

# IPSec LAN-to-LAN-Tunnel zwischen einem Catalyst 6500 mit dem VPN-Service-Modul und einem PIX-Firewall-Konfigurationsbeispiel

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfiguration für IPSec mithilfe eines Layer-2-Zugriffs- oder Trunk-Ports](#)

[Konfiguration für IPSec mit einem gerouteten Port](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Fehlerbehebung bei Befehlen](#)

[Zugehörige Informationen](#)

## Einführung

Dieses Dokument beschreibt die Erstellung eines IPSec LAN-to-LAN-Tunnels zwischen einem Cisco Catalyst Switch der Serie 6500 mit dem IPSec VPN-Dienstmodul (W) und einer Cisco PIX-Firewall.

## Voraussetzungen

### Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco IOS® Softwareversion 12.2(14)SY2 für die Catalyst Supervisor Engine der Serie 6000 mit IPSec VPN-Service-Modul

- Cisco PIX Firewall-Software Version 6.3(3)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#).

## Hintergrundinformationen

Das Catalyst 6500 VPN-Servicemodul verfügt über zwei Gigabit Ethernet (GE)-Ports ohne von außen sichtbare Anschlüsse. Diese Ports können nur zu Konfigurationszwecken adressiert werden. Port 1 ist immer der interne Port. Dieser Port verarbeitet den gesamten Datenverkehr vom und zum internen Netzwerk. Der zweite Port (Port 2) verarbeitet den gesamten Datenverkehr vom und zum WAN oder zu externen Netzwerken. Diese beiden Ports werden immer im 802.1Q-Trunking-Modus konfiguriert. Das VPN-Servicemodul verwendet eine Technik, die als Bump In The Wire (BITW) für den Paketfluss bezeichnet wird.

Pakete werden von einem Paar VLANs, einem Layer-3-VLAN innerhalb und einem Layer-2-VLAN außerhalb verarbeitet. Die Pakete von innen nach außen werden über eine Methode mit dem Namen Encoded Address Recognition Logic (EARL) an das interne VLAN weitergeleitet. Nachdem die Pakete verschlüsselt wurden, verwendet das VPN-Servicemodul das entsprechende externe VLAN. Beim Entschlüsselungsprozess werden die Pakete von außen nach innen mithilfe des externen VLAN zum VPN-Dienstmodul überbrückt. Nachdem das VPN-Servicemodul das Paket entschlüsselt und dem entsprechenden internen VLAN zugeordnet hat, leitet EARL das Paket an den entsprechenden LAN-Port weiter. Das Layer-3-interne VLAN und die Layer-2-externen VLANs sind mit dem Befehl **crypto connect vlan** verbunden. Die Catalyst Switches der Serie 6500 verfügen über drei Port-Typen:

- **Geroutete Ports** - Standardmäßig sind alle Ethernet-Ports geroutete Ports in Cisco IOS. Diesen Ports ist ein verborgenes VLAN zugeordnet.
- **Access Ports** - Diesen Ports ist ein externes oder VTP-VLAN (VLAN Trunk Protocol) zugeordnet. Sie können einem definierten VLAN mehrere Ports zuordnen.
- **Trunk-Ports** - Diese Ports enthalten viele externe oder VTP-VLANs, auf denen alle Pakete mit einem 802.1Q-Header gekapselt sind.

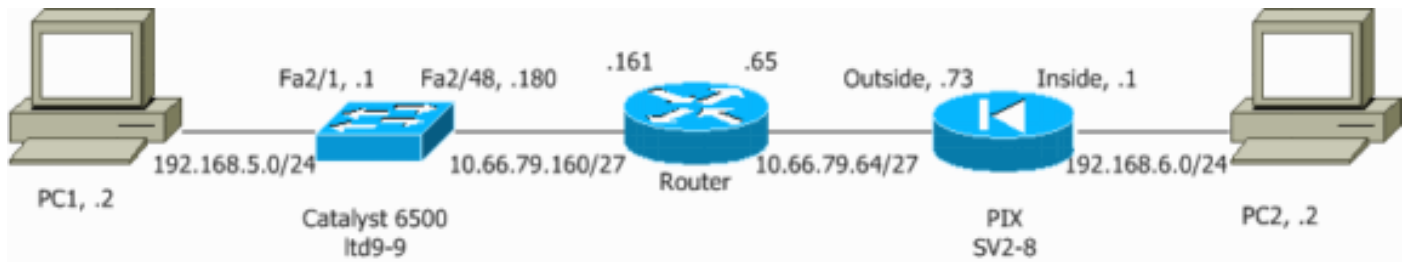
## Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

**Hinweis:** Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten.

## Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



## Konfiguration für IPsec mithilfe eines Layer-2-Zugriffs- oder Trunk-Ports

Führen Sie diese Schritte durch, um IPsec mithilfe eines Layer-2-Zugriffs- oder Trunk-Ports für die physische Außenschnittstelle zu konfigurieren.

1. Fügen Sie die internen VLANs dem internen Port des VPN-Dienstmoduls hinzu. Nehmen Sie an, das VPN-Service-Modul befindet sich in Steckplatz 4. Verwenden Sie VLAN 100 als internes VLAN und VLAN 209 als externes VLAN. Konfigurieren Sie die GE-Ports des VPN-Dienstmoduls wie folgt:

```
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. Fügen Sie die VLAN 100-Schnittstelle und die Schnittstelle hinzu, an der der Tunnel terminiert wird (in diesem Fall die Schnittstelle VLAN 209, wie hier gezeigt).

```
interface Vlan100
ip address 10.66.79.180 255.255.255.224
```

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

3. Konfigurieren Sie den externen physischen Port als Zugriffs- oder Trunk-Port (in diesem Fall FastEthernet 2/48, wie hier gezeigt).

```
!--- 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. Erstellen Sie die NAT umgehen. Fügen Sie diese Einträge der no nat-Anweisung hinzu, um die Verschachtelung zwischen diesen Netzwerken auszunehmen:

```
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. Erstellen Sie Ihre Crypto-Konfiguration und die Zugriffskontrollliste (ACL), die den zu verschlüsselnden Datenverkehr definiert. Erstellen Sie eine Crypto ACL (in diesem Fall ACL 100 - Interesting Traffic), die den Datenverkehr vom internen Netzwerk 192.168.5.0/24 zum Remote-Netzwerk 192.168.6.0/24 definiert. Beispiel:

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

Definieren Sie Ihre Richtlinienvorschläge für die Internet Security Association und das Key Management Protocol (ISAKMP):

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

Geben Sie diesen Befehl (in diesem Beispiel) ein, um vorinstallierte Schlüssel zu verwenden und zu definieren:

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

Legen Sie Ihre IPsec-Vorschläge wie folgt fest:

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

Erstellen Sie Ihre Crypto Map-Anweisung wie folgt:

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

6. Wenden Sie die Crypto Map auf die VLAN 100-Schnittstelle an. Beispiel:

```
interface vlan100
crypto map cisco
```

Diese Konfigurationen werden verwendet:

- [Catalyst 6500](#)
- [PIX-Firewall](#)

<b>Catalyst 6500</b>
----------------------

```

!--- 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

```

## PIX-Firewall

```

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

```

## Konfiguration für IPsec mit einem gerouteten Port

Führen Sie diese Schritte durch, um IPsec mithilfe eines gerouteten Layer-3-Ports für die physische Außenschnittstelle zu konfigurieren.

1. Fügen Sie die internen VLANs dem internen Port des VPN-Dienstmoduls hinzu. Nehmen Sie an, das VPN-Servicemodul befindet sich in Steckplatz 4. Verwenden Sie VLAN 100 als internes VLAN und VLAN 209 als externes VLAN. Konfigurieren Sie die GE-Ports des VPN-Dienstmoduls wie folgt:

```

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. Fügen Sie die VLAN 100-Schnittstelle und die Schnittstelle hinzu, an der der Tunnel terminiert wird (in diesem Fall FastEthernet2/48, wie hier gezeigt).

```

interface Vlan100
ip address 10.66.79.180 255.255.255.224

interface FastEthernet2/48

```



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

3. Erstellen Sie die NAT umgehen. Fügen Sie diese Einträge der no nat-Anweisung hinzu, um die Verschachtelung zwischen diesen Netzwerken auszunehmen:

```
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. Erstellen Sie die Verschlüsselungskonfiguration und die ACL, die den zu verschlüsselnden Datenverkehr definiert. Erstellen Sie eine ACL (in diesem Fall ACL 100), die den Datenverkehr vom internen Netzwerk 192.168.5.0/24 zum Remote-Netzwerk 192.168.6.0/24 definiert. Beispiel:

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

Definieren Sie Ihre ISAKMP-Richtlinienvorschläge wie folgt:

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

Geben Sie diesen Befehl (in diesem Beispiel) ein, um vorinstallierte Schlüssel zu verwenden und zu definieren:

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

Legen Sie Ihre IPsec-Vorschläge wie folgt fest:

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

Erstellen Sie Ihre Crypto Map-Anweisung wie folgt:

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

5. Wenden Sie die Crypto Map auf die VLAN 100-Schnittstelle an. Beispiel:

```
interface vlan100
crypto map cisco
```

Diese Konfigurationen werden verwendet:

- [Catalyst 6500](#)
- [PIX-Firewall](#)

### 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

```

## PIX-Firewall

```

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
```

## Überprüfen

Dieser Abschnitt enthält Informationen zur Bestätigung, dass Ihre Konfiguration ordnungsgemäß funktioniert.

Das [Output Interpreter Tool](#) (nur [registrierte](#) Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des Befehls show anzuzeigen**.

- **show crypto ipsec sa**: Zeigt die Einstellungen an, die von den aktuellen IPsec SAs verwendet werden.
- **show crypto isakmp sa** - Zeigt alle aktuellen IKE-SAs in einem Peer an.
- **show crypto vlan** - Zeigt das VLAN an, das der Verschlüsselungskonfiguration zugeordnet ist.
- **show crypto eli** - Zeigt die Statistiken des VPN-Dienstmoduls an.

Weitere Informationen zum Überprüfen und Beheben von IPsec finden Sie unter [IP Security Troubleshooting - Understanding and Using debug Commands](#).

## Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

### Fehlerbehebung bei Befehlen

**Hinweis:** Bevor Sie **Debugbefehle** ausgeben, lesen Sie [die](#) Informationen [Wichtige Informationen über Debug-Befehle](#).

- **debug crypto ipsec** - Zeigt die IPsec-Verhandlungen von Phase 2.

- **debug crypto isakmp** - Zeigt die ISAKMP-Verhandlungen von Phase 1.
- **debug crypto engine** - Zeigt den verschlüsselten Datenverkehr an.
- **clear crypto isakmp**: Löscht die SAs für Phase 1.
- **clear crypto sa**: Löscht die SAs für Phase 2.

Weitere Informationen zum Überprüfen und Beheben von IPSec finden Sie unter [IP Security Troubleshooting - Understanding and Using debug Commands](#).

## Zugehörige Informationen

- [IPSec-Support-Seite](#)
- [Konfigurieren der IPSec-Netzwerksicherheit](#)
- [Konfigurieren des Internet Key Exchange Security Protocol](#)
- [Technischer Support - Cisco Systems](#)