Configurar um túnel IPSec de site a site IKEv1 entre o ASA e o roteador Cisco IOS XE

Contents

Introdução

Este documento descreve como configurar um túnel IKEv1 site a site através da CLI entre um Cisco ASA e um roteador que executa o software Cisco IOS XE.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco IOS XE
- Cisco Adaptive Security Appliance (ASA)
- Conceitos gerais de IPSec

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ASAv executando o software Cisco versão 9.20(2)2
- Cisco CSRv executando o software Cisco IOS XE versão 17.03.03

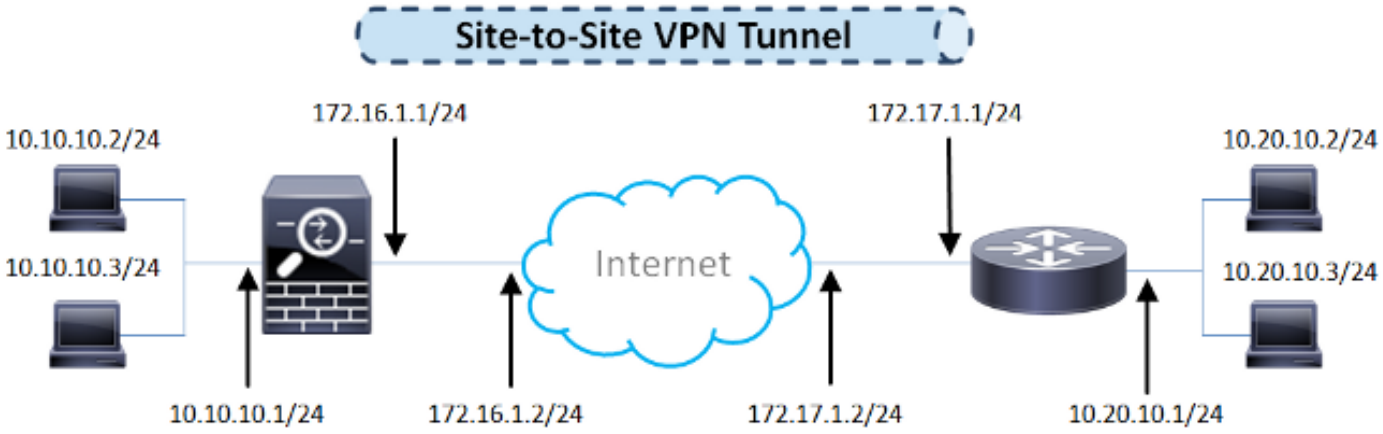
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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

Configurar

Esta seção descreve como concluir as configurações da CLI do roteador ASA e do Cisco IOS XE.

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, os nomes das interfaces e os níveis de segurança:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
```

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.

Configurar a política de IKEv1 e ativar o IKEv1 na interface externa

Para configurar as políticas de Internet Security Association and Key Management Protocol (ISAKMP) para as conexões IPSec Internet Key Exchange Version 1 (IKEv1), insira o`crypto ikev1 policy` comando:

```
<#root>
crypto ikev1 policy 10


 authentication pre-share
 encryption aes-256
 hash sha
 group 14
 lifetime 86400
```

Observação: existe uma correspondência de política IKEv1 quando ambas as políticas dos dois pares contêm os mesmos valores de parâmetro de autenticação, criptografia, hash e Diffie-Hellman. Para IKEv1, a política de peer remoto também deve especificar um tempo de vida menor ou igual ao tempo de vida na política que o iniciador envia. Se os tempos de vida não forem idênticos, o ASA usará o menor.

Observação: Se você não especificar um valor para um determinado parâmetro de política, o valor default será aplicado.

Você deve habilitar o IKEv1 na interface que termina o túnel VPN. Geralmente, essa é a interface externa (ou pública). Para habilitar o IKEv1, insira o`crypto ikev1 enable` comando no modo de configuração global:

```
<#root>

crypto ikev1 enable outside
```

Configurar o grupo de túneis (perfil de conexão LAN a LAN)

Para um túnel de LAN para LAN, o tipo de perfil de conexão é`ipsec-l2l`. Para configurar a chave pré-compartilhada IKEv1, entre no modo de configuração`tunnel-group ipsec-attributes`:

```
tunnel-group 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 ipsec-attributes
 ikev1 pre-shared-key cisco123
```

Configurar a ACL para o tráfego de VPN de interesse

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.

```
<#root>

object-group network

local-network


 network-object 10.10.10.0 255.255.255.0
object-group network
```

```
remote-network

 network-object 10.20.10.0 255.255.255.0

access-list asa-router-vpn extended permit ip object-group

local-network

 object-group

remote-network
```

> Observação: uma ACL para tráfego VPN usa os endereços IP origem e destino após a conversão de endereço de rede (NAT).

> Observação: uma ACL para o tráfego VPN deve ser espelhada em ambos os pares VPN.

> Observação: se houver necessidade de adicionar uma nova sub-rede ao tráfego protegido, basta adicionar uma sub-rede/host ao respectivo grupo de objetos e concluir uma alteração espelhada no peer da VPN remota.

Configurar uma isenção de NAT

> Observação: a configuração descrita nesta seção é opcional.

Normalmente, não deve haver NAT executado no tráfego VPN. Para isentar esse tráfego, você deve criar uma regra de NAT de identidade. A regra NAT de identidade simplesmente converte um endereço no mesmo endereço.

```
<#root>

nat (inside,outside) source static

local-network local-network

 destination static

remote-network remote-network

 no-proxy-arp route-lookup
```

Configurar o conjunto de transformação IKEv1

Um conjunto de transformação IKEv1 é uma combinação de protocolos de segurança e algoritmos que definem a forma como o ASA protege os dados. Durante as negociações da Associação de Segurança (SA) IPSec, os peers devem identificar um conjunto de transformação ou proposta que seja o mesmo para ambos os peers. Em seguida, o ASA aplica o conjunto de transformação correspondente ou a proposta para criar um SA que proteja os fluxos de dados na lista de acesso para esse mapa de criptografia.

Para configurar o conjunto de transformação IKEv1, insira o`crypto ipsec ikev1 transform-set`comando:

<#root>

```
crypto ipsec ikev1 transform-set ESP-AES256-SHA esp-aes-256 esp-sha-hmac
```

Configurar um mapa de criptografia e aplicá-lo a uma interface

Um mapa de criptografia define uma política de IPSec a ser negociada no IPSec SA e inclui:

- Uma lista de acesso para identificar os pacotes que a conexão IPSec permite e protege
- Identificação de pares
- Um endereço local para o tráfego de IPSec
- Os conjuntos de transformação IKEv1
- Discrição Perfeita (Opcional)

Aqui está um exemplo:

```
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES256-SHA
```

Em seguida, você pode aplicar o mapa de criptografia à interface:

<#root>

```
crypto map outside_map interface outside
```

Configuração final do ASA

Esta é a configuração final do ASA:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
!
object-group network local-network
 network-object 10.10.10.0 255.255.255.0
object-group network remote-network
 network-object 10.20.10.0 255.255.255.0
!
access-list asa-router-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 ikev1 policy 10
 authentication pre-share
 encryption aes-256
 hash sha
 group 14
 lifetime 86400
!
crypto ikev1 enable outside
!
crypto ipsec ikev1 transform-set ESP-AES256-SHA esp-aes-256 esp-sha-hmac
!
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES256-SHA
crypto map outside_map interface outside
!
tunnel-group 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 ipsec-attributes
 ikev1 pre-shared-key cisco123
!
```

Configuração CLI do roteador Cisco IOS XE

Configurar as interfaces

Se as interfaces do roteador Cisco IOS XE ainda não estiverem configuradas, pelo menos as interfaces LAN e WAN deverão ser configuradas. Aqui está um exemplo:

```
interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
 no shutdown
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
 no shutdown
```

Verifique se há 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.

Configurar a política de ISAKMP (IKEv1)

Para configurar as políticas de ISAKMP para as conexões IKEv1, insira o`crypto isakmp policy` comando no modo de configuração global. Aqui está um exemplo:

<#root>

```
crypto isakmp policy 10


 encryption aes 256
 hash sha
 authentication pre-share
 group 14
```

Observação: você pode configurar várias políticas IKE em cada peer que participa do IPSec. Quando a negociação IKE é iniciada, ela tenta encontrar uma política comum configurada em ambos os peers e começa com as políticas de prioridade mais alta especificadas no peer remoto.

Configurar uma chave ISAKMP de criptografia

Para configurar uma chave de autenticação pré-compartilhada, insira o`crypto isakmp key`comando no modo de configuração global:

<#root>

```
crypto isakmp key cisco123 address 172.16.1.1
```

Configurar uma ACL para o tráfego de VPN de interesse

Use a lista de acesso estendida ou nomeada para especificar o tráfego que deve ser protegido por criptografia. Aqui está um exemplo:

```
access-list 110 remark Interesting traffic access-list
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
```

Observação: uma ACL para tráfego VPN usa os endereços IP origem e destino após o NAT.

Observação: uma ACL para o tráfego VPN deve ser espelhada em ambos os pares VPN.

Configurar uma isenção de NAT

Observação: a configuração descrita nesta seção é opcional.

Normalmente, não deve haver NAT executado no tráfego VPN. Se a sobrecarga de NAT for usada, um mapa de rota deverá ser usado para isentar o tráfego VPN de interesse da conversão. Observe que na lista de acesso usada no mapa de rota, o tráfego VPN de interesse deve ser negado.

```
access-list 111 remark NAT exemption access-list
access-list 111 deny   ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 permit ip 10.20.10.0 0.0.0.255 any

route-map nonat permit 10
 match ip address 111

ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
```

Configurar um conjunto de transformação

Para definir um conjunto de transformação IPSec (uma combinação aceitável de protocolos e algoritmos de segurança), insira o`crypto ipsec transform-set`comando no modo de configuração global. Aqui está um exemplo:

```
<#root>

crypto ipsec transform-set ESP-AES256-SHA esp-aes 256 esp-sha-hmac


 mode tunnel
```

Configurar um mapa de criptografia e aplicá-lo a uma interface

Para criar ou modificar uma entrada de mapa de criptografia e entrar no modo de configuração do mapa de criptografia, insira o comando de configuração global crypto map. Para que a entrada do mapa de criptografia esteja completa, há alguns aspectos que devem ser definidos no mínimo:

- Os peers IPsec para os quais o tráfego protegido pode ser encaminhado devem ser definidos. Esses são os peers com os quais um SA pode ser estabelecido. Para especificar um peer IPSec em uma entrada de mapa de criptografia, insira o`set peer`comando.
- Os conjuntos de transformação aceitáveis para uso com o tráfego protegido devem ser definidos. Para especificar os conjuntos de transformação que podem ser usados com a entrada do mapa de criptografia, insira o`set transform-set`comando.
- O tráfego que deve ser protegido deve ser definido. Para especificar uma lista de acesso estendida para uma entrada de mapa de criptografia, insira o`match address`comando.

Aqui está um exemplo:

```
<#root>

crypto map outside_map 10 ipsec-isakmp


 set peer 172.16.1.1
 set transform-set ESP-AES256-SHA
 match address 110
```

A etapa final é aplicar o mapa de criptografia definido anteriormente a uma interface. Para aplicar isso, insira o comando de configuração de interface`crypto map`:

<#root>

```
interface GigabitEthernet0/0
```

crypto map outside_map

Configuração final do Cisco IOS XE

Esta é a configuração final da CLI do roteador Cisco IOS XE:

```
crypto isakmp policy 10
 encryption aes 256
 authentication pre-share
 group 14
crypto isakmp key cisco123 address 172.16.1.1
!
crypto ipsec transform-set ESP-AES256-SHA esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set ESP-AES256-SHA
 match address 110
!
interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
 crypto map outside_map
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
!
route-map nonat permit 10
 match ip address 111
!
access-list 110 remark Interesting traffic access-list
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 remark NAT exemption access-list
access-list 111 deny   ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 permit ip 10.20.10.0 0.0.0.255 any
```

Verificar

Antes de verificar se o túnel está ativo e se passa o tráfego, você deve garantir que o tráfego de interesse seja enviado para o roteador ASA ou para o roteador Cisco IOS XE.

Observação: no ASA, a ferramenta packet-tracer que corresponde ao tráfego de interesse pode ser usada para iniciar o túnel IPSec (como`packet-tracer input inside tcp 10.10.10.10 12345 10.20.10.10 80 detailed`por exemplo).

Fase 1 Verificação

Para verificar se a Fase 1 do IKEv1 está ativa no ASA, insira o comando show crypto isakmp sa. A saída esperada é para ver o estado`MM_ACTIVE`:

```
<#root>

ciscoasa#

show crypto isakmp sa


IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 172.17.1.1
    Type    : L2L             Role    : responder
    Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
ciscoasa#
```

Para verificar se a Fase 1 do IKEv1 está ativa no Cisco IOS XE, insira o`show crypto isakmp sa`comando. A saída esperada é para ver o estado`ACTIVE`:

```
<#root>

Router#

show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.16.1.1      172.17.1.1      QM_IDLE           2003 ACTIVE

IPv6 Crypto ISAKMP SA

Router#
```

Fase 2 Verificação

Para verificar se a Fase 2 do IKEv1 está ativa no ASA, insira o`show crypto ipsec sa`comando. A saída esperada é ver o SPI (Índice de Parâmetros de Segurança) de entrada e de saída. Se o tráfego passar pelo túnel, você deverá ver o incremento dos contadores encaps/decaps.

Observação: para cada entrada da ACL, uma SA de entrada/saída separada é criada, o que pode resultar em uma saída de comando`show crypto ipsec sa`longa (dependente do número de entradas ACE na ACL criptografada).

Aqui está um exemplo:

<#root>

```
ciscoasa#
```

`show crypto ipsec sa peer 172.17.1.1`

```
peer address: 172.17.1.1
    Crypto map tag: outside_map, seq num: 10, local addr: 172.16.1.1

access-list asa-router-vpn extended permit ip 10.10.10.0 255.255.255.0
   10.20.10.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
      current_peer: 172.17.1.1

#pkts encaps: 989, #pkts encrypt: 989, #pkts digest: 989
#pkts decaps: 989, #pkts decrypt: 989, #pkts verify: 989
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 989, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 172.16.1.1/0, remote crypto endpt.: 172.17.1.1/0
path mtu 1500, ipsec overhead 74(44), media mtu 1500
PMTU time remaining (sec): 0, DF policy: copy-df
ICMP error validation: disabled, TFC packets: disabled
current outbound spi: 5397114D
```

```
current inbound spi : 9B592959

inbound esp sas:
spi: 0x9B592959 (2606311769)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 2, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4373903/3357)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0xFFFFFFFF 0xFFFFD7FF

outbound esp sas:
spi: 0x5397114D (1402409293)
SA State: active
transform: esp-aes-256 esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 2, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (4373903/3357)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0x00000000 0x00000001

ciscoasa#
```

Para verificar se a Fase 2 do IKEv1 está ativa no Cisco IOS XE, insira o`show crypto ipsec sa`comando. A saída esperada é ver o SPI de entrada e de saída. Se o tráfego passar pelo túnel, você deverá ver o incremento dos contadores encaps/decaps.

Aqui está um exemplo:

<#root>

```
Router#
```

`show crypto ipsec sa peer 172.16.1.1`

```
interface: GigabitEthernet0/0
    Crypto map tag: outside_map, local addr 172.17.1.1

   protected vrf: (none)
local  ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
   current_peer 172.16.1.1 port 500
     PERMIT, flags={origin_is_acl,}
#pkts encaps: 989, #pkts encrypt: 989, #pkts digest: 989
#pkts decaps: 989, #pkts decrypt: 989, #pkts verify: 989
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
```

```
#send errors 0, #recv errors 0

local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
plaintext mtu 1438, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet3
current outbound spi: 0x9B592959(2606311769)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x5397114D(1402409293)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2003, flow_id: CSR:3, sibling_flags FFFFFFFF80004048, crypto map: outside_map
sa timing: remaining key lifetime (k/sec): (4607857/3385)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x9B592959(2606311769)
transform: esp-256-aes esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2004, flow_id: CSR:4, sibling_flags FFFFFFFF80004048, crypto map: outside_map
sa timing: remaining key lifetime (k/sec): (4607901/3385)
IV size: 16 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:

Router#
```

Verificação das Fases 1 e 2

Esta seção descreve os comandos que você pode usar no ASA ou no Cisco IOS XE para verificar os detalhes das Fases 1 e 2.

Insira o comando`show vpn-sessiondb`no ASA para verificação:

```
<#root>

ciscoasa#

show vpn-sessiondb detail l2l filter ipaddress 172.17.1.1


Session Type: LAN-to-LAN Detailed
```

```
Connection   : 172.17.1.1
Index        : 2                      IP Addr      : 172.17.1.1
Protocol     : IKEv1 IPsec
Encryption   : IKEv1: (1)AES256  IPsec: (1)AES256
Hashing      : IKEv1: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 98900                Bytes Rx     : 134504
Login Time   : 06:15:52 UTC Fri Sep 6 2024
Duration     : 0h:15m:07s
IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
  Tunnel ID    : 2.1
  UDP Src Port : 500                  UDP Dst Port : 500
  IKE Neg Mode : Main                 Auth Mode    : preSharedKeys
  Encryption   : AES256               Hashing      : SHA1
  Rekey Int (T): 86400 Seconds        Rekey Left(T): 84093 Seconds
  D/H Group    : 14
  Filter Name  :

IPsec:
  Tunnel ID    : 2.2
  Local Addr   : 10.10.10.0/255.255.255.0/0/0
  Remote Addr  : 10.20.10.0/255.255.255.0/0/0
  Encryption   : AES256               Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 3600 Seconds         Rekey Left(T): 3293 Seconds
  Rekey Int (D): 4608000 K-Bytes      Rekey Left(D): 4607901 K-Bytes
  Idle Time Out: 30 Minutes           Idle TO Left : 26 Minutes
  Bytes Tx     : 98900               Bytes Rx     : 134504
  Pkts Tx      : 989                 Pkts Rx      : 989

NAC:
  Reval Int (T): 0 Seconds            Reval Left(T): 0 Seconds
  SQ Int (T)   : 0 Seconds            EoU Age(T)   : 309 Seconds
  Hold Left (T): 0 Seconds            Posture Token:
  Redirect URL :

ciscoasa#
```

Insira o comando`show crypto session`no Cisco IOS XE para verificação:

<#root>

```
Router#
```

`show crypto session remote 172.16.1.1 detail`

```
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: GigabitEthernet0/0
```

```
Uptime: 00:03:36
Session status: UP-ACTIVE
Peer: 172.16.1.1 port 500 fvrf: (none) ivrf: (none)
      Phase1_id: 172.16.1.1
      Desc: (none)
  IKE SA: local 172.17.1.1/500 remote 172.16.1.1/500 Active
         Capabilities:(none) connid:1005 lifetime:23:56:23
  IPSEC FLOW: permit ip 10.20.10.0/255.255.255.0 10.10.10.0/255.255.255.0
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 989 drop 0 life (KB/Sec) 4449870/3383
        Outbound: #pkts enc'ed 989 drop 0 life (KB/Sec) 4449868/3383

Router#
```

Troubleshooting

Esta seção fornece informações que você pode usar para solucionar problemas da sua configuração.

Observação: consulte os documentos Informações Importantes sobre Comandos de Depuração e Troubleshooting de Segurança IP - Entendendo e Utilizando Comandos de Depuração da Cisco antes de utilizar os comandos de debug.

Ferramenta Verificador de LAN para LAN IPSec

Para verificar automaticamente se a configuração de LAN para LAN IPSec entre o ASA e o Cisco IOS XE é válida, você pode usar a ferramenta IPSec LAN para LANChecker. A ferramenta é projetada de modo que aceite um comando show tech ou show running-config de um roteador ASA ou Cisco IOS XE. Ele examina a configuração e tenta detectar se um túnel de IPSec LAN para LAN baseado em mapa de criptografia está configurado. Se configurado, ele executa uma verificação multiponto da configuração e destaca todos os erros e definições de configuração para o túnel que seria negociado.

Depurações do ASA

Para solucionar problemas de negociação de túnel IPSec IKEv1 em um firewall ASA, você pode usar estes debug comandos:

<#root>

```
debug crypto ipsec 127
debug crypto isakmp 127
debug ike-common 10
```

Observação: se o número de túneis VPN no ASA for significativo, o`debug crypto condition peer A.B.C.D`comando deverá ser usado antes de você habilitar as depurações para limitar as saídas de depuração para incluir somente o peer especificado.

Depurações do roteador Cisco IOS XE

Para solucionar problemas de negociação de túnel IPSec IKEv1 em um roteador Cisco IOS XE, você pode usar estes comandos de depuração:

<#root>

```
debug crypto ipsec
debug crypto isakmp
```

Observação: se o número de túneis VPN no Cisco IOS XE for significativo, o`debug crypto condition peer ipv4 A.B.C.D`deverá ser usado antes de você habilitar as depurações para limitar as saídas de depuração para incluir somente o peer especificado.

Dica: consulte o documento Soluções Mais Comuns de Troubleshooting de VPN IPSec de Acesso Remoto e L2L da Cisco para obter mais informações sobre como resolver problemas de VPN de site a site.

Referências

- Informações Importantes sobre Comandos de Depuração
- Troubleshooting de Segurança de IP - Entendendo e Utilizando Comandos debug
- Soluções de Troubleshooting Mais Comuns de VPN IPsec L2L e de Acesso Remoto
- Verificador de LAN para LAN IPSec
- Suporte Técnico e Documentação - Cisco Systems

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.