نفق IPSec LAN إلى LAN بين محول Catalyst وحدة النمطية لخدمة VPN والمثوم مع 6500 جدار حماية PIX تكوين

المحتويات

المقدمة

يصف هذا المستند كيفية إنشاء نفق IPSec LAN إلى LAN بين محول من السلسلة Cisco Catalyst 6500 Series مع الوحدة النمطية للخدمة (IPSec (W وجدار حماية Cisco PIX.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- برنامج IOS® الإصدار 12.2(14)SY2 من Cisco ل Catalyst 6000 Series Supervisor Engine، مع الوحدة النمطية لخدمة IPSec VPN
- برنامج جدار حماية Cisco PIX، الإصدار 6.3(3)

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة

المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

معلومات أساسية

تحتوي الوحدة النمطية لخدمة Catalyst 6500 VPN Service module على منفذي Gigabit Ethernet (GE) بدون موصلات ظاهرة خارجيا. هذه المنافذ قابلة للتوجيه لأغراض التكوين فقط. المنفذ 1 هو دائما المنفذ الداخلي. يعالج هذا المنفذ حركة مرور البيانات من الشبكة الداخلية وإليها. يعالج الميناء الثاني (ميناء 2) كل حركة مرور من وإلى ال WAN أو الشبكات الخارجية. يتم تكوين هذين المنفذين دائما في وضع التوصيل 802.1Q. تستخدم الوحدة النمطية لخدمة VPN تقنية تسمى التضاريس في السلك (BITW) لتدفق الحزمة.

تتم معالجة الحزم بواسطة زوج من شبكات VLAN، وطبقة واحدة من الطبقة 3 داخل شبكة VLAN وطبقة واحدة من الطبقة 2 خارج شبكة VLAN. يتم توجيه الحزم، من الداخل إلى الخارج، من خلال طريقة تسمى منطق التعرف على العنوان المشفر (EARL) إلى شبكة VLAN الداخلية. بعد تشفير الحزم، تستخدم الوحدة النمطية لخدمة VPN الشبكة المحلية الظاهرية (VLAN) المقابلة خارج VLAN. في عملية فك التشفير، يتم ربط الحزم من الخارج إلى الداخل إلى الوحدة النمطية لخدمة VPN باستخدام شبكة VLAN الخارجية. بعد أن تقوم الوحدة النمطية لخدمة VPN بفك تشفير الحزمة وتخطيط شبكة VLAN إلى الشبكة المحلية الظاهرية (VLAN) المقابلة داخل، يقوم إيرل بتوجيه الحزمة إلى منفذ LAN المناسب. جمعت الطبقة 3 داخل VLAN والطبقة 2 خارج VLANs مع **ال crypto يربط vlan** أمر. هناك ثلاثة نوع الميناء في المادة حفازة 6500 sery مفتاح:

- **المنافذ الموجهة**- بشكل افتراضي، يتم توجيه جميع منافذ الإيثرنت في Cisco IOS. تحتوي هذه المنافذ على شبكة VLAN مخفية مرتبطة بها.
- **منافذ الوصول**— تحتوي هذه المنافذ على شبكة محلية ظاهرية (VLAN) خارجية أو بروتوكول خط اتصال شبكات VLAN (VTP) مرتبط بها. أنت يستطيع صحبت أكثر من واحد ميناء إلى VLAN يعين.
- **منافذ خطوط الاتصال**— تحمل هذه المنافذ العديد من شبكات VLAN الخارجية أو VTP، والتي يتم على أساسها تضمين جميع الحزم باستخدام رأس 802.1Q.

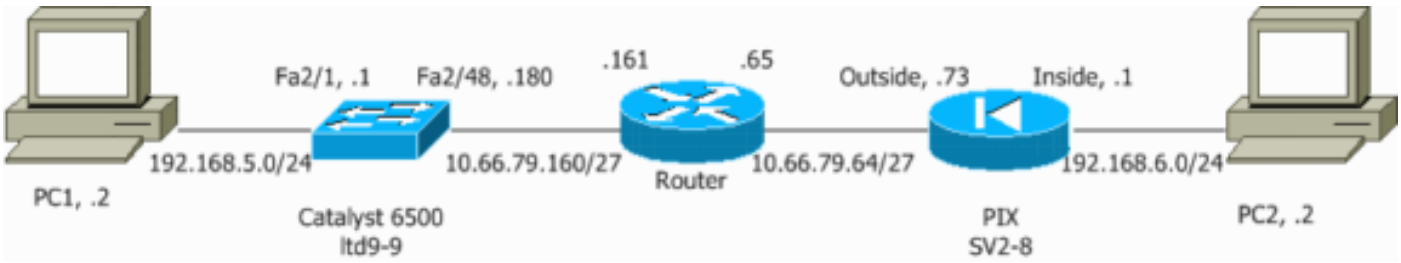
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للعثور على مزيد من المعلومات حول الأوامر المستخدمة في هذا المستند.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



تكوين IPSec باستخدام منفذ وصول أو خط اتصال من الطبقة 2

قم بإجراء هذه الخطوات لتكوين IPSec باستخدام التعليمات الخاصة بمنفذ وصول أو خط اتصال للطبقة 2 للواجهة المادية الخارجية.

1. أضفت ال VLANs داخلي إلى الميناء داخلي من ال VPN خدمة وحدة نمطية.افترضت أن ال VPN خدمة وحدة نمطية على شق مكان 4. أستخدم شبكة VLAN 100 كشبكة VLAN الداخلية وشبكة VLAN 209 كشبكة VLAN الخارجية. شكلت ال VPN خدمة وحدة نمطية GE ميناء مثل هذا:

```
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
```

أضفت ال VLAN 100 قارن والقارن حيث النفق يكون أنهيت (أي، في هذه الحالة، VLAN 209، كما هو موضح هنا).

```
interface Vlan100
 ip address 10.66.79.180 255.255.255.224

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

قم بتكوين المنفذ المادي الخارجي كمنفذ وصول أو خط اتصال (في هذه الحالة، FastEthernet 2/48، كما هو موضح هنا).

```
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. قم بإنشاء NAT الالتفافي. قم بإضافة هذه الإدخالات إلى جملة NAT بدون إستثناء الحد الفاصل بين هذه الشبكات:

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

```
nat (inside) 1 192.168.5.0 255.255.255.0
```

قم بإنشاء تكوين التشفير وقائمة التحكم في الوصول (ACL) التي تحدد حركة المرور التي سيتم تشفيرها.قم5.
بإنشاء قائمة تحكم في الوصول (ACL) للتشفير (في هذه الحالة، 100 ACL - حركة مرور مثيرة للاهتمام) التي تحدد حركة المرور من الشبكة الداخلية 24/192.168.5.0 إلى الشبكة البعيدة 24/192.168.6.0، مثل هذا:

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

قم بتعريف اقتراحات نهج اقتران أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP)، مثل هذا:

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

أصدرت هذا أمر (في هذا مثال) أن يستعمل ويعين مفتاح مشترك مسبقا:

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

قم بتحديد مقترحات IPSec، مثل ما يلي:

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

قم بإنشاء جملة خريطة التشفير، مثل هذا:

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

6. تطبيق خريطة التشفير على واجهة VLAN 100، مثل هذا:

```
interface vlan100
crypto map cisco
```

يتم إستخدام هذه التكوينات:

- Catalyst 6500
- جدار حماية 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
```

جدار حماية 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 :
```

تكوين IPSec باستخدام منفذ موجه

أنجزت هذا steps أن يشكل IPSec مع مساعدة من طبقة 3 مسحاج تخديد ميناء للقارن خارجي طبيعي.

1. أضفت ال VLANs داخلي إلى الميناء داخلي من ال VPN خدمة وحدة نمطية.افترضت أن ال VPN خدمة وحدة نمطية على شق مكان 4. أستخدم شبكة VLAN 100 كشبكة VLAN الداخلية وشبكة VLAN 209 كشبكة VLAN الخارجية. شكلت ال VPN خدمة وحدة نمطية GE ميناء مثل هذا:

```
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
```

أضفت ال VLAN 100 قارن والقارن حيث النفق يكون أنهيت (أي، في هذه الحالة، FastEthernet2/48، كما هو موضح هنا).

```
interface Vlan100
 ip address 10.66.79.180 255.255.255.224

interface FastEthernet2/48
 no ip address
 crypto connect vlan 100
```

3. قم بإنشاء NAT الالتفافي. قم بإضافة هذه الإدخالات إلى جملة NAT بدون إستثناء الحد الفاصل بين هذه الشبكات:

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

قم بإنشاء تكوين التشفير وقائمة التحكم في الوصول (ACL) التي تحدد حركة المرور التي سيتم تشفيرها.قم4. بإنشاء قائمة تحكم في الوصول (ACL) (في هذه الحالة، 100 ACL) التي تحدد حركة المرور من الشبكة الداخلية 24/192.168.5.0 إلى الشبكة البعيدة 24/192.168.6.0، مثل هذا:

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

قم بتحديد مقترحات نهج ISAKMP، مثل هذا:

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

أصدرت هذا أمر (في هذا مثال) أن يستعمل ويعين مفتاح مشترك مسبقا:

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

قم بتحديد مقترحات IPSec، مثل ما يلي:

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

قم بإنشاء جملة خريطة التشفير، مثل هذا:

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

5. تطبيق خريطة التشفير على واجهة VLAN 100، مثل هذا:

```
interface vlan100
crypto map cisco
```

يتم إستخدام هذه التكوينات:

- Catalyst 6500
- جدار حماية 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
```

جدار حماية 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 :
```

التحقق من الصحة

يوفر هذا القسم المعلومات للتأكد من أن التكوين لديك يعمل بشكل صحيح.

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

- **show crypto ipSec**— يعرض الإعدادات المستخدمة من قبل رسائل IPSec الحالية.
- **show crypto isakmp sa**— يعرض جميع شبكات IKE الحالية في نظير.
- **show crypto vlan**— يعرض شبكة VLAN المرتبطة بتكوين التشفير.
- **show crypto eli**— يعرض إحصائيات الوحدة النمطية لخدمة VPN.

للحصول على معلومات إضافية حول التحقق من IPSec واستكشاف أخطائه وإصلاحها، ارجع إلى أستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء واستخدامها.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات أستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

ملاحظة: قبل إصدار أوامر **debug**، راجع المعلومات المهمة في أوامر تصحيح الأخطاء.

- **debug crypto ipSec**—يعرض مفاوضات IPSec للمرحلة 2.
- **debug crypto isakmp**—يعرض مفاوضات ISAKMP للمرحلة 1.
- **debug crypto engine**—يعرض حركة مرور البيانات التي يتم تشفيرها.
- **مسح التشفير isakmp**—يعمل على مسح أسماء مناطق الوصول (SAs) المتعلقة بالمرحلة الأولى.
- **مسح التشفير sa**—يمسح أسماء مناطق الوصول (SA) المتعلقة بالمرحلة 2.

للحصول على معلومات إضافية حول التحقق من IPSec واستكشاف أخطائه وإصلاحها، ارجع إلى أستكشاف أخطاء أمان IP وإصلاحها - فهم أوامر تصحيح الأخطاء واستخدامها.

معلومات ذات صلة

- صفحة دعم IPSec
- تكوين أمان شبكة IPSec
- تكوين بروتوكول أمان Internet Key Exchange
- الدعم الفني - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).