Konfigurieren eines standortübergreifenden IKEv2-Tunnels zwischen zwei ASAs mithilfe von IKEv2 Multiple Key Exchange

Inhalt

Einleitung

In diesem Dokument wird die Konfiguration einer standortübergreifenden IKEv2-VPN-Verbindung zwischen zwei Cisco ASAs mithilfe von IKEv2 Multiple Key Exchanges beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Adaptive Security Appliance (ASA)

- Allgemeine IKEv2-Konzepte

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den Cisco ASAs mit Version 9.20.1.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Einschränkungen

Für IKEv2 Multiple Key Exchange gelten folgende Einschränkungen:

- Wird nur von der ASA CLI unterstützt
- Unterstützt auf Multi-Context- und HA-Geräten
- Nicht unterstützt auf geclusterten Geräten

Lizenzierung

Die Lizenzierungsanforderungen entsprechen denen für Site-to-Site-VPN auf den ASAs.

Hintergrundinformationen

Bedarf an zusätzlichen Schlüsselaustausch

Die Ankunft großer Quantencomputer stellt ein großes Risiko für Sicherheitssysteme dar, insbesondere für solche, die Kryptografie mit öffentlichem Schlüssel verwenden. Kryptographische Methoden, die für normale Computer als sehr schwierig galten, können von Quantencomputern leicht unterbrochen werden. Es besteht also die Notwendigkeit, auf neue quantenresistente Methoden umzusteigen, die auch als PQC-Algorithmen (Post-Quantum Cryptography) bezeichnet werden. Ziel ist es, die Sicherheit der IPsec-Kommunikation durch den Einsatz von mehreren Schlüsselaustauschverbindungen zu erhöhen. Dabei wird ein traditioneller Schlüsselaustausch mit einem Post-Quanten-Austausch kombiniert. Dieser Ansatz stellt sicher, dass der resultierende Austausch mindestens so stark ist wie der herkömmliche Schlüsselaustausch und eine zusätzliche Sicherheitsebene bietet.

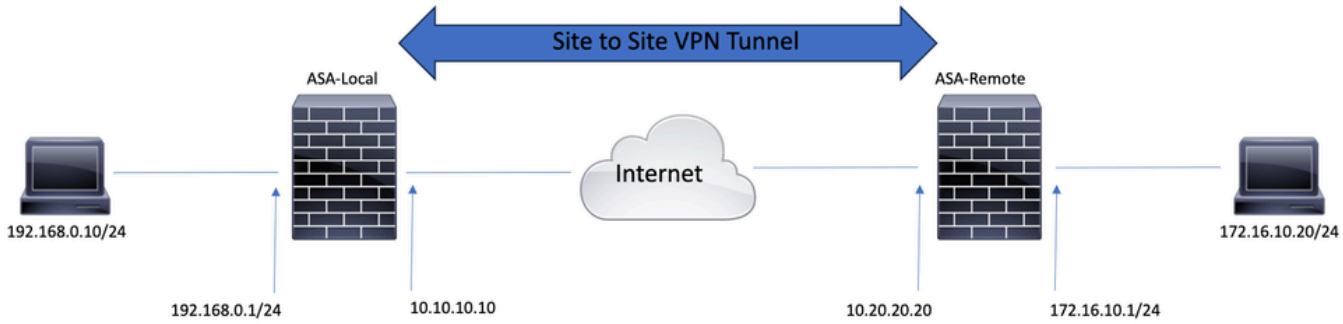
Geplant ist eine Verbesserung von IKEv2 durch die Unterstützung mehrerer Schlüsselaustausch. Diese zusätzlichen Schlüsselaustausch können Algorithmen verarbeiten, die vor Quantenbedrohungen sicher sind. Um Informationen über diese zusätzlichen Schlüssel auszutauschen, wird ein neuer Nachrichtentyp namens Intermediate Exchange eingeführt. Diese Schlüsselaustauschverbindungen werden mithilfe der regulären IKEv2-Methode und der SA-Payload ausgehandelt.

Konfigurieren

In diesem Abschnitt werden die ASA-Konfigurationen beschrieben.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:

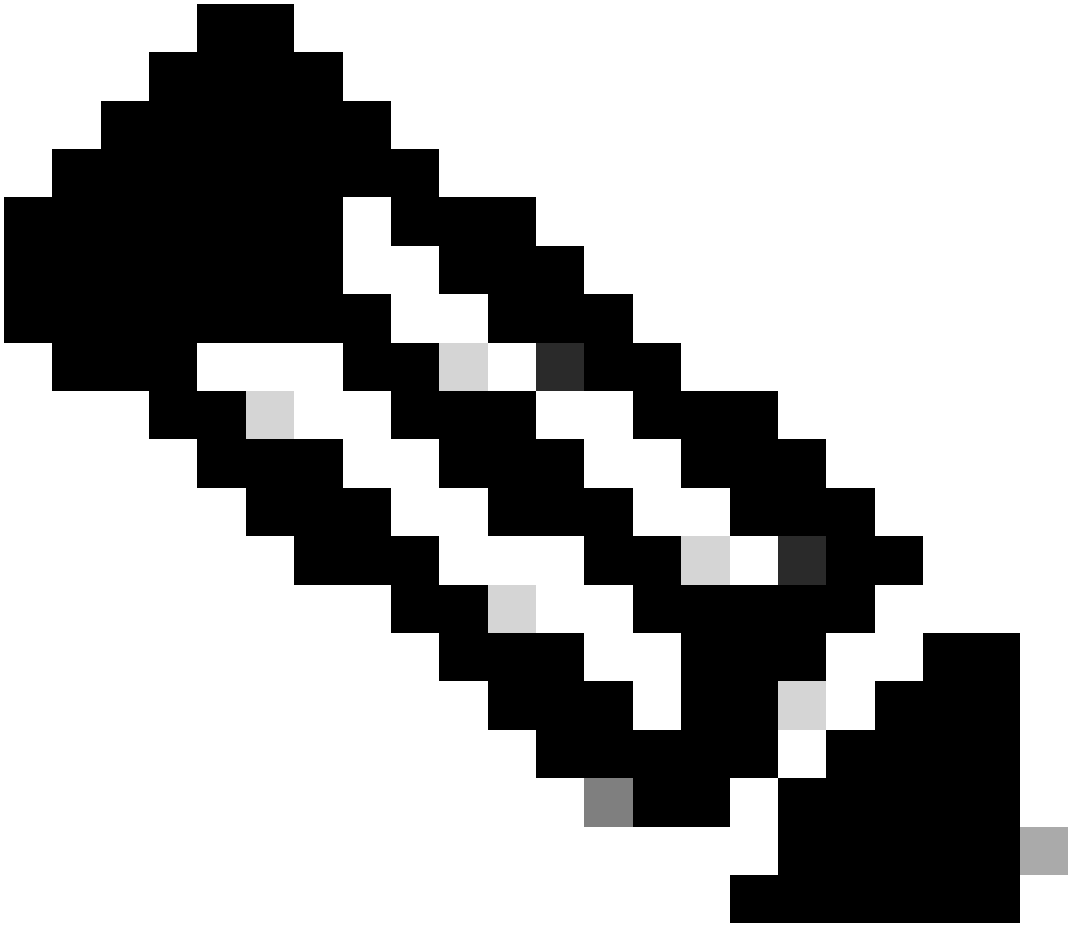


ASA-Konfiguration

ASA-Schnittstellen konfigurieren

Wenn die ASA-Schnittstellen nicht konfiguriert sind, stellen Sie sicher, dass Sie mindestens die IP-Adressen, Schnittstellennamen und Sicherheitsstufen konfigurieren:

```
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
```



Hinweis: Stellen Sie sicher, dass sowohl das interne als auch das externe Netzwerk, insbesondere der Remote-Peer, mit dem ein Site-to-Site-VPN-Tunnel eingerichtet wird, verbunden sind. Sie können einen Ping verwenden, um die grundlegenden Netzwerkverbindungen zu überprüfen.

Konfigurieren der IKEv2-Richtlinie mit Austausch mehrerer Schlüssel und Aktivieren von IKEv2 auf der externen Schnittstelle

Um die IKEv2-Richtlinien für diese Verbindungen zu konfigurieren, geben Sie die folgenden Befehle ein:

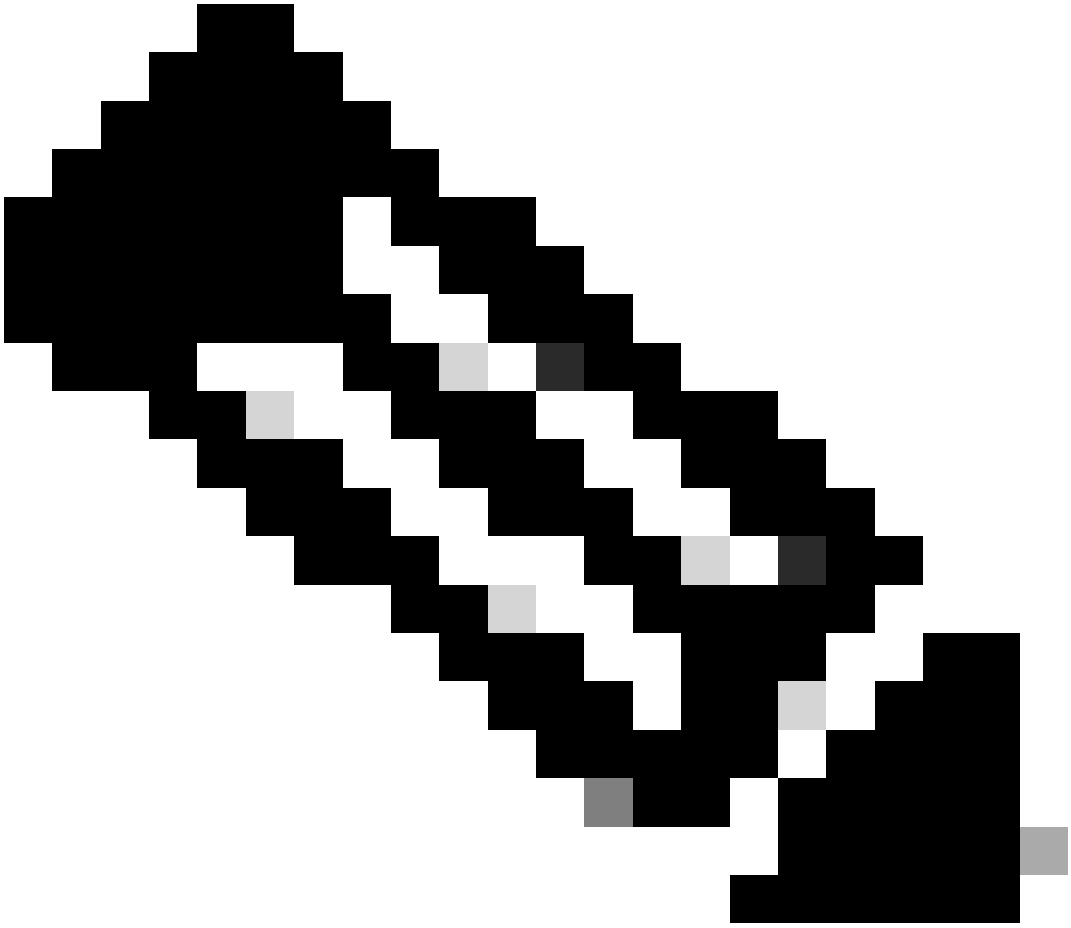
```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
```

Weitere Transformationen für den Schlüsselaustausch können unter crypto ikev2 policy mit dem additional-key-exchange Befehl konfiguriert werden. Insgesamt können sieben zusätzliche Exchange-Transformationen konfiguriert werden. In diesem Beispiel sind zwei weitere Austauschtransformationen konfiguriert (unter Verwendung der DH-Gruppen 21 und 31).

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

Die endgültige IKEv2-Richtlinie sieht wie folgt aus:

```
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
```



Hinweis: Eine IKEv2-Richtlinienübereinstimmung ist vorhanden, wenn beide Richtlinien der beiden Peers dieselben Werte für Authentifizierung, Verschlüsselung, Hash, Diffie-Hellman-Parameter und Zusätzliche Schlüsselaustausch-Parameter enthalten.

Sie müssen IKEv2 auf der Schnittstelle aktivieren, die den VPN-Tunnel terminiert. Normalerweise ist dies die externe (oder Internet-) Schnittstelle. Um IKEv2 zu aktivieren, geben Sie den crypto ikev2 enable outside Befehl im globalen Konfigurationsmodus ein.

Konfigurieren der Tunnelgruppe

Bei einem Site-to-Site-Tunnel ist der Verbindungsprofiltyp IPSec-l2l. Um den IKEv2 Pre-Shared Key zu konfigurieren, geben Sie die folgenden

Befehle ein:

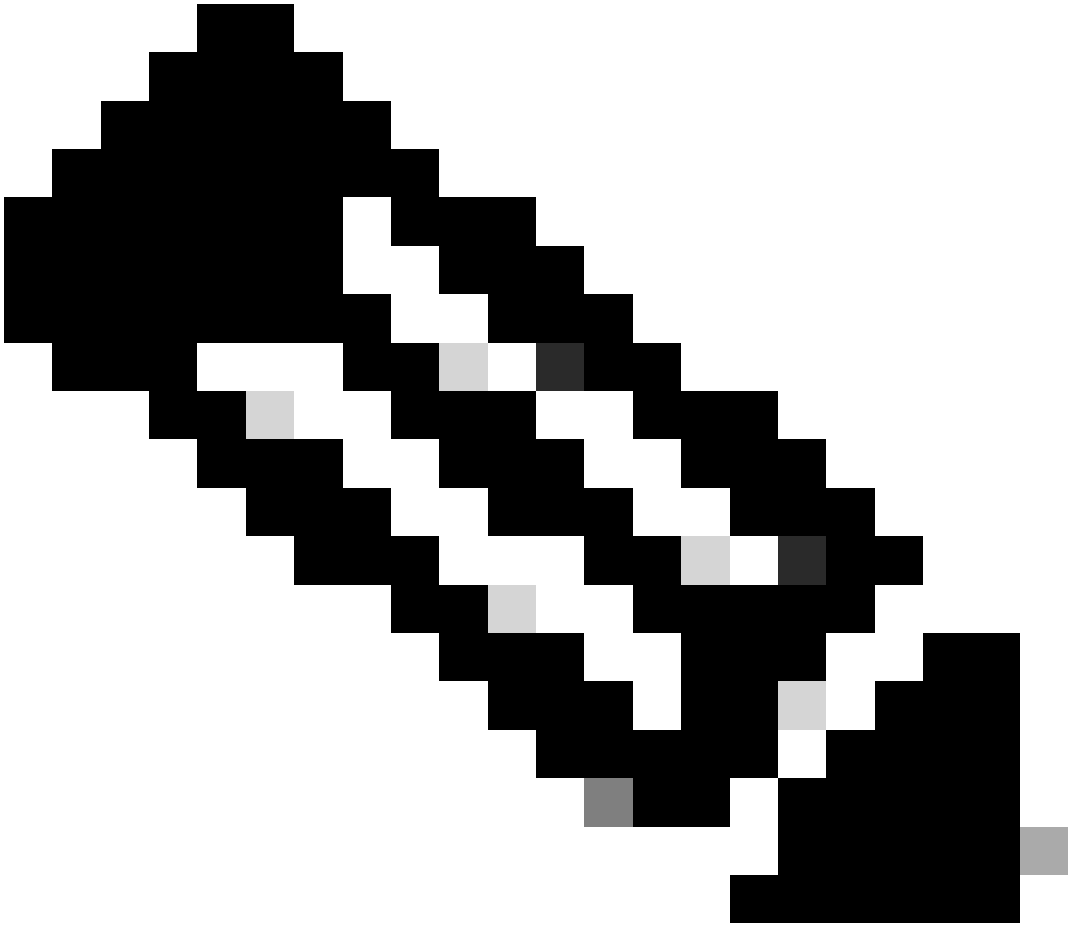
```
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
```

Konfigurieren von interessantem Datenverkehr und Krypto-ACL

Die ASA verwendet Zugriffskontrolllisten (Access Control Lists, ACLs), um den mit IPSec-Verschlüsselung zu schützenden Datenverkehr von dem Datenverkehr zu unterscheiden, der nicht geschützt werden muss. Es schützt die ausgehenden Pakete, die durch eine Application Control Engine (ACE) zugelassen werden, und stellt sicher, dass die eingehenden Pakete geschützt sind, die durch eine ACE zugelassen werden.

```
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
```



Hinweis: Der VPN-Peer muss über dieselbe ACL in einem gespiegelten Format verfügen.

Konfigurieren einer Identitäts-NAT (optional)

In der Regel wird eine Identitäts-NAT benötigt, um zu verhindern, dass der interessante Datenverkehr die dynamische NAT erreicht. Die in diesem Fall konfigurierte Identitäts-NAT lautet:

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

Konfigurieren des IKEv2-IPSec-Angebots

Der IKEv2 IPSec-Vorschlag dient zum Definieren einer Reihe von Verschlüsselungs- und Integritätsalgorithmen, um den Datenverkehr zu schützen. Dieses Angebot muss mit beiden VPN-Peers übereinstimmen, damit eine IPSec-Sicherheitszuordnung erfolgreich erstellt werden kann. In diesem Fall werden die folgenden Befehle verwendet:

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

Konfigurieren einer Kryptografiezuordnung und Anbinden der Schnittstelle

Eine Crypto Map kombiniert alle erforderlichen Konfigurationen und muss Folgendes enthalten:

- Eine Zugriffsliste, die mit dem zu verschlüsselnden Datenverkehr übereinstimmt (allgemein als Crypto ACL bezeichnet).
- Peer-Identifizierung
- Mindestens ein IKEv2 IPSec-Angebot

Die hier verwendete Konfiguration ist:

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

Der letzte Teil besteht darin, diese Crypto Map mithilfe des crypto map outside_map interface outside Befehls auf die externe (öffentliche) Schnittstelle anzuwenden.

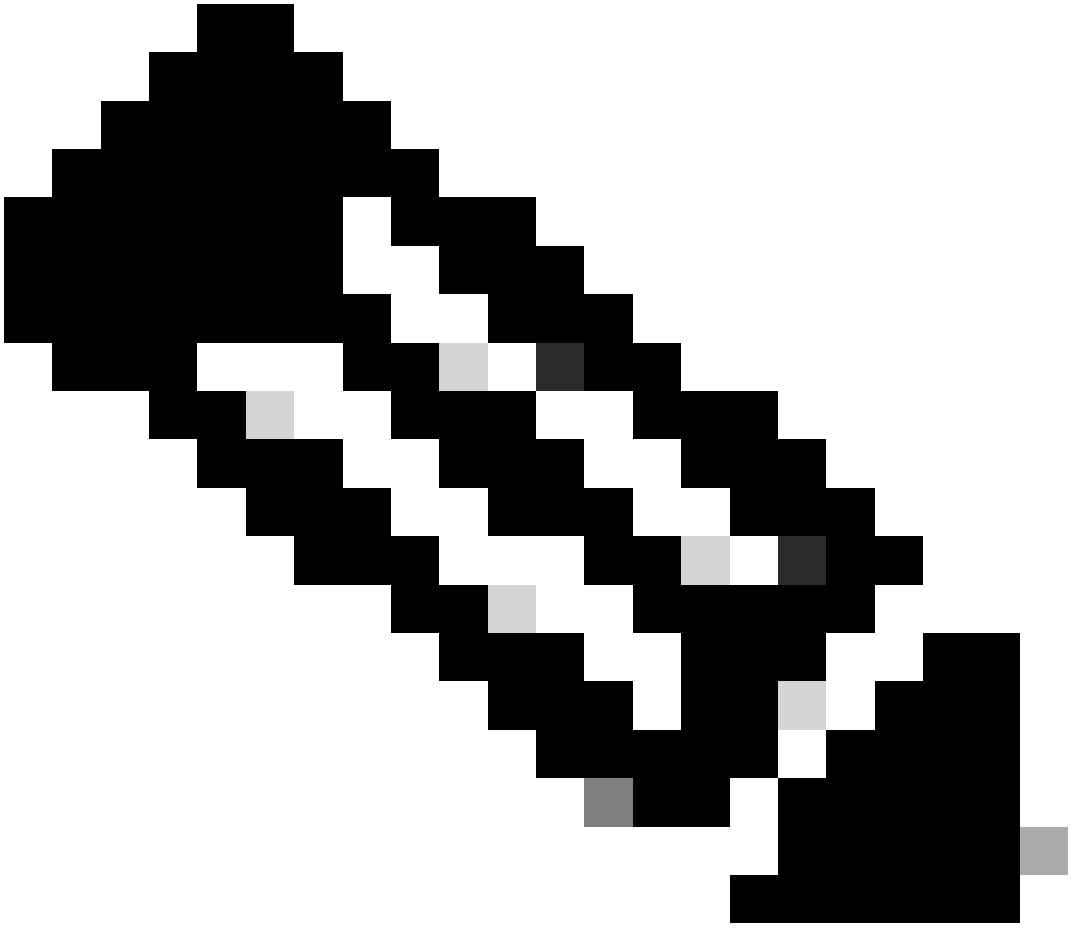
Abschließende Konfiguration der lokalen ASA

```
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
```

Abschließende Konfiguration der Remote-ASA

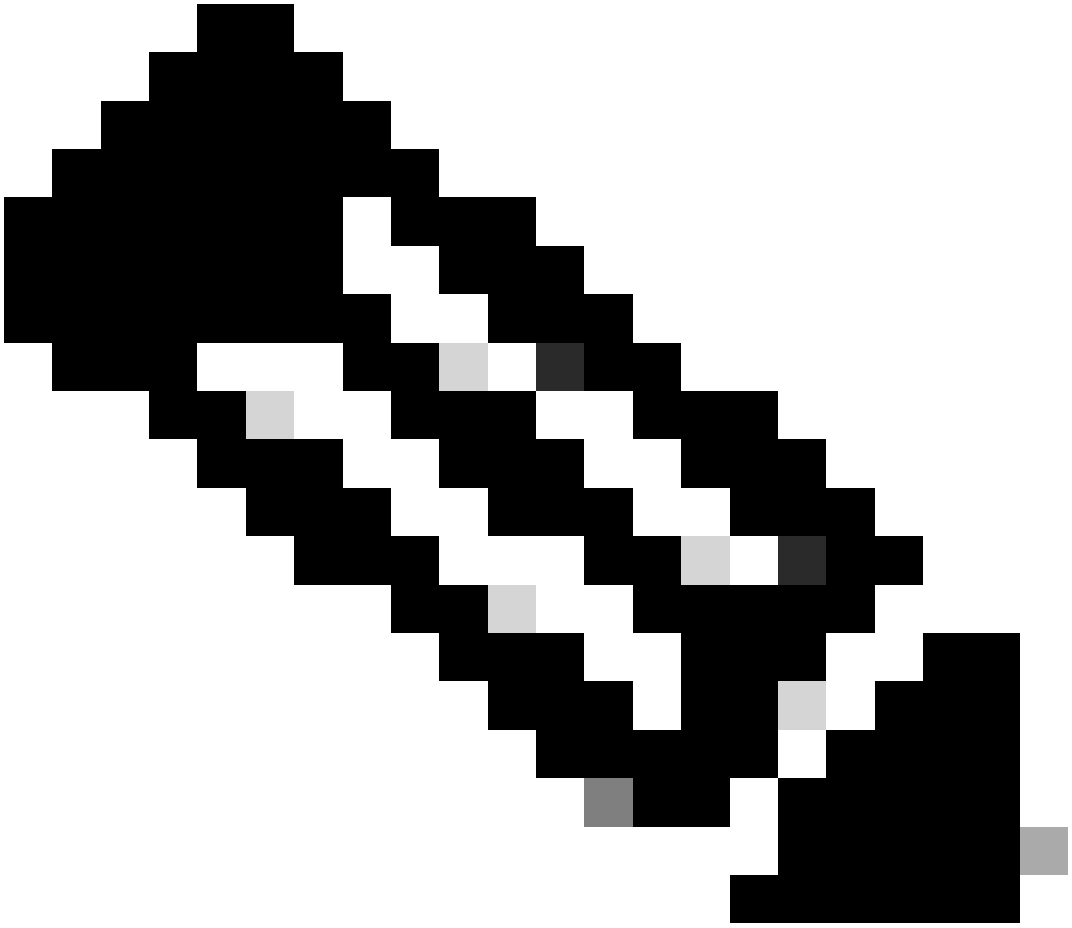
```
interface GigabitEthernet0/0 nameif outside security-level 0 ip address 10.20.20.20 255.255.255.0 ! interface GigabitEthernet0/1 nameif inside security-lev
```



Hinweis: Die ACL hat das gespiegelte Format, und die vorinstallierten Schlüssel sind an beiden Enden identisch.

Überprüfung

Bevor Sie überprüfen, ob der Tunnel in Betrieb ist und den Datenverkehr weiterleitet, müssen Sie sicherstellen, dass der interessante Datenverkehr an die ASAs gesendet wird.



Hinweis: Der Paket-Tracer wurde verwendet, um den Datenverkehrsfluss zu simulieren. Dies kann mithilfe des Befehls "Packet-Tracer" erfolgen; packet-tracer input inside icmp 192.168.0.11 8 0 172.16.10.11, der auf der lokalen ASA im Detail beschrieben wird.

Um die zusätzlichen Schlüsselaustausch zu validieren, können Sie den show crypto ikev2 sa Befehl verwenden. Wie in der Ausgabe zu sehen, können Sie die AKE-Parameter überprüfen, um die ausgewählten Austauschalgorithmen zu validieren.

<#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

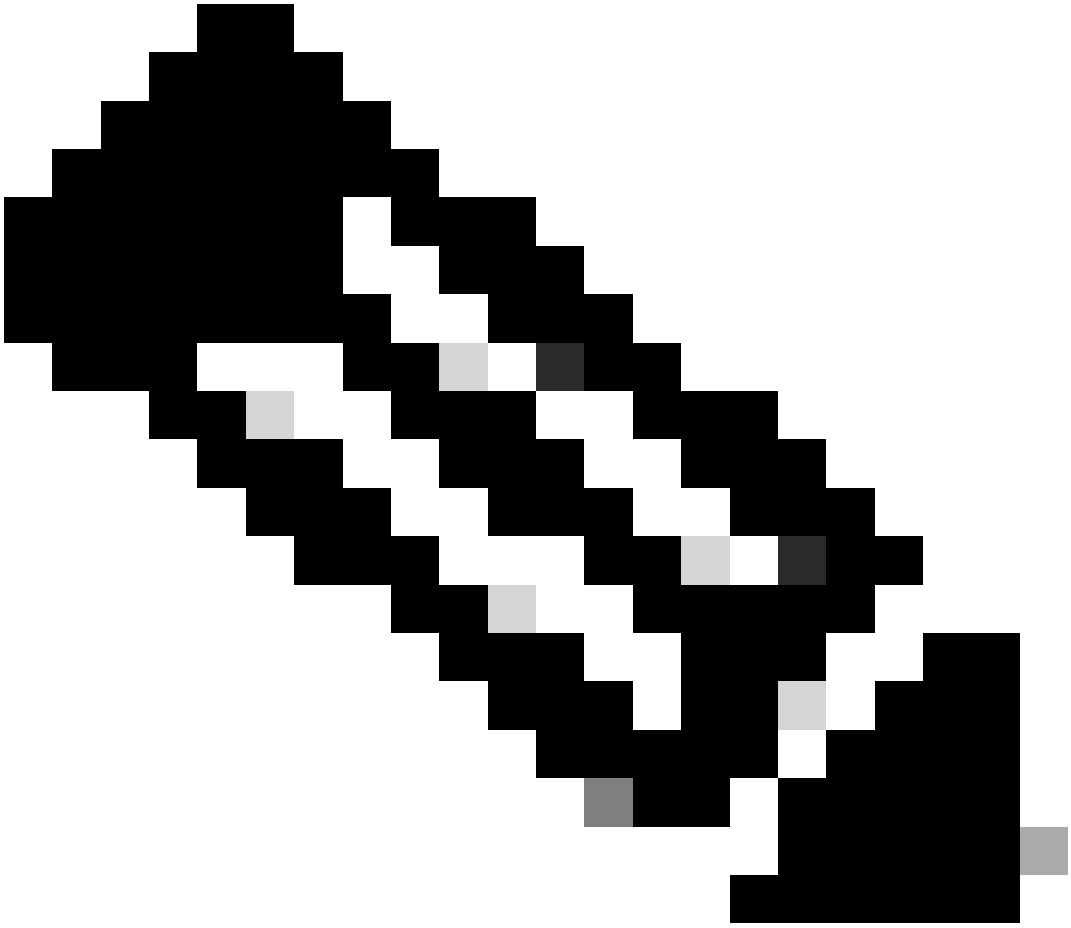
AKE1: 21 AKE2: 31

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

Fehlerbehebung

Die genannten Fehlerbehebungen können zur Fehlerbehebung im IKEv2-Tunnel verwendet werden:

debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127



Hinweis: Wenn Sie nur einen Tunnel (was der Fall sein muss, wenn das Gerät in der Produktion ist) beheben möchten, müssen Sie Debug-Vorgänge mit der debug crypto-Bedingung Peer X.X.X.X bedingt aktivieren.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.