PIX/ASA 7.x en hoger: Configuratievoorbeeld van PIX-to-PIX VPN-tunnels

Inhoud

Inleiding

Dit document beschrijft de procedure om VPN-tunnels tussen twee PIX-firewalls te configureren met behulp van Cisco Adaptieve Security Devices Manager (ASDM). ASDM is een op toepassingen gebaseerd configuratiegereedschap dat u moet helpen om uw PIX-firewall met een GUI in te stellen, te configureren en te bewaken. PIX-firewalls worden op twee verschillende locaties geplaatst.

Er wordt een tunnel gevormd met IPsec. IPsec vormt een combinatie van open standaarden die gegevensvertrouwelijkheid, gegevensintegriteit en verificatie van gegevensoorsprong tussen IPsec-peers bieden.

Opmerking: In PIX 7.1 en hoger wordt de opdracht voor de **systeemverbinding** gewijzigd in **licentie-vpn voor de systeemverbinding**. Deze opdracht maakt verkeer mogelijk dat het security apparaat in een VPN-tunnel invoert en vervolgens wordt gedecrypteerd, om de toegangslijsten van de interface te omzeilen. Het groepsbeleid en de toegangslijsten per gebruiker zijn nog steeds van toepassing op het verkeer. Gebruik het **geen** formulier van deze opdracht om deze optie uit te schakelen. Deze opdracht is niet zichtbaar in de CLI-configuratie.

Raadpleeg PIX 6.x: Eenvoudig PIX-to-PIX VPN Tunnel Configuration Voorbeeld om meer te weten te komen over hetzelfde scenario waarin de Cisco PIX security applicatie softwareversie 6.x uitvoert.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document specificeert dat deze peer de eerste bedrijfseigen uitwisseling start om de juiste peer te bepalen waaraan te verbinden.

- Cisco PIX 500 Series security applicatie met versie 7.x en hoger
- ASDM versie 5.x en hoger

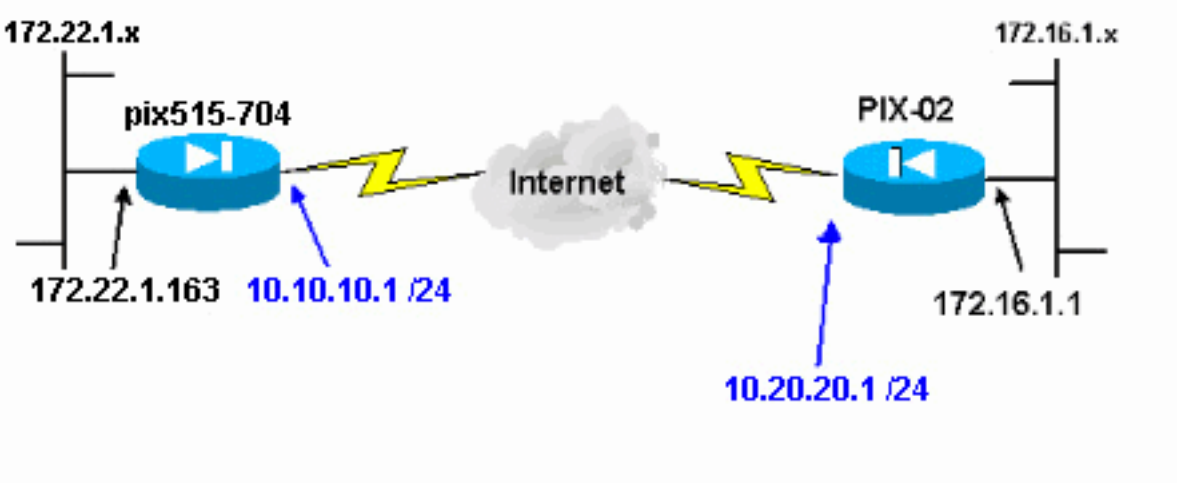
Opmerking: Raadpleeg HTTPS-toegang voor ASDM om de ASA te kunnen configureren door de ASDM.

Opmerking: De ASA 5500 Series versie 7.x/8.x heeft dezelfde software als PIX versie 7.x/8.x. De configuraties in dit document zijn van toepassing op beide productlijnen.

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

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

IPsec-onderhandeling kan in vijf stappen worden onderverdeeld en omvat twee IKE-fasen (Internet Key Exchange).

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 IPsec SA transformaties te onderhandelen. De onderhandelingen over het gedeelde beleid bepalen hoe de IPsec-tunnel tot stand wordt gebracht.
4. De IPsec-tunnel wordt gecreëerd en er worden gegevens tussen de IPsec-peers overgebracht, op basis van de IPsec-parameters die zijn ingesteld in de transformatiesets van IPsec.
5. De IPsec-tunnel eindigt wanneer de IPsec SA's worden verwijderd of wanneer hun levensduur verlopen.**Opmerking:** IPsec-onderhandeling tussen de twee PIX's mislukt als de SA's in beide IKE-fasen niet op de peers overeenkomen.

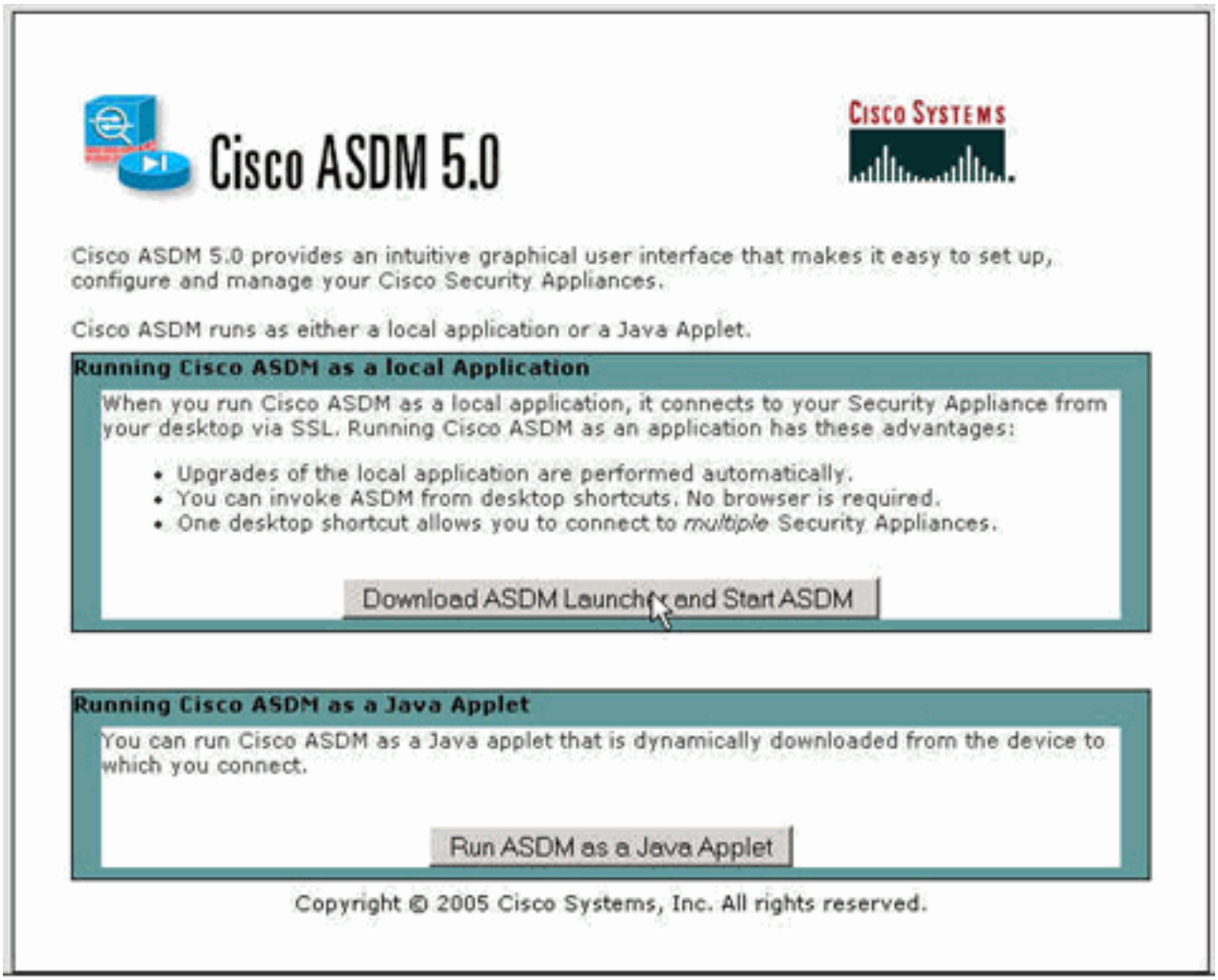
Configuratie

- ASDM-configuratie
- PIX-CLI-configuraties

ASDM-configuratie

Voer de volgende stappen uit:

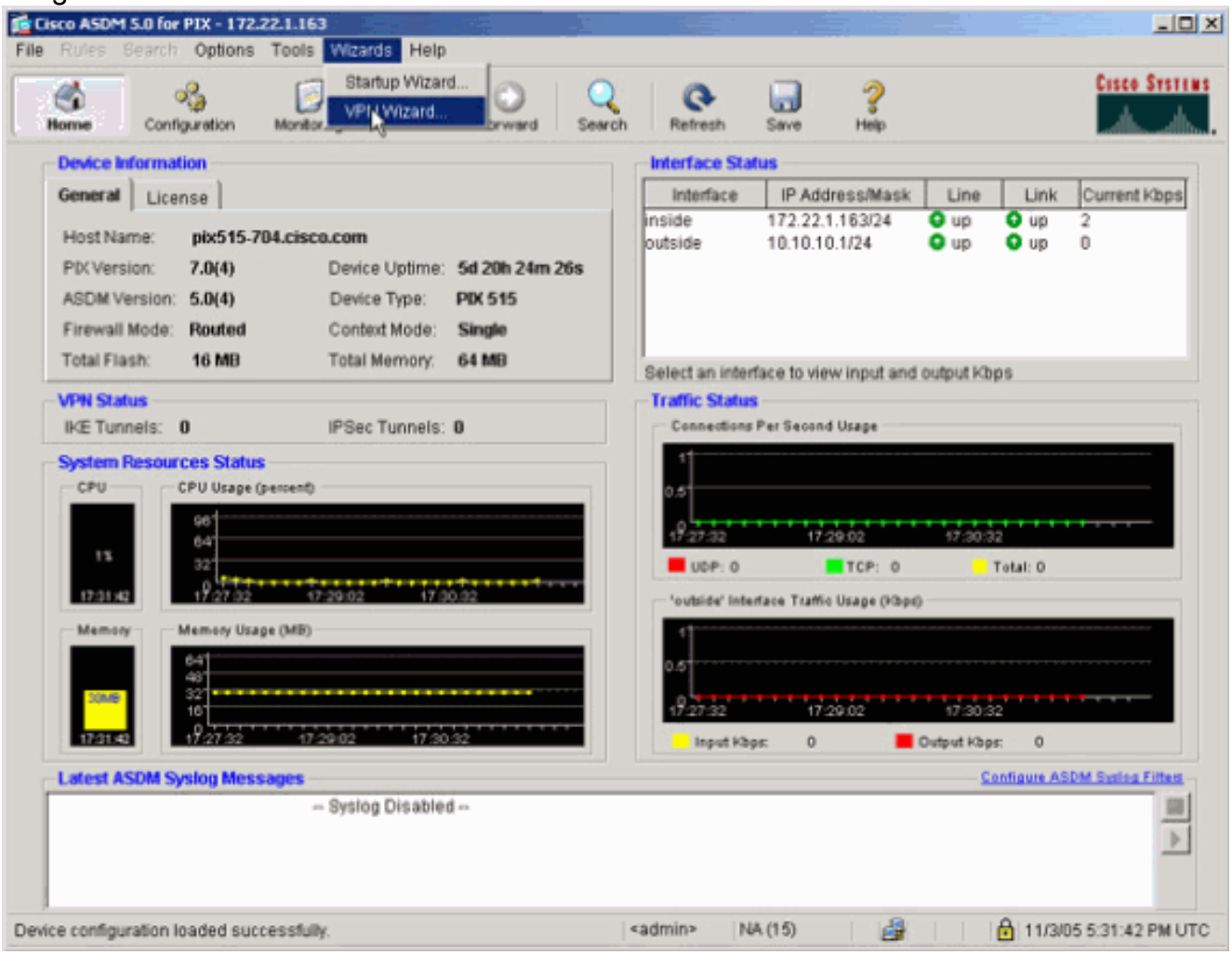
1. Open uw browser en type **https://<Inside_IP_Address_of_PIX>**om de ASDM in PIX te gebruiken.Vergeet niet alle waarschuwingen goed te keuren die uw browser u geeft met betrekking tot de SSL-certificatie. De standaard gebruikersnaam en wachtwoord zijn beide leeg.De PIX presenteert dit venster om de ASDM-toepassing te kunnen downloaden. Dit voorbeeld laadt de toepassing op de lokale computer en werkt niet in een Java-applet.



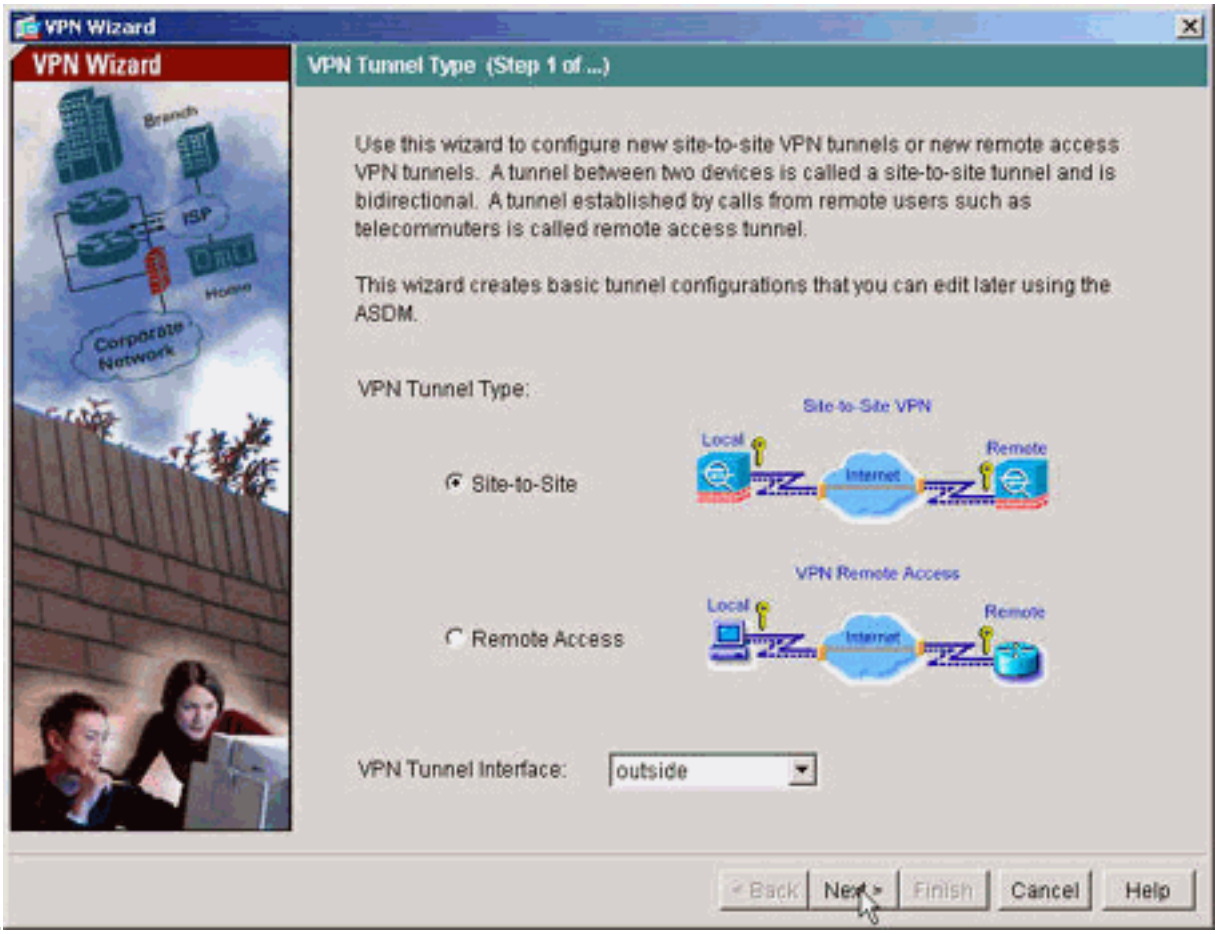
2. Klik op **Download ASDM Launcher en Start ASDM** om de installateur voor de ASDM-toepassing te downloaden.
3. Nadat de ASDM Launcher is gedownload, volgt u de aanwijzingen om de software te installeren en de Cisco ASDM Launcher uit te voeren.
4. Voer het IP-adres in voor de interface die u met de **http -** opdracht en een gebruikersnaam en wachtwoord hebt ingesteld als u er een hebt opgegeven.Dit voorbeeld gebruikt de standaard lege gebruikersnaam en het

wachtwoord.

5. Start de VPN-wizard als de ASDM-toepassing zich op de PIX heeft aangesloten.

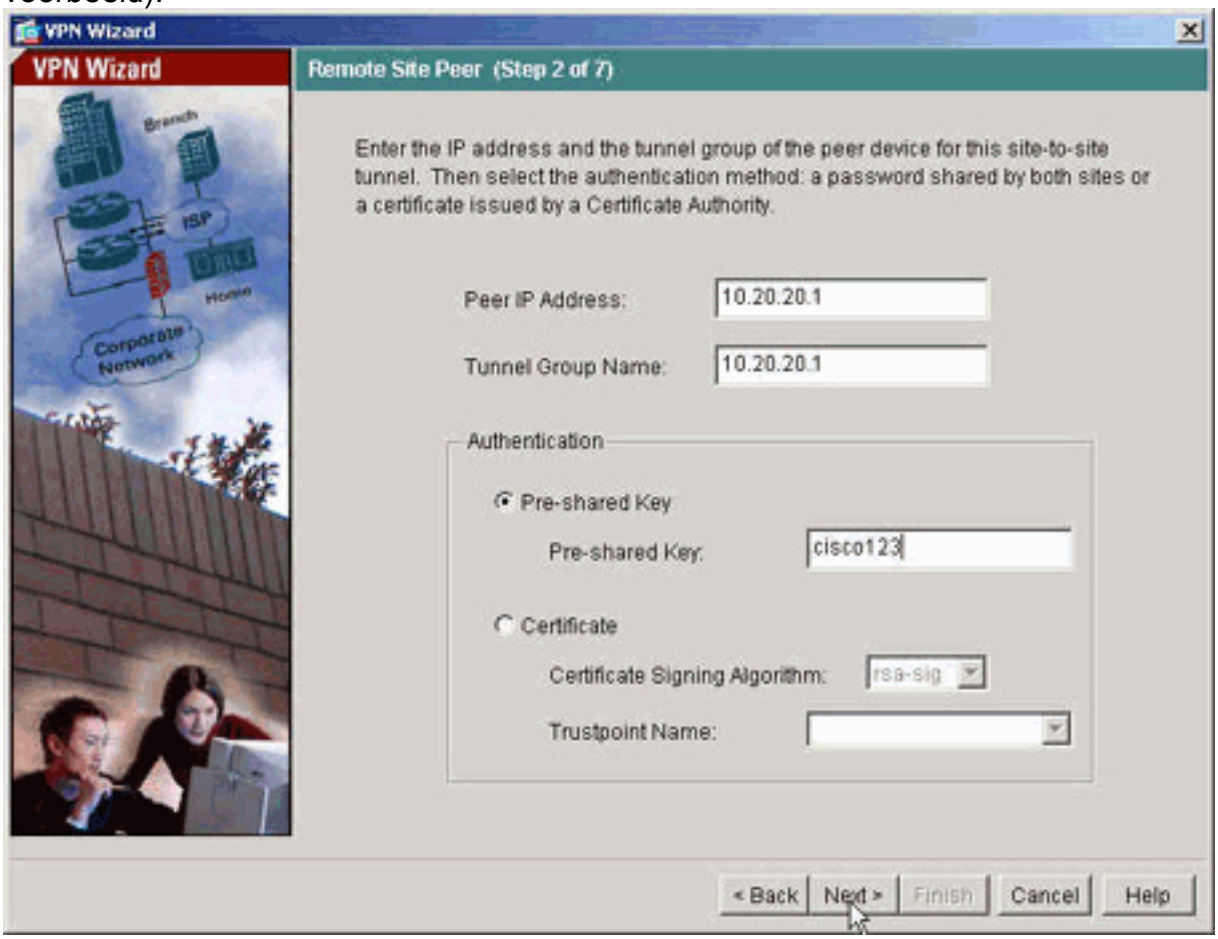


6. Kies het tunneltype **Site-to-Site**



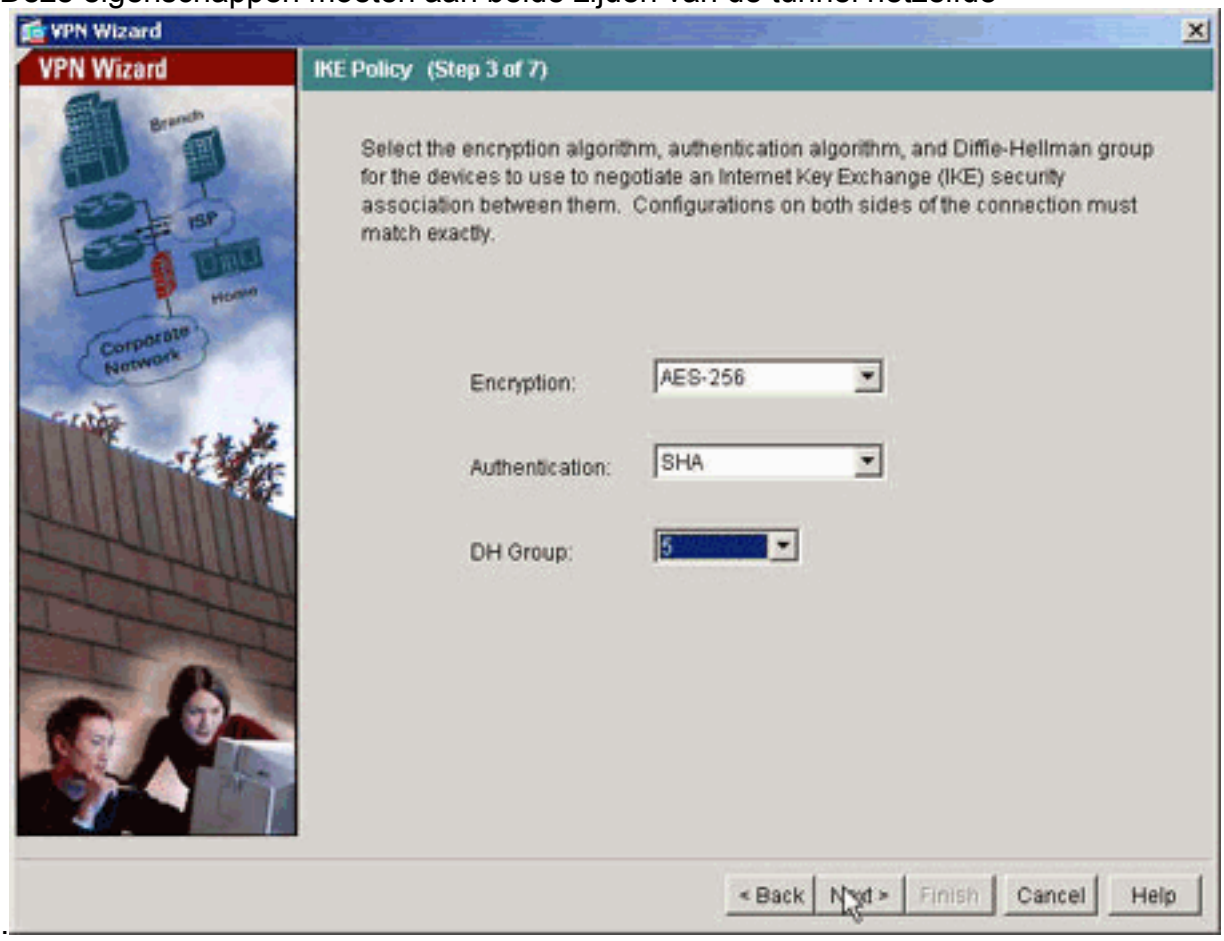
VPN.

7. Specificeer het externe IP-adres van de externe peer. Voer de te gebruiken verificatieinformatie in (vooraf gedeelde sleutel in dit voorbeeld).

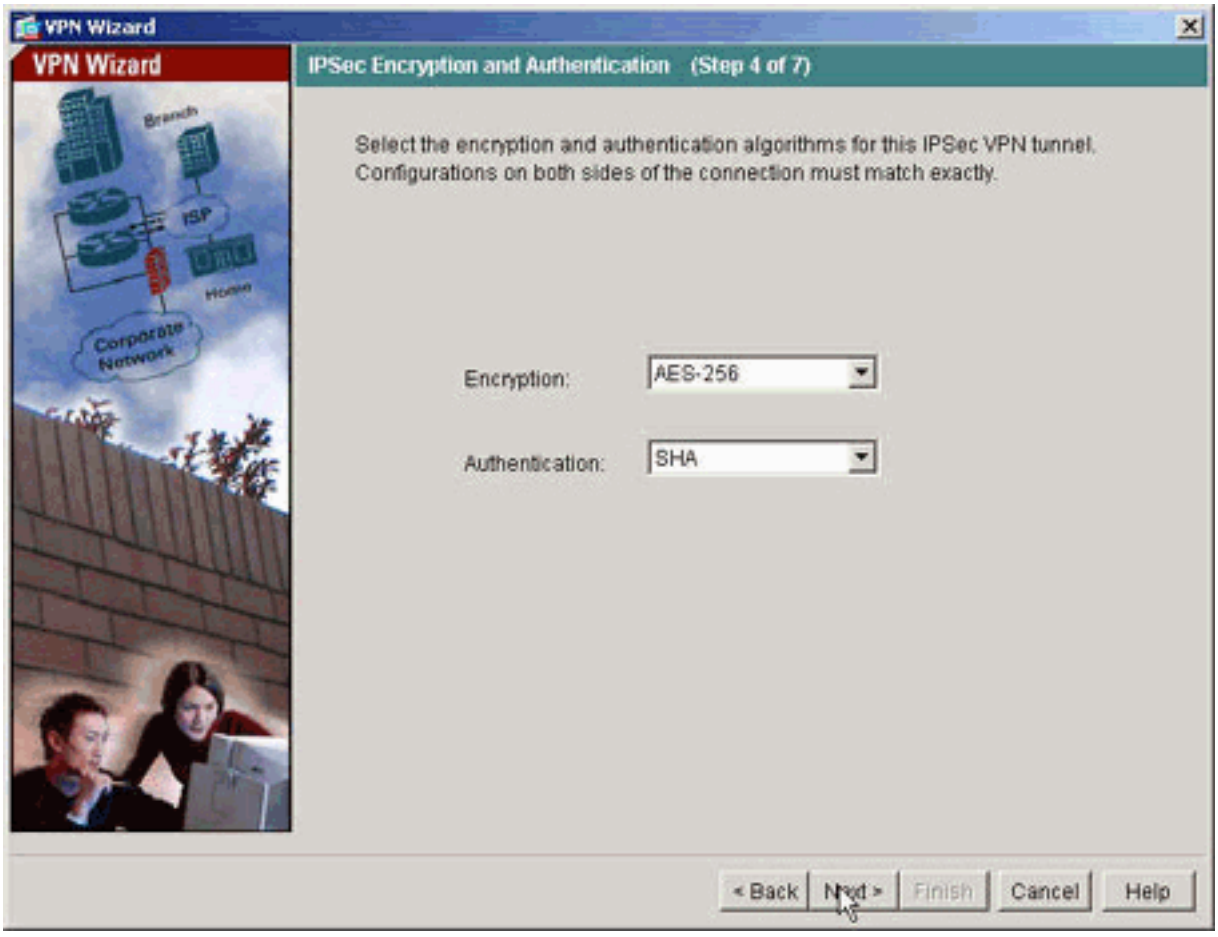


8. Specificeer de eigenschappen die voor IKE moeten worden gebruikt, ook bekend als "Fase

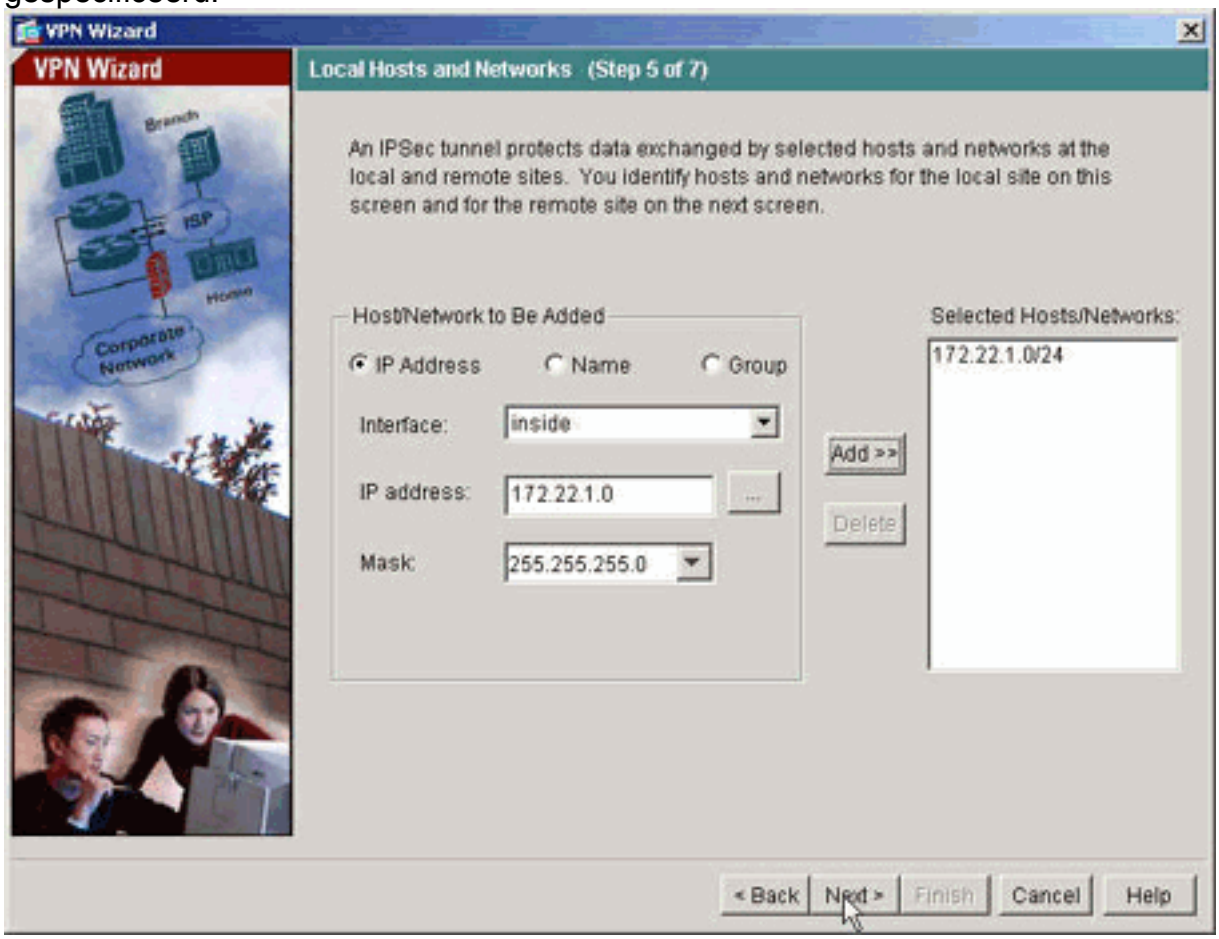
1". Deze eigenschappen moeten aan beide zijden van de tunnel hetzelfde zijn.



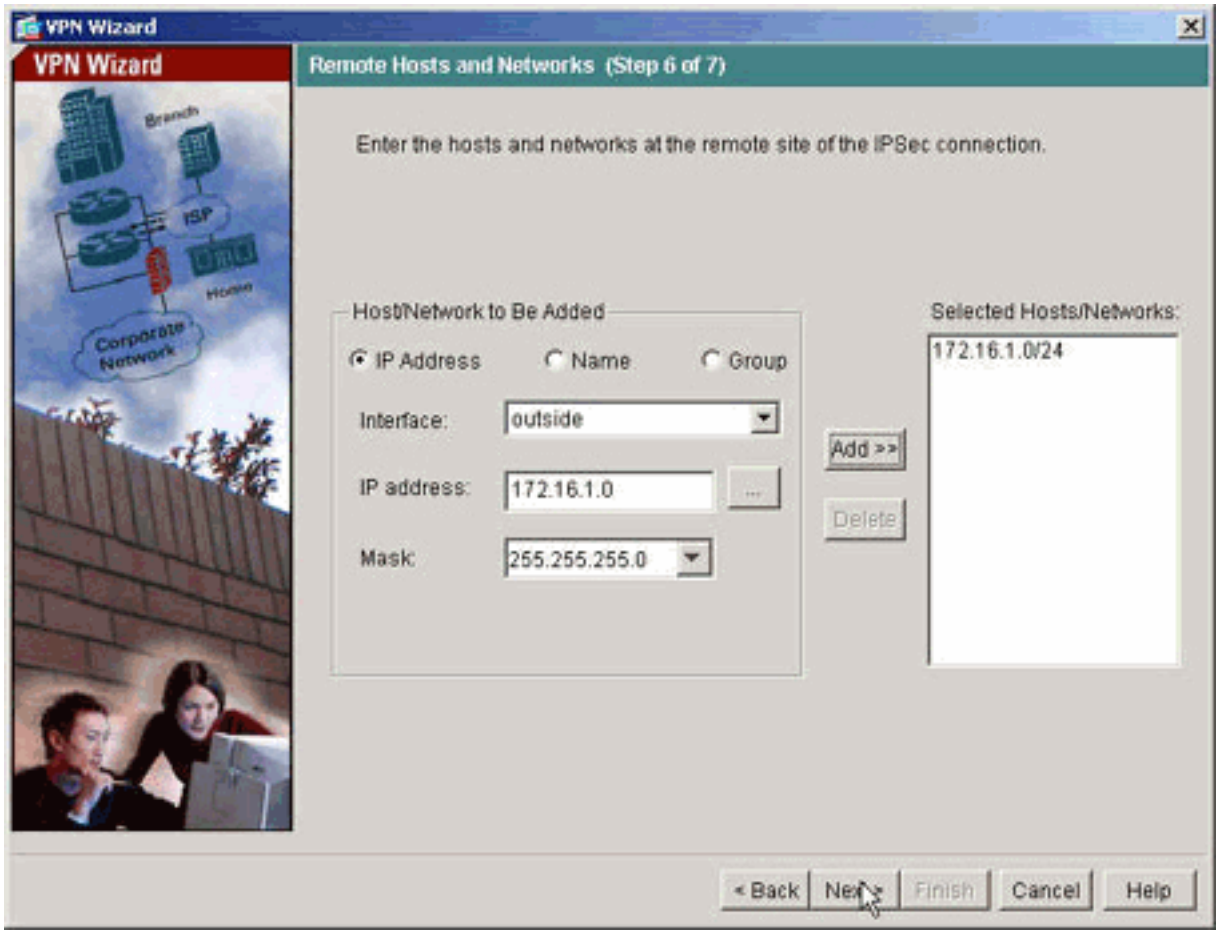
9. Specificeer de eigenschappen die voor IPsec moeten worden gebruikt, ook bekend als "Fase 2". Deze eigenschappen moeten aan beide zijden overeenkomen.



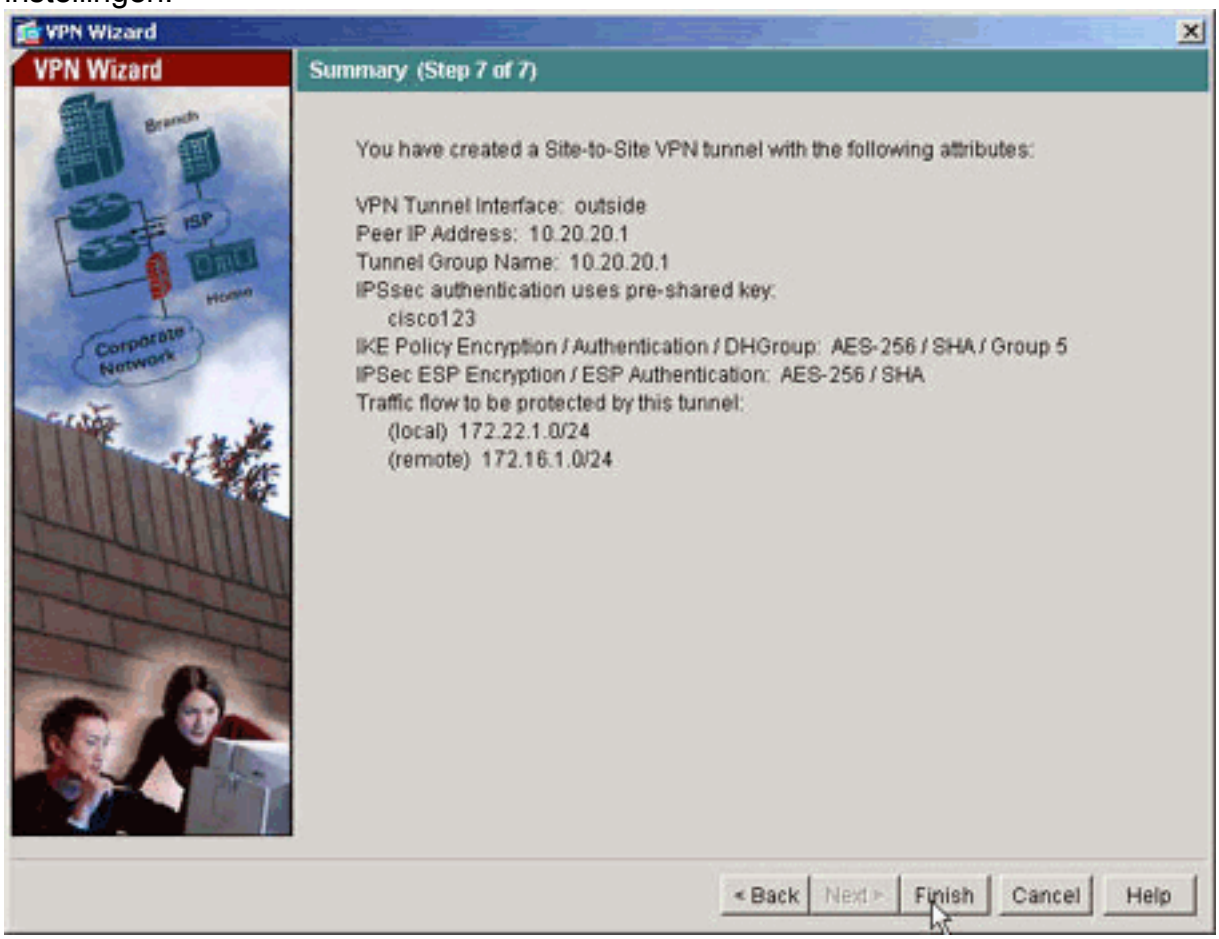
10. Specificeer de hosts waarvan het verkeer door de VPN-tunnel moet kunnen passeren. In deze stap, worden de lokale gastheren aan pix515-704 gespecificeerd.



11. De hosts en netwerken aan de afgelegen zijde van de tunnel worden gespecificeerd.



12. De eigenschappen die door de VPN Wizard worden gedefinieerd, worden in deze samenvatting weergegeven. Controleer de configuratie en klik op **Voltooien** wanneer u tevreden bent met de juiste instellingen.



PIX-CLI-configuratie

Px515-704

```
pixfirewall#show run
: Saved
PIX Version 7.1(1)
!
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names

!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.10.10.1 255.255.255.0
!--- Configure the outside interface. ! interface
Ethernet1 nameif inside security-level 100 ip address
172.22.1.163 255.255.255.0 !--- Configure the inside
interface. ! !-- Output suppressed ! passwd
2KFQnbNIdI.2KYOU encrypted ftp mode passive dns server-
group DefaultDNS domain-name default.domain.invalid
access-list inside_nat0_outbound extended permit ip
172.22.1.0 255.255.255.0 172 .16.1.0 255.255.255.0 !---
This access list (inside_nat0_outbound) is used with the
nat zero command. !--- This prevents traffic which
matches the access list from undergoing !--- network
address translation (NAT). The traffic specified by this
ACL is !--- traffic that is to be encrypted and !---
sent across the VPN tunnel. This ACL is intentionally !-
-- the same as (outside_cryptomap_20). !--- Two separate
access lists should always be used in this
configuration.

access-list outside_cryptomap_20 extended permit ip
172.22.1.0 255.255.255.0 172
.16.1.0 255.255.255.0
!--- This access list (outside_cryptomap_20) is used
with the crypto map !--- outside_map to determine which
traffic should be encrypted and sent !--- across the
tunnel. !--- This ACL is intentionally the same as
(inside_nat0_outbound). !--- Two separate access lists
should always be used in this configuration.

pager lines 24
mtu inside 1500
mtu outside 1500
no failover

asdm image flash:/asdm-511.bin
!--- Enter this command to specify the location of the
ASDM image. asdm history enable arp timeout 14400 nat
(inside) 0 access-list inside_nat0_outbound !--- NAT 0
prevents NAT for networks specified in the ACL
inside_nat0_outbound.

route outside 0.0.0.0 0.0.0.0 10.10.10.2 1

timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
```

```
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute


http server enable
!--- Enter this command in order to enable the HTTPS
server for ASDM. http 172.22.1.1 255.255.255.255 inside
!--- Identify the IP addresses from which the security
appliance !--- accepts HTTPS connections. no snmp-server
location no snmp-server contact !--- PHASE 2
CONFIGURATION ---! !--- The encryption types for Phase 2
are defined here. crypto ipsec transform-set ESP-AES-
256-SHA esp-aes-256 esp-sha-hmac !--- Define the
transform set for Phase 2. crypto map outside_map 20
match address outside_cryptomap_20 !--- Define which
traffic should be sent to the IPsec peer. crypto map
outside_map 20 set peer 10.20.20.1 !--- Sets the IPsec
peer crypto map outside_map 20 set transform-set ESP-
AES-256-SHA !--- Sets the IPsec transform set "ESP-AES-
256-SHA" !--- to be used with the crypto map entry
"outside_map". crypto map outside_map interface outside
!--- Specifies the interface to be used with !--- the
settings defined in this configuration. !--- PHASE 1
CONFIGURATION ---! !--- This configuration uses isakmp
policy 10. !--- Policy 65535 is included in the config
by default. !--- The configuration commands here define
the Phase !--- 1 policy parameters that are used. isakmp
enable outside isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256 isakmp policy 10
hash sha isakmp policy 10 group 5 isakmp policy 10
lifetime 86400 isakmp policy 65535 authentication pre-
share isakmp policy 65535 encryption 3des isakmp policy
65535 hash sha isakmp policy 65535 group 2 isakmp policy
65535 lifetime 86400 tunnel-group 10.20.20.1 type ipsec-
l2l !--- In order to create and manage the database of
connection-specific records !--- for ipsec-l2l-IPsec
(LAN-to-LAN) tunnels, use the tunnel-group !--- command
in global configuration mode. !--- For L2L connections
the name of the tunnel group MUST be the IP !--- address
of the IPsec peer.



tunnel-group 10.20.20.1 ipsec-attributes
 pre-shared-key *
!--- Enter the pre-shared-key in order to configure the
authentication method. telnet timeout 5 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map global_policy
class inspection_default inspect dns maximum-length 512
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
Cryptochecksum:ecb58c5d8ce805b3610b198c73a3d0cf : end
```

PIX-02

```
PIX Version 7.1(1)
!
```

```
hostname pixfirewall
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.20.20.1 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 172.16.1.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid

access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 172
.22.1.0 255.255.255.0
!--- Note that this ACL is a mirror of the
inside_nat0_outbound !--- ACL on pix515-704.

access-list outside_cryptomap_20 extended permit ip
172.16.1.0 255.255.255.0 172
.22.1.0 255.255.255.0
!--- Note that this ACL is a mirror of the
outside_cryptomap_20 !--- ACL on pix515-704.

pager lines 24
mtu inside 1500
mtu outside 1500
no failover
asdm image flash:/asdm-511.bin
no asdm history enable
arp timeout 14400
nat (inside) 0 access-list inside_nat0_outbound
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00
icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp
0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
crypto ipsec transform-set ESP-AES-256-SHA esp-aes-256
esp-sha-hmac
crypto map outside_map 20 match address
outside_cryptomap_20
crypto map outside_map 20 set peer 10.10.10.1
crypto map outside_map 20 set transform-set ESP-AES-256-
SHA
crypto map outside_map interface outside
isakmp enable outside
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption aes-256
isakmp policy 10 hash sha
isakmp policy 10 group 5
```

```
isakmp policy 10 lifetime 86400
tunnel-group 10.10.10.1 type ipsec-l2l
tunnel-group 10.10.10.1 ipsec-attributes
 pre-shared-key *
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect dns maximum-length 512
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:6774691244870705f858ad4e9b810874
: end
pixfirewall#
```

Reserve-site-to-site tunnel

Om het connectietype voor de optie Reserve Site-to-Site voor deze crypto kaart ingang te specificeren, gebruik de opdracht **crypto kaart om verbinding-type** in te stellen in mondiale configuratie modus. Gebruik het formulier van deze opdracht om terug te keren naar de standaardinstelling.

Syntaxis:

crypto map *map-name seq-num set* **connection-type {answer-only | originate-only | bidirectional}**

- **Alleen antwoord**-dit specificeert dat deze peer slechts op inkomende IKE verbindingen eerst reageert tijdens de eerste bedrijfseigen beurs om het juiste peer te bepalen waaraan te verbinden is.
- **bidirectioneel**—Dit specificeert dat deze peer verbindingen kan accepteren en initiëren gebaseerd op deze crypto map entry. Dit is het standaardtype voor verbinding tussen alle Site-naar-Site verbindingen.
- **originate-only**-This specificeert dat deze peer de eerste bedrijfseigen beurs in werking stelt om de aangewezen peer te bepalen waaraan te verbinden.

De opdracht **crypto kaart van het verbindingstype** specificeert de aansluitingstypen voor de functie Backup LAN-to-LAN. Hiermee kunnen meerdere reservekoppen worden gespecificeerd aan één

uiteinde van de verbinding. Deze optie werkt alleen tussen deze platforms:

- Twee Cisco ASA 5500 Series security apparaten
- Cisco ASA 5500 Series security applicatie en Cisco VPN 3000 Concentrator
- Cisco ASA 5500 Series security applicatie en een security applicatie die Cisco PIX security applicatie, versie 7.0 of hoger gebruikt

Om een back-up LAN-to-LAN verbinding te configureren raadt Cisco u aan één uiteinde van de verbinding te configureren als originate-only verbinding met het `originate-only` sleutelwoord en het einde met meerdere backup-peers als antwoord-only met het `alleen`-trefwoord. Op het originate-only eind, gebruik de **crypto kaart vastgestelde peer** opdracht om de prioriteit van de peers te bestellen. Het originate-only veiligheidsapparaat probeert om met de eerste peer in de lijst te onderhandelen. Als dit peer niet reageert, gaat het security apparaat te werk in de lijst totdat er een peer reageert of er geen peers meer in de lijst staan.

Als dit op deze manier wordt geconfigureerd probeert de originate-only peer in eerste instantie een eigen tunnel op te zetten en met een peer te onderhandelen. Hierna kan een peer een normale LAN-to-LAN verbinding opzetten en kunnen gegevens van één of andere kant de tunnelverbinding openen.

Opmerking: Als u VPN met meerdere IP-adressen van meerdere deelnemers voor een crypto-ingang hebt ingesteld, wordt VPN ingesteld met de backup-peer IP zodra de primaire peer omlaag gaat. Zodra de primaire peer echter terugkomt, loopt VPN niet vooruit op het primaire IP-adres. U moet de bestaande SA handmatig wissen om de onderhandeling van VPN opnieuw te openen om het over te schakelen op het primaire IP adres. Zoals de conclusie zegt, wordt de VPN-voorspelling niet ondersteund in de site-to-site tunnel.

Ondersteunde soorten verbindingen voor LAN-to-LAN

Afstandszijde	Centrale zijde
`Originate-Only`	`Answer-Only`
`Bi-Directional`	`Answer-Only`
`Bi-Directional`	`Bi-Directional`

Voorbeeld

Dit voorbeeld, dat in mondiale configuratiemodus is ingevoerd, vormt de **crypto kaart mymap** en stelt het connectie-type in om *alleen te starten*.

```
hostname(config)#crypto map outside_map 20 connection-type originate-only
```

Security Associations (SA's) wissen

Gebruik in de bevoorrechte modus van de PIX de volgende opdrachten:

- **Schakel [crypto] ipsec sa**-Verwijdert de actieve IPsec SAs. Het sleutelwoord *crypto* is optioneel.
- **Schakel [crypto] isakmp sa**—Verwijdert de actieve IKE SA's. Het sleutelwoord *crypto* is

optioneel.

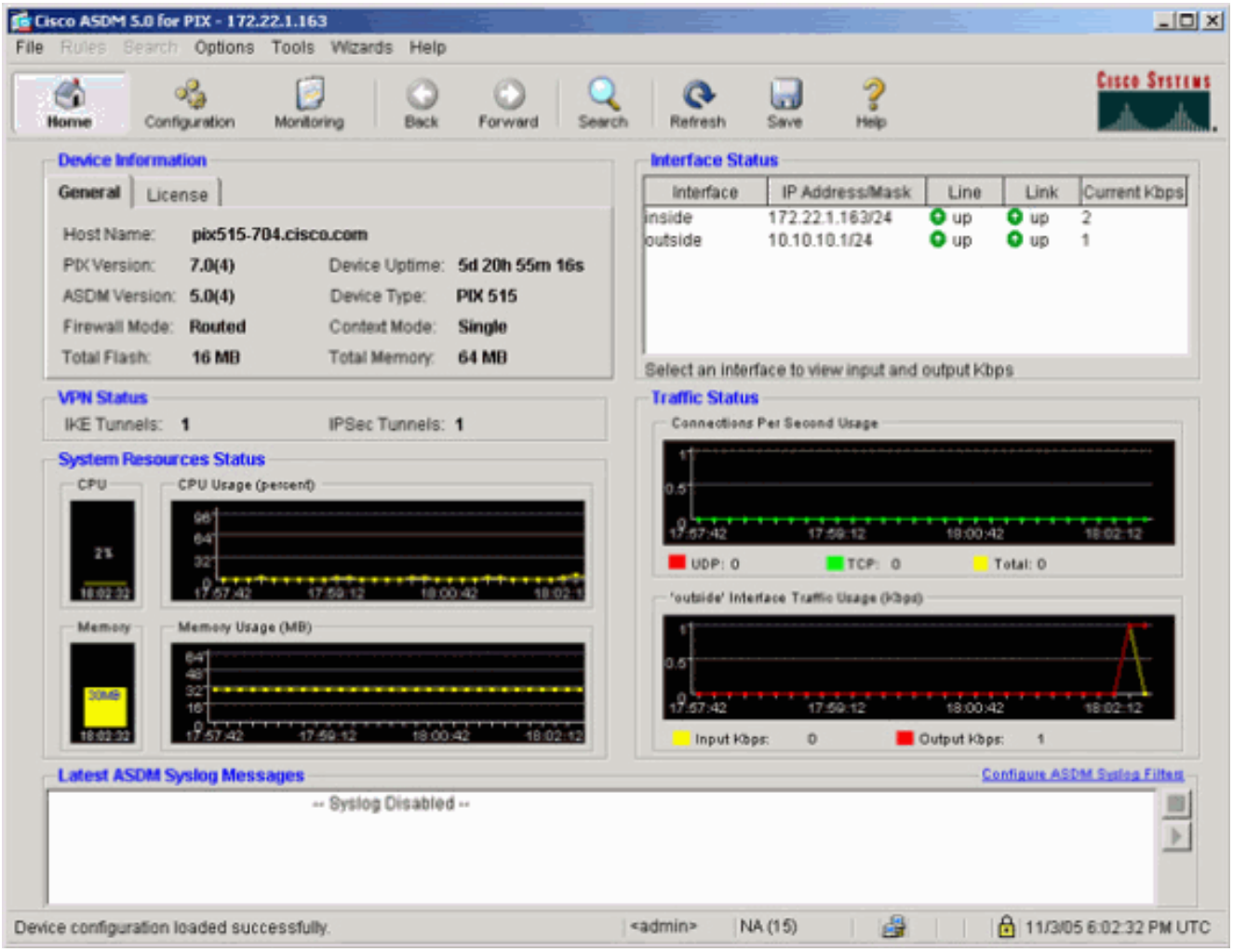
Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

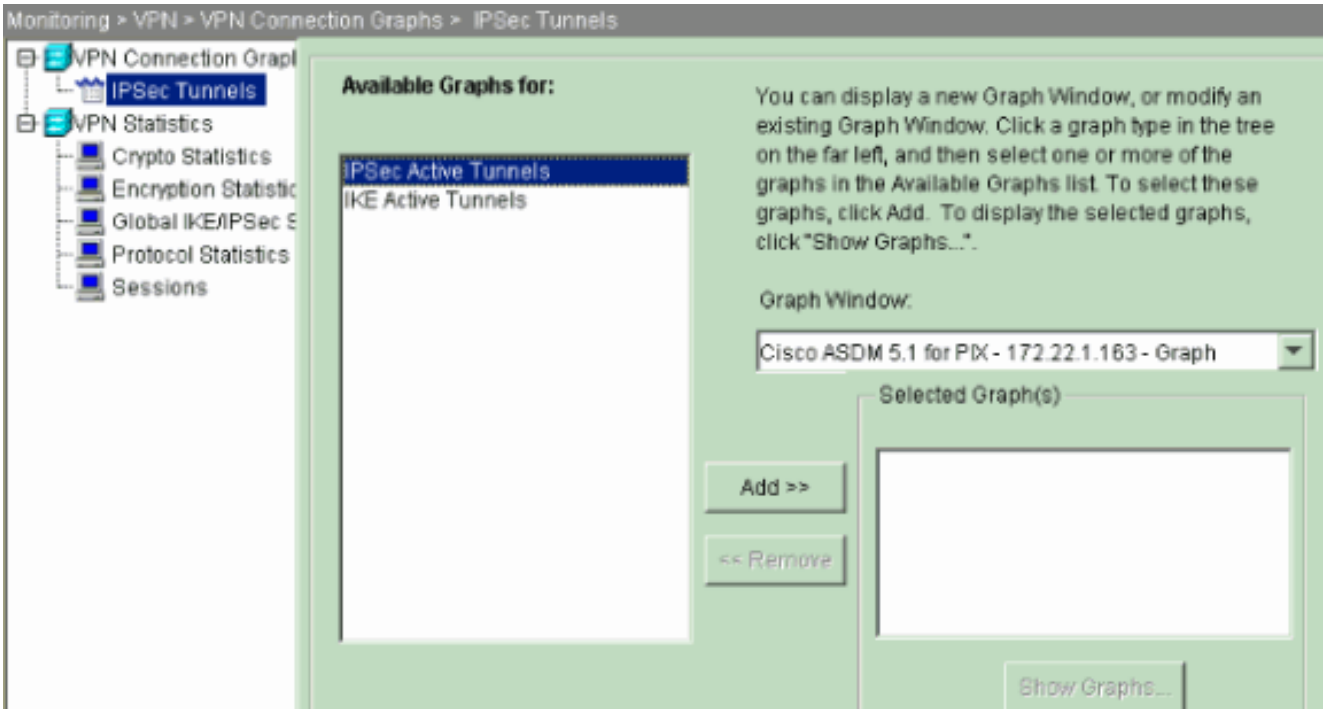
Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

Als er interessant verkeer naar de peer is, wordt de tunnel gevormd tussen pix515-704 en PIX-02.

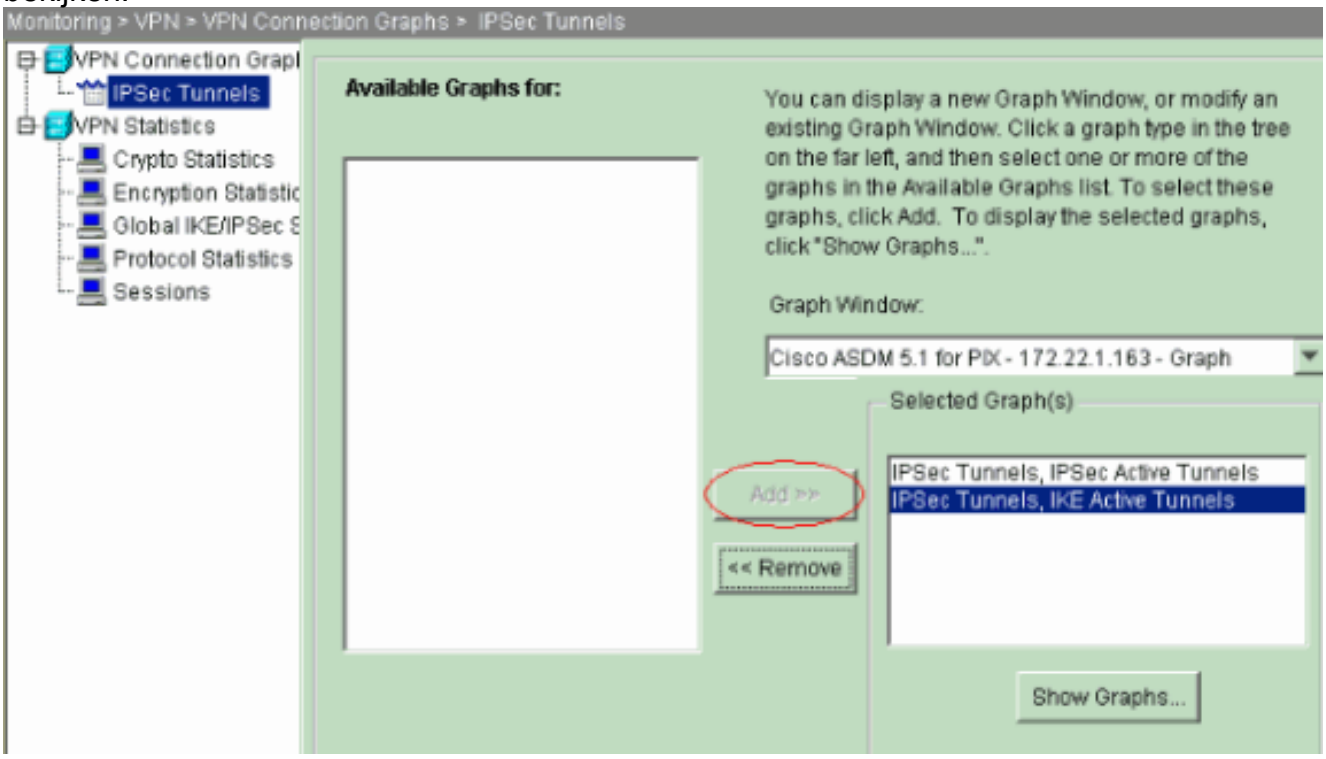
1. Bekijk de VPN-status onder **Home** in de ASDM om de vorming van de tunnel te controleren.



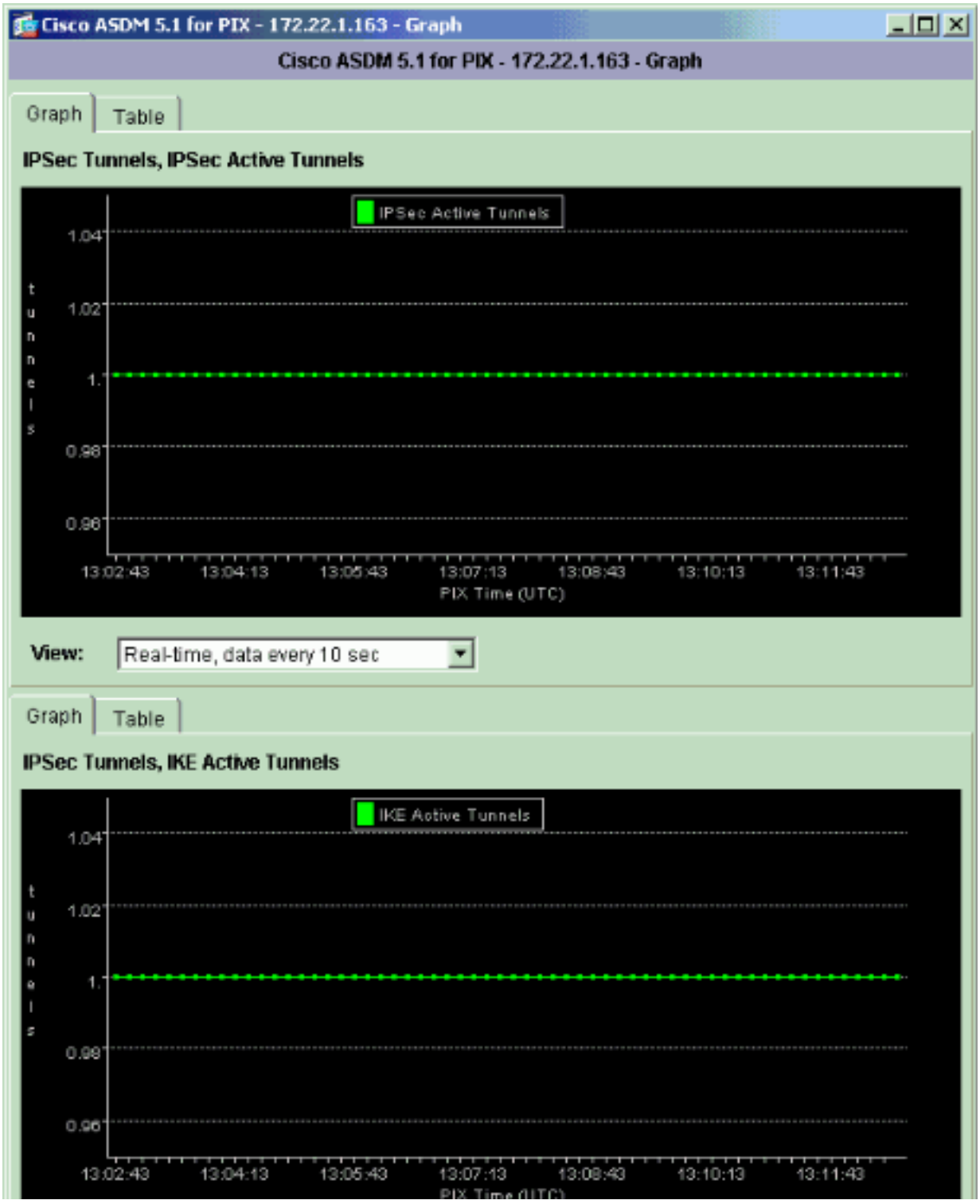
2. Kies **Bewaking > VPN > Connectieschakelaars > IPSec-tunnels** om de details over de tunnelvestiging te controleren.



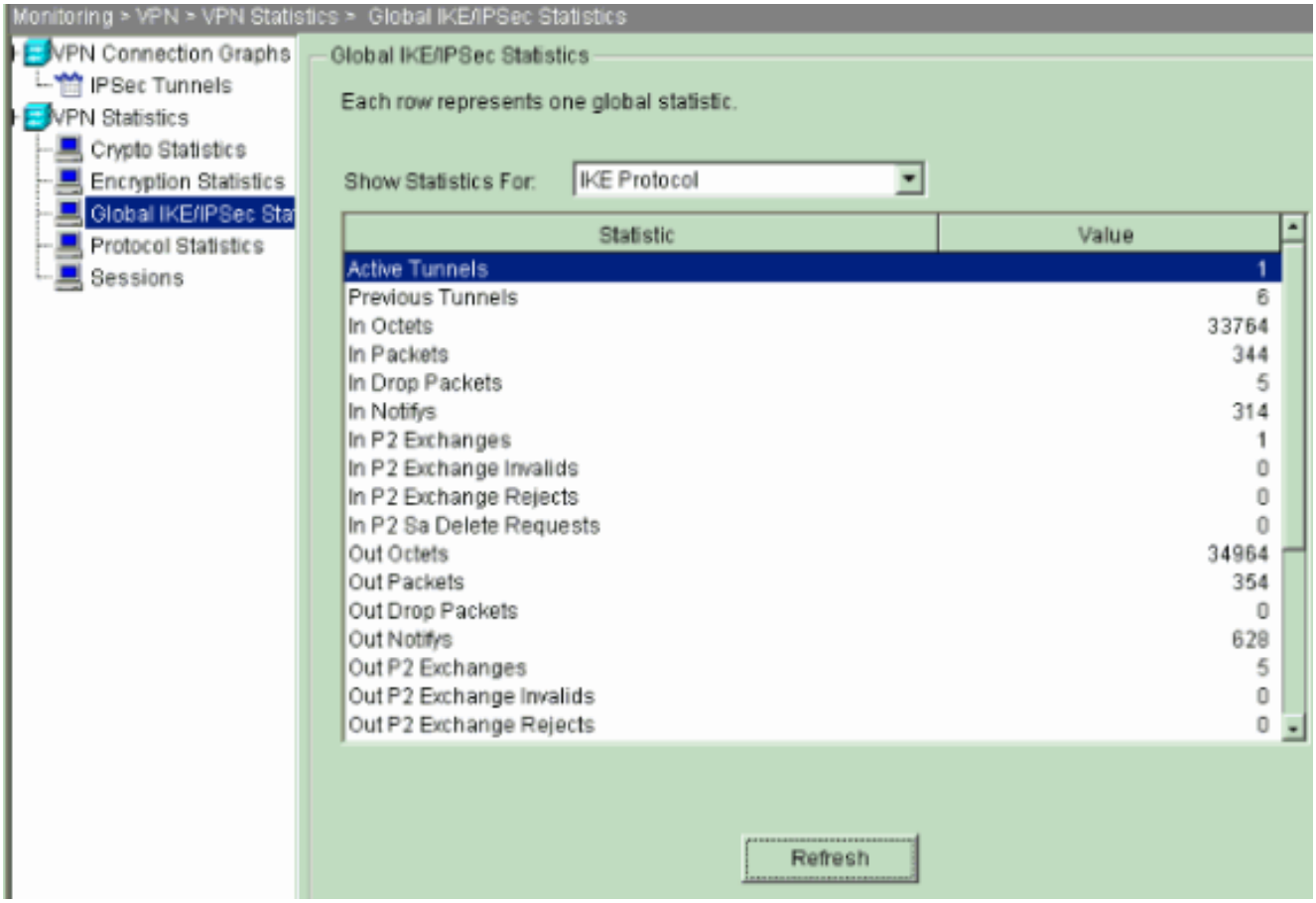
3. Klik op **Add** om de beschikbare grafieken te selecteren om in het grafiekvenster te bekijken.



4. Klik op **Grafieken tonen** om de grafieken van zowel actieve tunnels IKE als IPsec te bekijken.



5. Kies **Bewaking > VPN > Statistieken > Mondiale IKE/IPSec Statistieken** om meer te weten te komen over de statistische informatie van de VPN-tunnel.



U kunt ook de vorming van tunnels met CLI controleren. Geef de opdracht **show crypto isakmp als** opdracht uit om de vorming van tunnels te controleren en de **show crypto ipsec als** opdracht **uit** te **geven** om het aantal ingekapselde, gecodeerde pakketten, enzovoort te observeren.

Px515-704

```
pixfirewall(config)#show crypto isakmp sa

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1
Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 10.20.20.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

Px515-704

```
pixfirewall(config)#show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 20, local
addr: 10.10.10.1

     access-list outside_cryptomap_20 permit ip
172.22.1.0
       255.255.255.0 172.16.1.0 255.255.255.0
     local ident (addr/mask/prot/port):
(172.22.1.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port):
(172.16.1.0/255.255.255.0/0/0)
     current_peer: 10.20.20.1

      #pkts encaps: 20, #pkts encrypt: 20, #pkts digest:
```

```
20
      #pkts decaps: 20, #pkts decrypt: 20, #pkts verify:
20
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 20, #pkts comp failed: 0,
#pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.10.10.1, remote crypto
endpt.: 10.20.20.1

      path mtu 1500, ipsec overhead 76, media mtu 1500
      current outbound spi: 44532974

    inbound esp sas:
      spi: 0xA87AD6FA (2826622714)
         transform: esp-aes-256 esp-sha-hmac
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 1, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec):
(3824998/28246)
         IV size: 16 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x44532974 (1146300788)
         transform: esp-aes-256 esp-sha-hmac
         in use settings ={L2L, Tunnel, }
         slot: 0, conn_id: 1, crypto-map: outside_map
         sa timing: remaining key lifetime (kB/sec):
(3824998/28245)
         IV size: 16 bytes
         replay detection support: Y
```

Problemen oplossen

PFS

Bij IPsec-onderhandelingen zorgt Perfect Forward SecRITY (PFS) ervoor dat elke nieuwe cryptografische toets geen verband houdt met een eerdere toets. Schakel PFS op beide tunnelpeers in of uit, anders wordt de L2L IPsec-tunnel niet in PIX/ASA gecreëerd.

PFS wordt standaard uitgeschakeld. Om PFS toe te laten gebruik de opdracht **pfs** met het toelaten **sleutelwoord in groep-beleid configuratiewijze.** Om PFS uit te schakelen, voer het *in*.

```
hostname(config-group-policy)#pfs {enable | disable}
```

Om de PFS eigenschap uit de actieve configuratie te verwijderen, dient u de **geen** vorm van deze opdracht in te voeren. Een groepsbeleid kan een waarde voor PFS van een ander groepsbeleid erven. Typ **geen** formulier van deze opdracht om te voorkomen dat een waarde wordt geërfd.

```
hostname(config-group-policy)#no pfs
```

Beheer en toegang

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

De interne interface van de PIX kan niet van het andere uiteinde van de tunnel worden gepeld 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
```

Opdrachten debug

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

debug crypto isakmp-displays debug informatie over IPsec verbindingen en toont de eerste reeks eigenschappen die worden ontkend als gevolg van onverenigbaarheden op beide eindpunten.

debug van crypto isakmp

```
pixfirewall(config)#debug crypto isakmp 7
Nov 27 12:01:59 [IKEv1 DEBUG]: Pitcher: received a key
acquire message,
spi 0x0
Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE Initiator:
New Phase 1,
Intf 2, IKE Peer 10.20.20.1  local Proxy Address
172.22.1.0, remote
Proxy Address 172.16.1.0,  Crypto map (outside_map)
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing ISAKMP SA payload
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing Fragmentation
VID + extended capabilities payload
Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
SENDING Message
(msgid=0) with payloads : HDR +
 SA (1) + VENDOR (13) + NONE (0) total length : 148
Nov 27 12:01:59 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + VENDOR (13) + NONE (0)
total length : 112
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing SA payload
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Oakley
proposal is acceptable
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing VID payload
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, Received
Fragmentation VID
Nov 27 12:01:59 [IKEv1 DEBUG]: IP = 10.20.20.1, IKE Peer
included
IKE fragmentation capability flags
:  Main Mode:        True  Aggressive Mode:  True
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing ke payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing Cisco Unity VID payload
```

```
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing xauth V6 VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send IOS
VID
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
Constructing ASA spoofing IOS
Vendor ID payload (version: 1.0.0, capabilities:
20000001)
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
constructing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Send
Altiga/
Cisco VPN3000/Cisco ASA GW VID
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
SENDING Message (msgid=0)
with payloads : HDR + KE (4) + NONCE (10) + VENDOR (13)
+ VENDOR (13) + VENDOR (13)
+ VENDOR (13) + NONE (0) total length
 : 320
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
RECEIVED Message
(msgid=0) with payloads : HDR
+ KE (4) + NONCE (10) + VENDOR (13) + VENDOR (13) +
VENDOR (13) + VENDOR (13) +
NONE (0) total length : 320
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing ke payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing ISA_KE payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received
Cisco Unity client VID
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received
xauth V6 VID
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
Processing VPN3000/ASA
spoofing IOS Vendor ID payload (version: 1.0.0,
capabilities: 20000001)
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1, Received
Altiga/Cisco VPN3000/Cisco ASA
GW VID
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection
landed on tunnel_group 10.20.20.1
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1, Generating keys
for Initiator...
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Computing hash for ISAKMP
```

```
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
Constructing IOS keep alive payload:
proposal=32767/32767 sec.
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing dpd vid payload
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
SENDING Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE
(14) + VENDOR (13) +
NONE (0) total length : 119
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
RECEIVED Message (msgid=0)
with payloads : HDR + ID (5) + HASH (8) + IOS KEEPALIVE
(14) + VENDOR (13) +
NONE (0) total length : 96
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Computing hash for ISAKMP
Nov 27 12:02:00 [IKEv1 DEBUG]: IP = 10.20.20.1,
Processing IOS keep alive payload: proposal=32767/32767
sec.
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing VID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Received DPD VID
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Connection
landed on tunnel_group 10.20.20.1
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Oakley begin quick mode
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP =
10.20.20.1, PHASE 1 COMPLETED
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, Keep-alive
type for this connection: DPD
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Starting phase 1 rekey timer: 73440000 (ms)
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1, IKE got
SPI from key engine: SPI = 0x44ae0956
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
oakley constucting quick mode
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing blank hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing IPSec SA payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing IPSec nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing proxy ID
```

```
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Transmitting Proxy Id:
  Local subnet:  172.22.1.0  mask 255.255.255.0 Protocol
0  Port 0
  Remote subnet: 172.16.1.0  Mask 255.255.255.0 Protocol
0  Port 0
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
constructing qm hash payload
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
SENDING Message
(msgid=d723766b) with payloads
: HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID (5)
+ NOTIFY (11) +
NONE (0) total length : 200
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
RECEIVED Message
(msgid=d723766b) with payloads
 : HDR + HASH (8) + SA (1) + NONCE (10) + ID (5) + ID
(5) + NONE (0)
 total length : 172
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing hash payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing SA payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing nonce payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
processing ID payload
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
loading all IPSEC SAs
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Generating Quick Mode Key!
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
Generating Quick Mode Key!
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP =
10.20.20.1,
Security negotiation complete for LAN-to-LAN Group
(10.20.20.1)
Initiator, Inbound SPI = 0x44ae0956, Outbound SPI =
0x4a6429ba
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
oakley constructing final quick mode
Nov 27 12:02:00 [IKEv1]: IP = 10.20.20.1, IKE_DECODE
SENDING Message
(msgid=d723766b) with payloads
: HDR + HASH (8) + NONE (0) total length : 76
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
IKE got a KEY_ADD msg for SA: SPI = 0x4a6429ba
Nov 27 12:02:00 [IKEv1 DEBUG]: Group = 10.20.20.1, IP =
10.20.20.1,
```

```
Pitcher: received KEY_UPDATE, spi 0x44ae0956
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP =
10.20.20.1,
 Starting P2 Rekey timer to expire in 24480 seconds
Nov 27 12:02:00 [IKEv1]: Group = 10.20.20.1, IP =
10.20.20.1,
PHASE 2 COMPLETED (msgid=d723766b)
```

debug van crypto ipsec - displays debug informatie over IPsec-verbindingen.

crypto ipsec debug

```
pix1(config)#debug crypto ipsec 7

exec mode commands/options:
  <1-255>  Specify an optional debug level (default is
1)
  <cr>
pix1(config)# debug crypto ipsec 7
pix1(config)# IPSEC: New embryonic SA created @
0x024211B0,
    SCB: 0x0240AEB0,
    Direction: inbound
    SPI      : 0x2A3E12BE
    Session ID: 0x00000001
    VPIF num  : 0x00000001
    Tunnel type: l2l
    Protocol   : esp
    Lifetime   : 240 seconds
IPSEC: New embryonic SA created @ 0x0240B7A0,
    SCB: 0x0240B710,
    Direction: outbound
    SPI      : 0xB283D32F
    Session ID: 0x00000001
    VPIF num  : 0x00000001
    Tunnel type: l2l
    Protocol   : esp
    Lifetime   : 240 seconds
IPSEC: Completed host OBSA update, SPI 0xB283D32F
IPSEC: Updating outbound VPN context 0x02422618, SPI
0xB283D32F
    Flags: 0x00000005
    SA   : 0x0240B7A0
    SPI  : 0xB283D32F
    MTU  : 1500 bytes
    VCID : 0x00000000
    Peer : 0x00000000
    SCB  : 0x0240B710
    Channel: 0x014A45B0
IPSEC: Completed outbound VPN context, SPI 0xB283D32F
    VPN handle: 0x02422618
IPSEC: Completed outbound inner rule, SPI 0xB283D32F
    Rule ID: 0x01FA0290
IPSEC: New outbound permit rule, SPI 0xB283D32F
    Src addr: 10.10.10.1
    Src mask: 255.255.255.255
    Dst addr: 10.20.20.1
    Dst mask: 255.255.255.255
    Src ports
      Upper: 0
      Lower: 0
      Op   : ignore
```

```
    Dst ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Protocol: 50
    Use protocol: true
    SPI: 0xB283D32F
    Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0xB283D32F
    Rule ID: 0x0240AF40
IPSEC: Completed host IBSA update, SPI 0x2A3E12BE
IPSEC: Creating inbound VPN context, SPI 0x2A3E12BE
    Flags: 0x00000006
    SA   : 0x024211B0
    SPI  : 0x2A3E12BE
    MTU  : 0 bytes
    VCID : 0x00000000
    Peer : 0x02422618
    SCB  : 0x0240AEB0
    Channel: 0x014A45B0
IPSEC: Completed inbound VPN context, SPI 0x2A3E12BE
    VPN handle: 0x0240BF80
IPSEC: Updating outbound VPN context 0x02422618, SPI
0xB283D32F
    Flags: 0x00000005
    SA   : 0x0240B7A0
    SPI  : 0xB283D32F
    MTU  : 1500 bytes
    VCID : 0x00000000
    Peer : 0x0240BF80
    SCB  : 0x0240B710
    Channel: 0x014A45B0
IPSEC: Completed outbound VPN context, SPI 0xB283D32F
    VPN handle: 0x02422618
IPSEC: Completed outbound inner rule, SPI 0xB283D32F
    Rule ID: 0x01FA0290
IPSEC: Completed outbound outer SPD rule, SPI 0xB283D32F
    Rule ID: 0x0240AF40
IPSEC: New inbound tunnel flow rule, SPI 0x2A3E12BE
    Src addr: 172.16.1.0
    Src mask: 255.255.255.0
    Dst addr: 172.22.1.0
    Dst mask: 255.255.255.0
    Src ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Dst ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Protocol: 0
    Use protocol: false
    SPI: 0x00000000
    Use SPI: false
IPSEC: Completed inbound tunnel flow rule, SPI
0x2A3E12BE
    Rule ID: 0x0240B108
IPSEC: New inbound decrypt rule, SPI 0x2A3E12BE
    Src addr: 10.20.20.1
    Src mask: 255.255.255.255
    Dst addr: 10.10.10.1
    Dst mask: 255.255.255.255
    Src ports
```

```
      Upper: 0
      Lower: 0
      Op   : ignore
    Dst ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Protocol: 50
    Use protocol: true
    SPI: 0x2A3E12BE
    Use SPI: true
IPSEC: Completed inbound decrypt rule, SPI 0x2A3E12BE
    Rule ID: 0x02406E98
IPSEC: New inbound permit rule, SPI 0x2A3E12BE
    Src addr: 10.20.20.1
    Src mask: 255.255.255.255
    Dst addr: 10.10.10.1
    Dst mask: 255.255.255.255
    Src ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Dst ports
      Upper: 0
      Lower: 0
      Op   : ignore
    Protocol: 50
    Use protocol: true
    SPI: 0x2A3E12BE
    Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0x2A3E12BE
    Rule ID: 0x02422C78
```

Gerelateerde informatie

- Redundant tunnelvorming tussen firewalls met PDM
- Cisco PIX-firewallsoftware
- Cisco adaptieve security apparaatbeheer
- Cisco ASA 5500 Series adaptieve security applicaties
- Opdrachtreferenties van Cisco Secure PIX-firewall
- Security meldingen uit het veld (inclusief PIX)
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems