Een site-to-site IKEv2-tunnel tussen twee ASA's configureren met behulp van meerdere IKEv2-toetsuitwisselingen

Inhoud

Inleiding

Dit document beschrijft hoe u een site-to-site IKEv2 VPN-verbinding tussen twee Cisco ASA's kunt configureren met behulp van Meervoudige IKEv2-toetsuitwisselingen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco adaptieve security applicatie (ASA)

- Algemene IKEv2-concepten

Gebruikte componenten

De informatie in dit document is gebaseerd op de Cisco ASA's waarop 9.20.1 wordt uitgevoerd.

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.

Beperkingen

De Meervoudige Key Exchange IKEv2 heeft deze beperkingen:

- Alleen ondersteund op de ASA CLI
- Ondersteund op multi-context en HA-apparaten
- Niet ondersteund op geclusterde apparaten

Licentie

De licentievereisten zijn hetzelfde als voor Site-to-Site VPN op de ASA’s.

Achtergrondinformatie

Noodzaak van extra toetsuitwisselingen

De komst van grote quantumcomputers vormt een groot risico voor beveiligingssystemen, vooral voor die systemen die gebruikmaken van public-key cryptografie. Cryptografische methoden die als zeer moeilijk werden beschouwd voor reguliere computers kunnen gemakkelijk worden gebroken door kwantumcomputers. Dus de noodzaak ontstaat om te switches naar nieuwe kwantumresistente methoden, ook wel post-kwantumcryptografie (PQC) algoritmen genoemd. Het doel is de beveiliging van IPsec-communicatie te verbeteren door gebruik te maken van meerdere toetsuitwisselingen. Het gaat erom een traditionele sleuteluitwisseling te combineren met een post-quantum-uitwisseling. Deze benadering zorgt ervoor dat de resulterende uitwisseling minstens zo sterk is als de traditionele sleuteluitwisseling, wat een extra beveiligingslaag biedt.

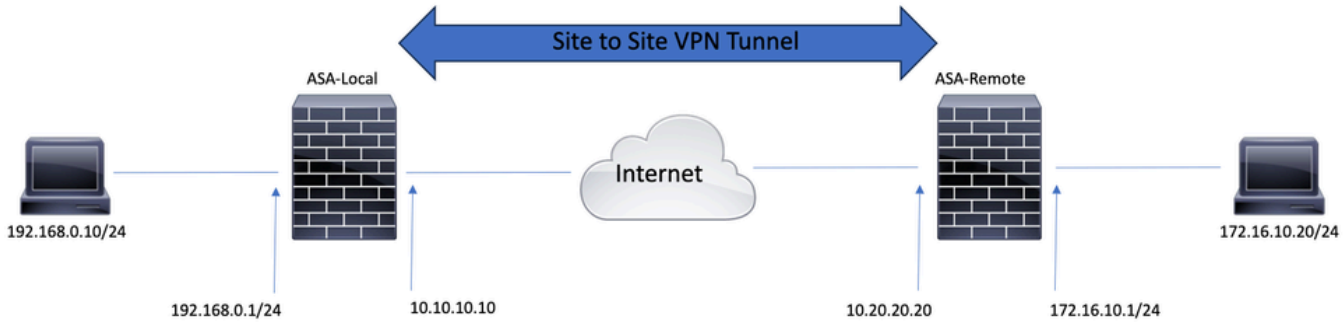
Het plan is om IKEv2 te verbeteren door ondersteuning toe te voegen voor meerdere sleuteluitwisselingen. Deze extra sleuteluitwisselingen kunnen omgaan met algoritmen die veilig zijn voor quantumbedreigingen. Om informatie over deze extra sleutels uit te wisselen, wordt een nieuw berichttype met de naam Intermediate Exchange geïntroduceerd. Deze belangrijke uitwisselingen worden onderhandeld met behulp van de reguliere IKEv2 methode, via de SA payload.

Configureren

In dit deel worden de ASA-configuraties beschreven.

Netwerkdiagram

Voor de informatie in dit document wordt gebruik gemaakt van deze netwerkinstelling:

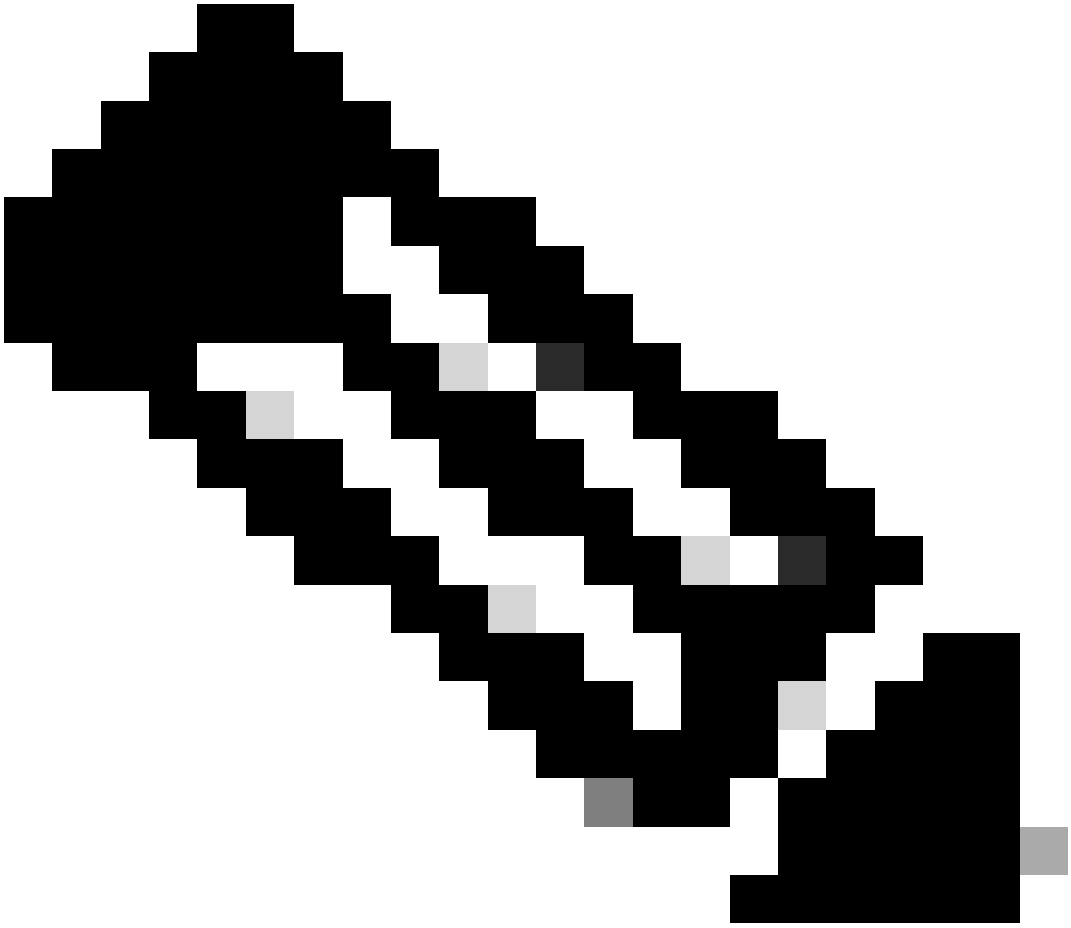


ASA-configuratie

De ASA-interfaces configureren

Als de ASA interfaces niet geconfigureerd zijn, zorg er dan voor dat u ten minste de IP-adressen, interfacenamen en beveiligingsniveaus configureert:

```
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.10.10.10 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
```



Opmerking: Zorg ervoor dat er connectiviteit is met zowel de interne als externe netwerken, vooral met de externe peer die wordt gebruikt om een site-to-site VPN-tunnel te maken. U kunt gebruiken pingelt om basisconnectiviteit te verifiëren.

Configureer het IKEv2-beleid met meerdere toetsuitwisseling en schakel IKEv2 in op de buiteninterface

Typ de volgende opdrachten om het IKEv2-beleid voor deze verbindingen te configureren:

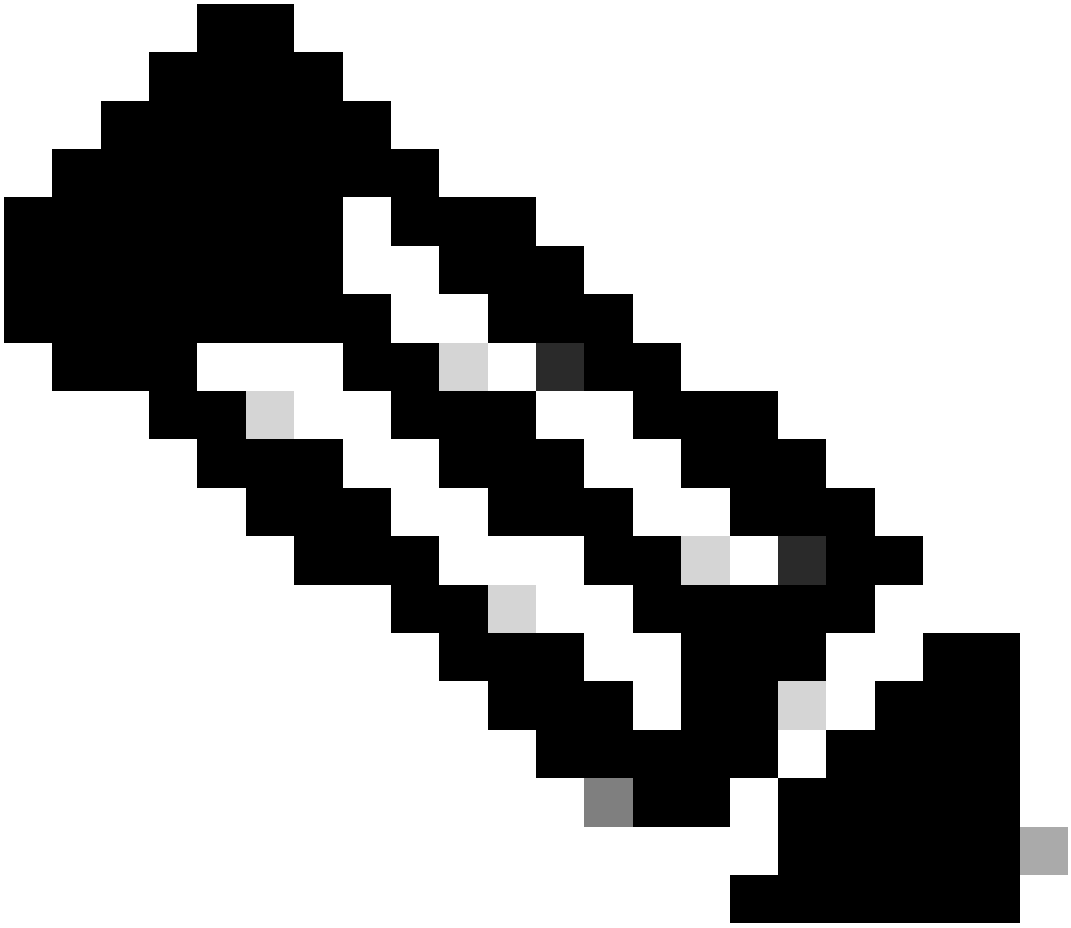
```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
```

Extra toetsuitwisselingstransformaties kunnen worden geconfigureerd onder crypto ikev2 policy het additional-key-exchange commando. In totaal kunnen zeven extra wisseltransformaties worden geconfigureerd. In dit voorbeeld zijn twee extra wisseltransformaties geconfigureerd (met DH-groepen 21 en 31).

```
additional-key-exchange 1 key-exchange-method 21 additional-key-exchange 2 key-exchange-method 31
```

Het definitieve IKEv2-beleid ziet er als volgt uit:

```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
 additional-key-exchange 1
  key-exchange-method 21
 additional-key-exchange 2
  key-exchange-method 31
```



Opmerking: er bestaat een IKEv2-beleidsovereenkomst wanneer beide beleidsregels van de twee peers dezelfde authenticatie, encryptie, hash, Diffie-Hellman parameter en additionele Key Exchange parameterwaarden bevatten.

U moet IKEv2 inschakelen op de interface die de VPN-tunnel beëindigt. Meestal is dit de externe (of internet) interface. Om IKEv2 in te schakelen, voert u de opdracht in in de globale configuratiemoduscrypto ikev2 enable outside.

De tunnelgroep configureren

Voor een Site-to-Site-tunnel is het type verbindingsprofiel IPSec-l2l. Om de IKEv2 preshared sleutel te configureren voert u de volgende

opdrachten in:

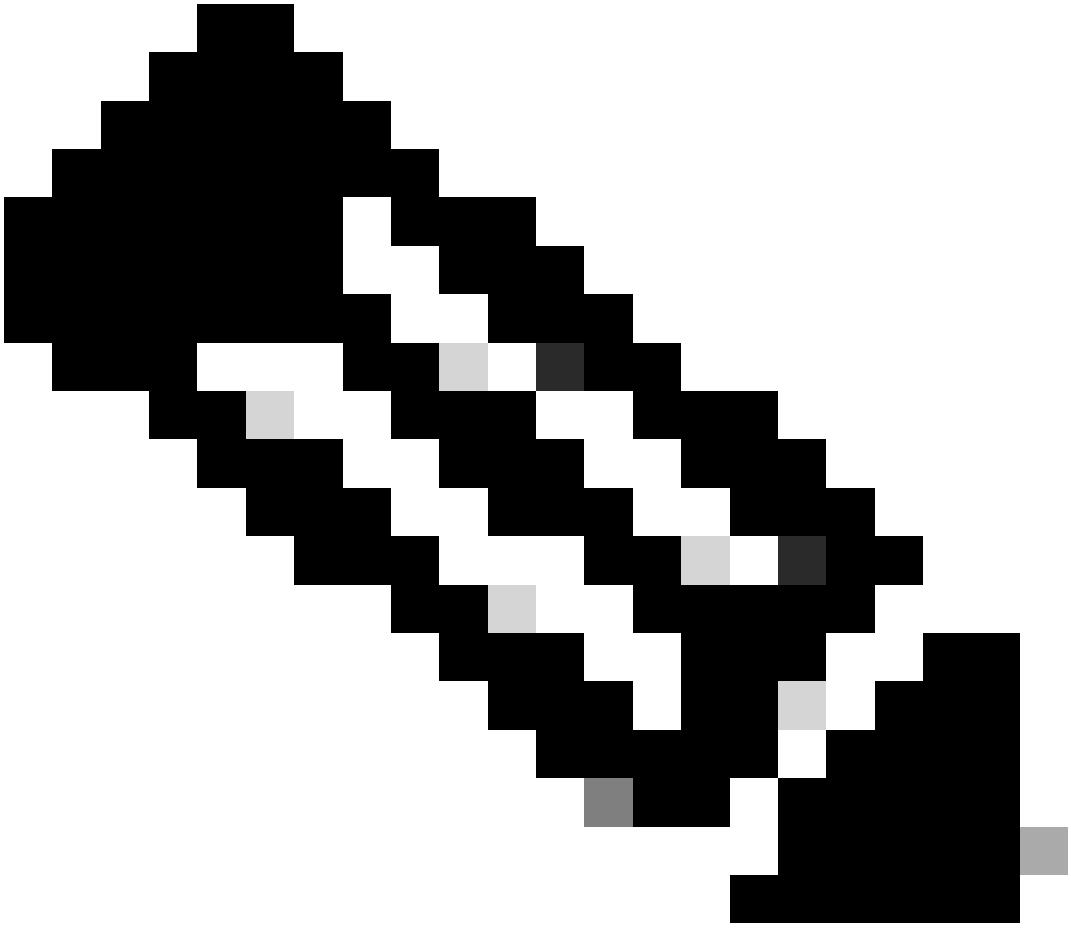
```
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
```

Interessant verkeer en crypto ACL configureren

ASA gebruikt ACL's (Access Control Lists) om het verkeer dat met IPSec-encryptie moet worden beveiligd, te onderscheiden van het verkeer dat geen bescherming nodig heeft. Het beschermt de uitgaande pakketten die overeenkomen met een licentie Application Control Engine (ACE) en zorgt ervoor dat de inkomende pakketten die overeenkomen met een licentie ACE bescherming hebben.

```
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
```



Opmerking: de VPN-peer moet dezelfde ACL in een gespiegeld formaat hebben.

Een Identity NAT configureren (optioneel)

Typisch, is een identiteit NAT nodig om het interessante verkeer te verhinderen dynamische NAT te raken. De Identity NAT die in dit geval is geconfigureerd is:

nat (inside,outside) source static local-network local-network destination static remote-network remote-network no-proxy-arp route-lookup

Het IKEv2 IPSec-voorstel configureren

Het IKEv2 IPSec-voorstel wordt gebruikt om een reeks coderings- en integriteitsalgoritmen te definiëren om het gegevensverkeer te beschermen. Dit voorstel moet overeenkomen met beide VPN-peers om met succes een IPSec SA te kunnen bouwen. De in dit geval gebruikte opdrachten zijn:

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

Configureer een Crypto-kaart en bind deze aan de interface

Een crypto-kaart combineert alle vereiste configuraties en moet noodzakelijkerwijs bevatten:

- Een toegangslijst om het verkeer aan te passen dat moet worden versleuteld (meestal Crypto ACL genoemd)
- Identificatie van peer
- Ten minste één IKEv2 IPSec-voorstel

De hier gebruikte configuratie is:

crypto map outside_map 1 match address asa-vpn crypto map outside_map 1 set peer 10.20.20.20 crypto map outside_map 1 set ikev2 ipsec-proposal IKEV

Het laatste deel past deze crypto kaart toe op de buiten (openbare) interface met behulp van de opdrachtcrypto map outside_map interface outside.

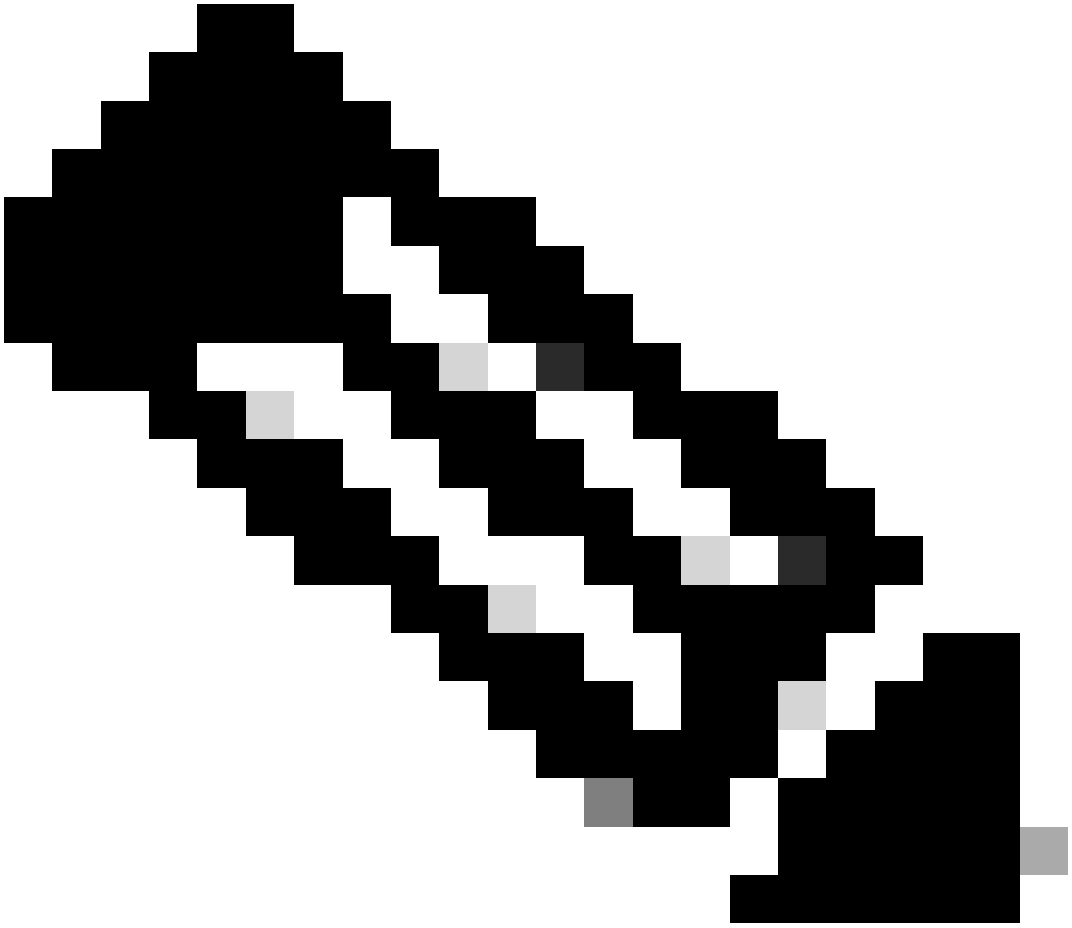
Laatste configuratie voor lokale ASA

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.10.10.10 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
```

```
 ip address 192.168.0.1 255.255.255.0
!
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
 additional-key-exchange 1
  key-exchange-method 21
 additional-key-exchange 2
  key-exchange-method 31
!
crypto ikev2 enable outside
!
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
!
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
!
nat (inside,outside) source static local-network local-network destination static remote-network remote-network no-proxy-arp route-lookup
!
crypto ipsec ikev2 ipsec-proposal IKEV2_TSET
 protocol esp encryption aes-256
 protocol esp integrity sha-256
!
crypto map outside_map 1 match address asa-vpn
crypto map outside_map 1 set peer 10.20.20.20
crypto map outside_map 1 set ikev2 ipsec-proposal IKEV2_TSET
!
crypto map outside_map interface outside
```

Definitieve configuratie van Remote ASA

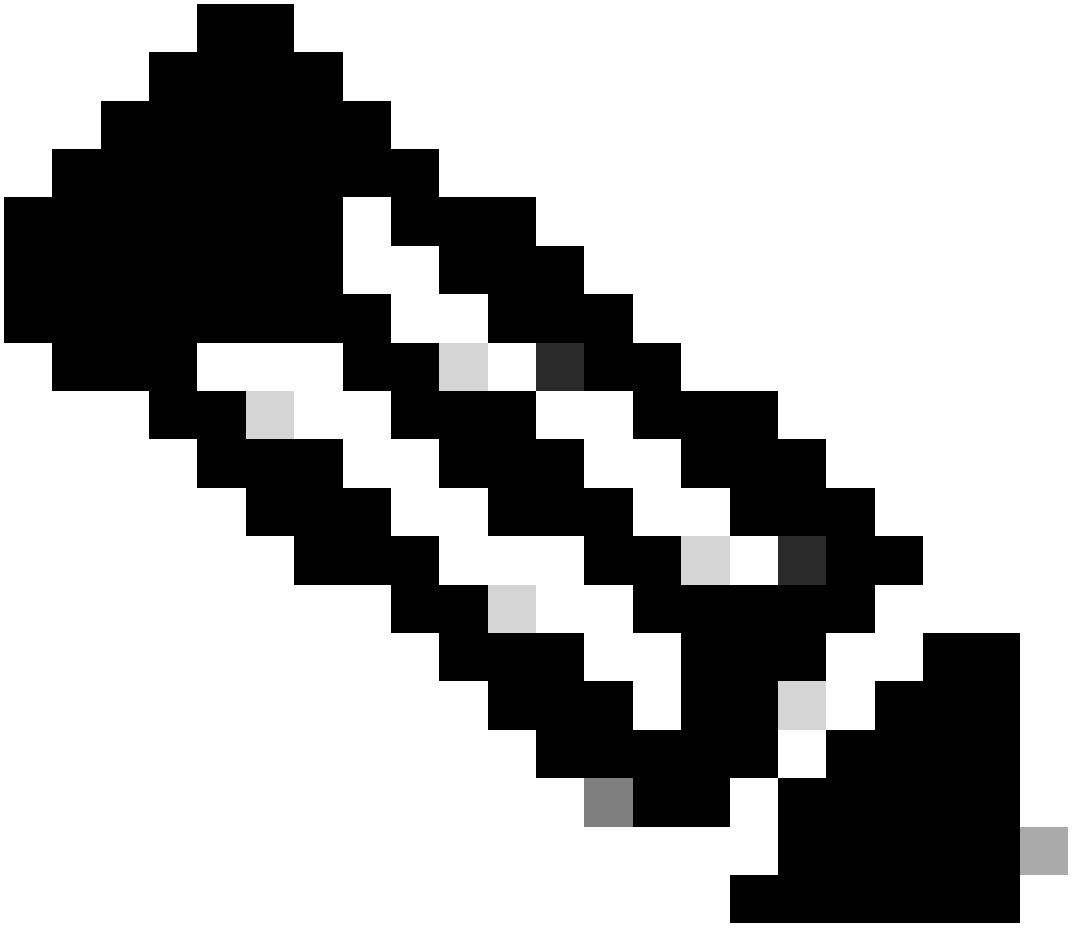
```
interface GigabitEthernet0/0 nameif outside security-level 0 ip address 10.20.20.20 255.255.255.0 ! interface GigabitEthernet0/1 nameif inside security-lev
```



Opmerking: de ACL heeft de gespiegelde indeling en de vooraf gedeelde sleutels zijn aan beide uiteinden hetzelfde.

Verifiëren

Alvorens u verifieert als de tunnel omhoog is en dat het het verkeer overgaat, moet u ervoor zorgen dat het interessante verkeer naar ASAs wordt verzonden.



Opmerking: de pakkettracer is gebruikt om de verkeersstroom te simuleren. Het kan worden gedaan met behulp van de Packet-tracer opdracht; packet-tracer input inside icmp 192.168.0.11 8 0 172.16.10.11 gedetailleerd op de Local-ASA.

Om de extra toetsuitwisselingen te valideren, kunt u de opdracht gebruikenshow crypto ikev2 sa. Zoals te zien in de output, kunt u de parameters van AKE controleren om de geselecteerde uitwisselingsalgoritmen te bevestigen.

<#root>

Local-ASA# show crypto ikev2 sa IKEv2 SAs: Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1 Tunnel-id Local Remote fvrf/ivrf Status R

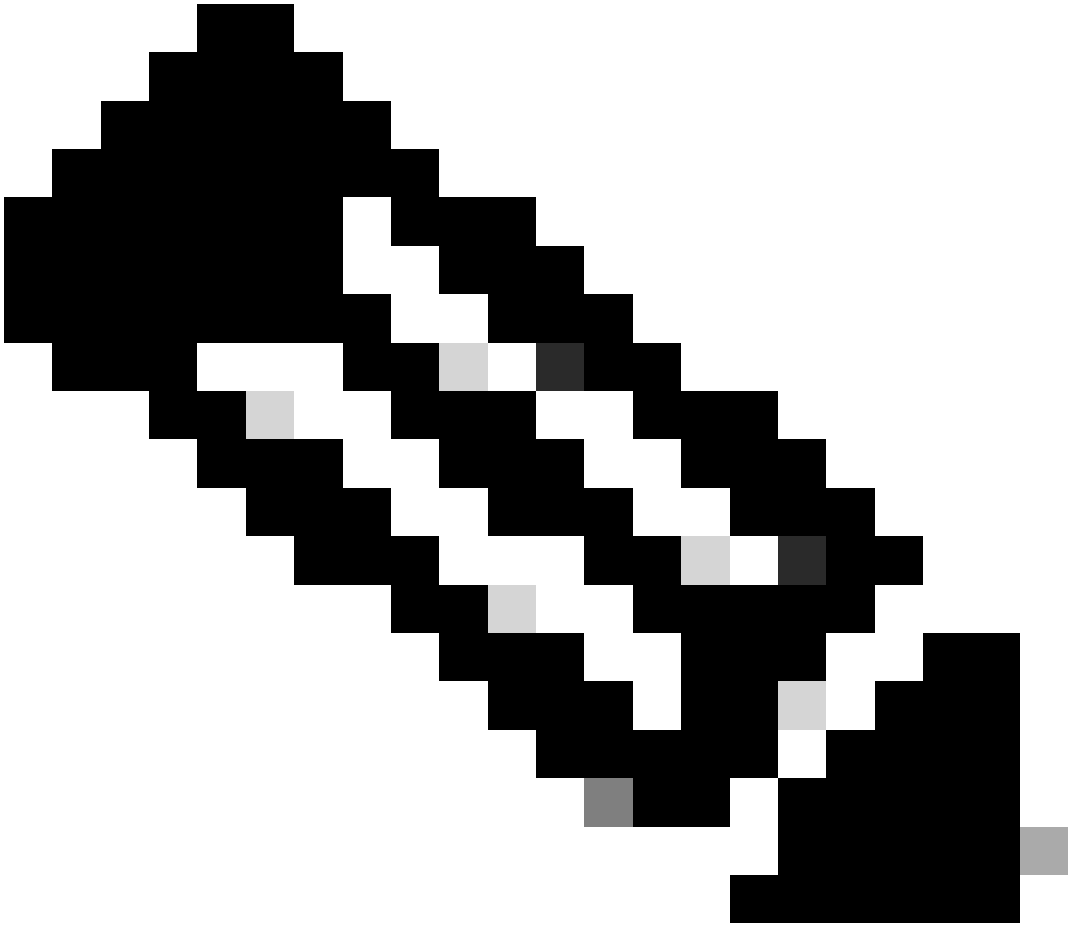
AKE1: 21 AKE2: 31

```
 Life/Active Time: 86400/7 sec Child sa: local selector 192.168.0.0/0 - 192.168.0.255/65535 remote sele
```

Problemen oplossen

De genoemde debugs kunnen gebruikt worden om problemen op te lossen in de IKEv2 tunnel:

debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127



Opmerking: als u slechts één tunnel wilt oplossen (wat het geval moet zijn als het apparaat in productie is), moet u debugs voorwaardelijk inschakelen met de debug crypto-voorwaarde peer X.X.X.X opdracht.

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.