Configurar um túnel IKEv2 site a site entre dois ASAs usando várias trocas de chave IKEv2

Contents

Introdução

Este documento descreve como configurar uma conexão VPN IKEv2 Site a Site entre dois Cisco ASAs usando Intercâmbio de Várias Chaves IKEv2.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Adaptive Security Appliance (ASA)
- Conceitos gerais de IKEv2

Componentes Utilizados

As informações neste documento são baseadas nos Cisco ASAs que executam 9.20.1.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Limitações

A troca de várias chaves IKEv2 tem estas limitações:

- Suportado somente no ASA CLI
- Compatível com dispositivos HA e multicontextos
- Não há suporte em dispositivos em cluster

Licenciamento

Os requisitos de licenciamento são os mesmos para VPN Site a Site nos ASAs.

Informações de Apoio

Necessidade de trocas de chaves adicionais

A chegada de grandes computadores quânticos representa um grande risco para os sistemas de segurança, especialmente aqueles que usam criptografia de chave pública. Métodos criptográficos que foram considerados muito difíceis para computadores regulares podem ser quebrados facilmente por computadores quânticos. Assim, surge a necessidade de mudar para novos métodos de resistência quântica, também chamados de algoritmos de criptografia pós-quântica (PQC). O objetivo é melhorar a segurança da comunicação IPsec usando várias trocas de chaves. Isso envolve a combinação de uma troca de chaves tradicional com uma pós-quântica. Essa abordagem garante que a troca resultante seja pelo menos tão forte quanto a troca de chaves tradicional, fornecendo uma camada adicional de segurança.

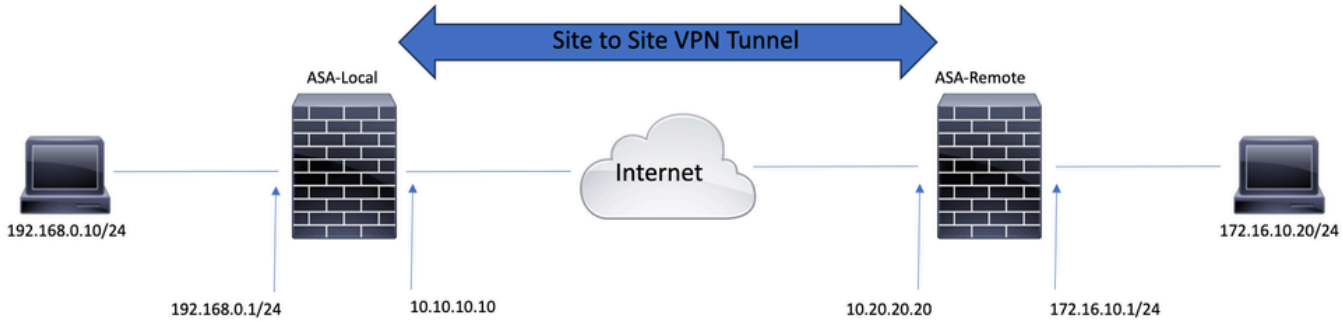
O plano é melhorar o IKEv2 adicionando suporte para várias trocas de chaves. Essas trocas de teclas extras podem lidar com algoritmos seguros contra ameaças quânticas. Para trocar informações sobre essas chaves adicionais, um novo tipo de mensagem chamado Intermediate Exchange é apresentado. Essas trocas de chaves são negociadas usando o método IKEv2 regular, através do payload SA.

Configurar

Esta seção descreve as configurações do ASA.

Diagrama de Rede

As informações neste documento usam esta configuração de rede:

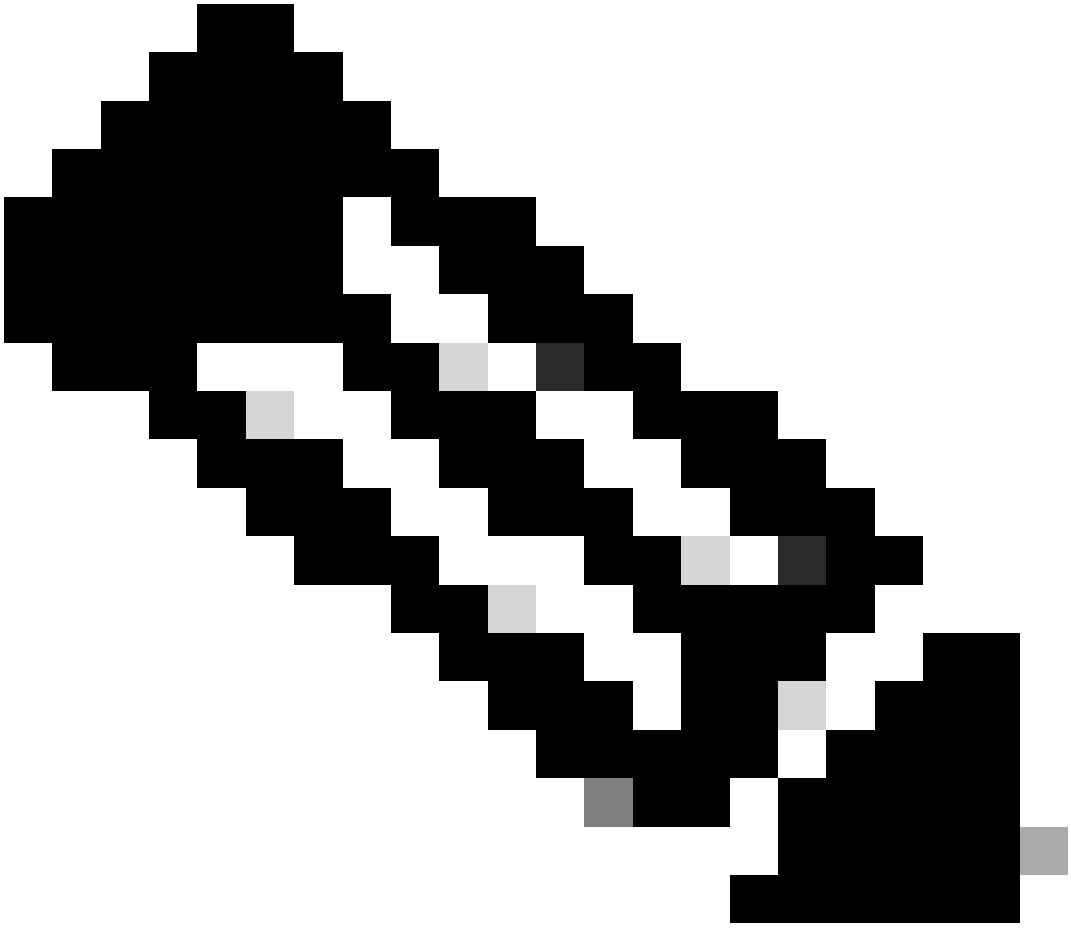


Configuração do ASA

Configurar as interfaces do ASA

Se as interfaces ASA não estiverem configuradas, certifique-se de configurar pelo menos os endereços IP, nomes de interface e níveis de segurança:

```
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
```



Observação: certifique-se de que haja conectividade com as redes internas e externas, especialmente com o peer remoto usado para estabelecer um túnel VPN site a site. Você pode usar um ping para verificar a conectividade básica.

Configure a política IKEv2 com a troca de várias chaves e habilite o IKEv2 na interface externa

Para configurar as políticas IKEv2 para essas conexões, insira estes comandos:

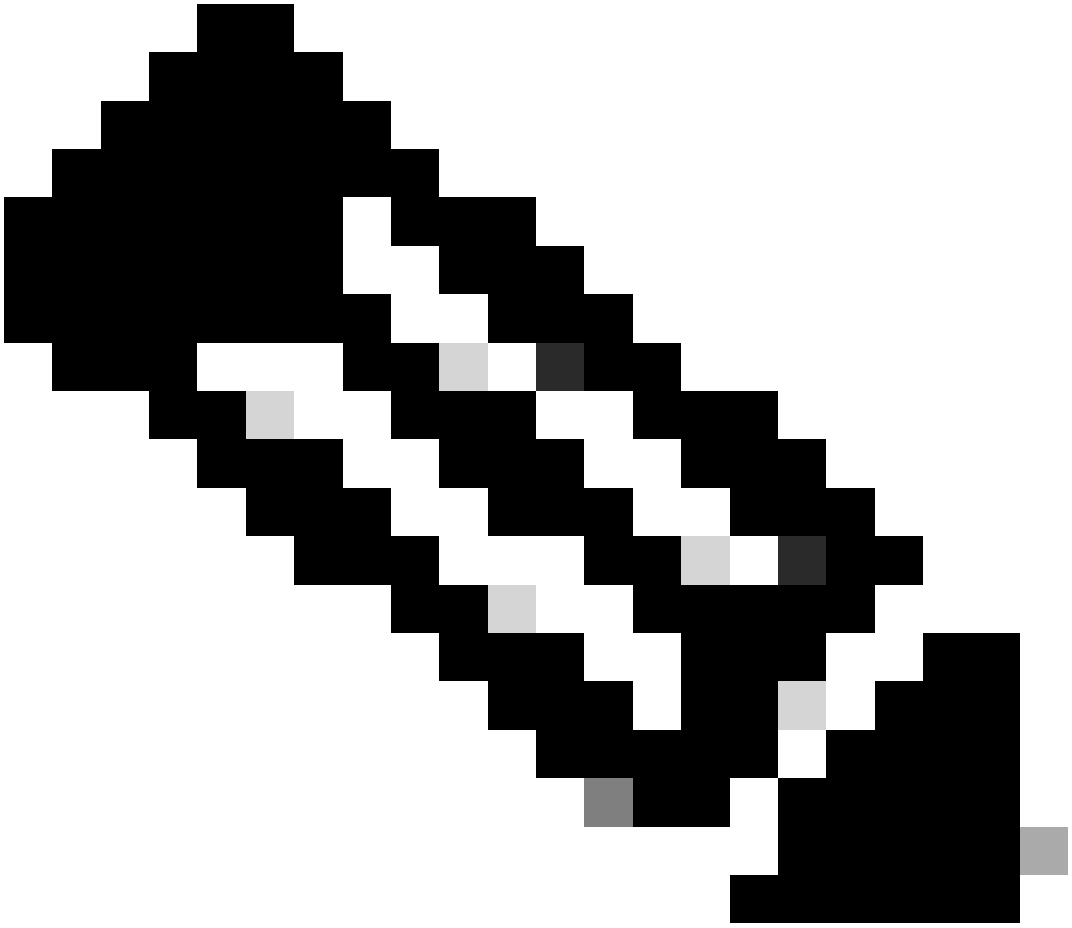
```
crypto ikev2 policy 10
 encryption aes-256
 integrity sha256
 group 20
 prf sha256
 lifetime seconds 86400
```

Transformações adicionais de troca de chaves podem ser configuradas sob crypto ikev2 policy o comandoadditional-key-exchange . Um total de sete transformações adicionais do Exchange podem ser configuradas. Neste exemplo, duas transformações de intercâmbio adicionais foram configuradas (usando grupos DH 21 e 31).

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

A política IKEv2 final se parece com esta:

```
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
```



Observação: existe uma correspondência de política IKEv2 quando ambas as políticas dos dois pares contêm os mesmos valores de autenticação, criptografia, hash, parâmetro Diffie-Hellman e parâmetro Additional Key Exchange.

Você deve habilitar o IKEv2 na interface que termina o túnel VPN. Geralmente, essa é a interface externa (ou de Internet). Para habilitar o IKEv2, insira o comandocrypto ikev2 enable outside no modo de configuração global.

Configurar o grupo de túneis

Para um túnel Site a Site, o tipo de perfil de conexão é IPSec-l2l. Para configurar a chave pré-compartilhada IKEv2, insira estes comandos:

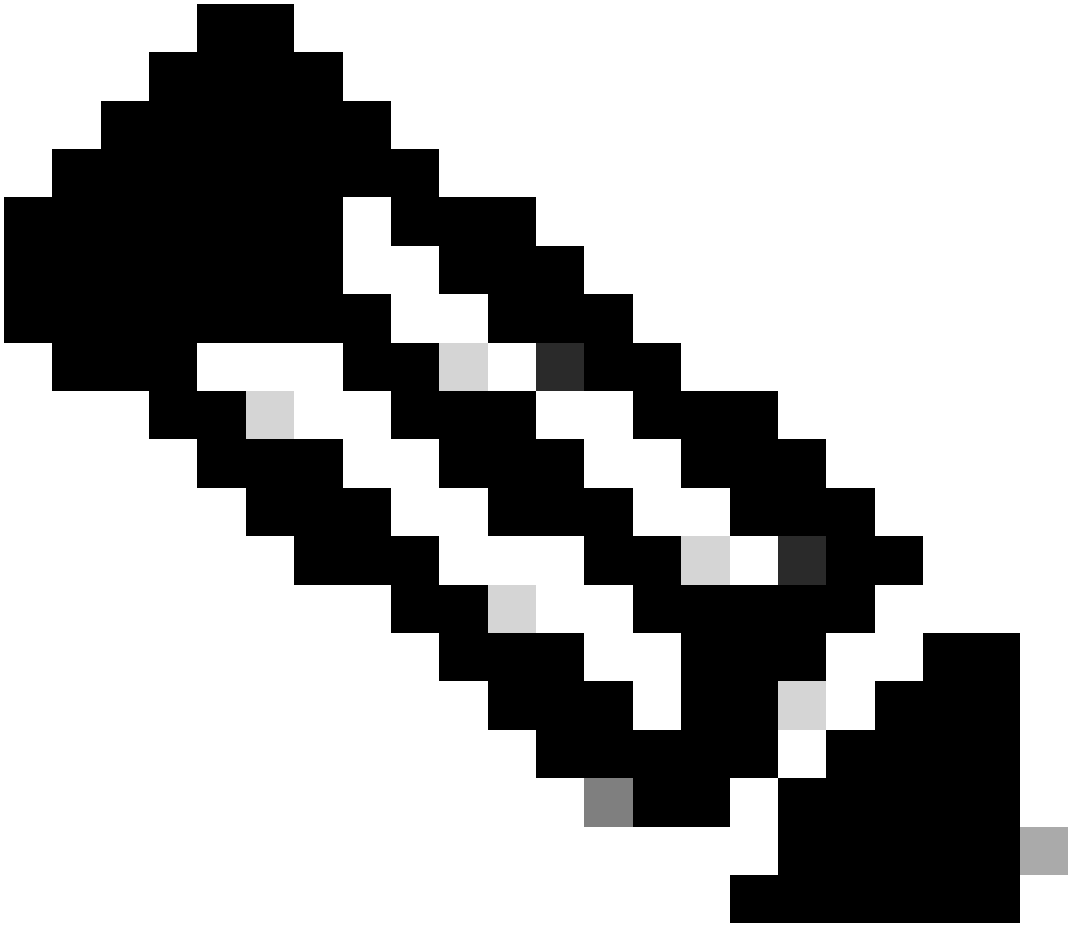
```
tunnel-group 10.20.20.20 type ipsec-l2l
tunnel-group 10.20.20.20 ipsec-attributes
 ikev2 remote-authentication pre-shared-key cisco
 ikev2 local-authentication pre-shared-key cisco
```

Configurar tráfego interessante e ACL de criptografia

O ASA usa Listas de Controle de Acesso (ACLs - Access Control Lists) para diferenciar o tráfego que deve ser protegido com criptografia IPSec do tráfego que não requer proteção. Ele protege os pacotes de saída que correspondem a um ACE (Application Control Engine, Mecanismo de controle de aplicativos) de permissão e garante que os pacotes de entrada que correspondem a um ACE de permissão tenham proteção.

```
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
```



Observação: o par VPN deve ter a mesma ACL em um formato espelhado.

Configurar um NAT de identidade (opcional)

Normalmente, um NAT de identidade é necessário para evitar que o tráfego interessante acesse o NAT dinâmico. O NAT de identidade que é configurado neste caso é:

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

Configurar a proposta IKEv2 IPSec

A proposta IKEv2 IPSec é usada para definir um conjunto de algoritmos de criptografia e integridade para proteger o tráfego de dados. Esta proposta deve corresponder a ambos os pares de VPN para criar um SA de IPSec com êxito. Os comandos usados nesse caso são:

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

Configurar um mapa de criptografia e vinculá-lo à interface

Um mapa de criptografia combina todas as configurações necessárias e deve necessariamente conter:

- Uma lista de acesso para corresponder ao tráfego que deve ser criptografado (comumente chamada de ACL criptografada)
- Identificação de Par
- Pelo menos uma proposta de IKEv2 IPSec

A configuração usada aqui é:

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

A parte final é aplicar esse mapa de criptografia à interface externa (pública) usando o comandocrypto map outside_map interface outside .

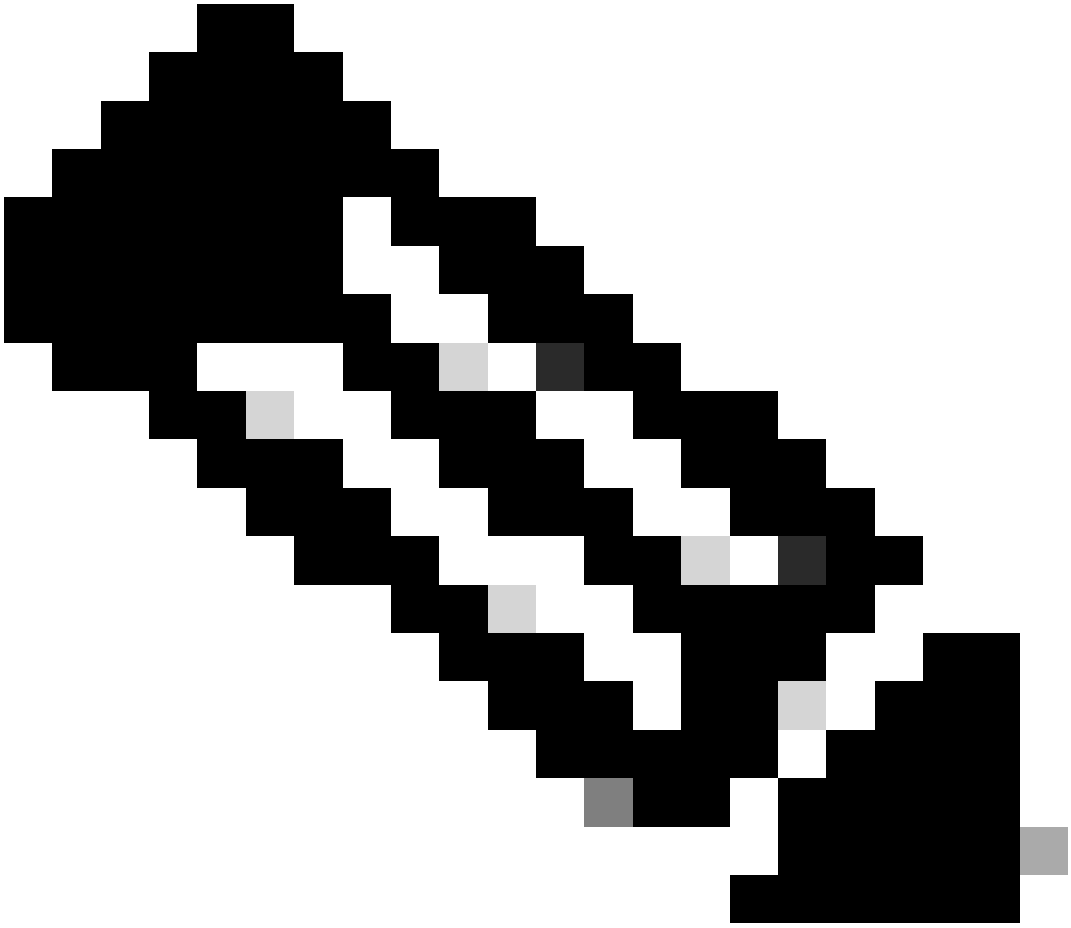
Configuração final do ASA local

```
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
```

Configuração final do ASA remoto

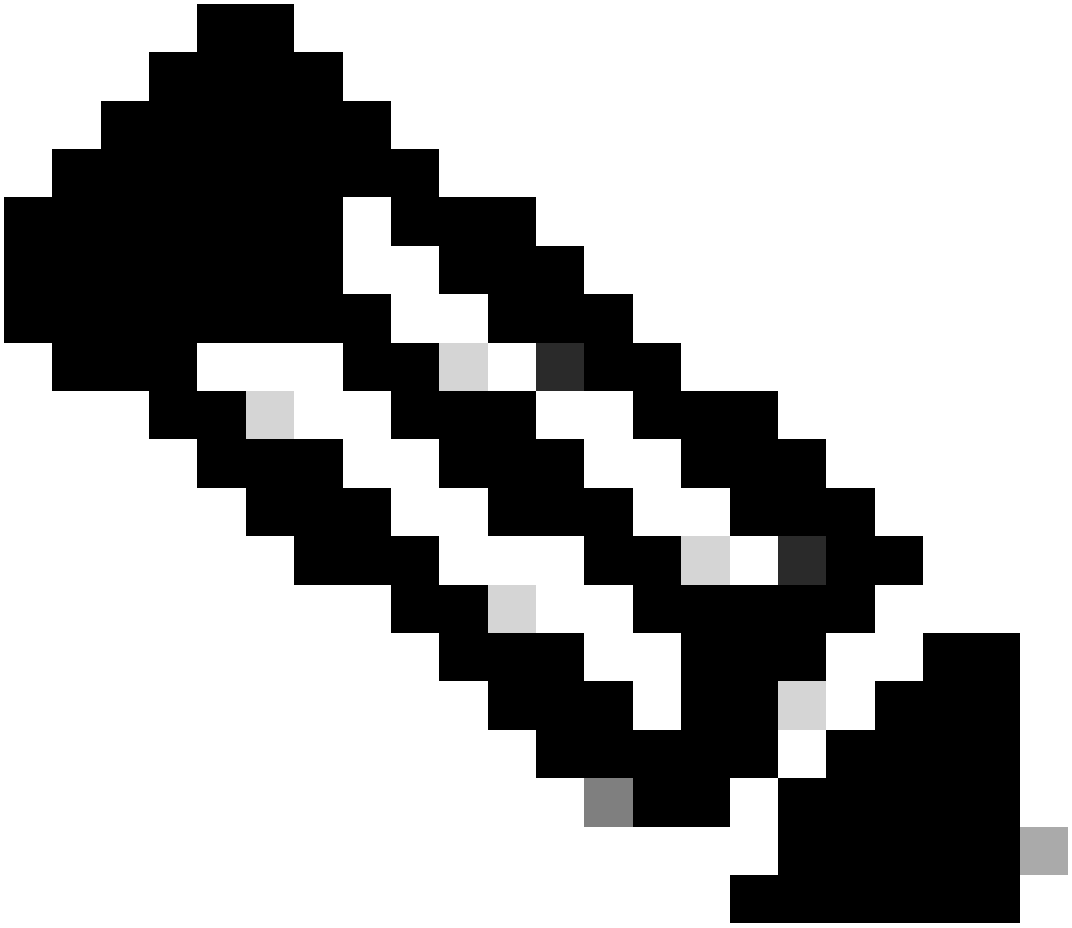
```
interface GigabitEthernet0/0 nameif outside security-level 0 ip address 10.20.20.20 255.255.255.0 ! interface GigabitEthernet0/1 nameif inside security-lev
```



Observação: a ACL está no formato espelhado e as chaves pré-compartilhadas são as mesmas em ambas as extremidades.

Verificar

Antes de verificar se o túnel está ativo e se está passando o tráfego, você deve garantir que o tráfego interessante esteja sendo enviado para os ASAs.



Observação: o packet tracer foi usado para simular o fluxo de tráfego. Isso pode ser feito usando o comando packet-tracer; packet-tracer input inside icmp 192.168.0.11 8 0 172.16.10.11 detalhado no Local-ASA.

Para validar as trocas de chave adicionais, você pode usar o show crypto ikev2 sa comando. Como visto na saída, você pode verificar os parâmetros AKE para validar os algoritmos de troca selecionados.

<#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

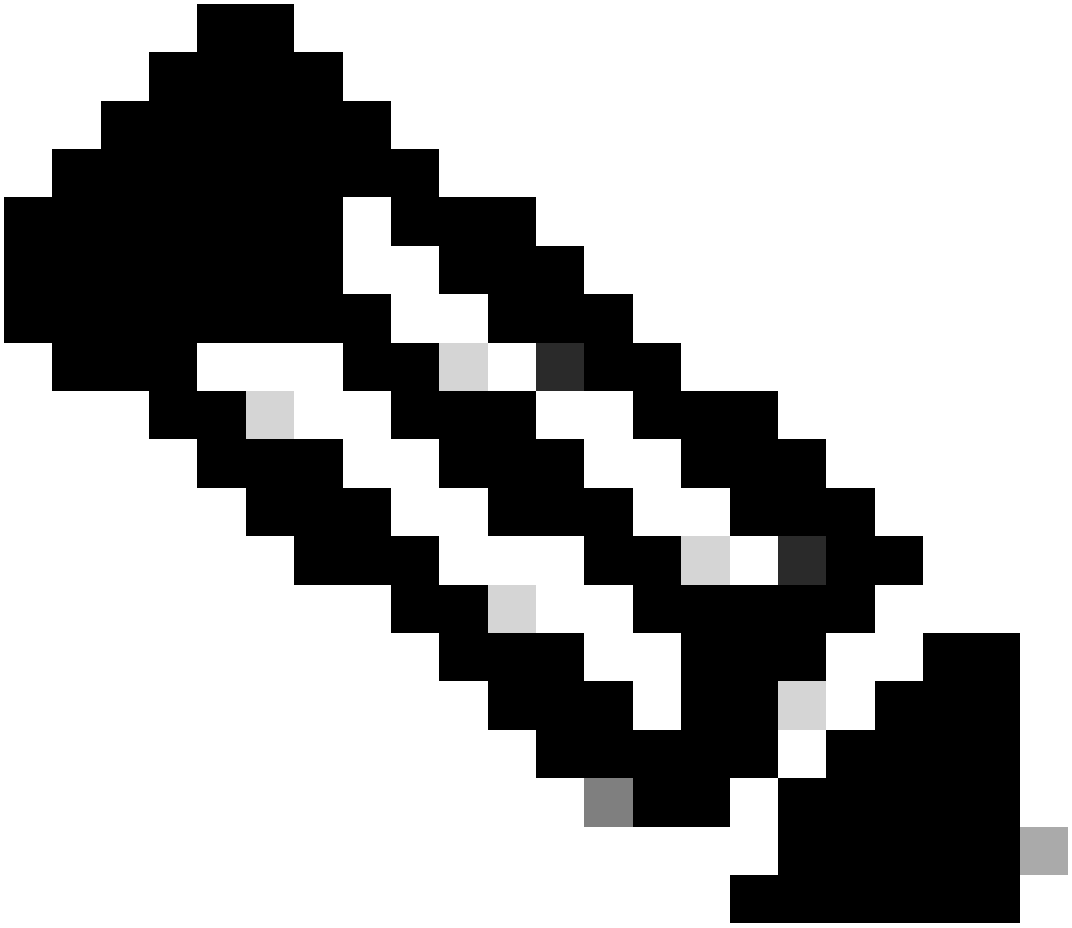
AKE1: 21 AKE2: 31

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

Troubleshooting

As depurações mencionadas podem ser usadas para solucionar problemas do túnel IKEv2:

debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127



Observação: se quiser solucionar problemas de apenas um túnel (que deve ser o caso se o dispositivo estiver em produção), você deverá ativar depurações condicionalmente usando o comando debug crypto condition peer X.X.X.X.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.