Ejemplo de Configuración de IPSec LAN a LAN entre un Catalyst 6500 con el Módulo de Servicio VPN y un Firewall PIX

Contenido

Introducción

Este documento describe cómo crear un túnel IPSec LAN a LAN entre un switch Cisco Catalyst 6500 Series con el módulo de servicio IPSec VPN (W) y un Cisco PIX Firewall.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Cisco IOS® Software Release 12.2(14)SY2 para Catalyst 6000 Series Supervisor Engine, con el módulo de servicio IPSec VPN
- Software Cisco PIX Firewall versión 6.3(3)

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.

Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Antecedentes

El módulo de servicio VPN Catalyst 6500 tiene dos puertos Gigabit Ethernet (GE) sin conectores visibles externamente. Estos puertos son direccionables sólo con fines de configuración. El puerto 1 es siempre el puerto interior. Este puerto gestiona todo el tráfico desde y hacia la red interna. El segundo puerto (puerto 2) gestiona todo el tráfico desde y hacia la WAN o las redes externas. Estos dos puertos siempre se configuran en el modo de enlace troncal 802.1Q. El módulo de servicio VPN utiliza una técnica denominada Bump In The Wire (BITW) para el flujo de paquetes.

Los paquetes son procesados por un par de VLAN, una Capa 3 dentro de VLAN y una Capa 2 fuera de VLAN. Los paquetes, desde el interior hasta el exterior, se enrutan a través de un método denominado Lógica de reconocimiento de direcciones codificadas (EARL) a la VLAN interna. Después de cifrar los paquetes, el módulo de servicio VPN utiliza la VLAN exterior correspondiente. En el proceso de descifrado, los paquetes del exterior al interior se puentean al módulo de servicio VPN usando la VLAN externa. Después de que el módulo de servicio VPN descifra el paquete y mapea la VLAN a la VLAN interna correspondiente, EARL enruta el paquete al puerto LAN apropiado. La Capa 3 dentro de la VLAN y la Capa 2 fuera de las VLAN se unen con el comando **crypto connect vlan**. Hay tres tipos de puertos en los switches Catalyst serie 6500:

- **Puertos enrutados**: de forma predeterminada, todos los puertos Ethernet son puertos enrutados en Cisco IOS. Estos puertos tienen una VLAN oculta asociada con ellos.
- **Puertos de acceso**: estos puertos tienen una VLAN de protocolo de enlace troncal (VTP) externa o VLAN asociada a ellos. Puede asociar más de un puerto a una VLAN definida.
- **Puertos troncales**: estos puertos llevan muchas VLAN externas o VTP, en las que todos los paquetes se encapsulan con un encabezado 802.1Q.

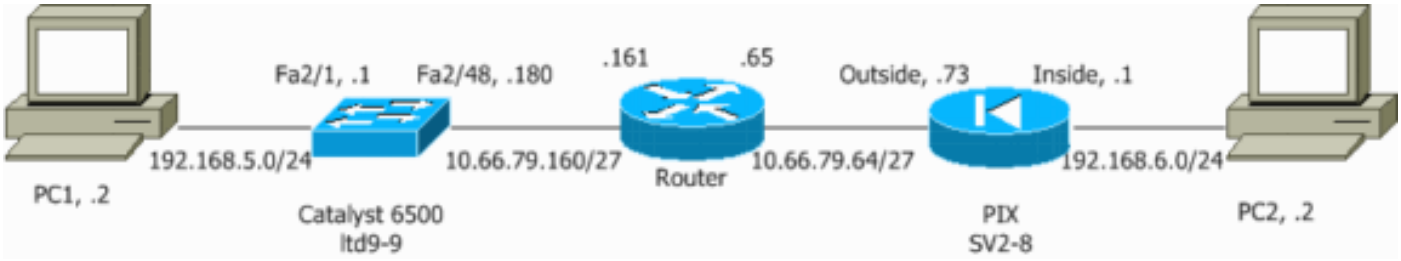
Configurar

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

Nota: Use la Command Lookup Tool (sólo clientes registrados) para obtener más información sobre los comandos utilizados en este documento.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



Configuración para IPSec con un Puerto Trunk o Acceso de Capa 2

Realice estos pasos para configurar IPSec con la ayuda de un acceso de Capa 2 o puerto troncal para la interfaz física externa.

1. Agregue las VLAN internas al puerto interno del módulo de servicio VPN.Suponga que el módulo de servicio VPN está en la ranura 4. Utilice VLAN 100 como VLAN interna y VLAN 209 como VLAN externa. Configure los puertos GE del módulo de servicio VPN de la siguiente manera:

```
interface GigabitEthernet4/1
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,1002-1005
 switchport mode trunk
 cdp enable

interface GigabitEthernet4/2
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,209,1002-1005
 switchport mode trunk
 cdp enable
 spanning-tree portfast trunk
```

2. Agregue la interfaz VLAN 100 y la interfaz donde se termina el túnel (que, en este caso, es la `interfaz Vlan 209`, como se muestra aquí).

```
interface Vlan100
 ip address 10.66.79.180 255.255.255.224

interface Vlan209
 no ip address
 crypto connect vlan 100
```

3. Configure el puerto físico externo como un puerto de acceso o troncal (en este caso, `FastEthernet 2/48`, como se muestra aquí).

```
!--- This is the configuration that uses an access port. interface FastEthernet2/48
 no ip address
 switchport
 switchport access vlan 209
 switchport mode access

!--- This is the configuration that uses a trunk port. interface FastEthernet2/48
```

```
no ip address switchport
switchport trunk encapsulation dot1q
switchport mode trunk
```

4. Cree la NAT de omisión. Agregue estas entradas a la sentencia no nat para eximir el nating entre estas redes:

```
access-list inside_nat0_outbound permit ip 192.168.5.0 0.0.0.255
192.168.6.0 0.0.0.255
global (outside) 1 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 192.168.5.0 255.255.255.0
```

5. Cree la configuración de criptografía y la lista de control de acceso (ACL) que define el tráfico que se va a cifrar.Cree una ACL criptográfica (en este caso, ACL 100 - Tráfico interesante) que defina el tráfico desde la red interna 192.168.5.0/24 a la red remota 192.168.6.0/24, de la siguiente manera:

```
access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

Defina sus propuestas de políticas de protocolo ISAKMP (Asociación de seguridad de Internet) y protocolo de administración de claves (Key Management Protocol), como las siguientes:

```
crypto isakmp policy 1
hash md5
authentication pre-share
group 2
```

Ejecute este comando (en este ejemplo) para utilizar y definir claves previamente compartidas:

```
crypto isakmp key cisco address 10.66.79.73
```

Defina las propuestas de IPSec de la siguiente manera:

```
crypto ipsec transform-set cisco esp-des esp-md5-hmac
```

Cree su declaración de mapa criptográfico de la siguiente manera:

```
crypto map cisco 10 ipsec-isakmp
 set peer 10.66.79.73
 set transform-set cisco
 match address 100
```

6. Aplique el mapa crypto a la interfaz VLAN 100, de la siguiente manera:

```
interface vlan100
crypto map cisco
```

Estas configuraciones se utilizan:

- Catalyst 6500
- Firewall PIX

Catalyst 6500

```
!--- Define the Phase 1 policy. crypto isakmp policy 1
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco address 10.66.79.73
!
!
!--- Define the encryption policy for this setup. crypto
ipsec transform-set cisco esp-des esp-md5-hmac
!
!--- Define a static crypto map entry for the peer !---
with mode ipsec-isakmp. !--- This indicates that
Internet Key Exchange (IKE) !--- is used to establish
the IPSec !--- security associations (SAs) to protect
the traffic !--- specified by this crypto map entry.
crypto map cisco 10 ipsec-isakmp
 set peer 10.66.79.73
 set transform-set cisco
 match address 100
!
!
no spanning-tree vlan 100
!
!
!
interface FastEthernet2/1
 ip address 192.168.5.1 255.255.255.0
!
!--- This is the outside Layer 2 port that allows !---
VLAN 209 traffic to enter. interface FastEthernet2/48 no
ip address switchport switchport trunk encapsulation
dot1q switchport mode trunk ! interface
GigabitEthernet4/1 no ip address flowcontrol receive on
flowcontrol send off switchport switchport trunk
encapsulation dot1q !--- VLAN 100 is defined as the
Interface VLAN (IVLAN).  switchport trunk allowed vlan
1,100,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet4/2
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
!--- The Port VLAN (PVLAN) configuration is handled
transparently by !--- the VPN service module without
user configuration !--- or involvement. It also is not
shown in the configuration. !--- Note: For every IVLAN,
a corresponding PVLAN exists.

 switchport trunk allowed vlan 1,209,1002-1005
 switchport mode trunk
 cdp enable
 spanning-tree portfast trunk
!
interface Vlan1
no ip address
shutdown
!
```

```
!--- This is the IVLAN that is configured to intercept
the traffic !--- destined to the secure port on which
the inside port !--- of the VPN service module is the
only port present. interface Vlan100 ip address
10.66.79.180 255.255.255.224  crypto map cisco
!--- This is the secure port that is a virtual Layer 3
interface. !--- This interface purposely does not have a
Layer 3 IP address !--- configured. This is normal for
the BITW process. !--- The IP address is moved from this
interface to the VLAN 100 to !--- accomplish BITW. This
brings the VPN service module into !--- the packet path.
interface Vlan209 no ip address  crypto connect vlan 100
!
ip classless

global (outside) 1 interface
!--- NAT 0 prevents NAT for networks specified in the
ACL inside_nat0_outbound. nat (inside) 0 access-list
inside_nat0_outbound nat (inside) 1 192.168.5.0
255.255.255.0 !--- Configure the routing so that the
device !--- is directed to reach its destination
network. ip route 0.0.0.0 0.0.0.0 10.66.79.161
!--- This access list (inside_nat0_outbound) is used
with the nat zero command. !--- This prevents traffic
which matches the access list from undergoing !---
network address translation (NAT). The traffic specified
by this ACL is !--- traffic that is to be encrypted and
!--- sent across the VPN tunnel. This ACL is
intentionally !--- the same as (100). !--- Two separate
access lists should always be used in this
configuration. access-list inside_nat0_outbound permit
ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255

!--- This is the crypto ACL. access-list 100 permit ip
192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

Firewall PIX

```
SV2-8(config)# show run
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
interface ethernet6 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
nameif ethernet3 intf3 security15
nameif ethernet4 intf4 security20
nameif ethernet5 intf5 security25
nameif ethernet6 intf6 security30
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname SV2-8
domain-name cisco.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 ils 389
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
!--- This is the traffic to the router. access-list 100
permit ip 192.168.6.0 255.255.255.0 192.168.5.0
255.255.255.0
access-list nonat permit ip 192.168.6.0 255.255.255.0
192.168.5.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
mtu intf6 1500
ip address outside 10.66.79.73 255.255.255.224
ip address inside 192.168.6.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
no ip address intf3
no ip address intf4
no ip address intf5
no ip address intf6
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
no failover ip address intf6
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 192.168.6.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 10.66.79.65 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 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
```

```
!--- These are IPSec policies. sysopt connection permit-
ipsec
crypto ipsec transform-set cisco esp-des esp-md5-hmac
crypto map cisco 10 ipsec-isakmp
crypto map cisco 10 match address 100
crypto map cisco 10 set peer 10.66.79.180
crypto map cisco 10 set transform-set cisco
crypto map cisco interface outside
!--- These are IKE policies. isakmp enable outside
isakmp key ******** address 10.66.79.180 netmask
255.255.255.255
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:244c86c9beab00bda8f790502ca74db9
: end
```

Configuración de IPSec con un Puerto Ruteado

Realice estos pasos para configurar IPSec con la ayuda de un puerto ruteado de Capa 3 para la interfaz física externa.

1. Agregue las VLAN internas al puerto interno del módulo de servicio VPN.Suponga que el módulo de servicio VPN está en la ranura 4. Utilice VLAN 100 como VLAN interna y VLAN 209 como VLAN externa. Configure los puertos GE del módulo de servicio VPN de la siguiente manera:

```
interface GigabitEthernet4/1
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,1002-1005
 switchport mode trunk
 cdp enable

interface GigabitEthernet4/2
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,209,1002-1005
 switchport mode trunk
 cdp enable
 spanning-tree portfast trunk
```

2. Agregue la interfaz VLAN 100 y la interfaz donde se termina el túnel (que, en este caso, es `FastEthernet2/48`, como se muestra aquí).

```
interface Vlan100
 ip address 10.66.79.180 255.255.255.224

interface FastEthernet2/48
```

```
 no ip address
 crypto connect vlan 100
```

3. Cree la NAT de omisión. Agregue estas entradas a la sentencia no nat para eximir el nating entre estas redes:
```
access-list inside_nat0_outbound permit ip 192.168.5.0 0.0.0.255
192.168.6.0 0.0.0.255
global (outside) 1 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 192.168.5.0 255.255.255.0
```
4. Cree su configuración de criptografía y la ACL que define el tráfico que se cifrará.Cree una ACL (en este caso, ACL 100) que defina el tráfico desde la red interna 192.168.5.0/24 a la red remota 192.168.6.0/24, de la siguiente manera:

   ```
   access-list 100 permit ip 192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
   ```

   Defina las propuestas de políticas ISAKMP, como esta:

   ```
   crypto isakmp policy 1
   hash md5
   authentication pre-share
   group 2
   ```

   Ejecute este comando (en este ejemplo) para utilizar y definir claves previamente compartidas:

   ```
   crypto isakmp key cisco address 10.66.79.73
   ```

   Defina las propuestas de IPSec de la siguiente manera:

   ```
   crypto ipsec transform-set cisco esp-des esp-md5-hmac
   ```

   Cree su declaración de mapa criptográfico de la siguiente manera:

   ```
   crypto map cisco 10 ipsec-isakmp
    set peer 10.66.79.73
    set transform-set cisco
    match address 100
   ```

5. Aplique el mapa crypto a la interfaz VLAN 100, de la siguiente manera:

   ```
   interface vlan100
   crypto map cisco
   ```

Estas configuraciones se utilizan:

- Catalyst 6500
- Firewall PIX

Catalyst 6500
`!--- Define the Phase 1 policy.` **`crypto isakmp policy 1`** **`hash md5`** **`authentication pre-share`**

```
 group 2
crypto isakmp key cisco address 10.66.79.73
!
!
!--- Define the encryption policy for this setup. crypto
ipsec transform-set cisco esp-des esp-md5-hmac
!
!--- Define a static crypto map entry for the peer !---
with mode ipsec-isakmp. !--- This indicates that IKE is
used to establish the !--- IPSec SAs to protect the
traffic !--- specified by this crypto map entry. crypto
map cisco 10 ipsec-isakmp
 set peer 10.66.79.73
 set transform-set cisco
 match address 100
!
!
no spanning-tree vlan 100
!
!
!
interface FastEthernet2/1
 ip address 192.168.5.1 255.255.255.0
!
!--- This is the secure port that is configured in
routed port mode. !--- This routed port mode does not
have a Layer 3 IP address !--- configured. This is
normal for the BITW process. !--- The IP address is
moved from this interface to the VLAN 100 to !---
accomplish BITW. This brings the VPN service module into
!--- the packet path. This is the Layer 2 port VLAN on
which the !--- outside port of the VPN service module
also belongs. ! interface FastEthernet2/48 no ip address
crypto connect vlan 100
!
interface GigabitEthernet4/1
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
!--- VLAN 100 is defined as the IVLAN.  switchport trunk
allowed vlan 1,100,1002-1005
 switchport mode trunk
 cdp enable
!
interface GigabitEthernet4/2
 no ip address
 flowcontrol receive on
 flowcontrol send off
 switchport
 switchport trunk encapsulation dot1q
!--- The PVLAN configuration is handled transparently by
the !--- VPN service module without user configuration
!--- or involvement. It also is not shown in the
configuration. !--- Note: For every IVLAN, a
corresponding PVLAN exists.

 switchport trunk allowed vlan 1,209,1002-1005
 switchport mode trunk
 cdp enable
 spanning-tree portfast trunk
!
interface Vlan1
```

```
no ip address
shutdown
!
!--- This is the IVLAN that is configured to intercept
the traffic !--- destined to the secure port on which
the inside port of the !--- VPN service module is the
only port present. interface Vlan100 ip address
10.66.79.180 255.255.255.224  crypto map cisco
!--- This is the secure port that is a virtual Layer 3
interface. !--- This interface purposely does not have a
Layer 3 IP address !--- configured. This is normal for
the BITW process. !--- The IP address is moved from this
interface to the VLAN 100 to !--- accomplish BITW. This
brings the VPN service module into !--- the packet path.
! ip classless global (outside) 1 interface !--- NAT 0
prevents NAT for networks specified in the ACL
inside_nat0_outbound. nat (inside) 0 access-list
inside_nat0_outbound nat (inside) 1 192.168.6.0
255.255.255.0 !--- Configure the routing so that the
device !--- is directed to reach its destination
network. ip route 0.0.0.0 0.0.0.0 10.66.79.161
!
!--- This access list (inside_nat0_outbound) is used
with the nat zero command. !--- This prevents traffic
which matches the access list from undergoing !---
network address translation (NAT). The traffic specified
by this ACL is !--- traffic that is to be encrypted and
!--- sent across the VPN tunnel. This ACL is
intentionally !--- the same as (100). !--- Two separate
access lists should always be used in this
configuration.



access-list inside_nat0_outbound permit ip 192.168.5.0
0.0.0.255 192.168.6.0 0.0.0.255

!--- This is the crypto ACL. access-list 100 permit ip
192.168.5.0 0.0.0.255 192.168.6.0 0.0.0.255
```

Firewall PIX

```
SV2-8(config)# show run
: Saved
:
PIX Version 6.3(3)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto shutdown
interface ethernet3 auto shutdown
interface ethernet4 auto shutdown
interface ethernet5 auto shutdown
interface ethernet6 auto shutdown
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 intf2 security10
nameif ethernet3 intf3 security15
nameif ethernet4 intf4 security20
nameif ethernet5 intf5 security25
nameif ethernet6 intf6 security30
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname SV2-8
```

```
domain-name cisco.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 ils 389
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
!--- This is the traffic to the router. access-list 100
permit ip 192.168.6.0 255.255.255.0 192.168.5.0
255.255.255.0
access-list nonat permit ip 192.168.6.0 255.255.255.0
192.168.5.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
mtu intf6 1500
ip address outside 10.66.79.73 255.255.255.224
ip address inside 192.168.6.1 255.255.255.0
ip address intf2 127.0.0.1 255.255.255.255
no ip address intf3
no ip address intf4
no ip address intf5
no ip address intf6
ip audit info action alarm
ip audit attack action alarm
no failover
failover timeout 0:00:00
failover poll 15
no failover ip address outside
no failover ip address inside
no failover ip address intf2
no failover ip address intf3
no failover ip address intf4
no failover ip address intf5
no failover ip address intf6
pdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 0 access-list nonat
nat (inside) 1 192.168.6.0 255.255.255.0 0 0
route outside 0.0.0.0 0.0.0.0 10.66.79.65 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 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
!--- These are IPSec policies. sysopt connection permit-
ipsec
crypto ipsec transform-set cisco esp-des esp-md5-hmac
crypto map cisco 10 ipsec-isakmp
crypto map cisco 10 match address 100
crypto map cisco 10 set peer 10.66.79.180
crypto map cisco 10 set transform-set cisco
crypto map cisco interface outside
!--- These are IKE policies. isakmp enable outside
isakmp key ******** address 10.66.79.180 netmask
255.255.255.255
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:244c86c9beab00bda8f790502ca74db9
: end
```

Verificación

En esta sección encontrará información que le permitirá confirmar que su configuración funcione 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 ipsec sa**: muestra la configuración utilizada por las SAs IPSec actuales.
- **show crypto isakmp sa — Muestra todas las IKE SAs actuales en un par.**
- **show crypto vlan**—Muestra la VLAN asociada con la configuración crypto.
- **show crypto eli**—Muestra las estadísticas del módulo de servicio VPN.

Para obtener información adicional sobre la verificación y resolución de problemas de IPSec, consulte Solución de problemas de seguridad IP - Introducción y uso de los comandos debug.

Troubleshoot

Esta sección proporciona la información para resolver problemas de su configuración.

Comandos para Troubleshooting

Nota: Antes de ejecutar **comandos debug**, consulte Información Importante sobre Comandos Debug.

- **depuración crypto ipsec — Muestra los IPSec Negotiations de la Fase 2.**
- **debug crypto isakmp — muestra las negociaciones ISAKMP para la fase 1.**
- **debug crypto engine — muestra el tráfico codificado.**

- **clear crypto isakmp**: borra las SA relacionadas con la Fase 1.
- **clear crypto sa**: borra las SA relacionadas con la Fase 2.

Para obtener información adicional sobre la verificación y resolución de problemas de IPSec, consulte Solución de problemas de seguridad IP - Introducción y uso de los comandos debug.

Información Relacionada

- Página de soporte de IPSec
- Configuración de seguridad de red IPSec
- Configuración del protocolo de seguridad de intercambio de claves de Internet
- Soporte Técnico - Cisco Systems