PIX/ASA 7.X : Voeg een nieuwe Tunnel of Externe Toegang aan een bestaande L2L VPN toe

Inhoud

Inleiding

Dit document bevat de stappen die vereist zijn om een nieuwe VPN-tunnel of een externe VPN-toegang toe te voegen aan een L2L VPN-configuratie die al bestaat. Raadpleeg Cisco ASA 5500 Series adaptieve security applicaties - Configuratievoorbeelden en TechNotes voor informatie over het maken van de oorspronkelijke IPSec VPN-tunnels en voor meer configuratievoorbeelden.

Voorwaarden

Vereisten

Zorg ervoor dat u correct de L2L IPSEC VPN-tunnel vormt die momenteel operationeel is voordat u deze configuratie probeert.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Twee ASA security apparaten die 7.x-code gebruiken
- Eén PIX-beveiligingsapparaat met 7,x-code

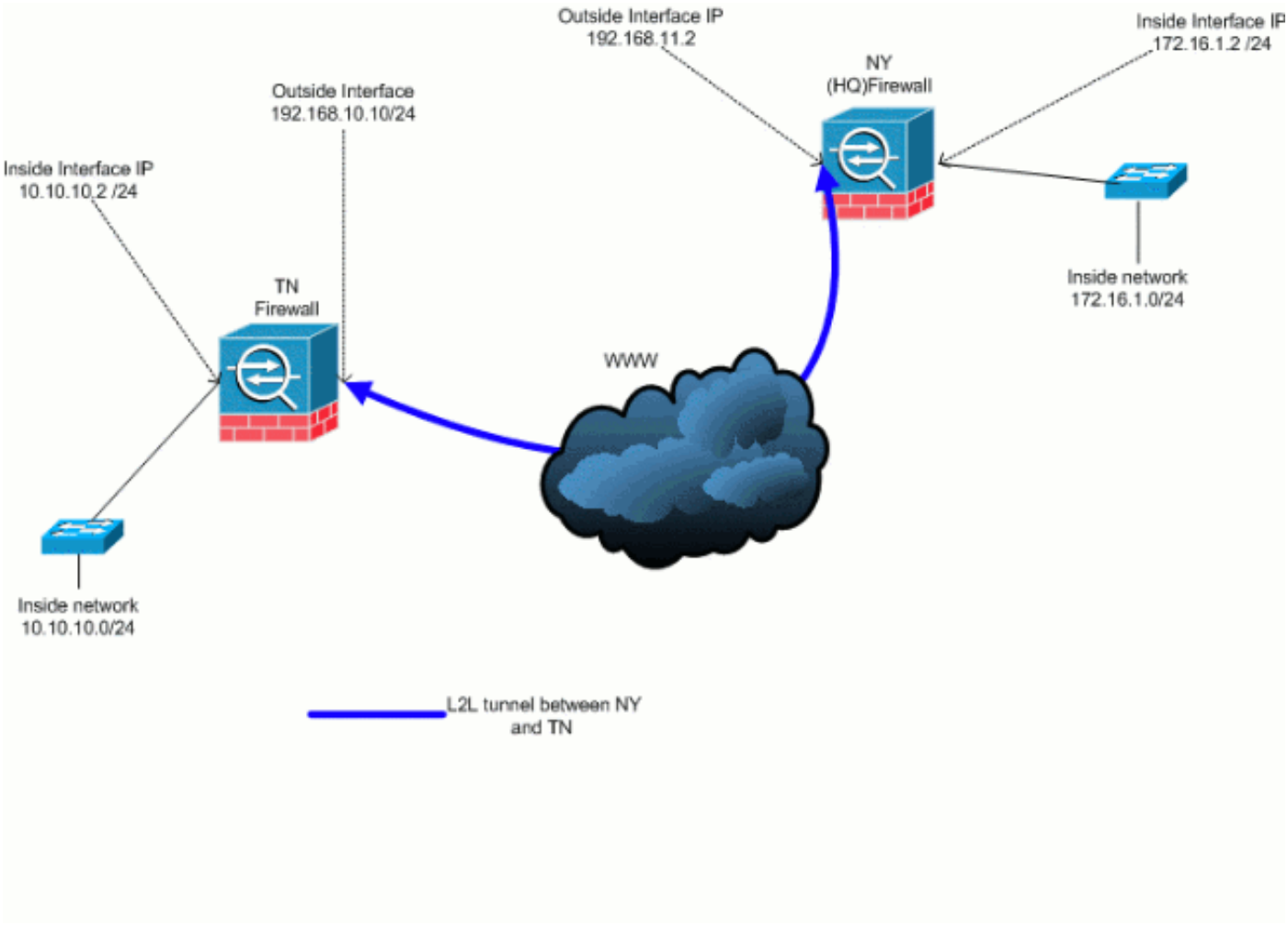
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

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

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:



Deze uitvoer is de huidige configuratie van het NY (HUB)-beveiligingsapparaat. In deze configuratie is er een IPSec L2L-tunnel ingesteld tussen NY(HQ) en TN.

Configuratie van huidige NY-firewall (HQ)
ASA-NY-HQ#**show running-config** : Saved :

```
ASA Version 7.2(2)
!
hostname ASA-NY-HQ
domain-name corp2.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.11.2 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name corp2.com
access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0
10.10.10.0 255.255.255.0
access-list outside_20_cryptomap extended permit ip
172.16.1.0 255.255.255.0
10.10.10.0 255.255.255.0

!--- Output is suppressed. nat-control global (outside)
1 interface nat (inside) 0 access-list
inside_nat0_outbound nat (inside) 1 172.16.1.0
255.255.255.0 route outside 0.0.0.0 0.0.0.0
192.168.11.100 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 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media
0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute no snmp-server location
no snmp-server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart crypto ipsec
transform-set ESP-3DES-SHA esp-3des esp-sha-hmac crypto
map outside_map 20 match address outside_20_cryptomap
crypto map outside_map 20 set peer 192.168.10.10 crypto
map outside_map 20 set transform-set ESP-3DES-SHA crypto
map outside_map interface outside crypto isakmp enable
outside crypto isakmp policy 10 authentication pre-share
```

```
encryption 3des hash sha group 2 lifetime 86400 crypto
isakmp nat-traversal 20 tunnel-group 192.168.10.10 type
ipsec-l2l tunnel-group 192.168.10.10 ipsec-attributes
pre-shared-key * telnet timeout 1440 ssh timeout 5
console timeout 0 ! class-map inspection_default match
default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map 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 prompt hostname context
Cryptochecksum:a3aa2afb37dcad447031b7b0c8ea65d3 : end
ASA-NY-HQ#
```

Achtergrondinformatie

Momenteel is er een bestaande L2L-tunnel opgezet tussen het kantoor van de NY (HQ) en het kantoor van TN. Uw bedrijf heeft onlangs een nieuw kantoor geopend dat in TX is gevestigd. Dit nieuwe kantoor vereist connectiviteit met lokale middelen die in de NY en TN kantoren zijn gevestigd. Daarnaast is er een aanvullende verplichting om werknemers de mogelijkheid te geven om van huis te werken en veilig toegang te krijgen tot middelen die zich op afstand op het interne netwerk bevinden. In dit voorbeeld wordt een nieuwe VPN-tunnel zo ingesteld dat er ook een VPN-server voor externe toegang wordt geïnstalleerd die zich in het NY-kantoor bevindt.

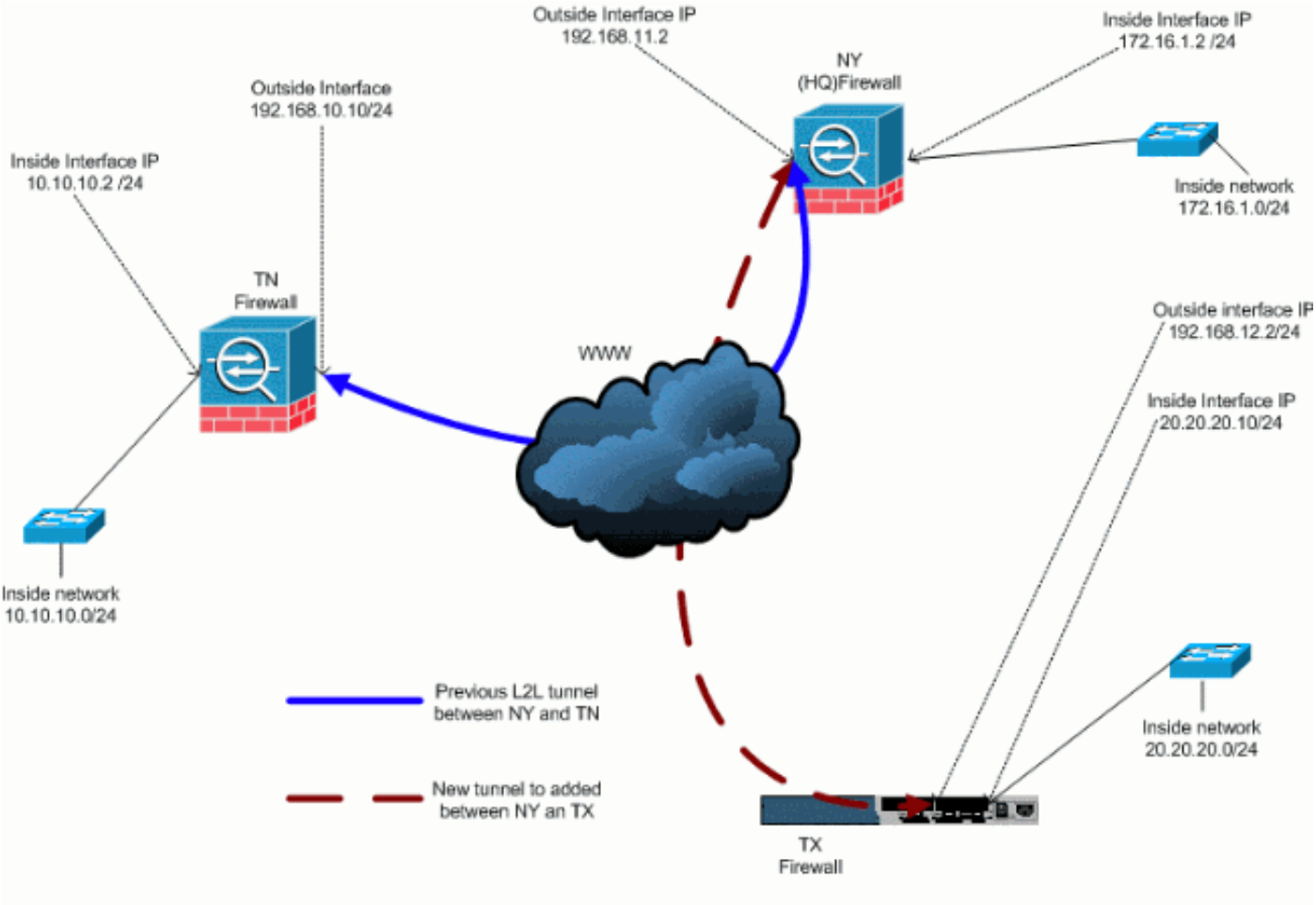
In dit voorbeeld, worden twee opdrachten gebruikt om de communicatie tussen de VPN-netwerken toe te staan en het verkeer te identificeren dat een tunneleffect of een versleuteling zou moeten hebben. Dit stelt u in staat om toegang tot het internet te hebben zonder dat u dat verkeer door de VPN-tunnel hoeft te sturen. Om deze twee opties te configureren geeft u de opdrachten **split-tunnel** en **hetzelfde security-verkeer** uit.

Split-tunneling stelt een IPSec-client voor toegang op afstand in staat om pakketten voorwaardelijk te sturen via een IPSec-tunnel in gecodeerde vorm, of naar een netwerkinterface in duidelijke tekstvorm. Als gesplitste tunneling ingeschakeld is, hoeven pakketten die niet gebonden zijn voor bestemmingen aan de andere kant van de IPSec-tunnel niet te worden versleuteld, over de tunnel te worden verzonden, te worden gedecrypteerd en vervolgens naar een eindbestemming te worden verzonden. Deze opdracht past dit gesplitste tunneling-beleid op een bepaald netwerk toe. De standaardinstelling is om al het verkeer te tunnelen. Om een gesplitst tunnelbeleid in te stellen, geeft u de opdracht **gesplitst tunnelbeleid** uit in de configuratie-modus van het groepsbeleid. Om het split-tunneling-beleid uit de configuratie te verwijderen, geeft u de **geen** vorm van deze opdracht uit.

Het security apparaat bevat een functie die een VPN-client in staat stelt om IPSec-beveiligd verkeer naar andere VPN-gebruikers te verzenden door dergelijk verkeer in en uit dezelfde interface toe te staan. Ze worden ook wel haarspelden genoemd en deze optie kan worden gezien als VPN-woordjes (clients) die verbinding maken via een VPN-hub (security applicatie). In een andere toepassing, kan deze optie inkomend VPN-verkeer terugsturen door de zelfde interface te gebruiken als niet-versleuteld verkeer. Dit is bijvoorbeeld handig voor een VPN-client die geen gesplitste tunneling heeft, maar tegelijkertijd een VPN moet benaderen en door het web moet bladeren. Om deze optie te configureren geeft u de **opdracht Dezelfde security *inter-interface* in de** mondiale configuratiemodus uit.

Voeg een extra L2L-tunnel toe aan de configuratie

Dit is het netwerkdiagram voor deze configuratie:



Stapsgewijze instructies

In dit gedeelte worden de vereiste procedures beschreven die moeten worden uitgevoerd op het HUB (NY Firewall) security apparaat. Raadpleeg PIX/ASA 7.x: Eenvoudig PIX-to-PIX VPN Tunnel Configuration Voorbeeld voor meer informatie over de configuratie van de gedeelde client (TX Firewall).

Voer de volgende stappen uit:

1. Maak deze twee nieuwe toegangslijsten die door de crypto kaart worden gebruikt om interessant verkeer te definiëren:
```
ASA-NY-HQ(config)#access-list outside_30_cryptomap
 extended permit ip 172.16.1.0 255.255.255.0
    20.20.20.0 255.255.255.0


ASA-NY-HQ(config)#access-list outside_30_cryptomap
 extended permit ip 10.10.10.0 255.255.255.0
    20.20.20.0 255.255.255.0
```
   Waarschuwing: om de communicatie te kunnen laten plaatsvinden, moet de andere kant van de tunnel het tegenovergestelde van deze ACL-ingang (toegangscontrolelijst) voor dat specifieke netwerk hebben.
2. Voeg deze ingangen aan het nee nat statement toe om het ding tussen deze netwerken vrij te stellen:
```
ASA-NY-HQ(config)#access-list inside_nat0_outbound
 extended permit ip 172.16.1.0 255.255.255.0
```

```
    20.20.20.0 255.255.255.0

ASA-NY-HQ(config)#access-list inside_nat0_outbound
 extended permit ip 10.10.10.0 255.255.255.0
    20.20.20.0 255.255.255.0

ASA-NY-HQ(config)#access-list inside_nat0_outbound
 extended permit ip 20.20.20.0 255.255.255.0
    10.10.10.0 255.255.255.0
```

Waarschuwing: om de communicatie te kunnen laten plaatsvinden, moet de andere kant van de tunnel het tegenovergestelde van deze ACL-ingang voor dat specifieke netwerk hebben.

3. Geef deze opdracht uit om een host in het TX VPN-netwerk toegang te geven tot de TN VPN-tunnel:

```
ASA-NY-HQ(config)#same-security-traffic permit
 intra-interface
```

Hierdoor kunnen VPN-peers met elkaar praten.

4. Maak de crypto kaartconfiguratie voor de nieuwe VPN-tunnel. Gebruik dezelfde transformatie die gebruikt werd in de eerste VPN-configuratie, aangezien alle fase 2-instellingen hetzelfde zijn.

```
ASA-NY-HQ(config)#crypto map outside_map 30 match
 address outside_30_cryptomap

ASA-NY-HQ(config)#crypto map outside_map 30 set
 peer 192.168.12.2

ASA-NY-HQ(config)#crypto map outside_map 30 set
 transform-set
 ESP-3DES-SHA
```

5. Maak de tunnelgroep die voor deze tunnel samen met eigenschappen nodig is om met de afstandsbediening te verbinden is gespecificeerd.

```
ASA-NY-HQ(config)#tunnel-group 192.168.12.2 type
 ipsec-l2l

ASA-NY-HQ(config)#tunnel-group 192.168.12.2
 ipsec-attributes

ASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key
cisco123
```

Opmerking: de pre-gedeeld toets moet precies aan beide zijden van de tunnel overeenkomen.

6. Nu je de nieuwe tunnel hebt ingericht, moet je interessant verkeer door de tunnel sturen om hem omhoog te halen. Om dit uit te voeren, geef de **bron ping** opdracht uit om een host op het binnennetwerk van de afstandstunnel te pingelen.In dit voorbeeld is een werkstation aan de andere kant van de tunnel met het adres 20.20.20.16 gepingd. Dit brengt de tunnel op tussen NY en TX. Er zijn twee tunnels verbonden met het kantoor van het hoofdkwartier. Als u geen toegang hebt tot een systeem achter de tunnel, raadpleeg de Meest gebruikelijke IPSec VPN-oplossingen voor probleemoplossing om een alternatieve oplossing te vinden voor het gebruik `van beheerstoegang`.

Configuratievoorbeeld

Voorbeeld Configuration 1

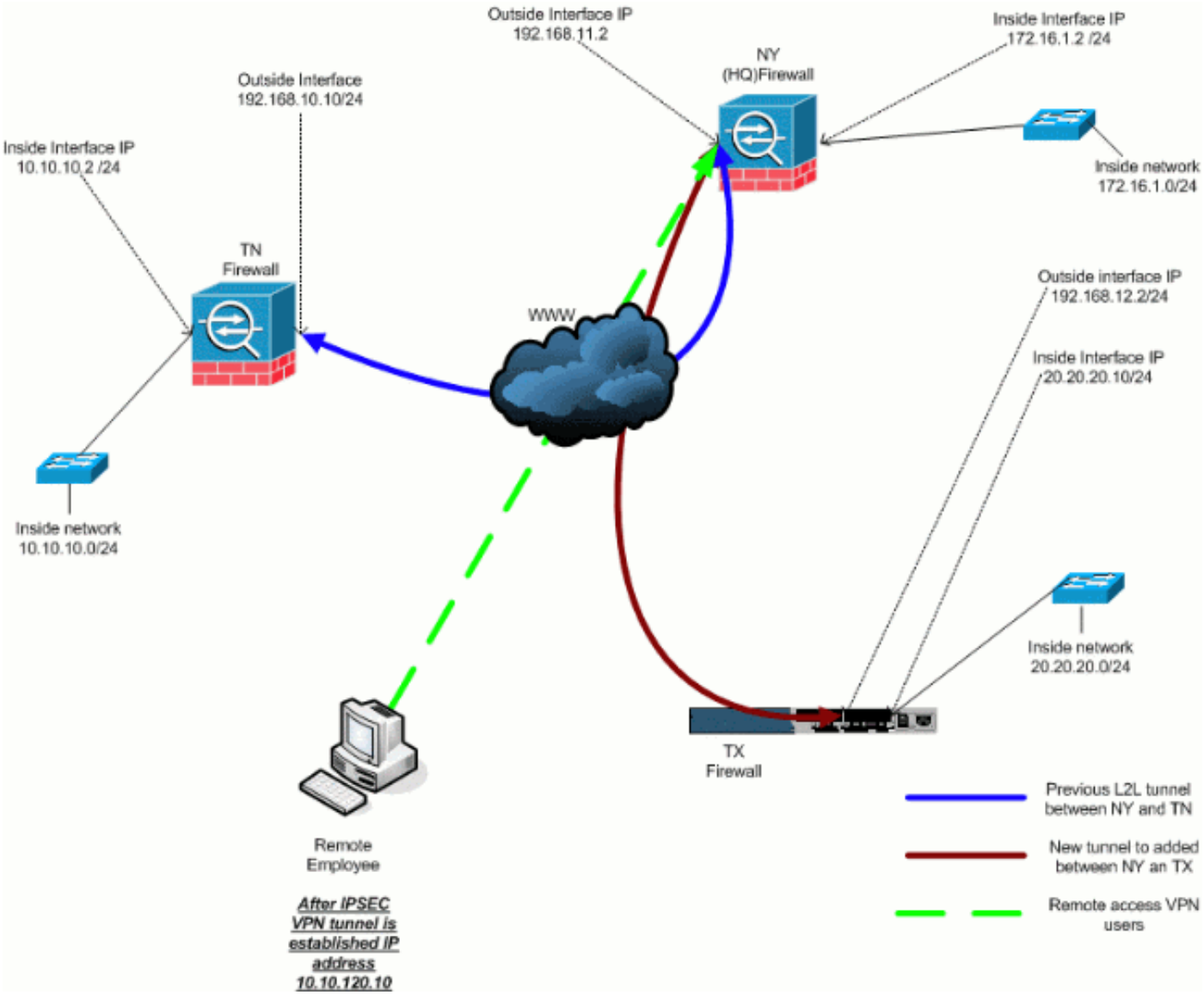
```
ASA-NY-HQ#show running-config

 : Saved
:
ASA Version 7.2(2)
!
hostname ASA-NY-HQ
domain-name corp2.com
enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.11.1 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name corp2.com
same-security-traffic permit intra-interface
access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip
10.10.10.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip
20.20.20.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list outside_20_cryptomap extended permit ip
172.16.1.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list outside_20_cryptomap extended permit ip
20.20.20.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list outside_30_cryptomap extended permit ip
172.16.1.0 255.255.255.0 20.20.20.0
```

```
255.255.255.0
access-list outside_30_cryptomap extended permit ip
10.10.10.0 255.255.255.0 20.20.20.0
255.255.255.0
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu man 1500
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 172.16.1.0 255.255.255.0
route outside 0.0.0.0 0.0.0.0 192.168.11.1 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 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
username sidney password 3xsopMX9gN5Wnf1W encrypted
privilege 15
aaa authentication telnet console LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
sha-hmac
crypto map outside_map 20 match address
outside_20_cryptomap
crypto map outside_map 20 set peer 192.168.10.10
crypto map outside_map 20 set transform-set ESP-3DES-SHA
crypto map outside_map 30 match address
outside_30_cryptomap
crypto map outside_map 30 set peer 192.168.12.2
crypto map outside_map 30 set transform-set ESP-3DES-SHA
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp nat-traversal  20
tunnel-group 192.168.10.10 type ipsec-l2l
tunnel-group 192.168.10.10 ipsec-attributes
 pre-shared-key *
tunnel-group 192.168.12.2 type ipsec-l2l
tunnel-group 192.168.12.2 ipsec-attributes
 pre-shared-key *
telnet timeout 1440
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
```

```
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  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
prompt hostname context
Cryptochecksum:5a184c8e5e6aa30d4108a55ac0ead3ae
: end
ASA-NY-HQ#
```

Een VPN-toegang op afstand toevoegen aan de configuratie

Dit is het netwerkdiagram voor deze configuratie:



Stapsgewijze instructies

Dit deel bevat de vereiste procedures om de mogelijkheden voor toegang op afstand toe te voegen en om externe gebruikers toegang te geven tot alle sites. Raadpleeg PIX/ASA 7.x ASDM: Beperk de Toegang tot het netwerk van gebruikers van Remote Access VPN voor meer informatie over hoe u de externe toegangsserver kunt configureren en de toegang kunt beperken.

Voer de volgende stappen uit:

1. Maak een IP-adrespool die gebruikt moet worden voor clients die via de VPN-tunnel verbonden zijn. Maak ook een basisgebruiker om toegang tot VPN te krijgen zodra de configuratie is voltooid.

```
ASA-NY-HQ(config)#ip local pool Hill-V-IP
 10.10.120.10-10.10.120.100 mask 255.255.255.0

ASA-NY-HQ(config)#username cisco password
 cisco111
```

2. Uitzondering van het specifieke verkeer op het feit dat het wordt geregistreerd.

```
ASA-NY-HQ(config)#access-list
 inside_nat0_outbound extended permit ip 172.16.1.0
    255.255.255.0 10.10.120.0 255.255.255.0
```

```
ASA-NY-HQ(config)#access-list
 inside_nat0_outbound extended permit ip 10.10.120.0
    255.255.255.0 10.10.10.0 255.255.255.0

ASA-NY-HQ(config)#access-list
 inside_nat0_outbound extended permit ip 10.10.120.0
    255.255.255.0 20.20.20.0 255.255.255.0
```

Merk op dat de communicatie tussen VPN-tunnels in dit voorbeeld is vrijgesteld.

3. Laat communicatie tussen de L2L tunnels toe die al gecreëerd zijn.

```
ASA-NY-HQ(config)#access-list
 outside_20_cryptomap extended permit ip 10.10.120.0
    255.255.255.0 10.10.10.0 255.255.255.0

ASA-NY-HQ(config)#access-list
 outside_30_cryptomap extended permit ip 10.10.120.0
    255.255.255.0 20.20.20.0 255.255.255.0
```

Dit staat verre toegangsgebruikers de mogelijkheid toe om met netwerken achter de gespecificeerde tunnels te communiceren.**Waarschuwing:** om de communicatie te kunnen laten plaatsvinden, moet de andere kant van de tunnel het tegenovergestelde van deze ACL-ingang voor dat specifieke netwerk hebben.

4. Configureer het verkeer dat versleuteld en verzonden zal worden over de VPN-tunnel.

```
ASA-NY-HQ(config)#access-list
 Hillvalley_splitunnel standard permit 172.16.1.0
    255.255.255.0

ASA-NY-HQ(config)#access-list
 Hillvalley_splitunnel standard permit 10.10.10.0
    255.255.255.0

ASA-NY-HQ(config)#access-list
 Hillvalley_splitunnel standard permit 20.20.20.0
    255.255.255.0
```

5. Configuratie van lokale Verificatie en beleidsinformatie, zoals wins, dns en IPSec protocollen, voor de VPN cliënten.

```
ASA-NY-HQ(config)#group-policy Hillvalley
 internal

ASA-NY-HQ(config)#group-policy Hillvalley
 attributes

ASA-NY-HQ(config-group-policy)#wins-server
value 10.10.10.20

ASA-NY-HQ(config-group-policy)#dns-server value
10.10.10.20

ASA-NY-HQ(config-group-policy)#vpn-tunnel-protocol
IPSec
```

6. Stel IPSec en algemene eigenschappen, zoals vooraf gedeelde sleutels en IP adrespools in, die door de tunnel van Hillvalley VPN zullen worden gebruikt.

```
ASA-NY-HQ(config)#tunnel-group Hillvalley
 ipsec-attributes

ASA-NY-HQ(config-tunnel-ipsec)#pre-shared-key
cisco1234

ASA-NY-HQ(config)#tunnel-group Hillvalley
```

```
 general-attributes

ASA-NY-HQ(config-tunnel-general)#address-pool
Hill-V-IP

ASA-NY-HQ(config-tunnel-general)#default-group-policy
Hillvalley
```

7. Maak het gesplitste tunnelbeleid dat ACL gebruikt dat in stap 4 gecreëerd wordt om te specificeren welk verkeer versleuteld en door de tunnel doorgegeven zal worden.

```
ASA-NY-HQ(config)#split-tunnel-policy
 tunnelspecified

ASA-NY-HQ(config)#split-tunnel-network-list value
 Hillvalley_splitunnel
```

8. Configuratie van de kristallijne om informatie in kaart te brengen die vereist is voor de VPN tunnelbouw.

```
ASA-NY-HQ(config)#crypto ipsec transform-set
 Hill-trans esp-3des esp-sha-hmac

ASA-NY-HQ(config)#crypto dynamic-map
 outside_dyn_map 20 set transform-set
 Hill-trans

ASA-NY-HQ(config)#crypto dynamic-map dyn_map 20
 set reverse-route

ASA-NY-HQ(config)#crypto map outside_map 65535
 ipsec-isakmp dynamic
 outside_dyn_map
```

Configuratievoorbeeld

Voorbeeld Configuration 2

```
ASA-NY-HQ#show running-config

 : Saved

hostname ASA-NY-HQ
ASA Version 7.2(2)

enable password WwXYvtKrnjXqGbu1 encrypted
names
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 192.168.11.2 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet0/2
 shutdown
 no nameif
 no security-level
```

```
 no ip address
!
interface Ethernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name corp2.com
same-security-traffic permit intra-interface

!--- This is required for communication between VPN
peers. access-list inside_nat0_outbound extended permit
ip 172.16.1.0 255.255.255.0 10.10.10.0 255.255.255.0
access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 20.20.20.0 255.255.255.0
access-list inside_nat0_outbound extended permit ip
10.10.10.0 255.255.255.0 20.20.20.0 255.255.255.0
access-list inside_nat0_outbound extended permit ip
20.20.20.0 255.255.255.0 10.10.10.0 255.255.255.0
access-list inside_nat0_outbound extended permit ip
10.10.120.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip
172.16.1.0 255.255.255.0 10.10.120.0
255.255.255.0
access-list inside_nat0_outbound extended permit ip
10.10.120.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list outside_20_cryptomap extended permit ip
172.16.1.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list outside_20_cryptomap extended permit ip
20.20.20.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list outside_20_cryptomap extended permit ip
10.10.120.0 255.255.255.0 10.10.10.0
255.255.255.0
access-list Hillvalley_splitunnel standard permit
172.16.1.0 255.255.255.0
access-list Hillvalley_splitunnel standard permit
10.10.10.0 255.255.255.0
access-list Hillvalley_splitunnel standard permit
20.20.20.0 255.255.255.0
access-list outside_30_cryptomap extended permit ip
172.16.1.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list outside_30_cryptomap extended permit ip
10.10.10.0 255.255.255.0 20.20.20.0
255.255.255.0
access-list outside_30_cryptomap extended permit ip
10.10.120.0 255.255.255.0 20.20.20.0
255.255.255.0
logging enable
logging asdm informational
```

```
mtu outside 1500
mtu inside 1500
mtu man 1500
ip local pool Hill-V-IP 10.10.120.10-10.10.120.100 mask
255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface
nat (inside) 0 access-list inside_nat0_outbound
nat (inside) 1 172.16.1.0 255.255.255.0
route outside 0.0.0.0 0.0.0.0 192.168.11.1 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 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
group-policy Hillvalley internal
group-policy Hillvalley attributes
 wins-server value 10.10.10.20
 dns-server value 10.10.10.20
 vpn-tunnel-protocol IPSec
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value Hillvalley_splitunnel
 default-domain value corp.com
username cisco password dZBmhhbNIN5q6rGK encrypted
aaa authentication telnet console LOCAL
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
sha-hmac
crypto ipsec transform-set Hill-trans esp-3des esp-sha-
hmac
crypto dynamic-map outside_dyn_map 20 set transform-set
Hill-trans
crypto dynamic-map dyn_map 20 set reverse-route
crypto map outside_map 20 match address
outside_20_cryptomap
crypto map outside_map 20 set peer 192.168.10.10
crypto map outside_map 20 set transform-set ESP-3DES-SHA
crypto map outside_map 30 match address
outside_30_cryptomap
crypto map outside_map 30 set peer 192.168.12.1
crypto map outside_map 30 set transform-set ESP-3DES-SHA

crypto map outside_map 65535 ipsec-isakmp dynamic
outside_dyn_map
crypto map outside_map interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp nat-traversal  20
tunnel-group 192.168.10.10 type ipsec-l2l
```

```
tunnel-group 192.168.10.10 ipsec-attributes
 pre-shared-key *
tunnel-group 192.168.12.2 type ipsec-l2l
tunnel-group 192.168.12.2 ipsec-attributes
 pre-shared-key *
tunnel-group Hillvalley type ipsec-ra
tunnel-group Hillvalley general-attributes
 address-pool Hill-V-IP
 default-group-policy Hillvalley
tunnel-group Hillvalley ipsec-attributes
 pre-shared-key *
telnet timeout 1440
ssh timeout 5
console timeout 0
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  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
prompt hostname context
Cryptochecksum:62dc631d157fb7e91217cb82dc161a48
ASA-NY-HQ#
```

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.

- **ping in x.x.x.x (IP adres van host aan tegenovergestelde kant van tunnel)** - Deze opdracht staat u toe om verkeer door de tunnel te sturen met behulp van het bronadres van de binneninterface.

Problemen oplossen

Raadpleeg deze documenten voor informatie die u kunt gebruiken om problemen met uw

configuratie op te lossen:

- Meest gebruikelijke oplossingen voor probleemoplossing in IPSec VPN
- IP-beveiligingsprobleemoplossing - Oplossingen begrijpen en gebruiken van debug-opdrachten
- Probleemoplossing met verbindingen via PIX en ASA

Gerelateerde informatie

- Een Inleiding aan IP Security (IPSec) encryptie
- Ondersteuning van IPSec-onderhandeling/IKE-protocollen
- Cisco ASA 5500 Series Opdrachten voor adaptieve security applicaties
- Technische ondersteuning en documentatie – Cisco Systems