PIX 6.x: Eenvoudig PIX-to-PIX VPN-tunnelconfiguratievoorbeeld

Inhoud

Inleiding

Deze configuratie maakt het mogelijk van twee Cisco Secure PIX-firewalls om een eenvoudige VPN-tunnel (Virtual Private Network) te draaien van PIX naar PIX via het internet of een openbaar netwerk dat IP-beveiliging (IPSec) gebruikt. IPSec is een combinatie van open standaarden die gegevensvertrouwelijkheid, gegevensintegriteit, en authenticatie van gegevensoorsprong tussen IPSec peers verstrekken.

Raadpleeg PIX/ASA 7.x: Eenvoudig PIX-to-PIX VPN Tunnel Configuration Voorbeeld voor meer informatie over hetzelfde scenario waarin Cisco Security Appliance softwareversie 7.x uitvoert.

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 Secure PIX 515E firewall met softwareversie 6.3(5)
- Cisco Secure PIX 515E firewall met softwareversie 6.3(5)

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

De onderhandeling van IPSec kan in vijf stappen worden verdeeld, die twee van Internet Key Exchange (IKE) - fasen omvatten.

1. Een IPSec-tunnel wordt geïnitieerd door interessant verkeer. Het verkeer wordt als interessant beschouwd wanneer het tussen de IPSec-peers reist.
2. In IKE Fase 1 onderhandelen de IPSec-peers over het vastgestelde beleid van de IKE Security Association (SA). Zodra de peers echt zijn bevonden, wordt er een beveiligde tunnel aangemaakt met behulp van Internet Security Association en Key Management Protocol (ISAKMP).
3. In IKE Fase 2, gebruiken de IPSec peers de geauthenticeerde en veilige tunnel om te onderhandelen over IPSec SA transformaties. De onderhandelingen over het gedeelde beleid bepalen hoe de IPSec-tunnel tot stand wordt gebracht.
4. De IPSec-tunnel wordt gecreëerd en gegevens worden tussen de IPSec-peers overgebracht op basis van de IPSec-parameters die in de IPSec-transformatiesets worden geconfigureerd.
5. De IPSec-tunnel eindigt wanneer de IPSec SAs worden verwijderd of wanneer hun levensduur verstrijkt.

Opmerking: De IPSec-onderhandeling tussen de twee PIX's mislukt als de SA's in beide IKE-fasen niet op de peers overeenkomen.

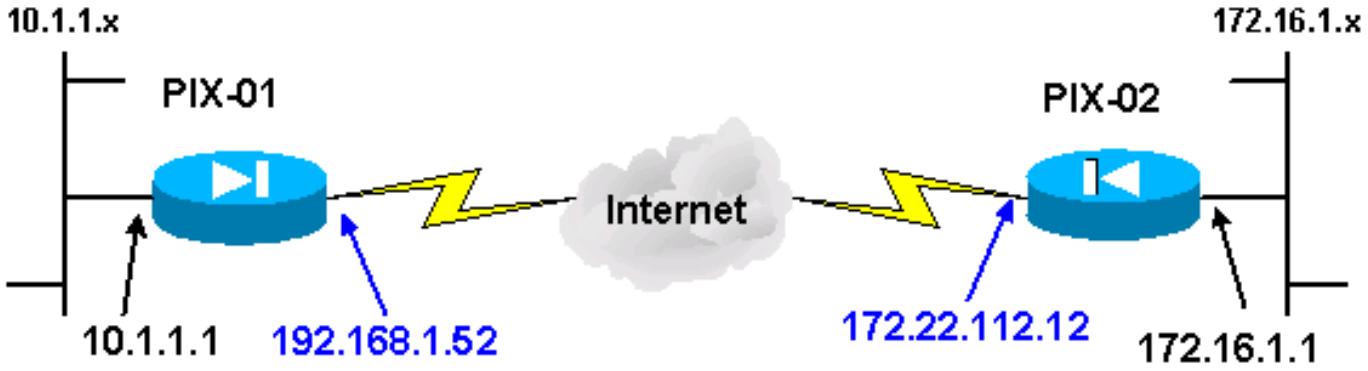
Configureren

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

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

Netwerkdiagram

Dit document gebruikt dit netwerkdiagram:



Opmerking: de IP-adresseringsschema's die in deze configuratie worden gebruikt, zijn niet wettelijk routeerbaar op het internet. Dit zijn RFC 1918 adressen die in een labomgeving gebruikt zijn.

Configuratie IKE en IPSec

De configuratie van IPSec op elke PIX varieert slechts wanneer u de peer informatie en de naamgevingsconventie die voor de crypto kaarten en transformatiesets wordt gekozen toevoegt. De configuratie kan worden geverifieerd met de **schrijfterminal** of de opdrachten **voor** de **show**. De relevante opdrachten zijn **toonaangevend**, **tonen** het **beleid van isakmp**, **tonen de toegangslijst**, **tonen crypto IPSec transformatie-set**, en **tonen crypto kaart.** Raadpleeg de referenties van de opdracht Cisco Secure PIX-firewall voor meer informatie over deze opdrachten.

Voltooi deze stappen om IPSec te configureren:

1. IKE instellen voor voorkeurstoetsen
2. Configureren IPSec
3. Netwerkadresomzetting (NAT) configureren
4. PIX-systeemopties instellen

IKE instellen voor voorkeurstoetsen

Geef de **isakmp opdracht** uit om IKE op de IPSec terminerende interfaces in te schakelen. In dit scenario is de externe interface de IPSec terminating interface op beide PIX's. IKE is ingesteld op beide PIX's. Deze opdrachten tonen alleen PIX-01.

```
isakmp enable outside
```

U moet ook het IKE-beleid definiëren dat tijdens de IKE-onderhandelingen wordt gebruikt. Geef de opdracht van het **beleid** van **isakmp uit** om dit te doen. Wanneer u deze opdracht geeft, moet u een prioriteitsniveau instellen, zodat het beleid op een unieke manier wordt bepaald. In dit geval wordt de hoogste prioriteit 1 aan het beleid toegekend. Het beleid is ook ingesteld voor het gebruik van een vooraf gedeelde sleutel, een MD5 hashing algoritme voor gegevensverificatie, een DES voor het inkapselen van Security Payload (ESP) en een Diffie-Hellman groep1. Het beleid is ook ingesteld om de SA leven te gebruiken.

```
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
```

De IKE-configuratie kan met de opdracht **Sisakmp-beleid** worden geverifieerd:

```
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
```

Geef tot slot de **opdracht** van de **toets** isakmp uit om de gedeelde toets te configureren en een peer-adres toe te wijzen. Dezelfde preShared key moet op de IPSec-peers overeenkomen bij gebruik van pregedeelde toetsen. Het adres verschilt, wat afhankelijk is van het IP-adres van de externe peer.

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

Het beleid kan met de **schrijfterminal** of de opdracht **isakmp worden** geverifieerd:

```
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
```

Configureren IPSec

IPSec wordt geïnitieerd wanneer één van de PIX's verkeer ontvangt dat voor het andere PIX-binnennetwerk bestemd is. Dit verkeer wordt beschouwd als interessant verkeer dat door IPSec moet worden beschermd. Een toegangslijst wordt gebruikt om te bepalen welk verkeer de IKE- en IPSec-onderhandelingen initieert. Deze toegangslijst maakt het verkeer mogelijk om van het 10.1.1.x-netwerk, via de IPSec-tunnel, naar het 172.16.1.x-netwerk te worden verzonden. De toegangslijst op de tegenovergestelde PIX configuratie spiegelt deze toegangslijst. Dit is geschikt voor PIX-01.

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

De IPSec transformatie set definieert het beveiligingsbeleid dat de peers gebruiken om de gegevensstroom te beveiligen. De IPSec transformatie wordt gedefinieerd door het gebruik van de **crypto IPSec transformatie-set** opdracht. Er moet een unieke naam worden gekozen voor de transformatie en er kunnen maximaal drie transformaties worden geselecteerd om de IPSec security protocollen te definiëren. Deze configuratie gebruikt slechts twee transformaties: **esp-hmac-md5** en **esp-des**.

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

Crypto kaarten zetten IPSec SAs op voor het gecodeerde verkeer. U moet een map naam en een volgnummer toewijzen om een crypto kaart te maken. Dan definieer je de crypto-kaartparameters. Het crypto-kaarttransam dat wordt getoond gebruikt IKE om IPSec SA's op te zetten, om alles te versleutelen dat toegang-lijst 101 aansluit, een vastgestelde peer heeft en de **chevelle** transformatie-set gebruikt om zijn veiligheidsbeleid voor verkeer uit te voeren.

```
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
```

Nadat je de crypto kaart definieert, pas de crypto kaart toe op een interface. De interface die u kiest moet de gebruikersinterface van IPSec zijn.

```
crypto map transam interface outside
```

Geef de **show crypto kaart** opdracht uit om de crypto kaart eigenschappen te verifiëren.

```
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, }
```

NAT configureren

Deze opdracht vertelt de PIX niet aan NAT verkeer dat als interessant voor IPSec wordt gezien. Zodoende is al het verkeer dat overeenkomt met de **toegangslijst**-opdrachtverklaringen vrijgesteld van de NAT-services.

```
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
```

PIX-systeemopties instellen

Omdat alle inkomende sessies expliciet moeten worden toegestaan door een toegangslijst of een geleider, wordt de opdracht van de **systeemverbinding vergunning-IPSec** gebruikt om alle inkomende IPSec gewaarmerkte algoritmesessies toe te staan. Met IPSec beschermd verkeer, kan de secundaire controle van de verbindingsleiding overtollig zijn en de tunnelcreatie veroorzaken om te falen. De systeemopdracht past verschillende PIX-firewallbeveiliging en configuratie functies aan.

```
sysopt connection permit-IPSec
```

Configuraties

Als u de output van een opdracht **schrijfterminal** van uw Cisco-apparaat hebt, kunt u Output Tolk gebruiken (alleen geregistreerde klanten) om mogelijke problemen en oplossingen weer te geven. U moet inloggen en JavaScript is ingeschakeld om uitvoertolk (alleen geregistreerde klanten) te gebruiken.

PIX-01 op 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 op 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
```

Verifiëren

Deze sectie verschaft informatie die u kunt gebruiken om te bevestigen dat uw configuratie correct werkt.

Bepaalde opdrachten met **show worden ondersteund door de tool** Output Interpreter (alleen voor geregistreerde klanten). Hiermee kunt u een analyse van de output van opdrachten met show genereren.

- **tonen crypto IPSec sa**-Deze opdracht toont de huidige status van de IPSec SAs en is nuttig in het bepalen of het verkeer wordt versleuteld.
- **toon crypto isakmp sa**-Deze opdracht toont de huidige staat van de IKE SAs.

PIX-01-show Opdrachten

PIX-01-show Opdrachten

```
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 show Opdrachten

PIX-02 show Opdrachten

```
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#
```

De interne interface van de PIX kan niet worden ingedrukt voor de samenstelling van tunnels tenzij de opdracht beheertoegang in de mondiale configuratiemodus is geconfigureerd.

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

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Opdrachten voor troubleshooting

Opmerking: de **heldere** opdrachten moeten in de configuratie modus worden uitgevoerd.

- **duidelijke crypto IPSec sa**-Deze opdracht stelt de IPSec SAs na mislukte pogingen terug om een VPN-tunnel te onderhandelen.
- **duidelijke crypto isakmp sa**-Deze opdracht stelt de ISAKMP SA's terug na mislukte pogingen om te onderhandelen over een VPN-tunnel.

Opmerking: Raadpleeg Belangrijke informatie over debug Commands voordat u **debug-**opdrachten afgeeft.

- **debug crypto IPSec**-Deze opdracht toont als een client onderhandelt over het IPSec-gedeelte van de VPN-verbinding.
- **debug crypto isakmp**-Deze opdracht toont of de peers onderhandelen over het ISAKMP-gedeelte van de VPN-verbinding.

Nadat de verbinding is voltooid, kan deze worden geverifieerd met de opdrachten **voor de show**.

Gerelateerde informatie

- PIX-ondersteuningspagina
- PIX-opdracht
- Verzoek om opmerkingen (RFC's)
- Ondersteuning van IPSec-onderhandeling/IKE-protocol
- Technische ondersteuning en documentatie – Cisco Systems