esp-aes-256 esp-sha-hmac
           in use settings ={L2L, Tunnel, }
           slot: 0, conn_id: 1, crypto-map: ciscopix
           sa timing: remaining key lifetime (sec):
28701
           IV size: 16 bytes
           replay detection support: Y

pix515-702#
```

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Cisco PIX Firewall Software
- Referencias de Comandos de Cisco Secure PIX Firewall
- Avisos de campos de productos de seguridad (incluido PIX)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico y Documentación - Cisco Systems