

Dynamische site naar site IKEv2 VPN-tunnelband tussen een ASA en een IOS routerconfiguratie voorbeeld

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Scenario 1](#)

[Netwerkdigram](#)

[Configuratie](#)

[Scenario 2](#)

[Netwerkdigram](#)

[Configuratie](#)

[Verifiëren](#)

[Statische ASA](#)

[Dynamische router](#)

[Dynamische router \(met Remote Dynamic ASA\)](#)

[Problemen oplossen](#)

Inleiding

Dit document beschrijft hoe u een site-to-site Internet Key Exchange, versie 2 (IKEv2) VPN-tunnels tussen een adaptieve security applicatie (ASA) en een Cisco-router kunt configureren waar de router een dynamisch IP-adres heeft en de ASA een statisch IP-adres op de openbare interfaces heeft.

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 IOS® versie 15.1(1)T of hoger
- Cisco ASA versie 8.4(1) of hoger

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.

Achtergrondinformatie

In dit document worden deze scenario's besproken:

- Scenario 1: Een ASA wordt geconfigureerd met een statisch IP-adres dat een benoemde tunnelgroep gebruikt en de router is geconfigureerd met een dynamisch IP-adres.
- Scenario 2: Een ASA wordt ingesteld met een dynamisch IP-adres en de router is ingesteld met een dynamisch IP-adres.
- Scenario 3: Dit scenario wordt hier niet besproken. In dit scenario wordt de ASA geconfigureerd met een statisch IP-adres maar gebruikt de DefaultL2LG roup tunnelgroep. De configuratie voor dit is vergelijkbaar met wat in het [artikel](#) Dynamic Site [to Site IKEv2 VPN wordt](#) beschreven [tussen twee ASA's](#) Configuration Voorbeeld.

Het grootste configuratieverschil tussen Scenarios 1 en 3 is de ID van Internet Security Association en Key Management Protocol (ISAKMP) die door de afstandsrouter wordt gebruikt. Wanneer de DefaultL2LGgroup op de statische ASA wordt gebruikt, moet de ISAKMP-ID van de peer op de router het adres van de ASA zijn. Als echter een genoemde tunnelgroep wordt gebruikt, moet de ISAKMP-ID van de peer op de router gelijk zijn aan de naam van de tunnelgroep die op de ASA is geconfigureerd. Dit wordt bereikt met deze opdracht op de router:

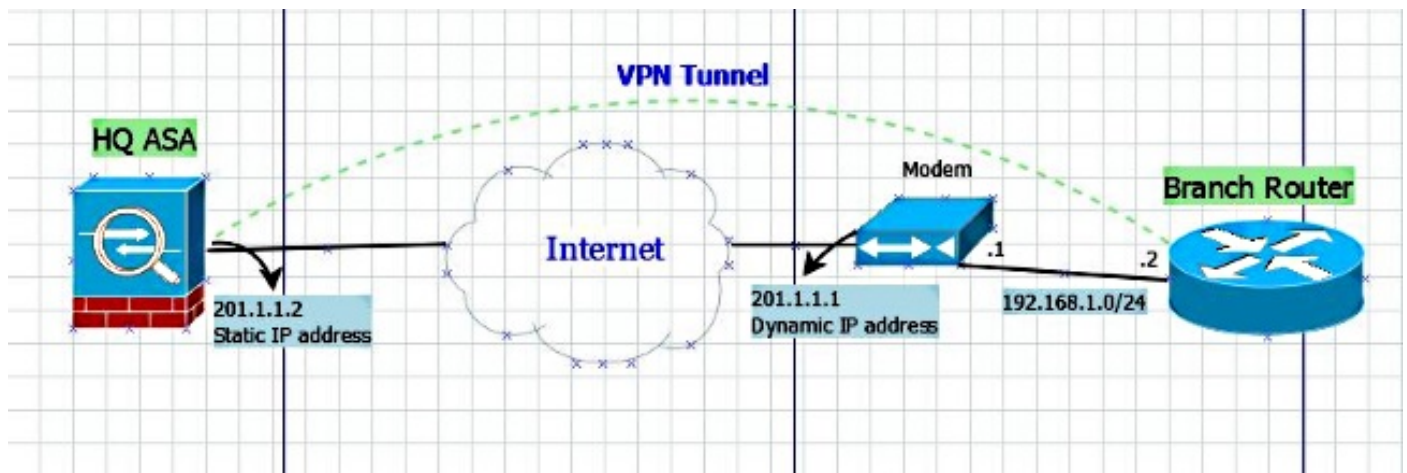
```
identity local key-id
```

Het voordeel van het gebruik van genoemde tunnelgroepen op de statische ASA is dat wanneer de DefaultL2LGgroup wordt gebruikt, de configuratie op de externe dynamische ASA's/routers, die de pre-gedeelde toetsen bevat, identiek moet zijn en niet veel granulariteit met de instelling van beleid toelaat.

Configureren

Scenario 1

Netwerkdigram



Configuratie

In deze sectie worden de configuratie op de ASA en de router beschreven die op de Benoemde tunnelgroepconfiguratie is gebaseerd.

Statische ASA-configuratie

```
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 201.1.1.2 255.255.255.0
!
crypto ipsec ikev2 ipsec-proposal ESP-AES-SHA
 protocol esp encryption aes
 protocol esp integrity sha-1
crypto ipsec security-association pmtu-aging infinite
crypto dynamic-map dmap 1 set ikev2 ipsec-proposal ESP-AES-SHA
crypto map vpn 1 ipsec-isakmp dynamic dmap
crypto map vpn interface outside
crypto ca trustpool policy
crypto ikev2 policy 1
 encryption 3des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 enable outside

group-policy Site-to-Site internal
group-policy Site-to-Site attributes
 vpn-tunnel-protocol ikev2
tunnel-group S2S-IKEv2 type ipsec-l2l
tunnel-group S2S-IKEv2 general-attributes
 default-group-policy Site-to-Site
tunnel-group S2S-IKEv2 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco321
 ikev2 local-authentication pre-shared-key cisco123
```

Dynamische routerconfiguratie

De Dynamische router is vrijwel dezelfde manier ingesteld als u normaal gesproken configureren in gevallen waarin de router een dynamische locatie is voor IKEv2 L2L-tunnel met de toevoeging van één opdracht zoals hieronder wordt getoond:

```
ip access-list extended vpn
 permit ip host 10.10.10.1 host 201.1.1.2

crypto ikev2 proposal L2L-Prop
 encryption 3des
 integrity sha1
 group 2 5
!
crypto ikev2 policy L2L-Pol
 proposal L2L-Prop
!
crypto ikev2 keyring L2L-Keyring
 peer vpn
 address 201.1.1.2
 pre-shared-key local cisco321
 pre-shared-key remote cisco123
!
crypto ikev2 profile L2L-Prof
 match identity remote address 201.1.1.2 255.255.255.255
 identity local key-id S2S-IKEv2
 authentication remote pre-share
 authentication local pre-share
 keyring local L2L-Keyring

crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
!
crypto map vpn 10 ipsec-isakmp
 set peer 201.1.1.2
 set transform-set ESP-AES-SHA
 set ikev2-profile L2L-Prof
 match address vpn
!
interface GigabitEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
 crypto map vpn
```

Dus bij elke dynamische peer, is de key-id anders en er moet een corresponderende tunnelgroep gecreëerd worden op de Static ASA met de juiste naam, wat ook de granulariteit verhoogt van het beleid dat uitgevoerd wordt op een ASA.

Scenario 2

Opmerking: deze configuratie is alleen mogelijk wanneer aan ten minste één kant een router is. Als beide kanten ASA's zijn, werkt deze opzet op dit moment niet. In versie 8.4 kan de ASA de Full Qualified Domain Name (FQDN) niet gebruiken met de **ingestelde peer** opdracht, maar [CSCus37350](#) is gevraagd om toekomstige releases.

Als het IP-adres van de externe ASA dynamisch is maar ook een FULL Qualified Domain Name is toegewezen voor zijn VPN-interface, dan definieer u in plaats van het IP-adres van de externe ASA nu FQDN van de externe ASA met deze opdracht op de router:

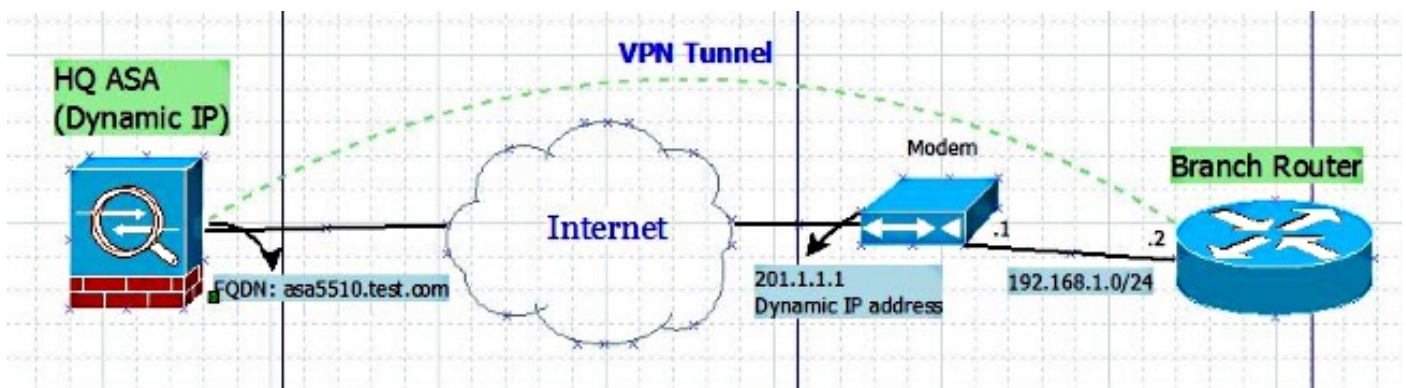
```
C1941(config)#do show run | sec crypto map
```

```
crypto map vpn 10 ipsec-isakmp  
set peer <FQDN> dynamic
```

Tip: Het **dynamische** sleutelwoord is facultatief. Wanneer u de hostname van een externe IPsec peer via de **setpeer** opdracht specificeert, kunt u het dynamische sleutelwoord ook uitgeven, dat de resolutie van de Server van de Naam van het Domein (DNS) van de hostname verdedigt tot onmiddellijk vóór de IPsec-tunnel werd gevestigd.

De uitstelresolutie stelt de Cisco IOS-software in staat om te detecteren of het IP-adres van de externe IPsec-peer is gewijzigd. Zodoende kan de software contact opnemen met de peer op het nieuwe IP adres. Als het dynamische sleutelwoord niet wordt uitgegeven, wordt de hostname opgelost onmiddellijk nadat het is gespecificeerd. Dus kan de Cisco IOS-software geen IP-adreswijziging detecteren en daarom probeert u verbinding te maken met het IP-adres dat eerder is opgelost.

Netwerkdigram



Configuratie

Dynamische ASA-configuratie

De configuratie op de ASA is hetzelfde als de [Static ASA Configuration](#) met slechts één uitzondering, namelijk dat het IP-adres op de fysieke interface niet statisch wordt gedefinieerd.

Routerconfiguratie

```
crypto ikev2 keyring L2L-Keyring  
peer vpn  
hostname asa5510.test.com  
pre-shared-key local cisco321  
pre-shared-key remote cisco123  
!  
crypto ikev2 profile L2L-Prof  
match identity remote fqdn domain test.com  
identity local key-id S2S-IKEv2
```

```
authentication remote pre-share
authentication local pre-share
keyring local L2L-Keyring
```

```
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
mode tunnel
```

```
crypto map vpn 10 ipsec-isakmp
set peer asa5510.test.com dynamic
set transform-set ESP-AES-SHA
set ikev2-profile L2L-Prof
match address vpn
```

Verifiëren

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

Statische ASA

- Dit is het resultaat van de **show crypto IKEv2 sa det** opdracht:

IKEv2 SAs:

Session-id:23, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id	Local	Remote	Status	Role
120434199	201.1.1.2/4500	201.1.1.1/4500	READY	RESPONDER

Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/915 sec
Session-id: 23
Status Description: Negotiation done
Local spi: 97272A4B4DED4A5C Remote spi: 67E01CB8E8619AF1
Local id: 201.1.1.2
Remote id: S2S-IKEv2
Local req mess id: 43 Remote req mess id: 2
Local next mess id: 43 Remote next mess id: 2
Local req queued: 43 Remote req queued: 2
Local window: 1 Remote window: 5
DPD configured for 10 seconds, retry 2
NAT-T is detected outside
Child sa: local selector 201.1.1.2/0 - 201.1.1.2/65535
remote selector 10.10.10.1/0 - 10.10.10.1/65535
ESP spi in/out: 0x853c02/0x41aa84f4
AH spi in/out: 0x0/0x0
CPI in/out: 0x0/0x0
Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
ah_hmac: None, comp: IPCOMP_NONE, mode tunnel

- Dit is het resultaat van de **show crypto ipsec** opdracht:

```
interface: outside
Crypto map tag: dmap, seq num: 1, local addr: 201.1.1.2

local ident (addr/mask/prot/port): (201.1.1.2/255.255.255.255/0/0)
```

```
remote ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0)
current_peer: 201.1.1.1
```

```
#pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
#pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

```
local crypto endpt.: 201.1.1.2/4500, remote crypto endpt.: 201.1.1.1/4500
path mtu 1500, ipsec overhead 82(52), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 41AA84F4
current inbound spi : 00853C02
```

inbound esp sas:

```
spi: 0x00853C02 (8731650)
  transform: esp-aes esp-sha-hmac no compression
  in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, }
  slot: 0, conn_id: 94208, crypto-map: dmap
  sa timing: remaining key lifetime (kB/sec): (4101119/27843)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x0000001F
```

outbound esp sas:

```
spi: 0x41AA84F4 (1101694196)
  transform: esp-aes esp-sha-hmac no compression
  in use settings ={L2L, Tunnel, NAT-T-Encaps, IKEv2, }
  slot: 0, conn_id: 94208, crypto-map: dmap
  sa timing: remaining key lifetime (kB/sec): (4055039/27843)
  IV size: 16 bytes
  replay detection support: Y
  Anti replay bitmap:
    0x00000000 0x00000001
```

Dynamische router

- Dit is het resultaat van de **show crypto IKEv2 als detail** opdracht:

IPv4 Crypto IKEv2 SA

Tunnel-id	Local	Remote	fvr/ivrf	Status
1	192.168.1.2/4500	201.1.1.2/4500	none/none	READY
Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK				
Life/Active Time: 86400/1013 sec				
CE id: 1023, Session-id: 23				
Status Description: Negotiation done				
Local spi: 67E01CB8E8619AF1		Remote spi: 97272A4B4DED4A5C		
Local id: S2S-IKEv2				
Remote id: 201.1.1.2				
Local req msg id: 2		Remote req msg id: 48		
Local next msg id: 2		Remote next msg id: 48		
Local req queued: 2		Remote req queued: 48		
Local window: 5		Remote window: 1		

DPD configured for 0 seconds, retry 0
Fragmentation not configured.
Extended Authentication not configured.
NAT-T is detected inside
Cisco Trust Security SGT is disabled
Initiator of SA : Yes

IPv6 Crypto IKEv2 SA

- Dit is het resultaat van de **show crypto ipsec** opdracht:

```
interface: GigabitEthernet0/0
  Crypto map tag: vpn, local addr 192.168.1.2

protected vrf: (none)
local ident (addr/mask/prot/port): (10.10.10.1/255.255.255.255/0/0)
remote ident (addr/mask/prot/port): (201.1.1.2/255.255.255.255/0/0)
current_peer 201.1.1.2 port 4500
  PERMIT, flags={origin_is_acl,}
  #pkts encaps: 6, #pkts encrypt: 6, #pkts digest: 6
  #pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 6
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0
  #pkts not decompressed: 0, #pkts decompress failed: 0
  #send errors 0, #recv errors 0

local crypto endpt.: 192.168.1.2, remote crypto endpt.: 201.1.1.2
plaintext mtu 1422, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current outbound spi: 0x853C02(8731650)
PFS (Y/N): N, DH group: none

inbound esp sas:
  spi: 0x41AA84F4(1101694196)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel UDP-Encaps, }
    conn id: 2006, flow_id: Onboard VPN:6, sibling_flags 80000040, crypto map: vpn
    sa timing: remaining key lifetime (k/sec): (4263591/2510)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
  spi: 0x853C02(8731650)
    transform: esp-aes esp-sha-hmac ,
    in use settings ={Tunnel UDP-Encaps, }
    conn id: 2005, flow_id: Onboard VPN:5, sibling_flags 80000040, crypto map: vpn
    sa timing: remaining key lifetime (k/sec): (4263591/2510)
    IV size: 16 bytes
    replay detection support: Y
    Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
```


Dynamische router (met Remote Dynamic ASA)

- Dit is het resultaat van de `show crypto IKEv2` als detail opdracht:

```
C1941#show cry ikev2 sa detailed
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
1 192.168.1.2/4500 201.1.1.2/4500 none/none READY
Encr: 3DES, Hash: SHA96, DH Grp:2, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/1516 sec
CE id: 1034, Session-id: 24
Status Description: Negotiation done
Local spi: 98322AED6163EE83 Remote spi: 092A1E5620F6AA9C
Local id: S2S-IKEv2
Remote id: asa5510.test.com
Local req msg id: 2 Remote req msg id: 73
Local next msg id: 2 Remote next msg id: 73
Local req queued: 2 Remote req queued: 73
Local window: 5 Remote window: 1
DPD configured for 0 seconds, retry 0
Fragmentation not configured.
Extended Authentication not configured.
NAT-T is detected inside
Cisco Trust Security SGT is disabled
Initiator of SA : Yes

IPv6 Crypto IKEv2 SA
```

Opmerking: De afstandsbediening en lokale ID in deze uitvoer is de **genoemde tunnelgroep** die u op de ASA definieerde om te controleren of u op de juiste tunnelgroep valt. Dit kan ook worden geverifieerd als u IKEv2 aan beide zijden reinigt.

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

De Output Interpreter Tool (alleen voor geregistreeerde klanten) ondersteunt bepaalde opdrachten met `show`. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht `show`.

Opmerking: Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met debug opgeeft.

Gebruik in de Cisco IOS-router:

```
deb crypto ikev2 error
deb crypto ikev2 packet
deb crypto ikev2 internal
```

Gebruik voor de ASA:

```
deb crypto ikev2 protocol
deb crypto ikev2 platform
```