Configurazione di un tunnel IKEv2 da sito a sito tra due appliance ASA con scambi di chiavi multipli IKEv2

Sommario

Introduzione

In questo documento viene descritto come configurare una connessione VPN IKEv2 da sito a sito tra due appliance ASA Cisco con scambio di più chiavi IKEv2.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Adaptive Security Appliance (ASA)

- Nozioni generali su IKEv2

Componenti usati

Per la stesura del documento, sono state usate appliance Cisco ASA con versione 9.20.1.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Limitazioni

Lo scambio di più chiavi IKEv2 presenta le seguenti limitazioni:

- Supportato solo sulla CLI dell'ASA
- Supportato su dispositivi multi-contesto e HA
- Non supportato nei dispositivi del cluster

Licenze

I requisiti delle licenze sono gli stessi della VPN da sito a sito sulle appliance ASA.

Premesse

Necessità di ulteriori scambi di chiavi

L'arrivo di computer quantistici di grandi dimensioni comporta un grande rischio per i sistemi di sicurezza, in particolare per quelli che utilizzano la crittografia a chiave pubblica. I metodi crittografici che si pensava fossero molto difficili per i normali computer possono essere facilmente rotti dai computer quantistici. Quindi, sorge la necessità di passare a nuovi metodi resistenti ai quanti, chiamati anche algoritmi di crittografia post-quantistica (PQC). Lo scopo è quello di migliorare la sicurezza delle comunicazioni IPsec utilizzando scambi di chiavi multipli. Ciò implica la combinazione di uno scambio di chiavi tradizionale con uno post-quantistico. Questo approccio garantisce che lo scambio risultante sia almeno altrettanto efficace del tradizionale scambio di chiavi, fornendo un ulteriore livello di sicurezza.

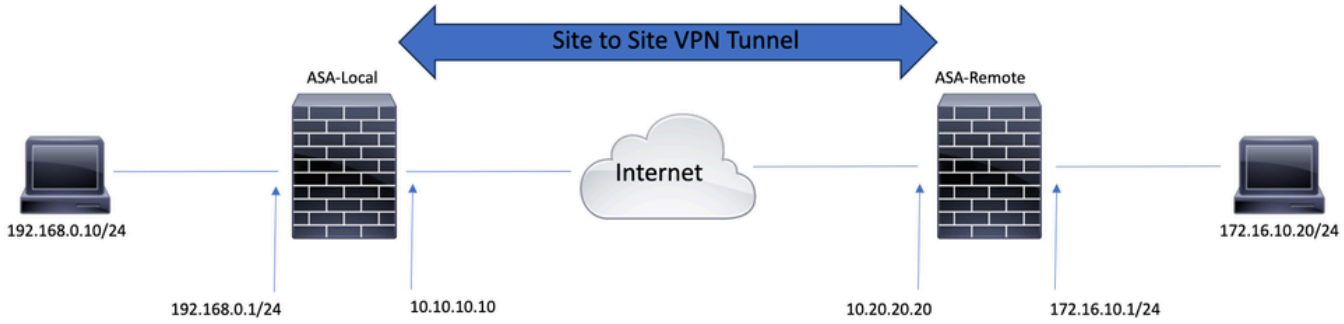
Il piano prevede il miglioramento di IKEv2 tramite l'aggiunta del supporto per più scambi di chiave. Questi scambi di chiave extra possono gestire algoritmi che sono al sicuro dalle minacce quantistiche. Per lo scambio di informazioni su queste chiavi aggiuntive, viene introdotto un nuovo tipo di messaggio denominato Intermediate Exchange. Questi scambi di chiave vengono negoziati utilizzando il normale metodo IKEv2, tramite il payload SA.

Configurazione

In questa sezione vengono descritte le configurazioni dell'ASA.

Esempio di rete

Per le informazioni di questo documento viene utilizzata la seguente configurazione della rete:

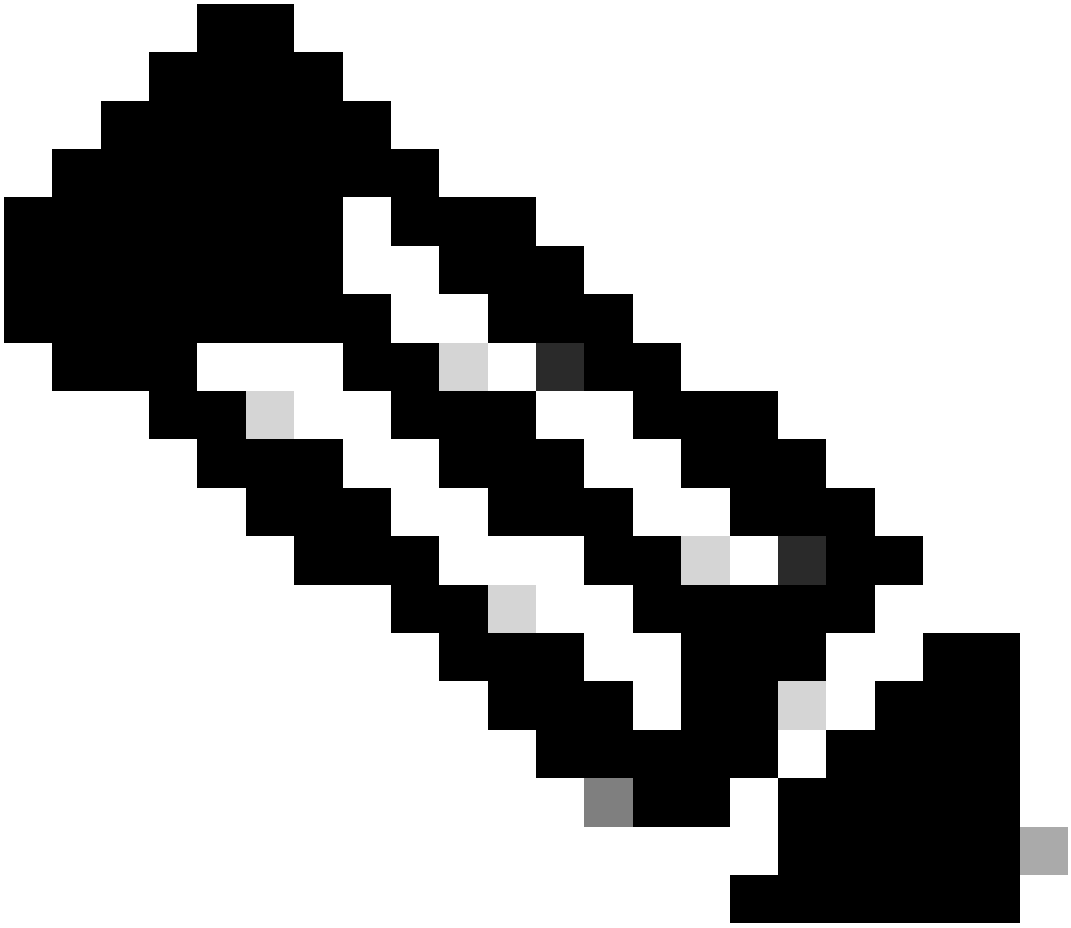


Configurazione ASA

Configurazione delle interfacce ASA

Se le interfacce ASA non sono configurate, verificare di configurare almeno gli indirizzi IP, i nomi delle interfacce e i livelli di sicurezza:

```
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
```



Nota: verificare la presenza di connettività sia alle reti interne che a quelle esterne, in particolare al peer remoto utilizzato per stabilire un tunnel VPN da sito a sito. È possibile usare un comando ping per verificare la connettività di base.

Configurazione del criterio IKEv2 con scambio di più chiavi e abilitazione di IKEv2 sull'interfaccia esterna

Per configurare i criteri IKEv2 per queste connessioni, immettere i seguenti comandi:

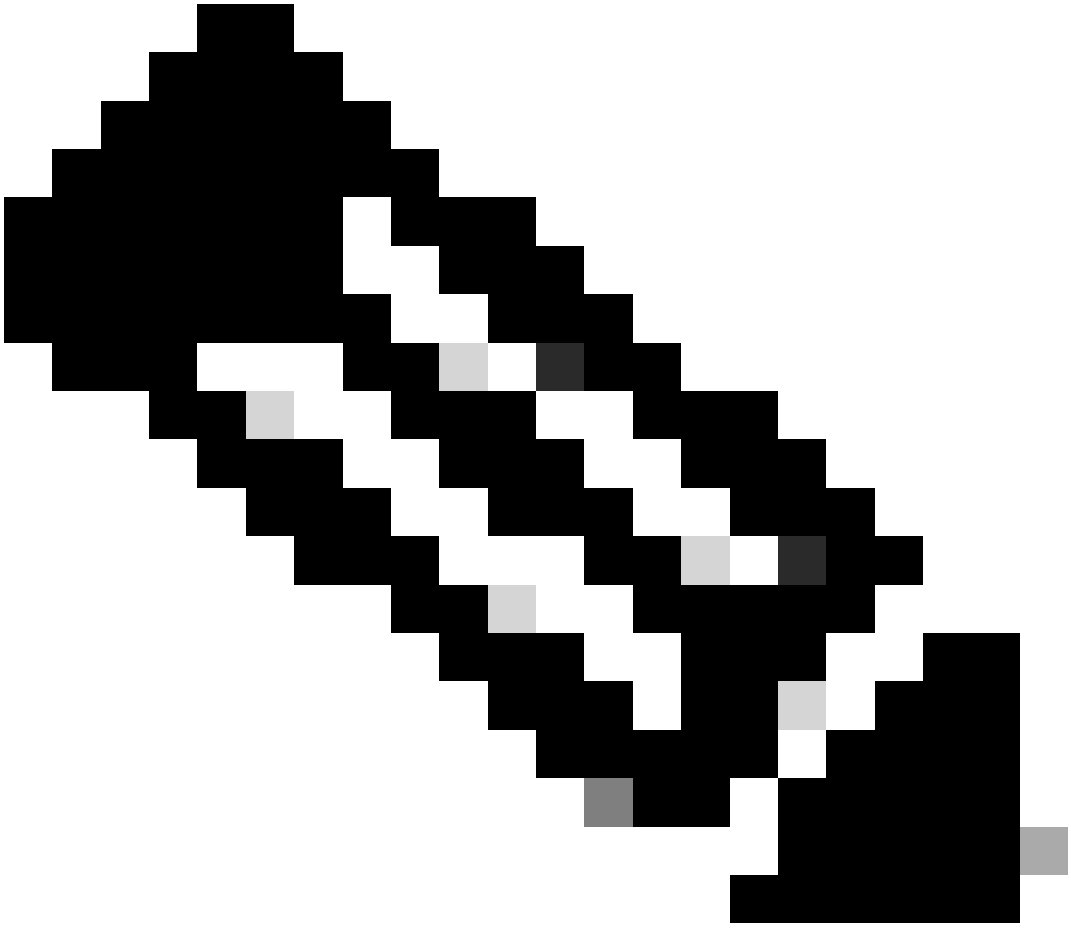
```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
```

È possibile configurare ulteriori trasformazioni di scambio chiave in crypto ikev2 policy utilizzando il comandoadditional-key-exchange. È possibile configurare un totale di sette trasformazioni di scambio aggiuntive. In questo esempio, sono state configurate due trasformazioni di scambio aggiuntive (utilizzando i gruppi DH 21 e 31).

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

Il criterio IKEv2 finale è simile al seguente:

```
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
```



Nota: esiste una corrispondenza di criteri IKEv2 quando entrambi i criteri dei due peer contengono gli stessi valori di autenticazione, crittografia, hash, parametro Diffie-Hellman e parametro Additional Key Exchange.

È necessario abilitare IKEv2 sull'interfaccia che termina il tunnel VPN. In genere, si tratta dell'interfaccia esterna o Internet. Per abilitare IKEv2, immettere il comandocrypto ikev2 enable outside in modalità di configurazione globale.

Configurazione del gruppo di tunnel

Per un tunnel da sito a sito, il profilo di connessione è IPSec-l2l. Per configurare la chiave già condivisa IKEv2, immettere i seguenti comandi:

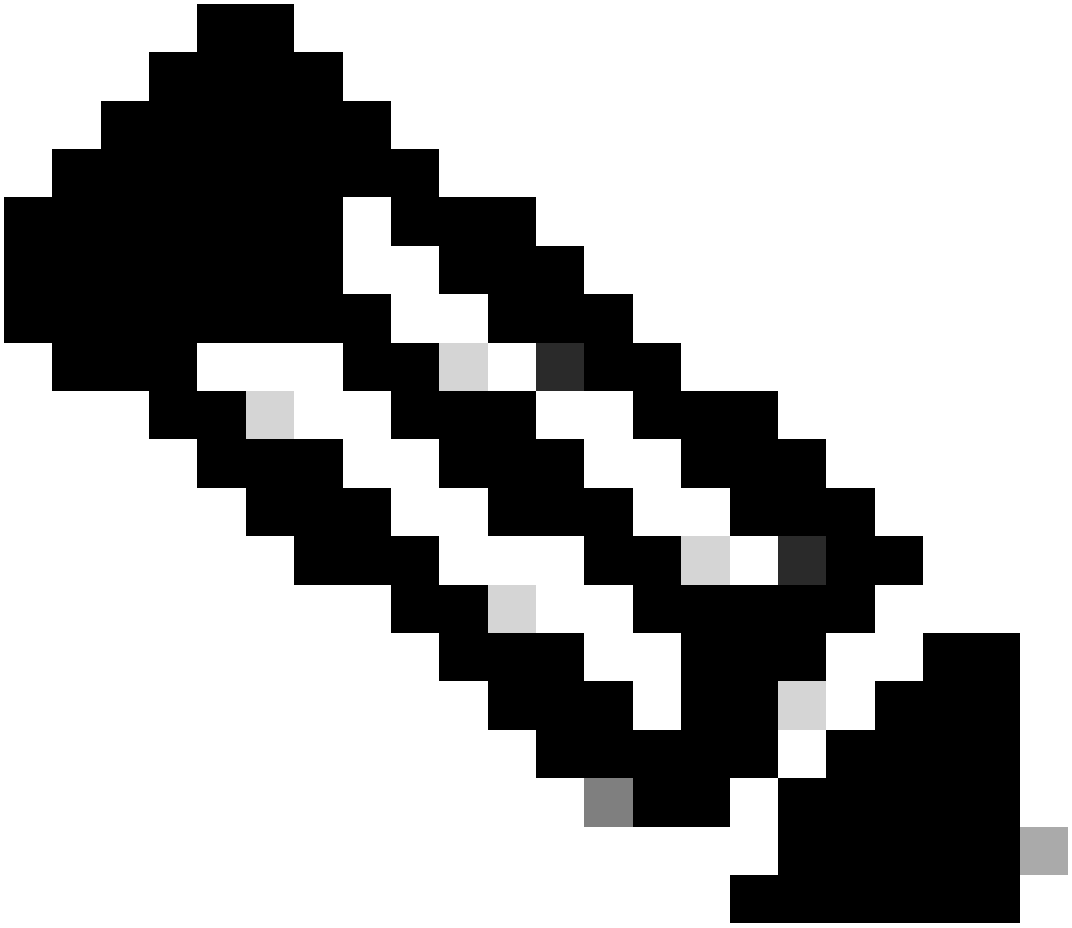
```
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
```

Configurazione di ACL di traffico e crittografia rilevanti

L'appliance ASA utilizza gli Access Control Lists (ACL) per distinguere il traffico che deve essere protetto con la crittografia IPSec dal traffico che non deve essere protetto. Protegge i pacchetti in uscita che corrispondono a una voce ACE (Application Control Engine) dell'autorizzazione e garantisce la protezione dei pacchetti in entrata che corrispondono a una voce ACE dell'autorizzazione.

```
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
```



Nota: il peer VPN deve avere lo stesso ACL in un formato con mirroring.

Configurazione di un NAT di identità (facoltativo)

In genere, è necessario un NAT di identità per evitare che il traffico interessante colpisca il NAT dinamico. Il NAT dell'identità configurato in questo caso è:

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

Configurazione della proposta IPSec IKEv2

La proposta IPSec IKEv2 viene utilizzata per definire una serie di algoritmi di crittografia e integrità allo scopo di proteggere il traffico di dati. Per poter creare un'associazione di protezione IPSec correttamente, questa proposta deve corrispondere a entrambi i peer VPN. I comandi utilizzati in questo caso sono:

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

Configurare una mappa crittografica e associarla all'interfaccia

Una mappa crittografica combina tutte le configurazioni richieste e deve necessariamente contenere:

- Un elenco degli accessi che corrisponda al traffico che deve essere crittografato (detto comunemente ACL di crittografia)
- Identificazione peer
- Almeno una proposta IPSec IKEv2

La configurazione utilizzata è:

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

La parte finale sta applicando questa mappa crittografica all'interfaccia esterna (pubblica) utilizzando il crypto map outside_map interface outside comando.

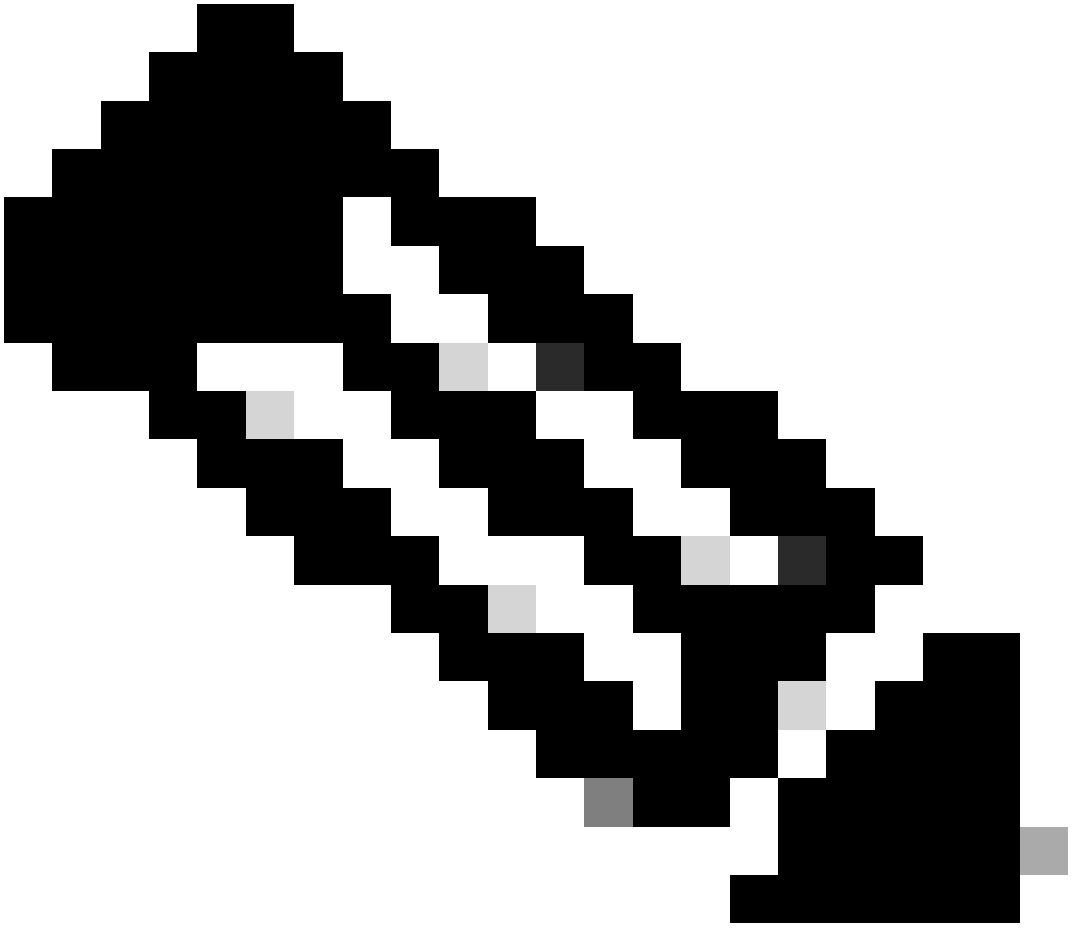
Configurazione finale ASA locale

```
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
```

Configurazione finale ASA remota

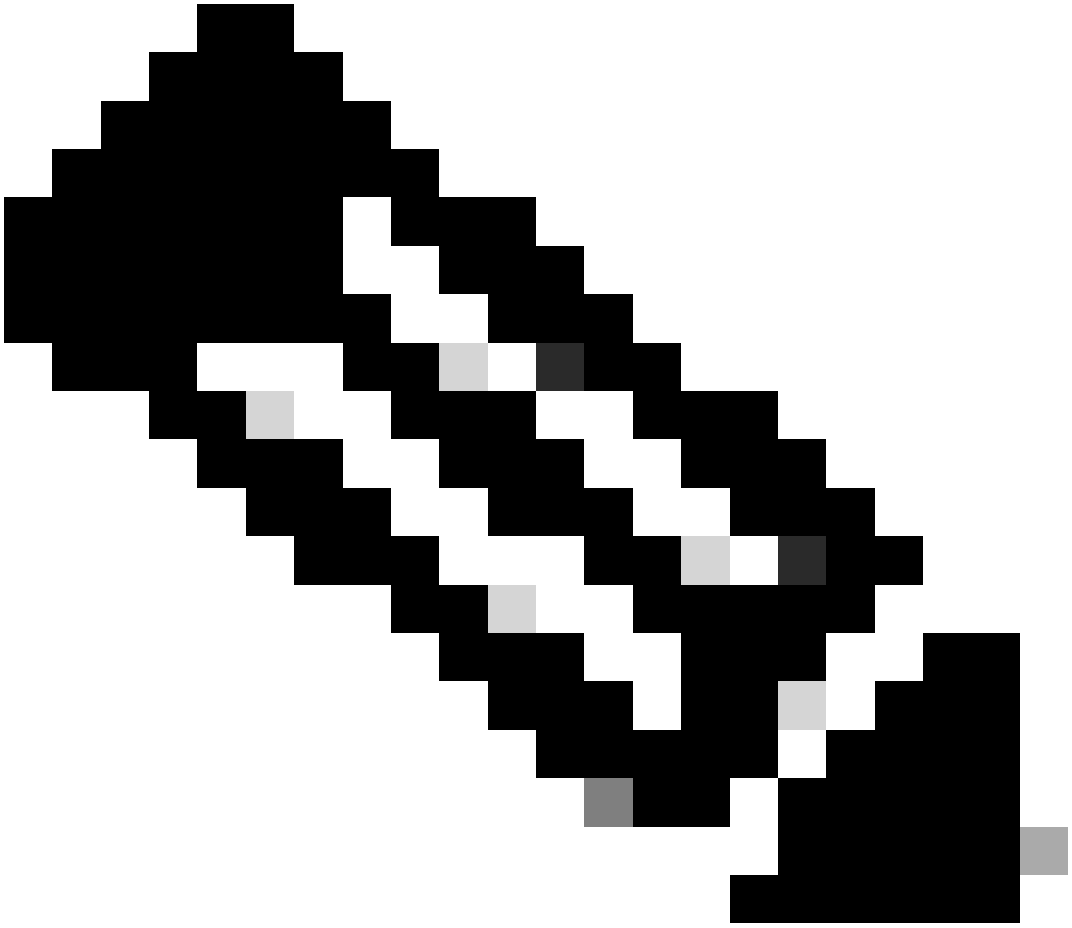
```
interface GigabitEthernet0/0 nameif outside security-level 0 ip address 10.20.20.20 255.255.255.0 ! interface GigabitEthernet0/1 nameif inside security-lev
```



Nota: l'ACL è nel formato con mirroring e le chiavi già condivise sono le stesse su entrambe le estremità.

Verifica

Prima di verificare se il tunnel è attivo e se sta attraversando il traffico, accertarsi che alle appliance ASA venga inviato traffico interessante.



Nota: il tracer del pacchetto è stato usato per simulare il flusso del traffico. A tale scopo, è possibile usare il comando packet-tracer; packet-tracer input inside icmp 192.168.0.11 8 0 172.16.10.11 dettagliato sull'appliance Local-ASA.

Per convalidare gli scambi di chiave aggiuntivi, è possibile utilizzare il show crypto ikev2 sa comando. Come mostrato nell'output, è possibile controllare i parametri AKE per convalidare gli algoritmi di scambio selezionati.

<#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

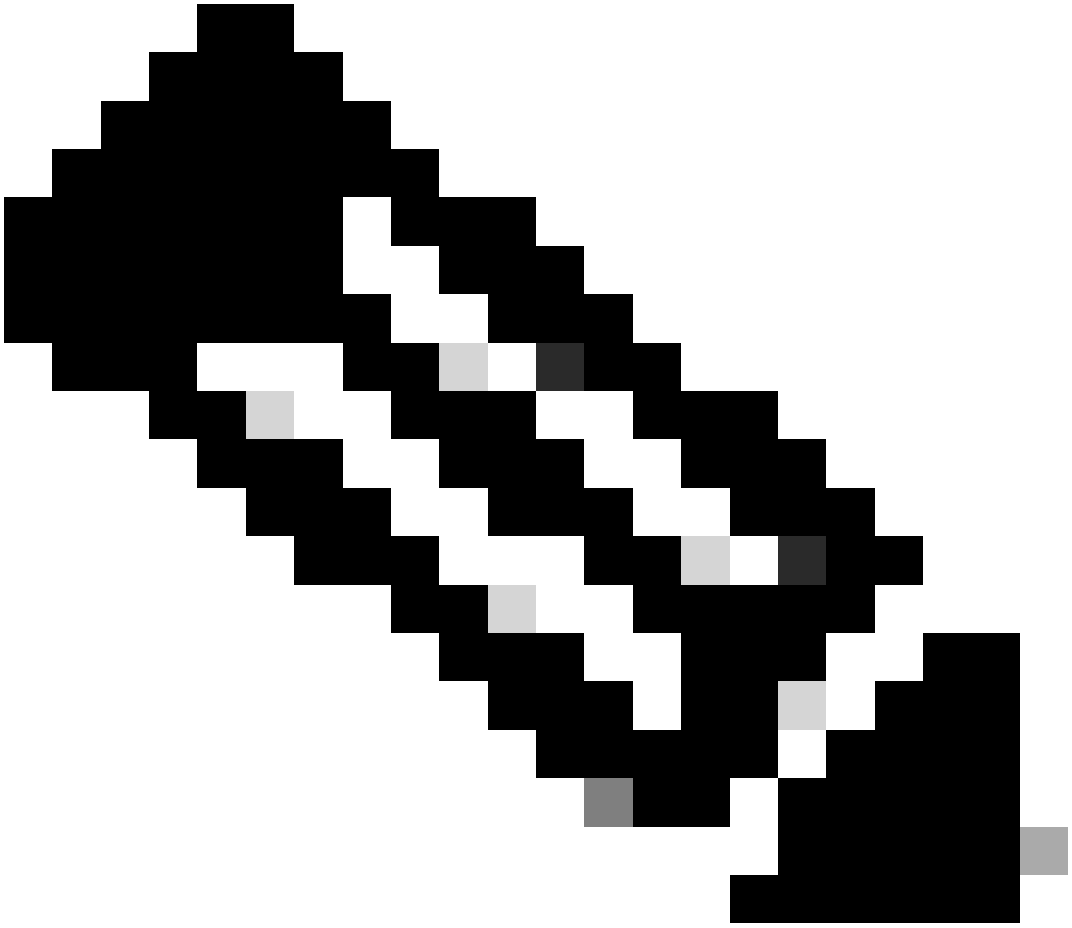
AKE1: 21 AKE2: 31

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

Risoluzione dei problemi

I debug menzionati possono essere usati per risolvere i problemi del tunnel IKEv2:

debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127



Nota: se si desidera risolvere i problemi relativi a un solo tunnel (come deve essere il caso se il dispositivo è in produzione), è necessario abilitare i debug in modo condizionale utilizzando il comando debug crypto condition peer X.X.X.X.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).