

# Configurar um túnel IPSec IKEv1 site a site entre um ASA e um roteador Cisco IOS

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração do ASA](#)

[Configurar as interfaces do ASA](#)

[Configurar a política de IKEv1 e ativar o IKEv1 na interface externa](#)

[Configurar o grupo de túneis \(perfil de conexão LAN a LAN\)](#)

[Configurar a ACL para o tráfego de VPN de interesse](#)

[Configurar uma isenção de NAT](#)

[Configurar o conjunto de transformação IKEv1](#)

[Configurar um mapa de criptografia e aplicá-lo a uma interface](#)

[Configuração final do ASA](#)

[Configuração CLI do roteador Cisco IOS](#)

[Configurar as interfaces](#)

[Configurar a política de ISAKMP \(IKEv1\)](#)

[Configurar uma chave ISAKMP de criptografia](#)

[Configurar uma ACL para o tráfego de VPN de interesse](#)

[Configurar uma isenção de NAT](#)

[Configurar um conjunto de transformação](#)

[Configurar um mapa de criptografia e aplicá-lo a uma interface](#)

[Configuração final do Cisco IOS](#)

[Verificar](#)

[Fase 1 Verificação](#)

[Fase 2 Verificação](#)

[Verificação das Fases 1 e 2](#)

[Troubleshoot](#)

[Ferramenta Verificador de LAN para LAN IPSec](#)

[Depurações do ASA](#)

[Depurações do Cisco IOS Router](#)

[Referências](#)

## Introduction

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

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

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

### Componentes Utilizados

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

- Cisco 5512-X Series ASA com software versão 9.4(1)
- Roteador de Serviços Integrados (ISR - Integrated Services Router) da Cisco série 1941 que executa o software Cisco IOS versão 15.4(3)M2

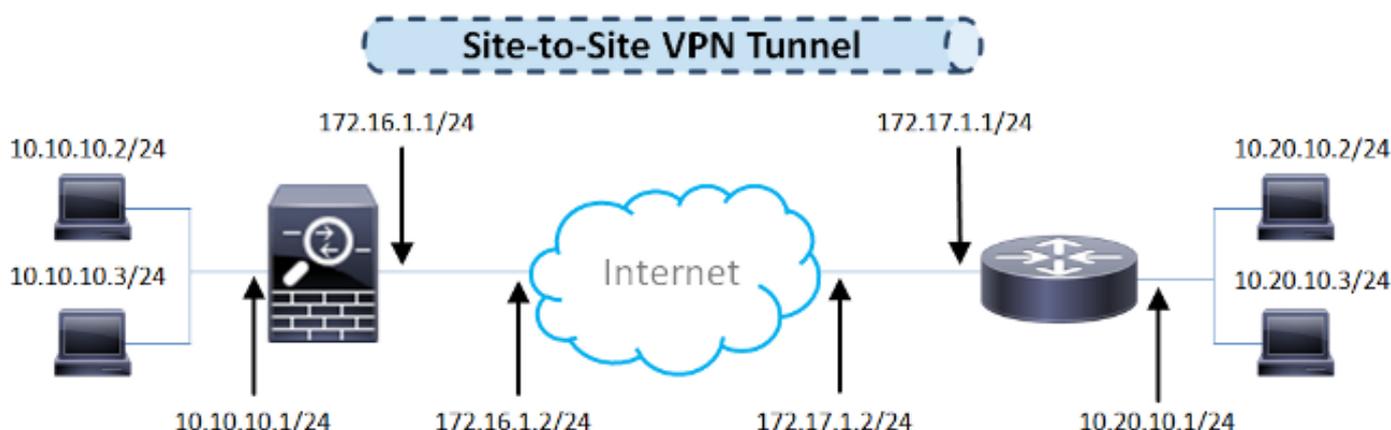
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Configurar

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

### 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 comando `crypto ikev1 policy` comando:

```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
 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 comando `crypto ikev1 enable` no modo de configuração global:

```
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, insira o comando `tunnel-group ipsec-attributes` modo de configuração global:

```
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.

```
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.

```
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 comando `crypto ipsec ikev1 transform-set` comando:

```
crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes 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

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-AES-SHA
```

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

```
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 ipsec ikev1 transform-set ESP-AES-SHA esp-aes 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-AES-SHA
crypto map outside_map interface outside

```

## Configuração CLI do roteador Cisco IOS

### Configurar as interfaces

Se as interfaces do roteador Cisco IOS 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 comando `crypto isakmp policy` no modo de configuração global. Aqui está um exemplo:

```

crypto isakmp policy 10
encr aes
authentication pre-share
group 2

```

**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 comando `crypto isakmp key` no modo de configuração global:

```
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 comando `crypto ipsec transform-set` no modo de configuração global. Aqui está um exemplo:

```
crypto ipsec transform-set ESP-AES-SHA esp-aes 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 comando `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 comando `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, digite o comando `match address` comando.

Aqui está um exemplo:

```
crypto map outside_map 10 ipsec-isakmp
set peer 172.16.1.1
set transform-set ESP-AES-SHA
match address 110
```

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

```
interface GigabitEthernet0/0
crypto map outside_map
```

## Configuração final do Cisco IOS

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

```
crypto isakmp policy 10
encr aes
authentication pre-share
group 2
crypto isakmp key cisco123 address 172.16.1.1
```

```

!
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
!
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set ESP-AES-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 Cisco IOS.

**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 ver o MM\_ACTIVE estado:

```
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, insira o comando `show crypto isakmp sa` comando. A saída esperada é ver o ACTIVE estado:

```
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       1005 ACTIVE

IPv6 Crypto ISAKMP SA

Router#
```

## Fase 2 Verificação

Para verificar se a Fase 2 do IKEv1 está ativa no ASA, insira o comando `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 longa `show crypto ipsec sa` saída do comando (dependente do número de entradas ACE na ACL criptografada).

Aqui está um exemplo:

```
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: 1005, #pkts encrypt: 1005, #pkts digest: 1005
  #pkts decaps: 1014, #pkts decrypt: 1014, #pkts verify: 1014
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 1005, #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: 8A9FE619
current inbound spi : D8639BD0
```

inbound esp sas:

```
spi: 0xD8639BD0 (3630406608)
transform: esp-aes esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (3914900/3519)
IV size: 16 bytes
replay detection support: Y
Anti replay bitmap:
0xFFFFFFFF 0xFFFFFFFF
```

outbound esp sas:

```
spi: 0x8A9FE619 (2325734937)
transform: esp-aes esp-sha-hmac no compression
in use settings ={L2L, Tunnel, IKEv1, }
slot: 0, conn_id: 8192, crypto-map: outside_map
sa timing: remaining key lifetime (kB/sec): (3914901/3519)
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, insira o comando `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:

```
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: 2024, #pkts encrypt: 2024, #pkts digest: 2024
#pkts decaps: 2015, #pkts decrypt: 2015, #pkts verify: 2015
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 26, #recv errors 0

local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current outbound spi: 0xD8639BD0(3630406608)
```

PFS (Y/N): N, DH group: none

inbound esp sas:

spi: 0x8A9FE619(2325734937)  
transform: esp-aes esp-sha-hmac ,  
in use settings ={Tunnel, }  
conn id: 2003, flow\_id: Onboard VPN:3, sibling\_flags 80000046,

crypto map: outside\_map

sa timing: remaining key lifetime (k/sec): (4449870/3455)  
IV size: 16 bytes  
replay detection support: Y  
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:

spi: 0xD8639BD0(3630406608)  
transform: esp-aes esp-sha-hmac ,  
in use settings ={Tunnel, }  
conn id: 2004, flow\_id: Onboard VPN:4, sibling\_flags 80000046,

crypto map: outside\_map

sa timing: remaining key lifetime (k/sec): (4449868/3455)  
IV size: 16 bytes  
replay detection support: Y  
Status: 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 para verificar os detalhes das Fases 1 e 2.

Digite o `show vpn-sessiondb` no ASA para verificação:

```
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)AES128 IPsec: (1)AES128
Hashing      : IKEv1: (1)SHA1 IPsec: (1)SHA1
Bytes Tx     : 100500                           Bytes Rx     : 101400
Login Time   : 18:06:02 UTC Wed Jul 22 2015
Duration     : 0h:05m: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   : AES128         Hashing        : SHA1
Rekey Int (T): 86400 Seconds  Rekey Left(T): 86093 Seconds
D/H Group    : 2
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     : AES128           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       : 100500           Bytes Rx      : 101400
Pkts Tx        : 1005             Pkts Rx      : 1014
```

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#

**Digite o show crypto session no Cisco IOS para verificação:**

```
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 2015 drop 0 life (KB/Sec) 4449870/3383
```

```
Outbound: #pkts enc'ed 2024 drop 26 life (KB/Sec) 4449868/3383
```

```
Router#
```

## Troubleshoot

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 debug comandos.

## 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 é válida, você pode usar a ferramenta [IPSec LAN para LANChecker](#). A ferramenta é projetada de modo que aceite um `show tech` or `show running-config` de um roteador ASA ou Cisco IOS. 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:

```
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` deve ser usado antes de habilitar as depurações para limitar as saídas de depuração para incluir somente o peer especificado.

## Depurações do Cisco IOS Router

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

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

**Observação:** se o número de túneis VPN no Cisco IOS for significativo, o `debug crypto condition peer ipv4 A.B.C.D` deve ser usado antes de você ativar 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.