PIX 6.x: Einfaches PIX-zu-PIX VPN-Tunnel-Konfigurationsbeispiel

Inhalt

Einführung

Mit dieser Konfiguration können zwei Cisco Secure PIX-Firewalls einen einfachen VPN-Tunnel (Virtual Private Network) von PIX zu PIX über das Internet oder ein beliebiges öffentliches Netzwerk, das IP-Sicherheit (IPSec) verwendet, ausführen. IPSec ist eine Kombination offener Standards, die Datensicherheit, Datenintegrität und Datenursprungsauthentifizierung zwischen IPSec-Peers bietet.

Siehe PIX/ASA 7.x: Einfaches PIX-zu-PIX VPN-Tunnel-Konfigurationsbeispiel für weitere Informationen zum Szenario, in dem die Cisco Security Appliance die Softwareversion 7.x ausführt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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

- Cisco Secure PIX 515E Firewall mit Softwareversion 6.3(5)
- Cisco Secure PIX 515E Firewall mit Softwareversion 6.3(5)

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

IPSec-Aushandlung kann in fünf Schritte unterteilt werden, die zwei IKE-Phasen (Internet Key Exchange) umfassen.

1. Ein IPSec-Tunnel wird durch interessanten Datenverkehr initiiert. Datenverkehr wird als interessant angesehen, wenn er zwischen den IPSec-Peers übertragen wird.
2. In IKE Phase 1 handeln die IPSec-Peers die festgelegte IKE Security Association (SA)-Richtlinie aus. Nach der Authentifizierung der Peers wird ein sicherer Tunnel mithilfe von Internet Security Association und Key Management Protocol (ISAKMP) erstellt.
3. In IKE Phase 2 verwenden die IPSec-Peers den authentifizierten und sicheren Tunnel, um IPSec SA-Transformationen auszuhandeln. Die Aushandlung der gemeinsam genutzten Richtlinie legt fest, wie der IPSec-Tunnel eingerichtet wird.
4. Der IPSec-Tunnel wird erstellt, und die Daten werden zwischen den IPSec-Peers übertragen, basierend auf den in den IPSec-Transformationssätzen konfigurierten IPSec-Parametern.
5. Der IPSec-Tunnel endet, wenn die IPSec-SAs gelöscht werden oder ihre Lebensdauer abläuft.

Hinweis: Die IPSec-Aushandlung zwischen den beiden PIX schlägt fehl, wenn die SAs in beiden IKE-Phasen auf den Peers nicht übereinstimmen.

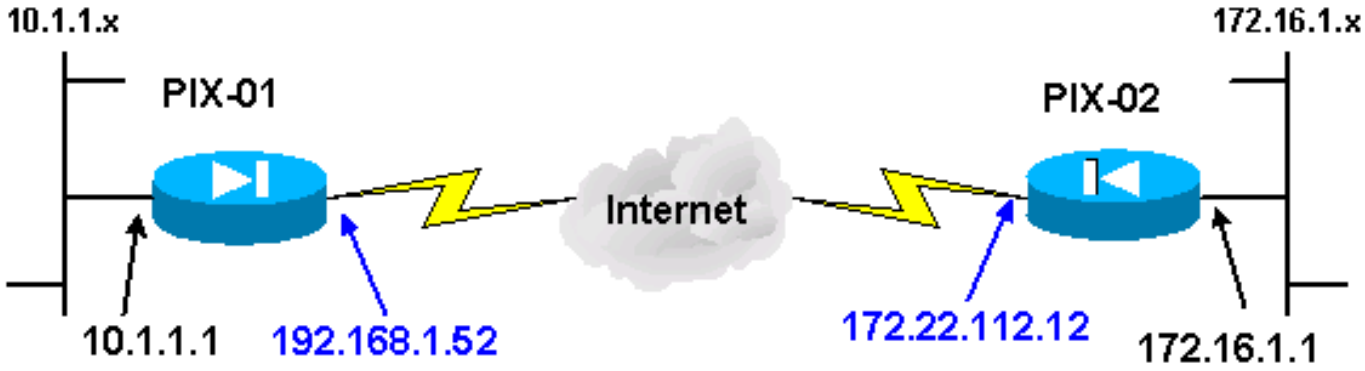
Konfigurieren

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

Dieses Dokument verwendet dieses Netzwerkdiagramm:



Hinweis: Die in dieser Konfiguration verwendeten IP-Adressierungsschemata sind im Internet nicht rechtlich routbar. Dies sind RFC 1918 -Adressen, die in einer Laborumgebung verwendet wurden.

IKE- und IPSec-Konfiguration

Die IPSec-Konfiguration auf jedem PIX variiert nur, wenn Sie die Peer-Informationen und die für die Crypto Maps und Transformationssätze gewählte Namenskonvention einfügen. Die Konfiguration kann mit den Befehlen **write terminal** oder **show** überprüft werden. Die relevanten Befehle sind **show isakmp**, **show isakmp policy**, **show access-list**, **show crypto IPSec-Transformationssatz** und **show crypto map.** Weitere Informationen zu diesen Befehlen finden Sie unter Cisco Secure PIX Firewall Command References.

Gehen Sie wie folgt vor, um IPSec zu konfigurieren:

1. IKE für vorinstallierte Schlüssel konfigurieren
2. IPSec konfigurieren
3. Konfigurieren der Network Address Translation (NAT)
4. Konfigurieren der PIX-Systemoptionen

IKE für vorinstallierte Schlüssel konfigurieren

Geben Sie den Befehl **isakmp enable** ein, um IKE auf den IPSec-Terminierungsschnittstellen zu aktivieren. In diesem Szenario ist die externe Schnittstelle die IPSec-Terminierungsschnittstelle auf beiden PIXs. IKE wird auf beiden PIX konfiguriert. Diese Befehle zeigen nur PIX-01 an.

```
isakmp enable outside
```

Sie müssen außerdem die IKE-Richtlinien definieren, die bei den IKE-Verhandlungen verwendet werden. Geben Sie den Befehl **isakmp policy** aus, um dies zu tun. Wenn Sie diesen Befehl ausgeben, müssen Sie eine Prioritätsebene zuweisen, damit die Richtlinien eindeutig identifiziert werden. In diesem Fall wird der Richtlinie die höchste Priorität von 1 zugewiesen. Die Richtlinie wird auch auf die Verwendung eines vorinstallierten Schlüssels, eines MD5-Hashing-Algorithmus für die Datenauthentifizierung, eines DES für die Encapsulating Security Payload (ESP) und einer Diffie-Hellman-Gruppe1 festgelegt. Die Richtlinie ist auch so festgelegt, dass sie die SA-Lebensdauer verwendet.

```
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
```

Die IKE-Konfiguration kann mit dem Befehl **show isakmp policy** überprüft werden:

```
PIX-01#show isakmp policy
Protection suite of priority 1
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm: Message Digest 5
authentication method: Pre-Shared Key
Diffie-Hellman group: #1 (768 bit)
lifetime: 1000 seconds, no volume limit
Default protection suite
encryption algorithm: DES - Data Encryption Standard (56 bit keys).
hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman group: #1 (768 bit)
lifetime: 86400 seconds, no volume limit
```

Geben Sie schließlich den Befehl **isakmp key** ein, um den vorinstallierten Schlüssel zu konfigurieren und eine Peer-Adresse zuzuweisen. Der gleiche vorinstallierte Schlüssel muss mit den IPSec-Peers übereinstimmen, wenn vorinstallierte Schlüssel verwendet werden. Die Adresse ist unterschiedlich und hängt von der IP-Adresse des Remote-Peers ab.

```
isakmp key ********** address 172.22.112.12 netmask 255.255.255.255
PIX-01#
```

Die Richtlinie kann mit dem Befehl **write terminal** oder **show isakmp** verifiziert werden:

```
PIX-01#show isakmp
isakmp enable outside
isakmp key ********** address 172.22.112.12 netmask 255.255.255.255
isakmp identity address
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
```

IPSec konfigurieren

IPSec wird initiiert, wenn einer der PIX-Geräte Datenverkehr empfängt, der für den anderen PIX im Netzwerk bestimmt ist. Dieser Datenverkehr gilt als interessanter Datenverkehr, der durch IPSec geschützt werden muss. Anhand einer Zugriffsliste wird bestimmt, welcher Datenverkehr die IKE- und IPSec-Verhandlungen initiiert. Diese Zugriffsliste ermöglicht das Senden von Datenverkehr aus dem 10.1.1.x-Netzwerk über den IPSec-Tunnel an das Netzwerk 172.16.1.x. Die Zugriffsliste in der anderen PIX-Konfiguration spiegelt diese Zugriffsliste wider. Dies ist für PIX-01 geeignet.

```
access-list 101 permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255.0
```

Der IPSec-Transformationssatz definiert die Sicherheitsrichtlinie, die Peers zum Schutz des Datenflusses verwenden. Die IPSec-Transformation wird mithilfe des Befehls **crypto IPSec-Transformationssatz** definiert. Für die Transformationskonfiguration muss ein eindeutiger Name ausgewählt werden. Es können bis zu drei Transformationen ausgewählt werden, um die IPSec-Sicherheitsprotokolle zu definieren. Diese Konfiguration verwendet nur zwei Transformationen: **esp-hmac-md5** und **esp-des**.

```
crypto IPSec transform-set chevelle esp-des esp-md5-hmac
```

Crypto Maps richten IPSec SAs für den verschlüsselten Datenverkehr ein. Sie müssen einen Kartennamen und eine Sequenznummer zuweisen, um eine Crypto Map zu erstellen. Anschließend definieren Sie die Parameter für die Crypto Map. Die angezeigte Verschlüsselungszuordnungstransaktion verwendet IKE zum Einrichten von IPSec-SAs, verschlüsselt alles, was mit der Zugriffsliste 101 übereinstimmt, verfügt über einen festgelegten Peer und verwendet das **günstige** Transformationssatz, um seine Sicherheitsrichtlinie für den Datenverkehr umzusetzen.

```
crypto map transam 1 IPSec-isakmp
crypto map transam 1 match address 101
crypto map transam 1 set peer 172.22.112.12
crypto map transam 1 set transform-set chevelle
```

Nachdem Sie die Crypto Map definiert haben, wenden Sie die Crypto Map auf eine Schnittstelle an. Bei der von Ihnen gewählten Schnittstelle muss es sich um die IPSec-Terminierungsschnittstelle handeln.

```
crypto map transam interface outside
```

Geben Sie den Befehl **show crypto map** aus, um die Attribute für die Crypto Map zu überprüfen.

```
PIX-01#show crypto map

Crypto Map: "transam" interfaces: { outside }

Crypto Map "transam" 1 IPSec-isakmp
Peer = 172.22.112.12
access-list 101 permit ip 10.1.1.0 255.255.255.0 172.16.1.0 255.255.255
Current peer: 172.22.112.12
Security association lifetime: 4608000 kilobytes/28800 seconds
PFS (Y/N): N
Transform sets={ chevelle, }
```

Konfigurieren von NAT

Dieser Befehl weist den PIX an, keinen für IPSec als interessanten Datenverkehr zu NAT zu erstellen. Somit ist der gesamte Datenverkehr, der den Befehlsanweisungen der **Zugriffsliste** entspricht, von den NAT-Diensten ausgenommen.

```
access-list NoNAT permit ip 10.1.1.0 255.255.255.0
172.16.1.0 255.255.255.0
nat (inside) 0 access-list NoNAT
```

Konfigurieren der PIX-Systemoptionen

Da alle eingehenden Sitzungen explizit von einer Zugriffsliste oder einem Kabelkanal zugelassen werden müssen, wird der Befehl **sysopt connection permit-IPSec** verwendet, um alle eingehenden IPSec-authentifizierten Verschlüsselungssitzungen zuzulassen. Bei IPSec-geschütztem Datenverkehr kann die sekundäre Kabelprüfung redundant sein und zum Ausfall der Tunnelerstellung führen. Der **sysopt**-Befehl passt verschiedene Sicherheits- und Konfigurationsfunktionen der PIX-Firewall an.

```
sysopt connection permit-IPSec
```

Konfigurationen

Wenn Sie die Ausgabe eines **Write Terminal**-Befehls von Ihrem Cisco Gerät haben, können Sie Output Interpreter (nur registrierte Kunden) verwenden, um potenzielle Probleme und Fixes anzuzeigen. Sie müssen angemeldet sein und JavaScript aktivieren, damit Sie Output Interpreter (nur registrierte Kunden) verwenden können.

PIX-01 bei 192.68.1.52

```
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX-01
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
!--- Defines interesting traffic that is protected by
the IPSec tunnel. access-list 101 permit ip 10.1.1.0
255.255.255.0 172.16.1.0 255.255.255.0
!--- Do not perform NAT for traffic to other PIX
Firewall. access-list NoNAT permit ip 10.1.1.0
255.255.255.0 172.16.1.0 255.255.255.0
pager lines 24
```

```
mtu outside 1500
mtu inside 1500
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
!--- Sets the outside address on the PIX Firewall. ip
address outside 192.168.1.52 255.255.255.0
!--- Sets the inside address on the PIX Firewall. ip
address inside 10.1.1.1 255.255.255.0
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
pdm history enable
arp timeout 14400
!--- This command tells the PIX not to NAT any traffic
!--- deemed interesting for IPSec. nat (inside) 0
access-list NoNAT
!--- Sets the default route to the default gateway.
route outside 0.0.0.0 0.0.0.0 192.168.1.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Allows IPSec traffic to pass through the PIX
Firewall !--- and does not require an additional conduit
!--- or access-list statements to permit IPSec traffic.
sysopt connection permit-IPSec
!--- IKE Phase 2: !--- The IPSec transform-set
"chevelle" uses esp-md5-hmac to provide !--- data
authentication.

crypto IPSec transform-set chevelle esp-des esp-md5-hmac
!--- Crypto maps set up the SAs for IPSec traffic. !---
Indicates that IKE is used to establish IPSec SAs.
crypto map transam 1 IPSec-isakmp
!--- Assigns interesting traffic to peer 172.22.112.12.
crypto map transam 1 match address 101
!--- Sets the IPSec peer. crypto map transam 1 set peer
172.22.112.12
!--- Sets the IPSec transform set "chevelle" !--- to be
used with the crypto map entry "transam". crypto map
transam 1 set transform-set chevelle
!--- Assigns the crypto map transam to the interface.
crypto map transam interface outside
```

```
!--- IKE Phase 1: !--- Enables IKE on the interface used
to terminate the IPSec tunnel

isakmp enable outside
!--- Sets the ISAKMP identity of the peer and !--- sets
the pre-shared key between the IPSec peers. !--- The
same preshared key must be configured on the !--- IPSec
peers for IKE authentication. isakmp key ********
address 172.22.112.12 netmask 255.255.255.255
!--- The PIX uses the IP address method by default !---
for the IKE identity in the IKE negotiations. isakmp
identity address
!--- The ISAKMP policy defines the set of parameters !--
- that are used for IKE negotiations. !--- If these
parameters are not set, the default parameters are used.
!--- The show isakmp policy command shows the
differences in !--- the default and configured policy.

isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

PIX-02 bei 172.22.112.12

```
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname PIX-02
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
!--- Defines interesting traffic that is protected by
the IPSec tunnel. access-list 101 permit ip 172.16.1.0
255.255.255.0 10.1.1.0 255.255.255.0
!--- Do not perform NAT for traffic to other PIX
Firewall. access-list NoNAT permit ip 172.16.1.0
255.255.255.0 10.1.1.0 255.255.255.0
pager lines 24
mtu outside 1500
mtu inside 1500
```

```
mtu intf2 1500
mtu intf3 1500
mtu intf4 1500
mtu intf5 1500
!--- Sets the outside address on the PIX Firewall. ip
address outside 172.22.112.12 255.255.255.0
!--- Sets the inside address on the PIX Firewall. ip
address inside 172.16.1.1 255.255.255.0
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
pdm history enable
arp timeout 14400
!--- This command tells the PIX not to NAT any traffic
!--- deemed interesting for IPSec. nat (inside) 0
access-list NoNAT
!--- Sets the default route to the default gateway.
route outside 0.0.0.0 0.0.0.0 172.22.112.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc
0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media
0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
!--- Allows IPSec traffic to pass through the PIX
Firewall !--- and does not require an additional conduit
!--- or access-list statements to permit IPSec traffic.
sysopt connection permit-IPSec
!--- IKE Phase 2:  !--- The IPSec transform set defines
the negotiated security policy !--- that the peers use
to protect the data flow. !--- The IPSec transform-set
"toyota" uses hmac-md5 authentication header !--- and
encapsulates the payload with des.

crypto IPSec transform-set toyota esp-des esp-md5-hmac
!--- Crypto maps set up the SAs for IPSec traffic. !---
Indicates that IKE is used to establish IPSec SAs.
crypto map bmw 1 IPSec-isakmp
!--- Assigns interesting traffic to peer 192.168.1.52.
crypto map bmw 1 match address 101
!--- Sets IPSec peer. crypto map bmw 1 set peer
192.168.1.52
!--- Sets the IPSec transform set "toyota" !--- to be
used with the crypto map entry "bmw". crypto map bmw 1
set transform-set toyota
!--- Assigns the crypto map bmw to the interface. crypto
map bmw interface outside
```

```
!--- IKE Phase 1: !--- Enables IKE on the interface used
to terminate IPSec tunnel.

isakmp enable outside
!--- Sets the ISAKMP identity of the peer and !--- sets
the preshared key between the IPSec peers. !--- The same
preshared key must be configured on the !--- IPSec peers
for IKE authentication. isakmp key ******** address
192.168.1.52 netmask 255.255.255.255
!--- The PIX uses the IP address method by default !---
for the IKE identity in the IKE negotiations. isakmp
identity address
!--- The ISAKMP policy defines the set of parameters !--
- that are used for IKE negotiations. !--- If these
parameters are not set, the default parameters are used.
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption des
isakmp policy 1 hash md5
isakmp policy 1 group 1
isakmp policy 1 lifetime 1000
telnet timeout 5
ssh timeout 5
console timeout 0
terminal width 80
Cryptochecksum:d41d8cd98f00b204e9800998ecf8427e
: end
```

Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom Output Interpreter Tool (nur registrierte Kunden) unterstützt, mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show crypto IPSec sa**: Dieser Befehl zeigt den aktuellen Status der IPSec-SAs an und ist hilfreich, um festzustellen, ob der Datenverkehr verschlüsselt wird.
- **show crypto isakmp sa**: Dieser Befehl zeigt den aktuellen Status der IKE-SAs an.

PIX-01 Befehle anzeigen

PIX-01 Befehle anzeigen

```
PIX-01#show crypto IPSec sa
interface: outside
Crypto map tag: transam, local addr. 192.168.1.52

local ident (addr/mask/prot/port):
(10.1.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(172.16.1.0/255.255.255.0/0/0)
current_peer: 172.22.112.12
PERMIT, flags={origin_is_acl,}
!--- This verifies that encrypted packets are being sent
!--- and received without any errors. #pkts encaps: 3,
#pkts encrypt: 3, #pkts digest 3
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
```

```
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0, #pkts
decompress failed: 0
#send errors 2, #recv errors 0

local crypto endpt.: 192.168.1.52, remote crypto endpt.:
172.22.112.12
path mtu 1500, IPSec overhead 56, media mtu 1500
current outbound spi: 6f09cbf1
!--- Shows inbound SAs that are established. inbound esp
sas:
spi: 0x70be0c04(1891503108)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: transam
sa timing: remaining key lifetime (k/sec):
(4607999/28430)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound pcp sas:
!--- Shows outbound SAs that are established. outbound
ESP sas:
spi: 0x6f09cbf1(1862913009)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: transam
sa timing: remaining key lifetime (k/sec):
(4607999/28430)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound PCP sas:

!--- The ISAKMP SA is in the quiescent state (QM_IDLE)
when it exists. !--- The ISAKMP SA is idle. The ISAKMP
SA remains authenticated with its !--- peer and can be
used for subsequent Quick Mode exchanges. PIX-01#show
crypto isakmp sa
     dst             src          state      pending
created
172.22.112.12    192.168.1.52    QM_IDLE         0
1Maui-PIX-01#
```

PIX-02 Befehle anzeigen

PIX-02 Befehle anzeigen

```
PIX-02#show crypto IPSec sa

interface: outside
Crypto map tag: bmw, local addr. 172.22.112.12

local ident (addr/mask/prot/port):
(172.16.1.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port):
(10.1.1.0/255.255.255.0/0/0)
```

```
current_peer: 192.168.1.52
PERMIT, flags={origin_is_acl,}
!--- This verifies that encrypted packets are !--- being
sent and recede without any errors. #pkts encaps: 3,
#pkts encrypt: 3, #pkts digest 3
#pkts decaps: 3, #pkts decrypt: 3, #pkts verify 3
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. Failed: 0, #pkts
decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 172.22.112.12, remote crypto
endpt.: 192.168.1.52
path mtu 1500, IPSec overhead 56, media mtu 1500
current outbound spi: 70be0c04
!--- Shows inbound SAs that are established. Inbound ESP
sas:
spi: 0x6f09cbf1(1862913009)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 1, crypto map: bmw
sa timing: remaining key lifetime (k/sec):
(4607999/28097)
IV size: 8 bytes
replay detection support: Y

inbound ah sas:

inbound PCP sas:
!--- Shows outbound SAs that are established. Outbound
ESP sas:
spi: 0x70be0c04(1891503108)
transform: esp-des esp-md5-hmac
in use settings ={Tunnel, }
slot: 0, conn id: 2, crypto map: bmw
sa timing: remaining key lifetime (k/sec):
(4607999/28097)
IV size: 8 bytes
replay detection support: Y

outbound ah sas:

outbound PCP sas:

!--- The ISAKMP SA is in the quiescent state (QM_IDLE)
when it exists. !--- The ISAKMP SA is idle. The ISAKMP
SA remains authenticated with its !--- peer and can be
used for subsequent Quick Mode exchanges. PIX-02#show
crypto isakmp sa
     dst             src          state      pending
created
172.22.112.12    192.168.1.52    QM_IDLE         0
PIX-02#
```

Die interne Schnittstelle des PIX kann erst dann für die Tunnelbildung gepingt werden, wenn der Befehl **für den Management-Zugriff** im globalen Konfigurationsmodus konfiguriert ist.

```
PIX-02(config)#management-access inside
PIX-02(config)#show management-access
management-access inside
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

Hinweis: Die **Clear** Befehle müssen im Konfigurationsmodus ausgeführt werden.

- **clear crypto IPSec sa**: Mit diesem Befehl werden die IPSec SAs nach fehlgeschlagenen Versuchen, einen VPN-Tunnel auszuhandeln, zurückgesetzt.
- **clear crypto isakmp sa**: Mit diesem Befehl werden die ISAKMP SAs nach fehlgeschlagenen Versuchen, einen VPN-Tunnel auszuhandeln, zurückgesetzt.

Hinweis: Lesen Sie vor dem Ausgabe von **Debug-**Befehlen unter Wichtige Informationen zu Debug-Befehlen nach.

- **debug crypto IPSec** - Dieser Befehl zeigt an, ob ein Client über den IPSec-Teil der VPN-Verbindung verhandelt.
- **debug crypto isakmp**: Dieser Befehl zeigt an, ob die Peers über den ISAKMP-Teil der VPN-Verbindung verhandeln.

Nachdem die Verbindung abgeschlossen ist, kann sie mithilfe der Befehle **show** überprüft werden.

Zugehörige Informationen

- PIX-Support-Seite
- PIX-Befehlsreferenz
- Request for Comments (RFCs)
- Support-Seite für IPSec Negotiation/IKE-Protokoll
- Technischer Support und Dokumentation - Cisco Systems