IPsec LAN-to-LAN tunnels tussen Catalyst 6500 met de VPN-servicemodule en een Cisco IOS routerconfiguratie voorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u een IPsec LAN-to-LAN tunnel kunt maken tussen een Cisco Catalyst 6500 Series switch met de VPN Acceleration Service module en een Cisco IOS® router.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS-softwarerelease 12.2(14)SY2 voor Catalyst 6000 Supervisor Engine, met de IPsec VPN servicemodule
- Cisco 3640 router die Cisco IOS-softwarerelease 12.3(4)T draait

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg voor meer informatie over documentconventies de technische Tips van Cisco.

Achtergrondinformatie

De Catalyst 6500 VPN servicemodule heeft twee Gigabit Ethernet (GE) poorten zonder extern zichtbare connectors. Deze havens zijn uitsluitend bestemd voor configuratiedoeleinden. Port 1 is altijd de binnenpoort. Deze poort verwerkt al verkeer van en naar het binnennetwerk. De tweede poort (poort 2) behandelt al verkeer van en naar WAN of externe netwerken. Deze twee poorten worden altijd ingesteld in 802.1Q trunking-modus. De de servicemodule van VPN gebruikt een techniek die Bump in The Wire (BITW) wordt genoemd voor pakketstroom.

Packets worden verwerkt door een paar VLAN's, één Layer 3 binnen VLAN en één Layer 2 buiten VLAN. De pakketten, van binnenuit tot buiten, worden door een methode die wordt genoemd Encoded Address Recognition Logic (EARL) aan de binnenkant van VLAN routeerd. Nadat het de pakketten heeft versleuteld gebruikt de VPN-servicemodule het corresponderende VLAN. In het decryptie proces, worden de pakketten van de buitenkant tot de binnenkant aan de VPN servicemodule verbonden die het buitenVLAN gebruikt. Nadat de VPN-servicemodule het pakket decrypteert en het VLAN met de bijbehorende binnenste VLAN-indeling in kaart brengt, routeert EARL het pakket naar de juiste LAN-poort. Layer 3 binnen VLAN en Layer 2 buiten VLAN's worden aangesloten bij elkaar door de **crypto verbinding met VLAN-**opdracht uit te geven. Er zijn drie typen havens in de Catalyst 6500 Series switches:

- Standaard worden alle Ethernet-poorten routed poorten gelegd. Deze poorten hebben een verborgen VLAN dat aan hen is gekoppeld.
- **Toegangspoorten**-Deze poorten hebben een extern of VLAN Trunk Protocol (VTP) VLAN dat met hen verbonden is. U kunt meer dan één poort koppelen naar een gedefinieerd VLAN.
- **Trunk-poorten**—Deze poorten dragen veel externe of VTP VLAN's, waarop alle pakketten zijn ingekapseld met een 802.1Q header.

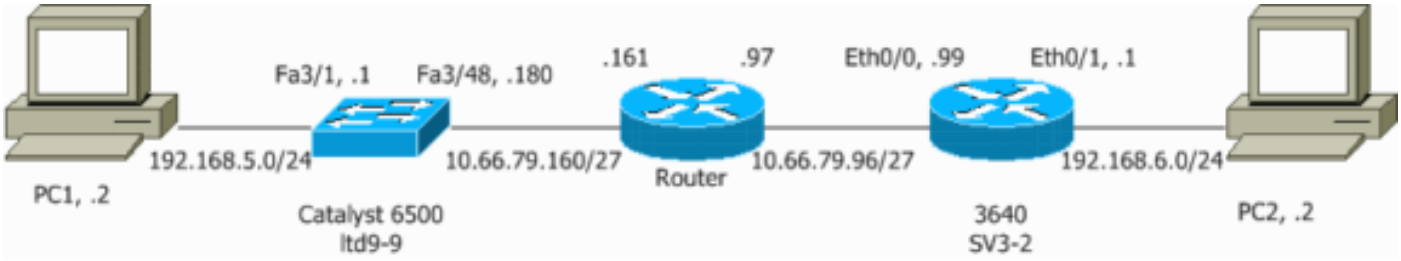
Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

N.B.: Gebruik het Opdrachtupgereedschap (alleen geregistreerde klanten) om meer informatie te vinden over de opdrachten die in dit document worden gebruikt.

Netwerkdiagram

Dit document gebruikt de netwerkinstellingen die in dit diagram worden weergegeven:



Configuratie voor IPsec met een Layer 2 access of Trunk-poort

Voer deze stappen uit om IPsec te configureren met behulp van een Layer 2-toegang of boomstampoort voor de externe fysieke interface.

1. Voeg de binnen VLAN's aan de binnenpoort van de VPN servicemodule toe.Stel dat de VPN-servicemodule op sleuf 4 staat. Gebruik VLAN 100 als inwendig VLAN en VLAN 209 als het externe VLAN. Configureer de VPN-servicemodule GE-poorten zoals deze:

```
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. Voeg de interface VLAN 100 en de interface toe waar de tunnel wordt beëindigd (die, in dit geval, `interface VLAN 209` is, zoals hier getoond).

```
interface Vlan100
 ip address 10.66.79.180 255.255.255.224

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

3. Configureer de externe fysieke poort als een toegang of boomstampoort (die in dit geval `FastEthernet 3/48` is, zoals hier wordt getoond).

```
!--- This is the configuration that uses an access port. interface FastEthernet3/48
 no ip address
 switchport
 switchport access vlan 209
 switchport mode access

!--- This is the configuration that uses a trunk port. interface FastEthernet3/48
 no ip address switchport
```

```
switchport trunk encapsulation dot1q
switchport mode trunk
```

4. Maak de Bypass NAT. Voeg deze ingangen aan het nee nat statement toe om het ding tussen deze netwerken vrij te stellen:
```
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. Maak uw crypto configuratie en de toegangscontrolelijst (ACL) die het te versleutelen verkeer definieert.Maak een ACL (in dit geval, ACL 100) die het verkeer van het binnennetwerk 192.168.5.0/24 aan het verre netwerk 192.168.6.0/24 definieert, zoals dit:

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

   Definieer je beleidsvoorstellen van de Internet Security Association en Key Management Protocol (ISAKMP), zoals deze:

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

   Geef deze opdracht (in dit voorbeeld) uit om vooraf gedeelde toetsen te gebruiken en te definiëren.

   ```
   crypto isakmp key cisco address 10.66.79.99
   ```

   Defineer uw IPsec-voorstellen als volgt:

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

   Maak je crypto plattegrond zoals deze:

   ```
   crypto map cisco 10 ipsec-isakmp
   set peer 10.66.79.99
   set transform-set cisco
   match address 100
   ```

6. Pas de crypto kaart op de interface van VLAN 100 toe, zoals dit:

   ```
   interface vlan100
   crypto map cisco
   ```

Deze configuraties worden gebruikt.

- Catalyst 6500
- Cisco IOS-router

Catalyst 6500

```
!--- Define the Phase 1 policy. crypto isakmp policy 1
 hash md5
```

```
 authentication pre-share
 group 2
crypto isakmp key cisco address 10.66.79.99
!
!
!--- 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 10.66.79.99
 set transform-set cisco
 match address 100
!
!
no spanning-tree vlan 100
!
!
!
interface FastEthernet3/1
 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 FastEthernet3/48 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 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
!--- 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
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 !--- 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
```

Cisco IOS-router

```
SV3-2#show run
Building configuration...

Current configuration : 1268 bytes
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!--- Define the Phase 1 policy. crypto isakmp policy 1
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco address 10.66.79.180
```

```
!
!
!--- 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 10.66.79.180
 set transform-set cisco
 match address 100
!
!
!--- Apply the crypto map to the interface. interface
Ethernet0/0 ip address 10.66.79.99 255.255.255.224 half-
duplex crypto map cisco
!
interface Ethernet0/1
 ip address 192.168.6.1 255.255.255.0
 half-duplex
 no keepalive
!
!
ip http server
no ip http secure-server
ip classless
!--- Configure the routing so that the device !--- is
directed to reach its destination network. ip route
0.0.0.0 0.0.0.0 10.66.79.97
!
!
!--- This is the crypto ACL. access-list 100 permit ip
192.168.6.0 0.0.0.255 192.168.5.0 0.0.0.255
!
!
control-plane
!
!
line con 0
line aux 0
line vty 0 4
!
end
```

Configuratie voor IPsec met behulp van een Routed Port

Voer deze stappen uit om IPsec te configureren met behulp van een Layer 3 routepoort voor de externe fysieke interface.

1. Voeg de binnen VLAN's aan de binnenpoort van de VPN servicemodule toe.Stel dat de VPN-servicemodule op sleuf 4 staat. Gebruik VLAN 100 als inwendig VLAN en VLAN 209 als het externe VLAN. Configureer de VPN-servicemodule GE-poorten zoals deze:

```
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. Voeg de interface VLAN 100 en de interface toe waar de tunnel wordt beëindigd (die, in dit geval, `FastEthernet3/48` is, zoals hier getoond).

```
interface Vlan100
 ip address 10.66.79.180 255.255.255.224

interface FastEthernet3/48
 no ip address
 crypto connect vlan 100
```

3. Maak de Bypass NAT. Voeg deze ingangen aan het nee nat statement toe om het ding tussen deze netwerken vrij te stellen:

```
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. Maak uw crypto configuratie en ACL die het te versleutelen verkeer definieert.Maak een ACL (in dit geval, ACL 100) die het verkeer van het binnennetwerk 192.168.5.0/24 aan het verre netwerk 192.168.6.0/24 definieert, zoals dit:

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

Definieer je beleidsvoorstellen van ISAKMP zoals deze:

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

Geef deze opdracht (in dit voorbeeld) uit om vooraf gedeelde toetsen te gebruiken en te definiëren:

```
crypto isakmp key cisco address 10.66.79.99
```

Defineer uw IPsec-voorstellen als volgt:

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

Maak je crypto plattegrond zoals deze:

```
crypto map cisco 10 ipsec-isakmp
 set peer 10.66.79.99
 set transform-set cisco
```

```
 match address 100
```

5. Pas de crypto kaart op de interface van VLAN 100 toe, zoals dit:

```
interface vlan100
crypto map cisco
```

Deze configuraties worden gebruikt.

- Catalyst 6500
- Cisco IOS-router

Catalyst 6500

```
!--- Define the Phase 1 policy. crypto isakmp policy 1
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco address 10.66.79.99
!
!
!--- 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 10.66.79.99
 set transform-set cisco
 match address 100
!
!
no spanning-tree vlan 100
!
!
!
interface FastEthernet3/1
 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 FastEthernet3/48 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
!
ip classless
!--- 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
!
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 !--- 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
```

Cisco IOS-router

```
SV3-2# show run
Building configuration...

Current configuration : 1268 bytes
!
version 12.3
```

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname SV3-2
!
boot-start-marker
boot-end-marker
!
!
no aaa new-model
ip subnet-zero
!
ip audit notify log
ip audit po max-events 100
ip ssh break-string
no ftp-server write-enable
!
!--- Define the Phase 1 policy. crypto isakmp policy 1
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco address 10.66.79.180
!
!
!--- 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 10.66.79.180
 set transform-set cisco
 match address 100
!
!
!--- Apply the crypto map to the interface. interface
Ethernet0/0 ip address 10.66.79.99 255.255.255.224 half-
duplex crypto map cisco
!
interface Ethernet0/1
 ip address 192.168.6.1 255.255.255.0
 half-duplex
 no keepalive
!
!
ip http server
no ip http secure-server
ip classless
!--- Configure the routing so that the device !--- is
directed to reach its destination network. ip route
0.0.0.0 0.0.0.0 10.66.79.97
!
!
!--- This is the crypto ACL. access-list 100 permit ip
192.168.6.0 0.0.0.255 192.168.5.0 0.0.0.255
!
!
control-plane
!
!
line con 0
```

```
line aux 0
line vty 0 4
!
end
```

Verifiëren

Deze sectie verschaft de informatie om te bevestigen dat uw configuratie correct werkt.

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **toon crypto ipsec sa**-Toont de instellingen die zijn gebruikt door de huidige IPsec SAs.
- **toon crypto isakmp sa**-toont alle huidige IKE SAs bij een peer.
- **toon crypto vlan** - toont VLAN verbonden aan de crypto configuratie.
- **toont crypto eli**—toont de statistieken van de VPN-servicemodule.

Raadpleeg voor meer informatie over het controleren en oplossen van IPsec de probleemoplossing bij IP-beveiliging - Oplossingen begrijpen en gebruiken van debug-opdrachten.

Problemen oplossen

Deze sectie verschaft de informatie om uw configuratie problemen op te lossen.

Opdrachten voor troubleshooting

Opmerking: Voordat u **debug-**opdrachten afgeeft, raadpleegt u Belangrijke informatie over debug-opdrachten.

- **debug crypto ipsec** - toont de IPsec onderhandelingen van fase 2.
- **debug crypto isakmp** — toont de ISAKMP-onderhandelingen van fase 1.
- **debug crypto motor** - toont het verkeer dat wordt versleuteld.
- **duidelijke crypto isakmp** — ontruimt de SA's in verband met fase 1.
- **duidelijke crypto sa** — ontruimt de SA's in verband met fase 2.

Raadpleeg voor meer informatie over het controleren en oplossen van IPsec de probleemoplossing bij IP-beveiliging - Oplossingen begrijpen en gebruiken van debug-opdrachten.

Gerelateerde informatie

- IPsec-ondersteuningspagina
- IPsec-netwerkbeveiliging configureren
- Het configureren van Internet Key Exchange-beveiligingsprotocol
- Technische ondersteuning - Cisco-systemen