# Migreren van op beleid gebaseerde Crypto Tunnel naar routegebaseerde Crypto Tunnel op ASA

## Inhoud



## Inleiding

Dit document beschrijft de migratie van op beleid gebaseerde tunnels naar op route gebaseerde tunnels op ASA.

## Voorwaarden

### Vereisten

Cisco raadt u aan deze onderwerpen te kennen:

- Basiskennis van IKEv2-IPSec VPN-concepten.
- Kennis van IPSec VPN op ASA en de configuratie ervan.

### Gebruikte componenten

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

- Cisco ASA: ASA-codeversie 9.8(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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

# Configureren

## Stappen voor migratie:

1. Bestaande op beleid gebaseerde VPN-configuratie verwijderen
2. IPsec-profiel configureren
3. Virtual Tunnel Interface (VTI) configureren
4. Statische routing of dynamisch routingprotocol configureren

## Configuraties

Bestaande op beleid gebaseerde tunnel:

1. Interfaceconfiguratie:

Uitgaande interface waar de cryptokaart gebonden is.

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.10.10.10 255.255.255.0
```

2. IKEv2-beleid:

Het definieert de parameters voor fase 1 van het IPsec-onderhandelingsproces.

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
```

3. Tunnelgroep:

Het definieert parameters voor VPN-verbindingen. Tunnelgroepen zijn essentieel voor het configureren van site-to-site VPN's, omdat ze informatie bevatten over de peer, verificatiemethoden en verschillende verbindingsparameters.

```
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
```

4. Crypto ACL:

Het bepaalt het verkeer dat versleuteld en door de tunnel gestuurd moet worden.

```
object-group network local-network
 network-object 192.168.0.0 255.255.255.0
object-group network remote-network
 network-object 172.16.10.0 255.255.255.0

access-list asa-vpn extended permit ip object-group local-network object-group remote-network
```

5. Crypto IPSec-voorstel:

Het definieert het IPsec-voorstel, dat de coderings- en integriteitsalgoritmen voor fase 2 van de IPsec-onderhandeling specificeert.

```
crypto ipsec ikev2 ipsec-proposal IKEV2_TSET
 protocol esp encryption aes-256
 protocol esp integrity sha-256
```

6. Crypto Map Config:

Het definieert het beleid voor IPsec VPN-verbindingen, inclusief het verkeer dat versleuteld moet worden, de peers en het ipsec-voorstel dat eerder is geconfigureerd. Het is ook gebonden aan de interface die het VPN-verkeer verwerkt.

```
crypto map outside_map 10 match address asa-vpn
crypto map outside_map 10 set peer 10.20.20.20
crypto map outside_map 10 set ikev2 ipsec-proposal IKEV2_TSET

crypto map outside_map interface outside
```

Migratie van beleidstunnels naar routecontracten:

1. Bestaande op beleid gebaseerde VPN-configuratie verwijderen:
   Verwijder eerst de bestaande, op beleid gebaseerde VPN-configuratie. Dit omvat de crypto-kaartvermeldingen voor die peer, ACL's en alle bijbehorende instellingen.

```
no crypto map outside_map 10 match address asa-vpn
no crypto map outside_map 10 set peer 10.20.20.20
no crypto map outside_map 10 set ikev2 ipsec-proposal IKEV2_TSET
```

2. IPsec-profiel configureren:
   Definieer een IPsec-profiel met de bestaande IKEv2 ipsec-voorstel of transformatie-set.

```
crypto ipsec profile PROPOSAL_IKEV2_TSET
 set ikev2 ipsec-proposal IKEV2_TSET
```

3. Configureer de Virtual Tunnel Interface (VTI):
   Maak een Virtual Tunnel Interface (VTI) en pas het IPsec-profiel erop toe.

```
interface Tunnel1
 nameif VPN-BRANCH
 ip address 10.1.1.2 255.255.255.252
 tunnel source interface outside
 tunnel destination 10.20.20.20
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile PROPOSAL_IKEV2_TSET
```

4. Configuratie van statische routing of dynamisch routingprotocol:
   Voeg statische routes toe of vorm een dynamisch routeringsprotocol om verkeer door de tunnelinterface te leiden. In dit scenario maken we gebruik van statische routing.

   Statische routing:

```
route VPN-BRANCH 172.16.10.0 255.255.255.0 10.1.1.10
```

# Verifiëren

Na het migreren van een op beleid gebaseerde VPN naar een route gebaseerde VPN met Virtual

Tunnel Interfaces (VTI's) op een Cisco ASA, is het cruciaal om te verifiëren dat de tunnel correct is geïnstalleerd en werkt. Hier zijn verschillende stappen en opdrachten die u kunt gebruiken om de status te verifiëren en indien nodig problemen op te lossen.

1. Controleer de tunnelinterface
Controleer de status van de tunnelinterface om er zeker van te zijn dat deze is ingesteld.

<#root>

```
ciscoasa# show interface Tunnel1

Interface Tunnel1 "VPN-BRANCH", is up, line protocol is up

Hardware is Virtual Tunnel Interface
Description: IPsec VPN Tunnel to Remote Site
Internet address is
10.1.1.2/24

MTU 1500 bytes, BW 10000 Kbit/sec, DLY 500000 usec
65535 packets input, 4553623 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
65535 packets output, 4553623 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 late collisions, 0 deferred
0 input reset drops, 0 output reset drops
Tunnel source 10.10.10.10, destination 10.20.20.20

Tunnel protocol/transport IPSEC/IP
Tunnel protection
IPsec profile PROPOSAL_IKEV2_TSET
```

Deze opdracht geeft informatie over de tunnelinterface, waaronder de operationele status, IP-adres en tunnelbron/bestemming. Zoek deze indicatielampjes:
· De interfacestatus is omhoog.
· De status van het lijnprotocol is omhoog.

2. Controleer IPsec Security Associations (SA's)

Controleer de status van de IPsec SA's om er zeker van te zijn dat de tunnel succesvol is onderhandeld.

<#root>

```
ciscoasa# show crypto ipsec sa

interface: Tunnel1
Crypto map tag: Tunnel1-head-0, seq num: 1, local addr:

10.10.10.10



local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer:

10.20.20.20



#pkts encaps: 1000, #pkts encrypt: 1000, #pkts digest: 1000



#pkts decaps: 1000, #pkts decrypt: 1000, #pkts verify: 1000


#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 1000, #pkts compr. failed: 0, #pkts decompress failed: 0

local crypto endpt.:

10.10.10.10

/500, remote crypto endpt.:

10.20.20.20

/500
path mtu 1500, ipsec overhead 74, media mtu 1500
current outbound spi: 0xC0A80101(3232235777)
current inbound spi : 0xC0A80102(3232235778)


inbound esp sas:



spi: 0xC0A80102(3232235778)


transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={Tunnel, }
slot: 0, conn id: 2001, flow_id: CSR:1, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (kB/sec): (4608000/3540)
IV size: 16 bytes
replay detection support: Y

Status: ACTIVE



outbound esp sas:



spi: 0xC0A80101(3232235777)
```

```
transform: esp-aes-256 esp-sha-256-hmac no compression
in use settings ={Tunnel, }
slot: 0, conn id: 2002, flow_id: CSR:2, crypto map: Tunnel1-head-0
sa timing: remaining key lifetime (kB/sec): (4608000/3540)
IV size: 16 bytes
replay detection support: Y
```

**Status: ACTIVE**

Deze opdracht geeft de status weer van de IPsec SA's, inclusief tellers voor ingekapselde en gedecapsuleerde pakketten. Zorg ervoor dat:
· Er zijn actieve SA's voor de tunnel.
· De inkapselings- en decapsulatietellers worden steeds hoger, wat op de doorstroming van het verkeer wijst.

Voor meer gedetailleerde informatie kunt u gebruik maken van:

<#root>

```
ciscoasa# show crypto ikev2 sa

IKEv2 SAs:
```

**Session-id:2, Status:UP-ACTIVE**

```
, IKE count:1, CHILD count:1

Tunnel-id Local Remote Status Role
3363898555
```

**10.10.10.10/500 10.20.20.20/500 READY INITIATOR**

```
Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:20, Auth sign: PSK, Auth verify: PSK
Life/Active Time: 86400/259 sec
```

Deze opdracht toont de status van de IKEv2 SA's, die zich in de Ready-status bevindt.

3. Controleer de routing
Controleer de routeringstabel om er zeker van te zijn dat de routes door de tunnelinterface worden gericht.

<#root>

```
ciscoasa# show route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF Intra, IA - OSPF Inter, E1 - OSPF External Type 1
```

```
E2 - OSPF External Type 2, N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2
i - IS-IS, su - IS-IS summary null, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route, H - NHRP, l - LISP
+ - replicated route, % - next hop override

S 0.0.0.0 0.0.0.0 [1/0] via 203.0.113.2, outside

C 10.1.1.0 255.255.255.0 is directly connected, Tunnel1


S 172.16.10.0 255.255.255.0 [1/0] via 10.1.1.10, Tunnel1
```

Zoek routes die door de tunnelinterface worden geleid.

# Problemen oplossen

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

1. Controleer de routeconfiguratie van de ASA.

2. Om problemen op te lossen in de IKEv2-tunnel, kunt u deze debugs gebruiken:

```
debug crypto condition peer <peer IP address>
debug crypto ikev2 platform 255
debug crypto ikev2 protocol 255
debug crypto ipsec 255
```

3. Om de verkeerskwestie op de ASA op te lossen, neemt u pakketopname en controleert u de configuratie.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.