使用IKEv2多個金鑰交換在兩個ASA之間配置站點到站點IKEv2隧道

目錄

簡介

本文檔介紹如何使用IKEv2多金鑰交換配置兩台Cisco ASA之間的站點到站點IKEv2 VPN連線。

必要條件

需求

思科建議您瞭解以下主題：

- 思科調適型安全裝置(ASA)
- 一般IKEv2概念

採用元件

本文檔中的資訊基於運行9.20.1的Cisco ASA。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

限制

IKEv2多金鑰交換具有以下限制：

- 僅在ASA CLI上受支援
- 支援多情景和HA裝置
- 叢集裝置不支援

授權

許可要求與ASA上的站點到站點VPN相同。

背景資訊

需要其他金鑰交換

大量子電腦的到來給安全系統帶來了巨大的風險，特別是使用公鑰加密的系統。量子電腦可以輕易地破壞那些被認為對普通電腦來說非常困難的密碼編譯方法。因此，人們需要轉向新的量子抗性方法，也稱為後量子密碼術(PQC)演算法。目的是透過使用多個金鑰交換來增強IPsec通訊的安全性。這包括將傳統的金鑰交換與量子之後的金鑰交換相結合。此方法可確保結果交換至少與傳統金鑰交換一樣強大，從而提供一層安全保護。

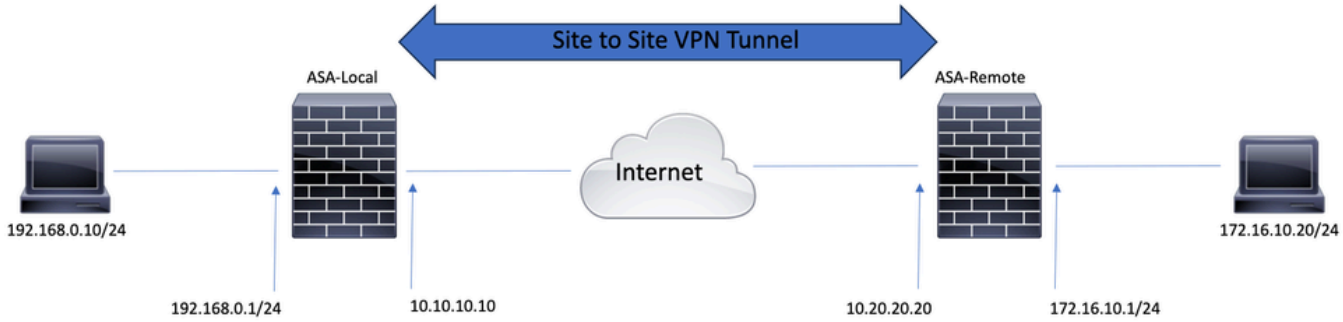
計畫透過增加對多個金鑰交換的支援來改進IKEv2。這些額外的金鑰交換可以處理免受量子威脅的演算法。為了交換有關這些附加金鑰的資訊，引入了一種稱為中間交換的新消息型別。這些金鑰交換透過SA負載使用常規IKEv2方法協商。

設定

本節介紹ASA配置。

網路圖表

本檔案中的資訊使用以下網路設定：

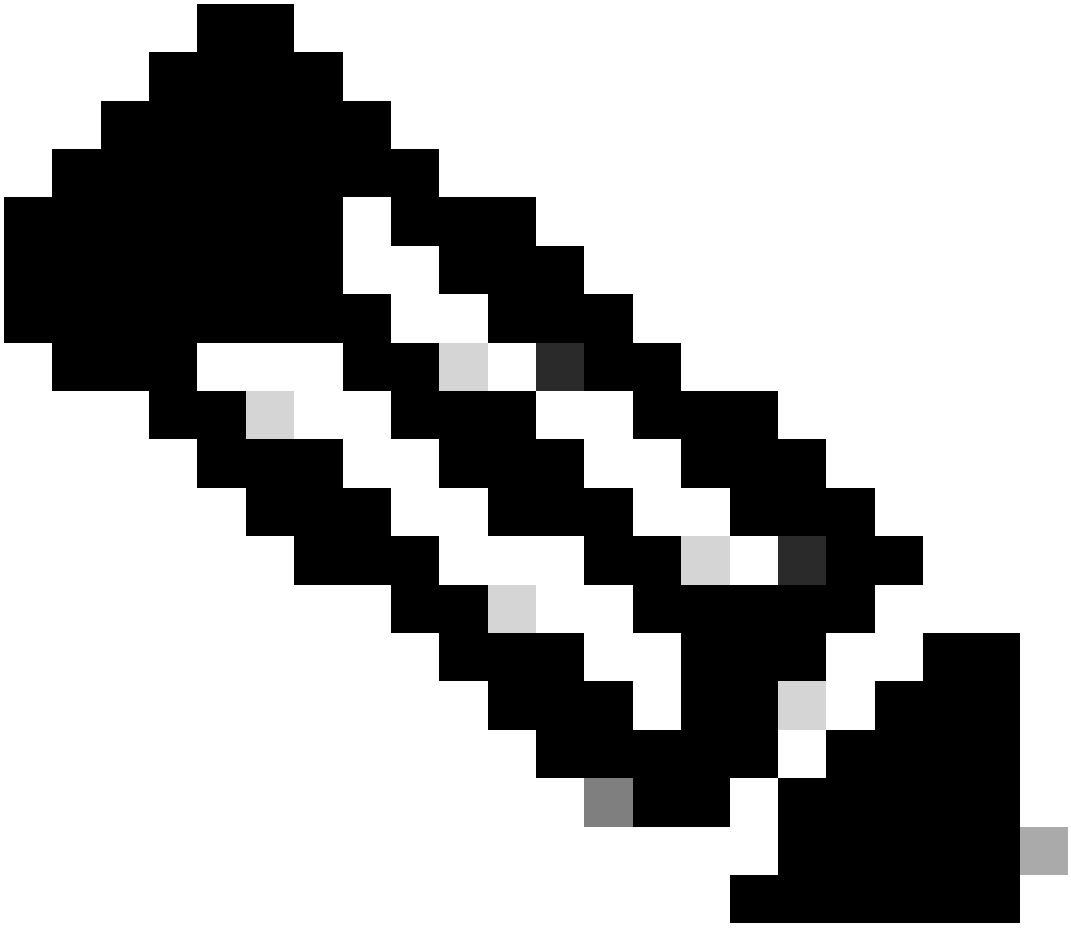


ASA配置

配置ASA介面

如果未配置ASA介面，請確保至少配置IP地址、介面名稱和安全級別：

```
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
```



注意：請確保連線到內部和外部網路，特別是用於建立站點到站點VPN隧道的遠端對等體。您可以使用ping驗證基本連線。

配置具有多個金鑰交換的IKEv2策略並在外部介面上啟用IKEv2

要為這些連線配置IKEv2策略，請輸入以下命令：

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

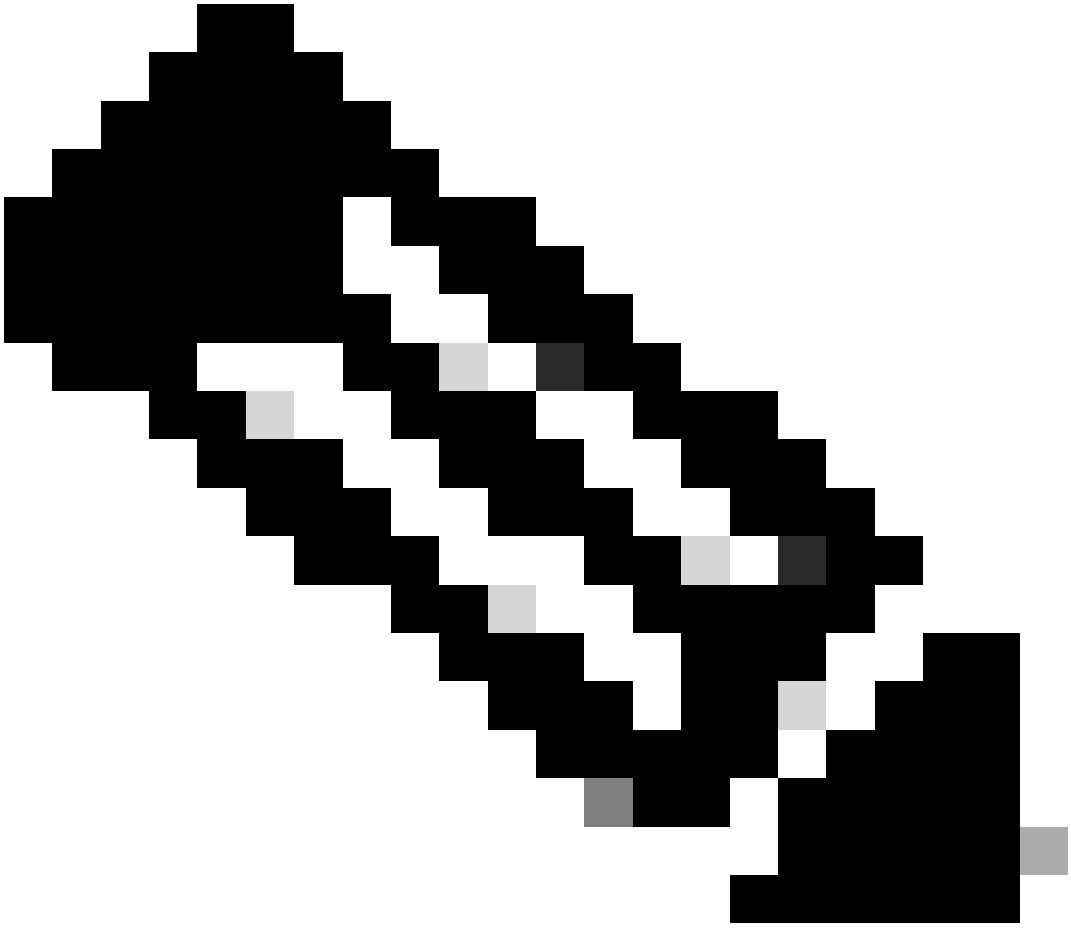
可以在crypto ikev2 policy下使用additional-key-exchange命令配置其他金鑰交換轉換。總共可以配置七種額外的exchange轉換。在本

示例中，配置了另外兩個交換轉換（使用DH組21和31）。

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

最終的IKEv2策略如下所示：

```
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
```



注意：如果來自兩個對等體的兩個策略都包含相同的身份驗證、加密、雜湊、Diffie-Hellman引數和其他金鑰交換引數值，則存在IKEv2策略匹配。

必須在終止VPN隧道的介面上啟用IKEv2。通常，這是外部（或網際網路）介面。要啟用IKEv2，請在全局配置模式下輸入crypto ikev2 enable outside命令。

配置隧道組

對於站點到站點隧道，連線配置檔案型別為IPSec-l2l。要配置IKEv2預共用金鑰，請輸入以下命令：

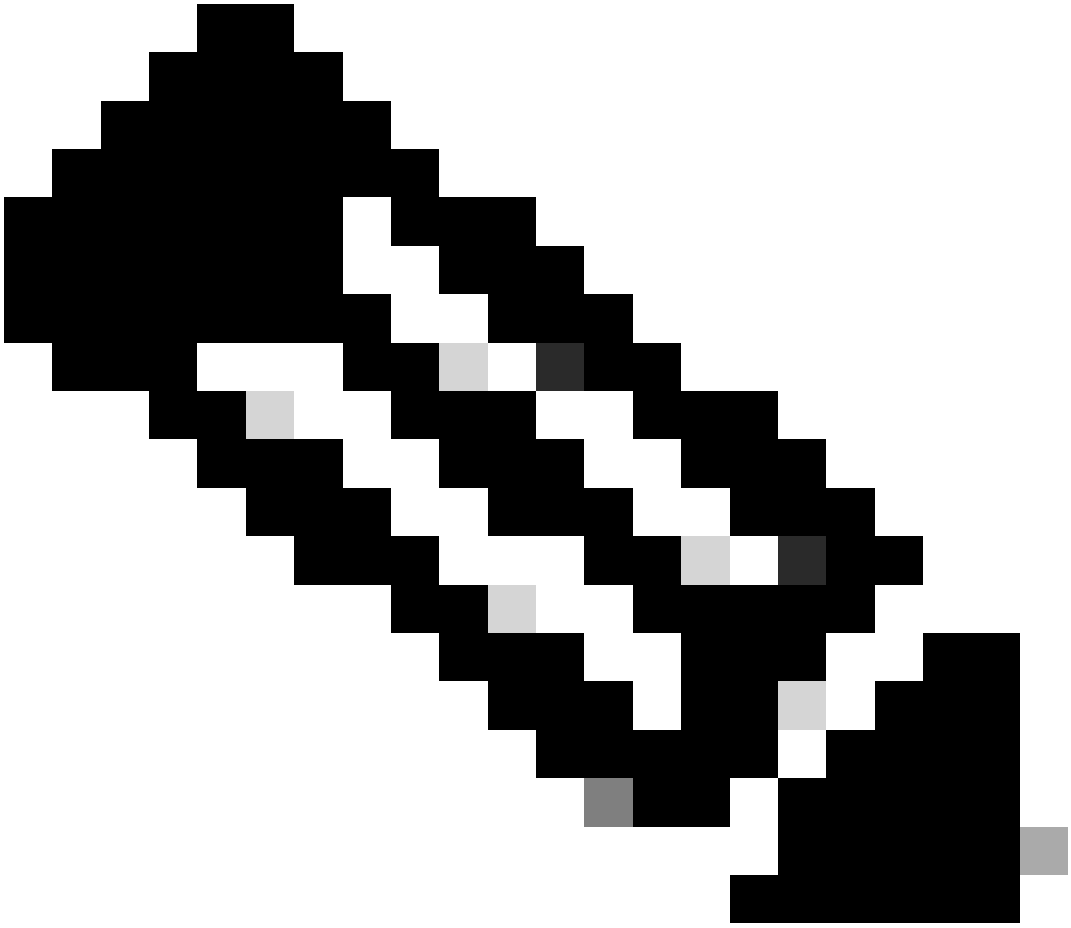
```
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
```

配置相關流量和加密ACL

ASA使用訪問控制清單(ACL)來區分必須使用IPSec加密保護的流量和不需要保護的流量。它保護與permit Application Control Engine (ACE)匹配的出站資料包，並確保與permit ACE匹配的入站資料包具有保護。

```
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
```



注意：VPN對等體必須具有映象格式的同一ACL。

配置身份NAT（可選）

通常需要使用身份NAT來防止相關流量到達動態NAT。在這種情況下，配置的標識NAT是：

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

配置IKEv2 IPSec提議

IKEv2 IPSec提議用於定義一組加密和完整性演算法，以保護資料流量。此建議必須匹配兩個VPN對等體，才能成功構建IPSec SA。本例中使用的命令包括：

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

配置加密對映並將其繫結到介面

加密對映結合了所有必需的配置，並且必須包含：

- 匹配必須加密的流量（通常稱為加密ACL）的訪問清單
- 對等辨識
- 至少一個IKEv2 IPSec提議

此處使用的配置如下：

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

最後一部分是使用crypto map outside_map interface outside命令將此加密對映應用於外部（公共）介面。

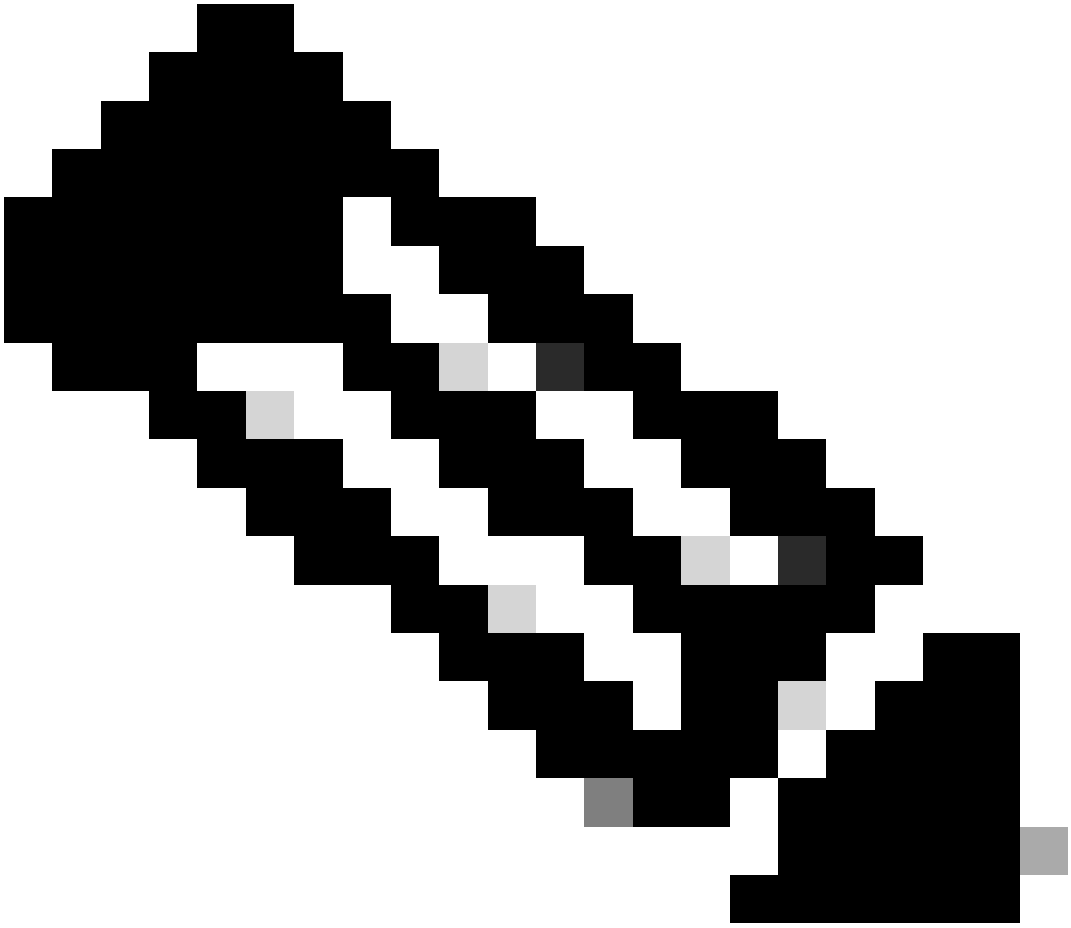
本地ASA最終配置

```
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
```

遠端ASA最終配置

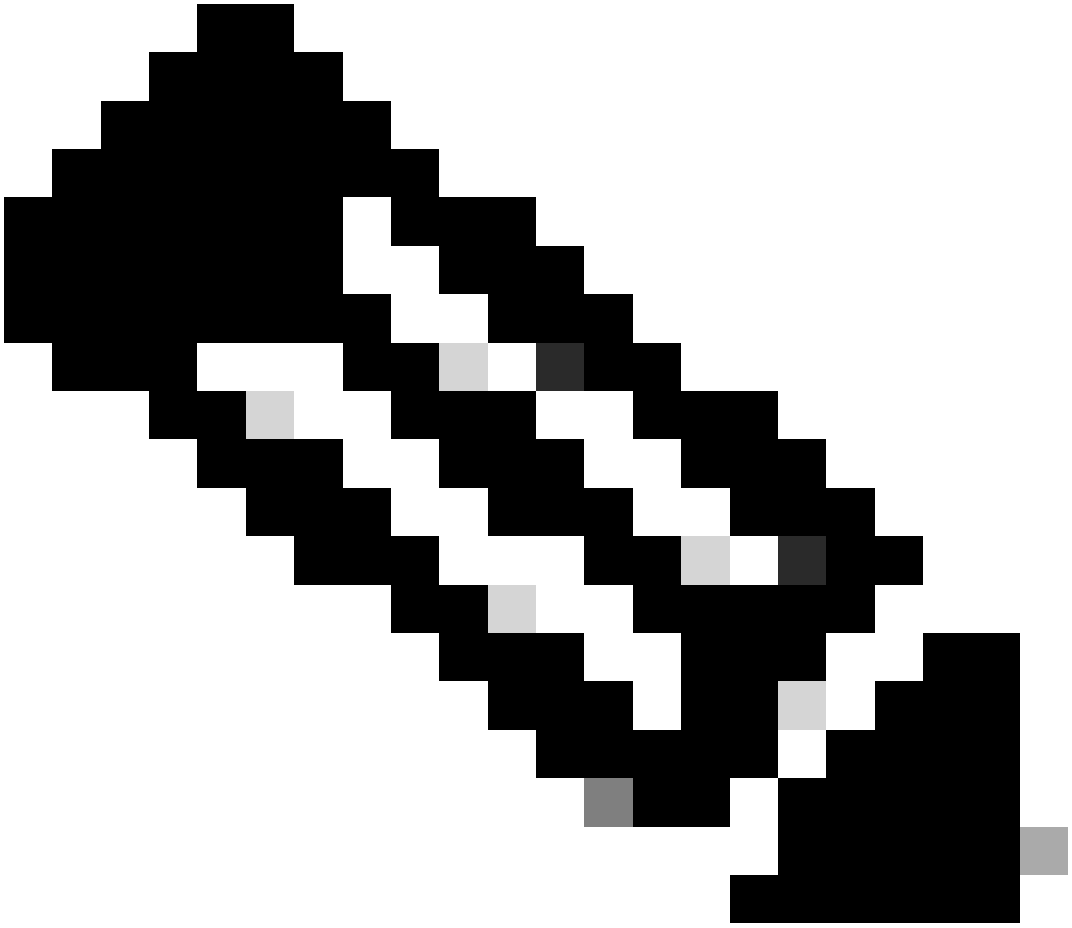
```
interface GigabitEthernet0/0 nameif outside security-level 0 ip address 10.20.20.20 255.255.255.0 ! interface GigabitEthernet0/1 nameif inside security-lev
```



注意：ACL採用映象格式，並且兩端的預共用金鑰相同。

驗證

在驗證隧道是否已啟用並且正在傳遞流量之前，必須確保相關流量被傳送到ASA。



注意：Packet Tracer用於模擬資料流。可使用Packet Tracer命令完成此任務；packet-tracer input inside icmp 192.168.0.11 8 0 172.16.10.11，詳見本地ASA。

要驗證其他金鑰交換，您可以使用show crypto ikev2 sa命令。如輸出所示，您可以檢查AKE引數以驗證所選交換演算法。

<#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

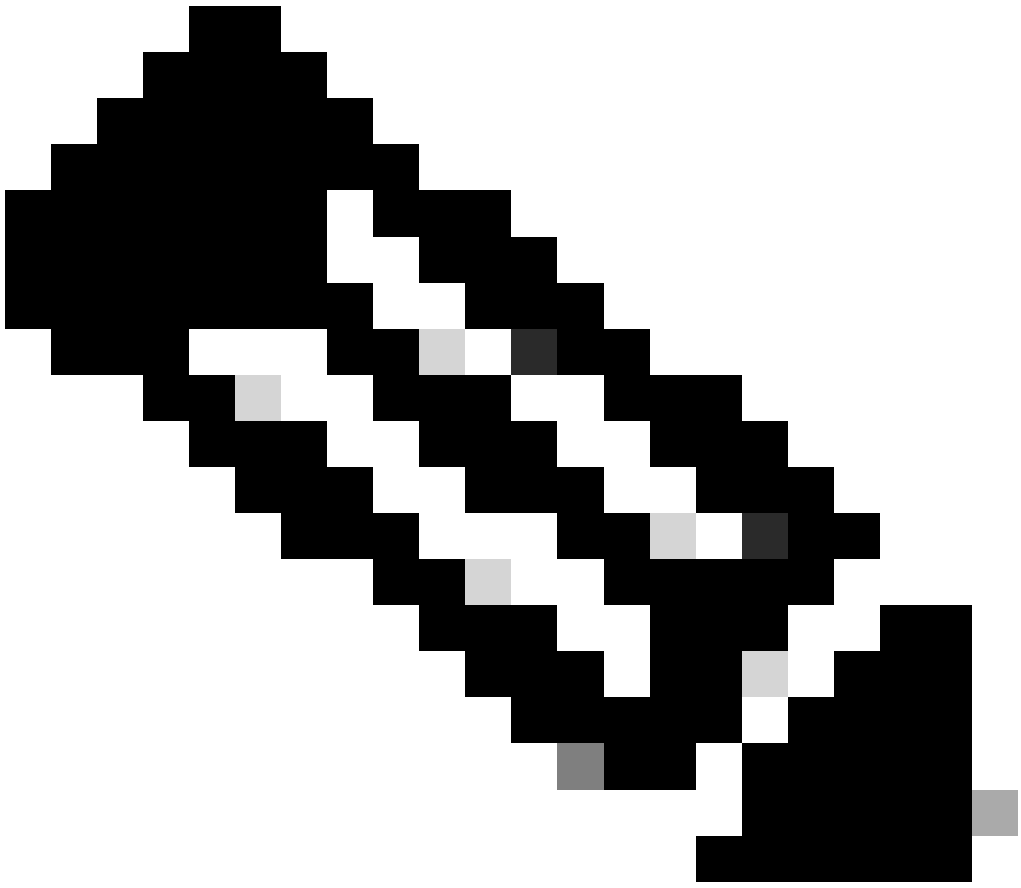
AKE1: 21 AKE2: 31

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

疑難排解

上述調試可用於對IKEv2隧道進行故障排除：

debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127



注意：如果您希望僅對一個隧道進行故障排除（如果裝置處於生產狀態，則情況必須如此），則必須使用debug crypto condition peer X.X.X.X命令有條件地啟用調試。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。