Configuración de un túnel IKEv2 de sitio a sitio entre dos ASA mediante intercambios de claves múltiples IKEv2

Contenido

Introducción

Este documento describe cómo configurar una conexión VPN IKEv2 de sitio a sitio entre dos Cisco ASA mediante Intercambios de claves múltiples IKEv2.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Dispositivo de seguridad Cisco Adaptive Security Appliance (ASA)

- Conceptos generales de IKEv2

Componentes Utilizados

La información de este documento se basa en los Cisco ASA que ejecutan 9.20.1.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Limitaciones

El Intercambio de claves múltiples IKEv2 tiene estas limitaciones:

- Solo es compatible con ASA CLI
- Compatible con dispositivos de alta disponibilidad y multicontexto
- No compatible con dispositivos agrupados

Licencias

Los requisitos de licencia son los mismos que para la VPN de sitio a sitio en los ASA.

Antecedentes

Necesidad de intercambios de claves adicionales

La llegada de grandes ordenadores cuánticos supone un gran riesgo para los sistemas de seguridad, especialmente los que utilizan criptografía de clave pública. Los métodos criptográficos que se pensaba que eran muy duros para los ordenadores normales pueden ser rotos fácilmente por los ordenadores cuánticos. Por lo tanto, surge la necesidad de cambiar a métodos nuevos y resistentes a los datos cuánticos, también llamados algoritmos de criptografía poscuántica (PQC). El objetivo es mejorar la seguridad de la comunicación IPsec mediante el uso de varios intercambios de claves. Esto implica combinar un intercambio de claves tradicional con uno poscuántico. Este enfoque garantiza que el intercambio resultante sea al menos tan fuerte como el intercambio de claves tradicional, lo que proporciona una capa adicional de seguridad.

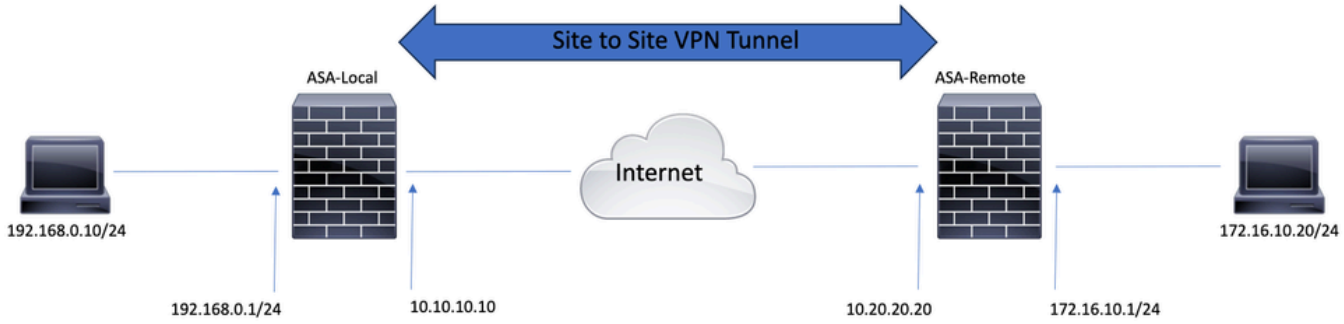
El plan consiste en mejorar IKEv2 añadiendo compatibilidad con varios intercambios de claves. Estos intercambios de claves adicionales pueden gestionar algoritmos que están a salvo de las amenazas cuánticas. Para intercambiar información sobre estas claves adicionales, se introduce un nuevo tipo de mensaje denominado Intermediate Exchange. Estos intercambios de claves se negocian utilizando el método IKEv2 normal, a través de la carga útil SA.

Configurar

Esta sección describe las configuraciones de ASA.

Diagrama de la red

La información de este documento utiliza esta configuración de red:

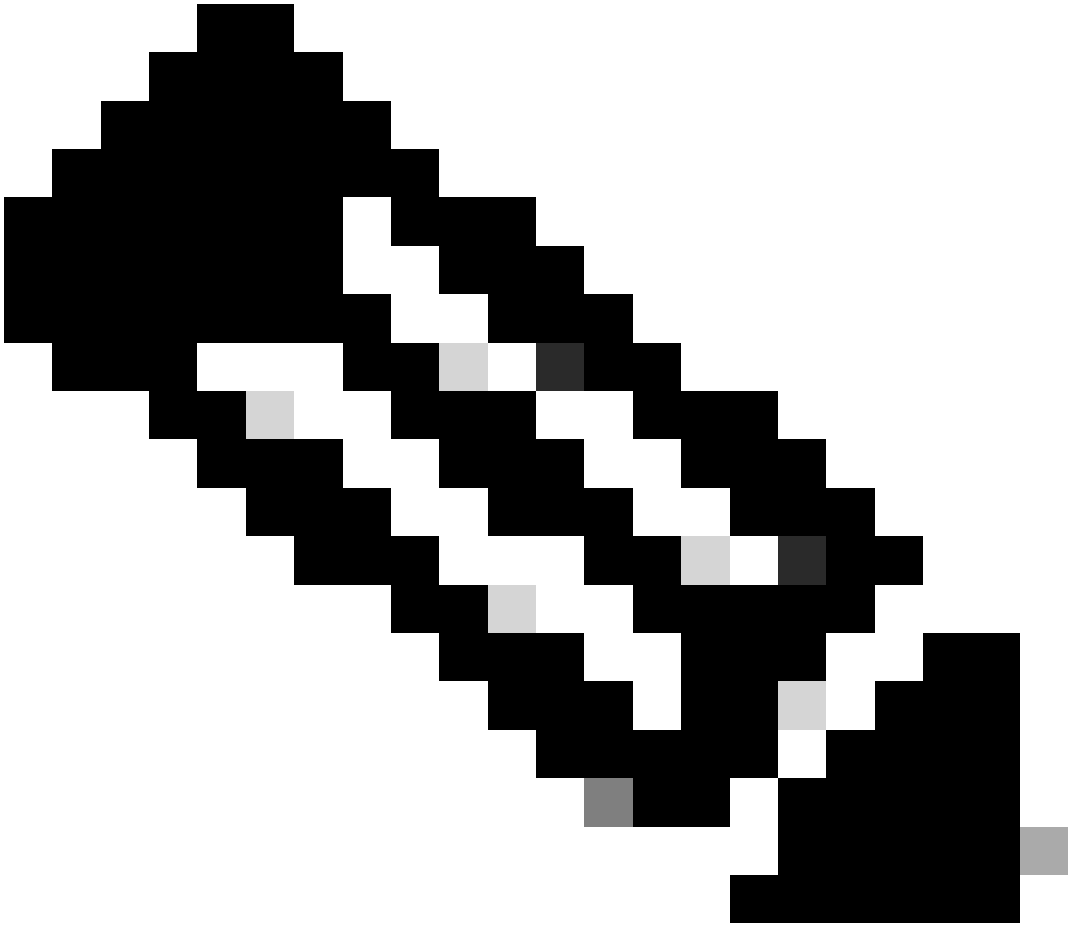


Configuración de ASA

Configuración de las interfaces ASA

Si las interfaces ASA no están configuradas, asegúrese de configurar al menos las direcciones IP, los nombres de interfaz y los niveles de seguridad:

```
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: Asegúrese de que haya conectividad tanto con las redes internas como con las externas, especialmente con el par remoto que se utiliza para establecer un túnel VPN de sitio a sitio. Puede utilizar un ping para verificar la conectividad básica.

Configuración de la política IKEv2 con Intercambio de claves múltiples y activación de IKEv2 en la interfaz externa

Para configurar las políticas IKEv2 para estas conexiones, ingrese estos comandos:

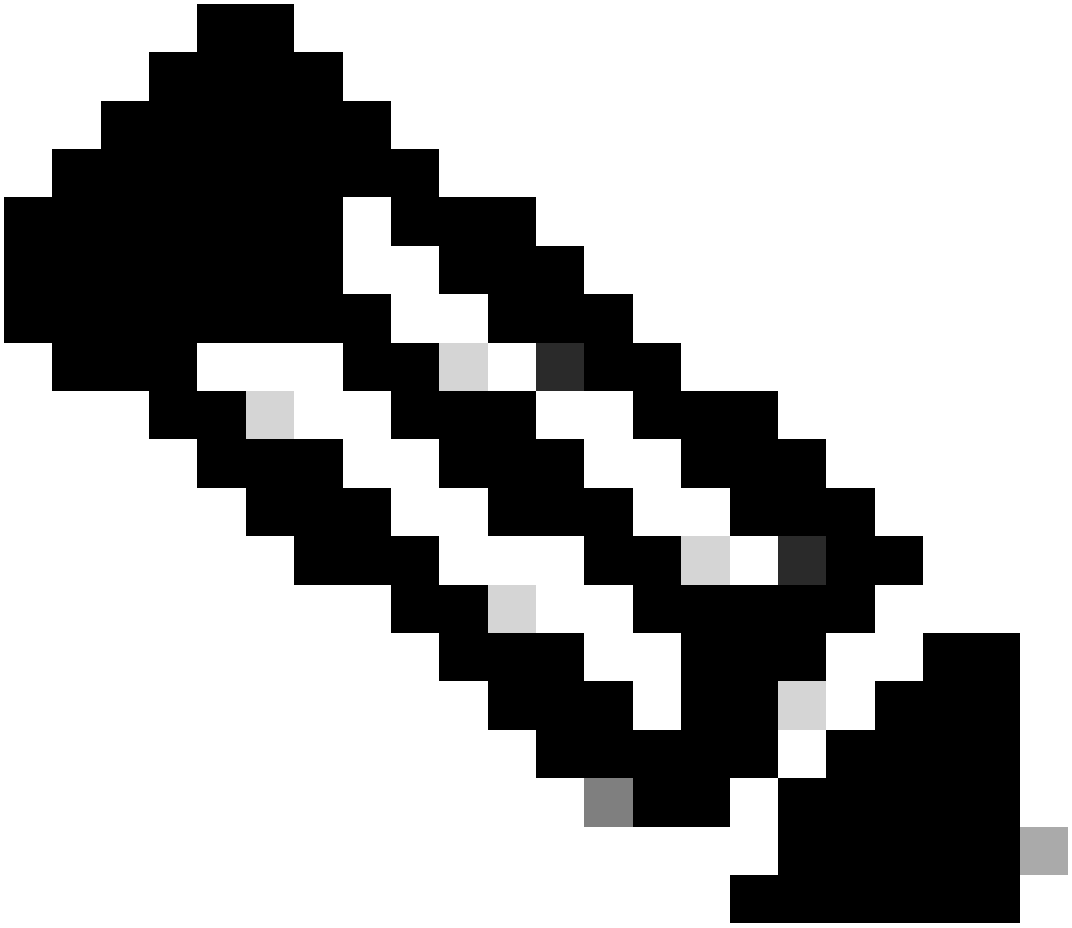
```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
```

Se pueden configurar transformaciones de intercambio de claves adicionales crypto ikev2 policy mediante el additional-key-exchange comando. Se pueden configurar un total de siete transformaciones de intercambio adicionales. En este ejemplo, se han configurado dos transformaciones de intercambio adicionales (utilizando los grupos DH 21 y 31).

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

La política IKEv2 final tiene este aspecto:

```
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: existe una coincidencia de política IKEv2 cuando ambas políticas de los dos peers contienen los mismos valores de parámetro de autenticación, cifrado, hash, Diffie-Hellman y Additional Key Exchange.

Debe habilitar IKEv2 en la interfaz que termina el túnel VPN. Normalmente, se trata de la interfaz externa (o de Internet). Para habilitar IKEv2, ingrese el crypto ikev2 enable outside comando en el modo de configuración global.

Configuración del Grupo de Túnel

Para un túnel de sitio a sitio, el tipo de perfil de conexión es IPSec-l2l. Para configurar la clave previamente compartida IKEv2, ingrese estos

comandos:

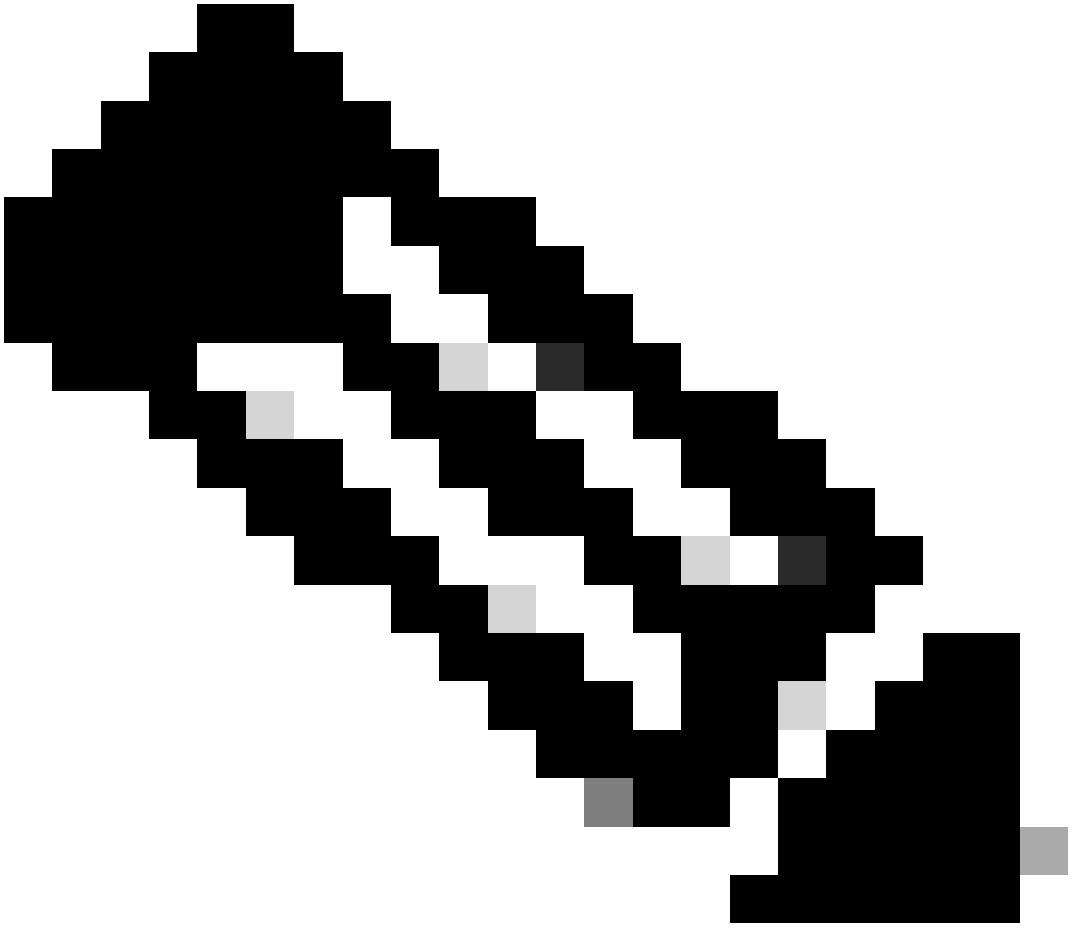
```
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
```

Configuración de tráfico interesante y ACL criptográfica

ASA utiliza listas de control de acceso (ACL) para diferenciar el tráfico que debe protegerse con cifrado IPSec del tráfico que no requiere protección. Protege los paquetes salientes que coinciden con un permit Application Control Engine (ACE) y garantiza que los paquetes entrantes que coinciden con un permit ACE tengan protección.

```
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: El par VPN debe tener la misma ACL en un formato duplicado.

Configurar una identidad NAT (opcional)

Normalmente, se necesita una identidad NAT para evitar que el tráfico interesante llegue a la NAT dinámica. La identidad NAT que se configura en este caso es:

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

Configuración de la propuesta IPSec de IKEv2

La propuesta IPSec de IKEv2 se utiliza para definir un conjunto de algoritmos de cifrado e integridad con el fin de proteger el tráfico de datos. Esta propuesta debe coincidir con ambos puntos de VPN para crear una SA IPSec correctamente. Los comandos utilizados en este caso son:

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

Configurar un mapa criptográfico y vincularlo a la interfaz

Un mapa criptográfico combina todas las configuraciones necesarias y debe contener necesariamente:

- Una lista de acceso que coincida con el tráfico que se debe cifrar (comúnmente conocida como Crypto ACL)
- Identificación de pares
- Al menos una propuesta IKEv2 IPSec

La configuración utilizada aquí es:

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 final es aplicar este mapa criptográfico a la interfaz externa (pública) mediante el crypto map outside_map interface outside comando.

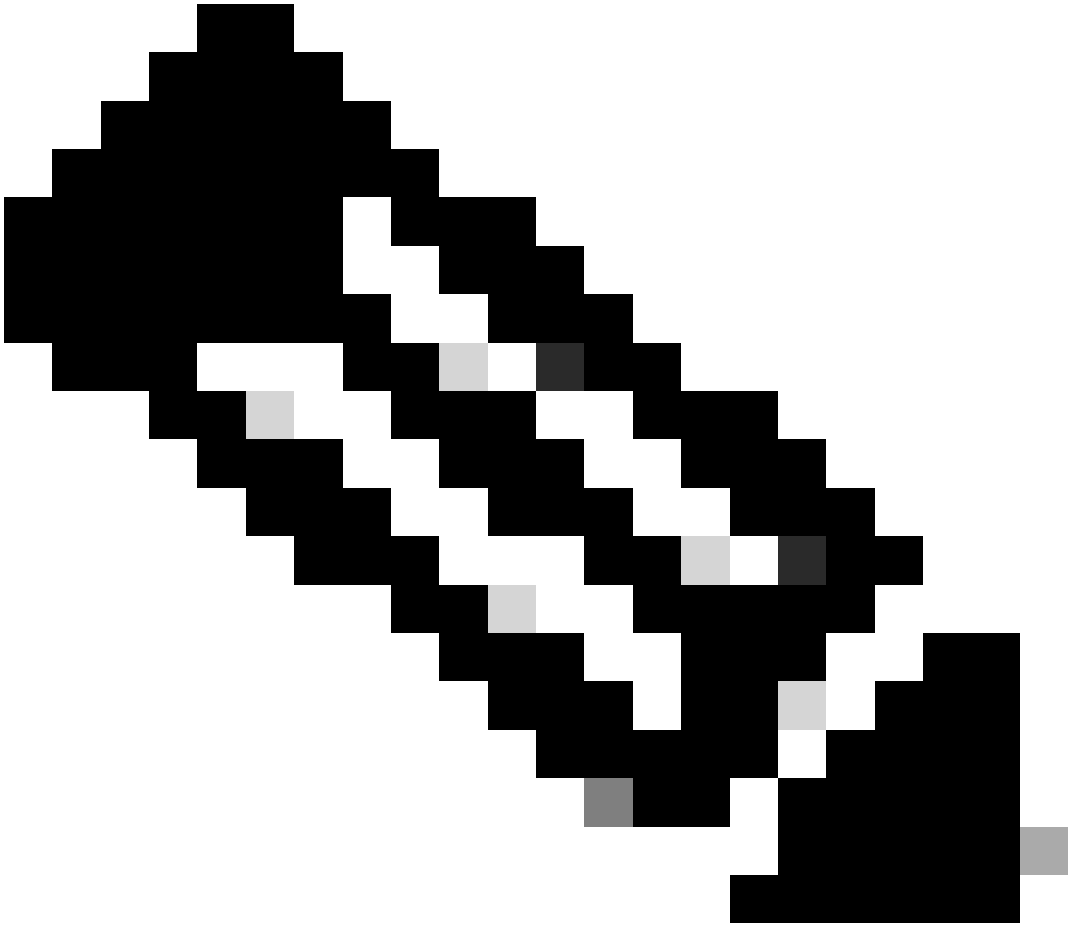
Configuración final de ASA local

```
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
```

Configuración final remota de ASA

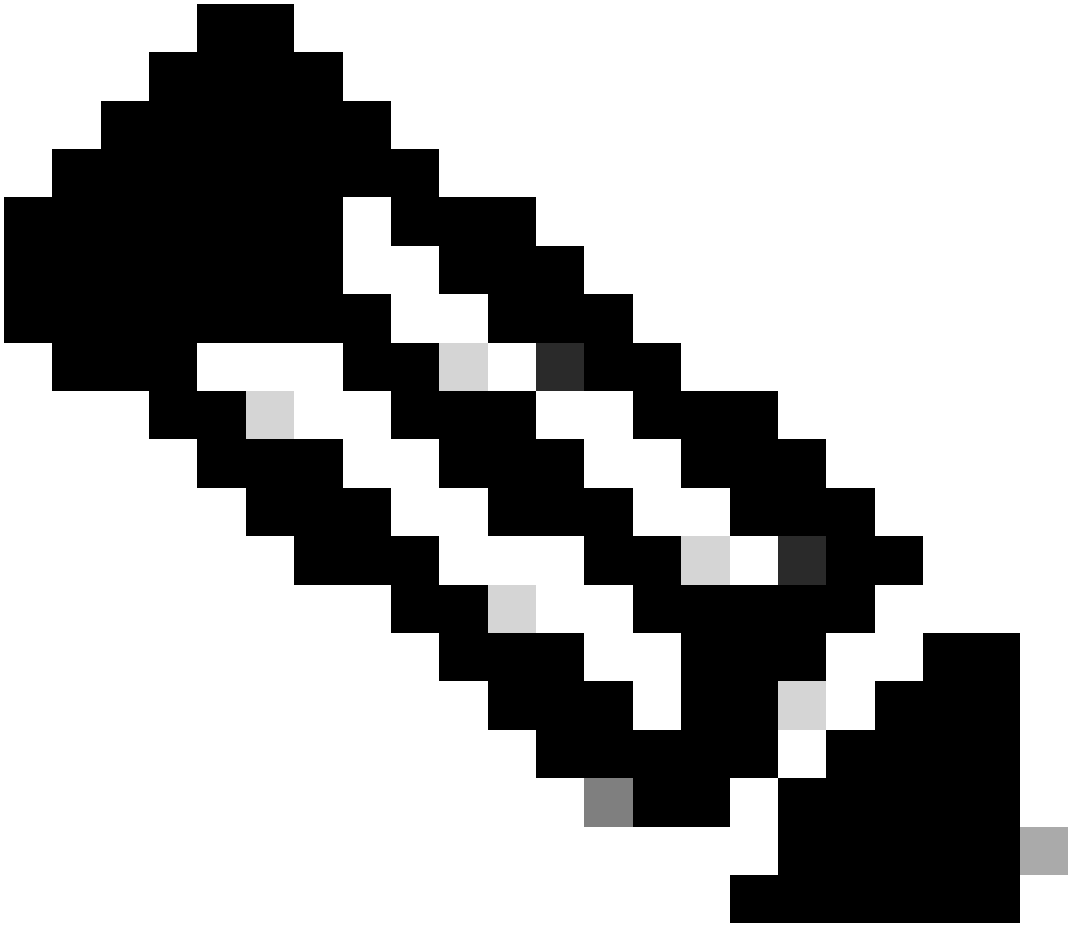
```
interface GigabitEthernet0/0 nameif outside security-level 0 ip address 10.20.20.20 255.255.255.0 ! interface GigabitEthernet0/1 nameif inside security-lev
```



Nota: La ACL está en el formato duplicado y las claves previamente compartidas son las mismas en ambos extremos.

Verificación

Antes de verificar si el túnel está activo y que está pasando el tráfico, debe asegurarse de que el tráfico interesante se envía a los ASA.



Nota: El rastreador de paquetes se utilizó para simular el flujo de tráfico. Se puede hacer usando el comando packet-tracer; packet-tracer input inside icmp 192.168.0.11 8 0 172.16.10.11 detallado en el Local-ASA.

Para validar los intercambios de claves adicionales, puede utilizar el show crypto ikev2 sa comando. Como se ve en el resultado, puede verificar los parámetros AKE para validar los algoritmos de intercambio seleccionados.

<#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

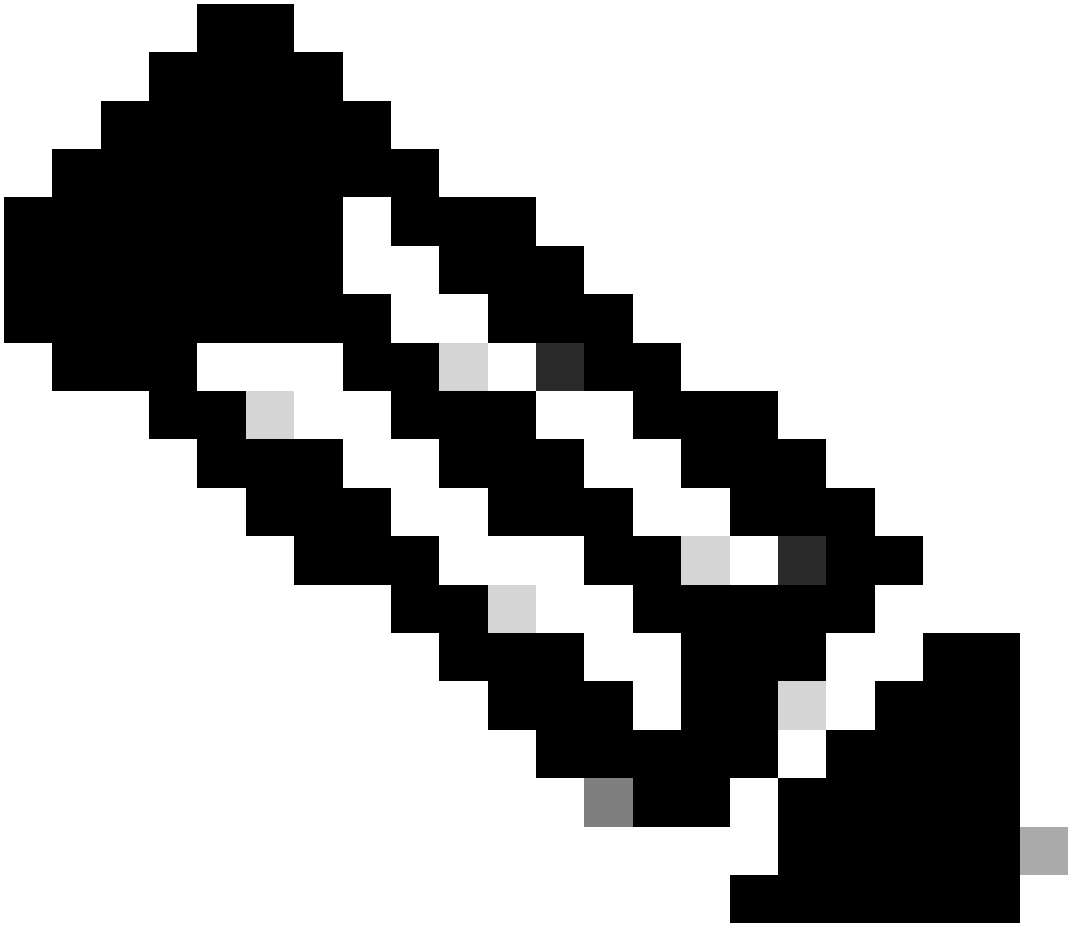
AKE1: 21 AKE2: 31

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

Troubleshoot

Las depuraciones mencionadas se pueden utilizar para resolver problemas del túnel IKEv2:

debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127



Nota: Si desea resolver problemas de un solo túnel (lo que debe ocurrir si el dispositivo está en producción), debe habilitar los debugs condicionalmente mediante el comando debug crypto condition peer X.X.X.X.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).