Entender e usar os comandos de depuração para solucionar problemas de IPsec

Contents

Introdução

Este documento descreve os comandos de depuração comuns usados para solucionar problemas de IPsec no Cisco IOS®Software e no PIX/ASA.

Pré-requisitos

Requisitos

Este original supõe que você configurou o IPsec. Consulte Negociação IPSec/Protocolos IKE para obter mais detalhes.

Componentes Utilizados

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

- Cisco IOS® Software
  - Conjunto de recursos do IPsec.
  - 56i—Indica recurso único Data Encryption Standard (DES) (no Cisco IOS® Software Release 11.2 e posterior).
  - k2—Indica o recurso DES triplo (no Cisco IOS® Software Release 12.0 e posterior). O DES triplo está disponível no Cisco 2600 Series e mais tarde.
- PIX — V5.0 e mais tarde, que exige chave de licença uma única ou do DES triplo a fim ativar.

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.

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Informações de Apoio

Refira à mais comum L2L e Acesso Remoto IPsec VPN Troubleshooting Solutions para obter informações sobre as soluções mais comuns aos problemas do IPSec VPN.

Ele contém uma lista de verificação de procedimentos comuns que você pode tentar antes de começar a solucionar problemas em uma conexão e ligar para o Suporte Técnico da Cisco.

Depurações do software Cisco IOS®

Os tópicos nesta seção descrevem os comandos debug do software Cisco IOS®. Consulte Negociação IPSec/Protocolos IKE para obter mais detalhes.

show crypto isakmp sa

Esse comando mostraInternet Security Association Management Protocol (ISAKMP) Security Associations (SAs)o construído entre os peers.

```
dst          src        state     conn-id     slot
10.1.0.2  10.1.0.1   QM_IDLE    1           0
```

show crypto ipsec sa

Este comando mostra o IPsec SAs construído entre peers. O túnel criptografado é construído entre 10.1.0.1 e 10.1.0.2 para o tráfego que vai entre redes 10.1.0.0 e 10.1.1.0.

Você pode ver as duas Encapsulating Security Payload (ESP) SAs criadas de entrada e de saída. O cabeçalho de autenticação (AH) não é usado, pois não há SAs de AH.

Esta saída mostra um exemplo do**show crypto ipsec sa**comando.

```
<#root>

  interface: FastEthernet0
    Crypto map tag: test, local addr.

10.1.0.1

   local  ident (addr/mask/prot/port): (

10.1.0.0/255.255.255.0/0/0

)
   remote ident (addr/mask/prot/port): (
```

10.1.1.0/255.255.255.0/0/0

)
   current_peer:

10.1.0.2

     PERMIT, flags={origin_is_acl,}

#pkts encaps: 7767918, #pkts encrypt: 7767918, #pkts digest 7767918
**   #pkts decaps: 7760382, #pkts decrypt: 7760382, #pkts verify 7760382**

    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 1, #recv errors 0

     local crypto endpt.: 10.1.0.1, remote crypto endpt.: 10.1.0.2

     path mtu 1500, media mtu 1500
     current outbound spi: 3D3
     inbound

esp

 sas:
      spi: 0x136A010F(325714191)
        transform:

esp-3des esp-md5-hmac

 ,
        in use settings ={

Tunnel

, }
        slot: 0, conn id: 3442, flow_id: 1443, crypto map: test
        sa timing:

remaining key lifetime (k/sec): (4608000/52)

        IV size: 8 bytes
        replay detection support: Y
     inbound

ah

 sas:
     inbound pcp sas:
inbound pcp sas:
outbound

esp

 sas:
   spi: 0x3D3(979)
    transform:

esp-3des esp-md5-hmac

 ,
    in use settings ={

Tunnel

, }
    slot: 0, conn id: 3443, flow_id: 1444, crypto map: test

```
    sa timing:

 remaining key lifetime (k/sec): (4608000/52)

    IV size: 8 bytes
    replay detection support: Y
outbound

ah

 sas:
outbound pcp sas:
```

show crypto engine connection active

Este comando mostra cada fase 2 SA construído e a quantidade de tráfego enviado.

Como a fase 2 Security Associations (SAs)é unidirecional, cada SA mostra o tráfego em apenas uma direção (as criptografias são de saída e as descriptografias são de entrada).

debug crypto isakmp

Esta saída mostra um exemplo do **debug crypto isakmp**comando.

<#root>

```
processing SA payload. message ID = 0
Checking ISAKMP transform against priority 1 policy
    encryption DES-CBC
          hash SHA
    default group 2
    auth pre-share
    life type in seconds
    life duration (basic) of 240

atts are acceptable

. Next payload is 0
processing KE payload. message ID = 0
processing NONCE payload. message ID = 0
processing ID payload. message ID = 0
SKEYID state generated
processing HASH payload. message ID = 0
SA has been authenticated
processing SA payload. message ID = 800032287
```

debug crypto ipsec

Este comando mostra a origem e o destino dos pontos finais do túnel IPsec.Src_proxy e dest_proxysão as sub-redes do cliente.

sa createdDuas mensagens aparecem com uma em cada direção. (Quatro mensagens aparecem se

você executa o ESP e o AH.)

Esta saída mostra um exemplo do**debug crypto ipsec**comando.

<#root>

```
Checking IPSec proposal 1transform 1, ESP_DES
attributes in transform:
    encaps is 1
    SA life type in seconds
    SA life duration (basic) of 3600
    SA life type in kilobytes
    SA life duration (VPI) of 0x0 0x46 0x50 0x0
HMAC algorithm is SHA
```

atts are acceptable.
Invalid attribute combinations between peers will show up as "atts
** not acceptable".**

```
IPSEC(validate_proposal_request): proposal part #2,
(key eng. msg.) dest= 10.1.0.2, src=10.1.0.1,
      dest_proxy= 10.1.1.0/0.0.0.0/0/0,
      src_proxy= 10.1.0.0/0.0.0.16/0/0,
      protocol= ESP, transform= esp-des esp-sha-hmac
      lifedur= 0s and 0kb,
      spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 203563166 for SA
      from 10.1.0.2 to 10.1.0.1 for prot 2
IPSEC(spi_response): getting spi 194838793 for SA
      from 10.1.0.2 to 10.1.0.1 for prot 3
IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): ,
  (key eng. msg.) dest=
```

10.1.0.2

```
, src=
```

10.1.0.1

```
,
```

dest_proxy= 10.1.1.0/255.255.255.0/0/0,
**   src_proxy= 10.1.0.0/255.255.255.0/0/0,**

```
      protocol=
```

ESP

```
, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xC22209E(203563166), conn_id= 3,
              keysize=0, flags= 0x4
IPSEC(initialize_sas): ,
  (key eng. msg.) src=
```

10.1.0.2

```
, dest=
```

10.1.0.1,

```
 src_proxy= 10.1.1.0/255.255.255.0/0/0,
      dest_proxy= 10.1.0.0/255.255.255.0/0/0,

      protocol=
```

ESP

```
, transform= esp-des esp-sha-hmac
      lifedur= 3600s and 4608000kb,
      spi= 0xDED0AB4(233638580), conn_id= 6,
              keysize= 0, flags= 0x4
IPSEC(create_sa):
```

sa created

```
,
      (sa) sa_dest= 10.1.0.2, sa_prot= 50,
      sa_spi= 0xB9D0109(194838793),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
 IPSEC(create_sa):
```

sa created

```
,
      (sa) sa_dest= 10.1.0.2, sa_prot= 50,
      sa_spi= 0xDED0AB4(233638580),
      sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
```

Exemplo de mensagens de erro

Estes exemplos de mensagem de erro foram gerados dos comandos debug alistados aqui:

- **debug crypto ipsec**
- **debug crypto isakmp**
- **debug crypt engine**

Verificação da repetição falhada

Esta saída mostra um exemplo do"Replay Check Failed"erro:

```
%CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed connection id=#.
```

Esse erro é o resultado de uma reordenação no meio de transmissão (especialmente se existirem caminhos paralelos) ou caminhos desiguais de pacotes processados dentro do Cisco IOS® para pacotes grandes versus pequenos, além de carga.

Mude o conjunto de transformação para refletir isto. O reply check é visto somente quando o transform-set esp-md5-hmac está habilitado. Para suprimir esta mensagem de erro, desabiliteesp-md5-hmace execute

somente criptografia.

Consulte o bug da Cisco IDCSCdp19680 (somente clientes registrados).

QM FSM Error

O túnel do IPsec L2L VPN não vem acima no PIX Firewall ou no ASA, e a Mensagem de Erro QM FS aparece.

Uma razão possível é que as identidades de proxy, como tráfego incomumAccess Control List (ACL),ou ACL criptografada, não correspondem em ambas as extremidades.

Verifique a configuração em ambos os dispositivos, e certifique-se de que os crypto ACLs combinam.

Outra razão possível é uma incompatibilidade dos parâmetros do conjunto de transformação. Verifique se em ambas as extremidades os gateways VPN usam o mesmo conjunto de transformação com os mesmos parâmetros exatos.

Endereço local inválido

Esta saída mostra um exemplo da Mensagem de Erro:

```
IPSEC(validate_proposal): invalid local address 10.2.0.2
ISAKMP (0:3): atts not acceptable. Next payload is 0
ISAKMP (0:3): SA not acceptable!
```

Esta Mensagem de Erro é atribuída a um destes dois problemas comuns:

- **crypto map map-name local-address interface-id**O comando faz com que o roteador use um endereço incorreto como identidade, pois força o roteador a usar um endereço especificado.
- Crypto map é aplicado à interface incorreta ou não é aplicado de forma alguma. Verifique a configuração a fim assegurar-se de que o mapa de criptografia seja aplicado à interface correta.

Mensagem IKE de X.X.X.X falhou em sua verificação de sanidade ou está malformada

Este erro de debug aparece se as chaves pré-compartilhada nos peers não combinam. A fim fixar este problema, verifique as chaves pré-compartilhadas em ambos os lados.

```
1d00H:%CRPTO-4-IKMP_BAD_MESSAGE: IKE message from 198.51.100.1 failed its
 sanity check or is malformed
```

Processo de Modo Principal Falhou com Par

Este é um exemplo da mensagem`Main Mode`de erro. A falha do modo principal sugere que a política da fase 1 não combina em ambos os lados.

```
1d00h: ISAKMP (0:1): atts are not acceptable. Next payload is 0
1d00h: ISAKMP (0:1); no offers accepted!
1d00h: ISAKMP (0:1): SA not acceptable!
1d00h: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode failed with
peer at 198.51.100.1
```

Um comando show crypto isakmp sa mostra a ISAKMP SA em que`MM_NO_STATE`está. Isto também significa que o modo principal falhou.

```
dst          src        state             conn-id         slot
10.1.1.2  10.1.1.1   MM_NO_STATE        1           0
```

Verifique se a política da fase 1 está em ambos os peers, e assegure-se de que todos os atributos combinem.

```
Encryption DES or 3DES
Hash MD5 or SHA
Diffie-Hellman Group 1 or 2
Authentication {rsa-sig | rsa-encr | pre-share
```

Identidades de proxy não suportadas

Esta mensagem aparece em debugs se a lista de acessos para o tráfego de IPSec não combina.

```
1d00h: IPSec(validate_transform_proposal): proxy identities not supported
1d00h: ISAKMP: IPSec policy invalidated proposal
1d00h: ISAKMP (0:2): SA not acceptable!
```

As listas de acesso em cada peer precisam se espelhar (todas as entradas precisam ser reversíveis). Este exemplo ilustra este ponto.

```
Peer A
access-list 150 permit ip 172.21.113.0 0.0.0.255 172.21.114.0 0.0.0.255
```

```
access-list 150 permit ip host 10.2.0.8 host 172.21.114.123
Peer B
access-list 150 permit ip 172.21.114.0 0.0.0.255 172.21.113.0 0.0.0.255
access-list 150 permit ip host 172.21.114.123 host 10.2.0.8
```

Proposta de Transformação Não Suportada

Esta mensagem aparece se a fase 2 (IPsec) não combina em ambos os lados. Isto ocorre o mais frequentemente se há uma má combinação ou uma incompatibilidade no grupo da transformação.

```
1d00h: IPSec (validate_proposal): transform proposal
   (port 3, trans 2, hmac_alg 2) not supported
1d00h: ISAKMP (0:2) : atts not acceptable. Next payload is 0
1d00h: ISAKMP (0:2) SA not acceptable
```

Certifique-se de que haja correspondência do conjunto de transformações nos dois lados.

```
crypto ipsec transform-set transform-set-name transform1
[transform2 [transform3]]
? ah-md5-hmac
? ah-sha-hmac
? esp-des
? esp-des and esp-md5-hmac
? esp-des and esp-sha-hmac
? esp-3des and esp-md5-hmac
? esp-3des and esp-sha-hmac
? comp-lzs
```

Nenhum Cert e nenhuma chave com peer remoto

Esta mensagem indica que o endereço de peer configurado no roteador está errado ou mudou. Verifique que o endereço de peer está correto e que o endereço pode ser alcançado.

```
1d00h: ISAKMP: No cert, and no keys (public or pre-shared) with
remote peer 198.51.100.2
```

Endereço de correspondente X.X.X.X não encontrado

Essa mensagem de erro é exibida normalmente com VPN 3000 Concentrator a mensagem "Message: No proposal chosen(14)" de erro. Isso ocorre porque as conexões são host a host.

A configuração de roteador tem as propostas do IPsec em uma ordem onde a proposta escolhida

para o roteador combine a lista de acessos, mas não no peer.

A lista de acessos tem uma rede maior que inclua o host que cruza o tráfego. A fim de corrigir isto, faça a proposta de roteador para esta conexão de concentrador-à-roteador primeiramente na linha.

Isto permite que combine o host específico primeiramente.

```
20:44:44: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.0.2.15, src=198.51.100.6,
    dest_proxy= 10.0.0.76/255.255.255.255/0/0 (type=1),
    src_proxy= 198.51.100.23/255.255.255.255/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
20:44:44: IPSEC(validate_transform_proposal):
   peer address 198.51.100.6 not found
```

O pacote de IPsec tem o SPI inválido

Esta saída é um exemplo de Mensagem de Erro:

```
%PIX|ASA-4-402101: decaps: recd IPSEC packet has
invalid spi for destaddr=dest_address, prot=protocol, spi=number
```

O pacote IPsec recebido especifica um Security Parameters Index (SPI) pacote que não existe no Security Associations Database (SADB). Esta pode ser uma condição temporária devido a:

- Pequenas diferenças no envelhecimento de Security Sssociations (SAs) entre os correspondentes IPsec.
- As SAs locais foram limpas.
- Pacotes incorreto enviados pelo ipsec peer.

Isso é possivelmente um ataque.

Ação recomendada:

O peer possivelmente não reconhece que as SAs locais foram limpas. Se uma nova conexão é estabelecida do roteador local, os dois peers podem então restabelecer com sucesso. Caso contrário, se o problema ocorrer por mais de um breve período, tente estabelecer uma nova conexão ou entre em contato com o administrador desse peer.

PSEC(initialize_sas): IDs de proxy inválidas

O erro "21:57:57: IPSEC(initialize_sas): invalid proxy IDs"indica que a identidade de proxy recebida não corresponde à identidade de proxy configurada de acordo com a lista de acesso.

A fim assegurar-se de que ambos combinam, verifique a saída do comando debug.

Na saída do comando debug da solicitação de proposta, a access-list 103 permit ip 10.1.1.0 0.0.0.255 10.1.0.0 0.0.0.255 não corresponde.

A lista de acessos é rede-específica em uma extremidade e host-específica no outro.

```
21:57:57: IPSEC(validate_proposal_request): proposal part #1,
  (key eng. msg.) dest= 192.0.2.1, src=192.0.2.2,
    dest_proxy= 10.1.1.1/255.255.255.0/0/0 (type=4),
    src_proxy= 10.2.0.1/255.255.255.0/0/0 (type=4)
```

Reservado diferente de zero no Payload 5

Isto significa que as chaves ISAKMP não combinam. Rekey/restaurado a fim assegurar a precisão.

O algoritmo de hash oferecido não combina a política

Se as políticas de ISAKMP configuradas não combinam a política proposta pelo peer remoto, o roteador tenta a política padrão de 65535.

Se isso também não combina, ela falha a negociação de ISAKMP.

Um usuário recebe uma mensagem de"Hash algorithm offered does not match policy!""Encryption algorithm offered does not match policy!"erro nos roteadores.

<#root>

```
=RouterA=
3d01h: ISAKMP (0:1): processing SA payload. message ID = 0
3d01h: ISAKMP (0:1): found peer pre-shared key matched 203.0.113.22
ISAKMP (0:1):
```

Checking ISAKMP transform 1 against priority 1 policy

```
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0:1):
```

Hash algorithm offered does not match policy!

```
ISAKMP (0:1):
```

atts are not acceptable. Next payload is 0

```
=RouterB=
ISAKMP (0:1):
```

Checking ISAKMP transform 1 against priority 65535 policy

```
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash MD5
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP:      life type in seconds
ISAKMP:      life duration (VPI) of  0x0 0x1 0x51 0x80
ISAKMP (0:1):
```

Encryption algorithm offered does not match policy!

```
ISAKMP (0:1):
```

atts are not acceptable. Next payload is 0

```
ISAKMP (0:1):
```

no offers accepted!

```
ISAKMP (0:1):
```

phase 1 SA not acceptable!

Verificação HMAC Falhou

Esta mensagem de erro é relatada quando há uma falha na verificação doHash Message Authentication Codeno pacote IPsec. Isto acontece geralmente quando o pacote é corrompido de alguma maneira.

<#root>

```
Sep 22 11:02:39 203.0.113.16 2435:
Sep 22 11:02:39:
```

%MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure

```
Sep 22 11:02:39 203.0.113.16 2436:
Sep 22 11:02:39:
```

**%MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value = 0x20000,
PktEngReturn_MACMiscompare**

Se você ocasionalmente encontrar essa mensagem de erro, poderá ignorá-la. No entanto, se isso se tornar mais frequente, será necessário investigar a origem da corrupção do pacote. Isto pode ser devido a um defeito no acelerador de criptografia.

Peer remoto não responde

Este Mensagem de Erro é encontrada quando há uma má combinação ajustada da transformação. Verifique se os conjuntos de transformação correspondentes estão configurados em ambos os peers.

Todas as propostas IPSec SA foram consideradas inaceitáveis

Essa mensagem de erro ocorre quando os parâmetros de IPSec da fase 2 não correspondem entre os sites local e remoto.

Para resolver esse problema, especifique os mesmos parâmetros no conjunto de transformação para que eles correspondam e a VPN seja estabelecida com êxito.

Criptografia de pacote de informação/erro de descriptografia

Esta saída é um exemplo de Mensagem de Erro:

```
HW_VPN-1-HPRXERR: Virtual Private Network (VPN) Module0/2: Packet Encryption/Decryption
error, status=4615
```

Esta mensagem de erro é possivelmente devido a uma destas razões:

- Fragmentação — Os pacotes criptografados fragmentados são processos comutados, que forçam os pacotes comutados rapidamente a serem enviado ao cartão VPN antes dos pacotes comutados por processo.

Se pacotes comutados rapidamente suficientes são processados antes dos pacotes comutados por processamento, o número de seqüência ESP ou AH para o pacote comutado por processamento torna-se velho, e quando o pacote chega no cartão VPN, seu número de seqüência está fora do indicador da repetição.

Isto causa os erros do número de seqüência AH ou ESP (4615 e 4612, respectivamente), dependentes de qual capsulagem você usa.

- Entradas de cache antigas — Um outro exemplo em que este poderia possivelmente acontecer é quando uma entrada de cache do fast-switch torna-se velho e o primeiro pacote com uma falha de cache torna o processo comutado.

Soluções

1. Retire qualquer tipo de autenticação no 3DES conjunto de transformação, e use ESP-DES/3DES. Isso efetivamente desabilita a proteção de autenticação/antireprodução, que (por sua vez) evita erros de queda de pacotes relacionados ao tráfego IPsec não ordenado (misto) %HW_VPN-1-HPRXERR: Hardware VPN0/2: Packet Encryption/Decryption error, status=4615.

2. Uma solução que se aplica ao motivo mencionado aqui é definir o tamanho dos Maximum Transmission Unit (MTU) fluxos de entrada para menos de 1400 bytes. Incorpore este comando a fim ajustar o tamanho da unidade de transmissão máxima (MTU) de córregos de entrada a menos de 1400 bytes:

```
ip tcp adjust-mss 1300
```

3. Desabilite o cartão AIM.
4. Desligue o interruptor rápido/CEF nas interfaces do roteador. Para remover a switching rápida, use este comando no modo de configuração de interface:

```
no ip route-cache
```

Os pacotes recebem o erro devido à falha da seqüência ESP

Está aqui um exemplo de Mensagem de Erro:

```
%C1700_EM-1-ERROR: packet-rx error: ESP sequence fail
```

Este Mensagem de Erro geralmente indica uma destas possíveis circunstâncias:

- Os pacotes de criptografia do IPsec são enviados fora de serviço pelo roteador de criptografia devido a um mecanismo de QoS do desconfigurado.
- Os pacotes IPsec recebidos pelo roteador de descriptografia estão fora de serviço devido a uma reorganização de pacotes em um dispositivo intermediário.
- O pacote de IPsec recebido é fragmentado e exige a remontagem antes da verificação de autenticação e da decifração.

Solução

1. Desabilite QoS para o tráfego de IPSec na criptografia ou nos roteadores intermediários.
2. Habilite a pré-fragmentação do IPsec no roteador de criptografia.

```
<#root>
Router(config-if)#
crypto ipsec fragmentation before-encryption
```

3. Ajuste o valor MTU a um tamanho que não tenha que ser fragmentado.

```
<#root>

Router(config)#

interface type [slot_#/]port_#
```

```
<#root>

Router(config-if)#

ip mtu MTU_size_in_bytes
```

4. Atualize a imagem do Cisco IOS® para a imagem estável disponível mais recente nessa trilha.

Se o tamanho da MTU for alterado em qualquer roteador, todos os túneis terminados nessa interface deverão ser desativados.

Planeje concluir essa solução alternativa durante um tempo de inatividade programado.

Erro tentando estabelecer o túnel VPN no 7600 Series Router

Este erro é recebido quando você tenta estabelecer um túnel VPN no 7600 Series Router:

```
crypto_engine_select_crypto_engine: can't handle any more
```

Este erro ocorre porque a criptografia de software não é suportada nos 7600 Series Routers. Os 7600 Series Router não apoiam a terminação do túnel sem o hardware IPsec SPA. O VPN é apoiado somente com um cartão IPSEC-SPA no 7600 Router.

Debugs de PIX

show crypto isakmp sa

Esse comando mostra o ISAKMP SA construído entre peers.

```
dst          src        state     conn-id     slot
10.1.0.2  10.1.0.1   QM_IDLE    1           0
```

Na saída show crypto isakmp sa, o estado deve ser sempre `QM_IDLE`. Se o estado é MM_KEY_EXCH, significa que ou a chave pré-compartilhada configurada não está correta ou os endereços IP do peer são diferentes.

<#root>

```
PIX(config)#
```

show crypto isakmp sa

```
Total     : 2
Embryonic : 1
        dst               src        state     pending     created
 192.168.254.250   10.177.243.187    MM_KEY_EXCH   0           0
```

Você pode retificar isto quando você configura corretamente o endereço IP ou a chave pré-compartilhada.

show crypto ipsec sa

Este comando mostra o IPsec SAs construído entre peers. Um túnel criptografado é construído entre 10.1.0.1 e 10.1.0.2 para o tráfego que vai entre redes 10.1.0.0 e 10.1.1.0.

Você pode ver os dois SAs ESP criados interna e externamente. O AH não é usado desde que não há nenhum AH SA.

Um exemplo do**show crypto ipsec sa**comando é mostrado nesta saída.

<#root>

```
interface: outside
    Crypto map tag: vpn, local addr. 10.1.0.1
   local  ident (addr/mask/prot/port): (
```

10.1.0.0/255.255.255.0/0/0

```
)
   remote ident (addr/mask/prot/port): (
```

10.1.0.2/255.255.255.255/0/0

```
)
   current_peer: 10.2.1.1
```

dynamic allocated peer ip: 10.1.0.2

```
     PERMIT, flags={}
    #pkts encaps: 345, #pkts encrypt: 345, #pkts digest 0
    #pkts decaps: 366, #pkts decrypt: 366, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0,
    #pkts decompress failed: 0, #send errors 0, #recv errors 0
     local crypto endpt.: 10.1.0.1, remote crypto endpt.: 10.1.0.2
     path mtu 1500, ipsec overhead 56, media mtu 1500
     current outbound spi: 9a46ecae
     inbound
```

esp

```
 sas:
```

```
      spi: 0x50b98b5(84646069)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={
```

Tunnel

```
, }
        slot: 0, conn id: 1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (460800/21)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:

     inbound pcp sas:

     outbound
```

esp

```
 sas:
      spi: 0x9a46ecae(2588339374)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={
```

Tunnel

```
, }
        slot: 0, conn id: 2, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (460800/21)
        IV size: 8 bytes
        replay detection support: Y
    outbound ah sas:
```

debug crypto isakmp

Este comando indica as informações de debug sobre conexões IPsec e mostra o primeiro grupo de atributos que são negados devido às incompatibilidades em ambas as extremidades.

A segunda tentativa de correspondência (tentar 3DES em vez de DES eSecure Hash Algorithm (SHA)isso é aceitável, e a SA ISAKMP é construída.

Este debug é de um cliente dial-up que aceita um endereço IP (10.32.8.1) fora do pool local. Uma vez que ISAKMP SA é construído, os atributos do IPsec são negociados e encontrados aceitáveis.

O PIX ajusta-se ao IPsec SAs como visto aqui. Esta saída mostra um exemplo do**debug crypto isakmp**comando.

<#root>

```
crypto_isakmp_process_block: src 10.1.0.1, dest 10.1.0.2
OAK_AG exchange
ISAKMP (0): processing SA payload. message ID = 0
ISAKMP (0): Checking ISAKMP transform 1 against priority 1 policy
ISAKMP:      encryption DES-CBC
ISAKMP:      hash MD5
```

```
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP (0):
```

atts are not acceptable

```
. Next payload is 3
ISAKMP (0): Checking ISAKMP transform 3 against priority 1 policy
ISAKMP:      encryption 3DES-CBC
ISAKMP:      hash SHA
ISAKMP:      default group 1
ISAKMP:      auth pre-share
ISAKMP (0):
```

atts are acceptable

```
. Next payload is 3
ISAKMP (0): processing KE payload. message ID = 0
ISAKMP: Created a peer node for 10.1.0.2
OAK_QM exchange
ISAKMP (0:0): Need config/address
ISAKMP (0:0): initiating peer config to 10.1.0.2. ID = 2607270170 (0x9b67c91a)
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.1.0.2, dest 10.1.0.1
ISAKMP_TRANSACTION exchange
ISAKMP (0:0): processing transaction payload from 10.1.0.2.
   message ID = 2156506360
ISAKMP: Config payload CFG_ACK
ISAKMP (0:0):
```

peer accepted the address!

```
ISAKMP (0:0): processing saved QM.
oakley_process_quick_mode:
OAK_QM_IDLE
ISAKMP (0): processing SA payload. message ID = 818324052
ISAKMP : Checking IPSec proposal 1
ISAKMP: transform 1, ESP_DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
IPSEC(validate_proposal): transform proposal
   (prot 3, trans 2, hmac_alg 1) not supported
ISAKMP (0):
```

atts not acceptable.

```
 Next payload is 0
ISAKMP : Checking IPSec proposal 2
ISAKMP: transform 1, ESP_3DES
ISAKMP:   attributes in transform:
ISAKMP:      authenticator is HMAC-MD5
ISAKMP:      encaps is 1
ISAKMP (0):
```

atts are acceptable.

```
ISAKMP (0): processing NONCE payload. message ID = 818324052
ISAKMP (0): processing ID payload. message ID = 81
ISAKMP (0): ID_IPV4_ADDR src 10.32.8.1 prot 0 port 0
ISAKMP (0): processing ID payload. message ID = 81
ISAKMP (0): ID_IPV4_ADDR dst 10.1.0.1 prot 0 port 0
INITIAL_CONTACTIPSEC(key_engine): got a queue event...
```

debug crypto ipsec

Este comando indica informações de debug sobre conexões IPSec.

<#root>

```
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xd532efbd(3576885181) for SA
        from  10.1.0.2  to  10.1.0.1  for prot 3
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 10.1.0.2, dest 10.1.0.1
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0):
```

Creating IPSec SAs
inbound SA from 10.1.0.2 to 10.1.0.1
(proxy 10.32.8.1 to 10.1.0.1.)
has spi 3576885181 and conn_id 2 and flags 4
outbound SA from 10.1.0.1 to 10.1.0.2
(proxy 10.1.0.1 to 10.32.8.1)
has spi 2749108168 and conn_id 1 and flags 4IPSEC(key_engine):
got a queue event...
IPSEC(initialize_sas

```
): ,
  (key eng. msg.) dest= 10.1.0.1, src=10.1.0.2,
    dest_proxy= 10.1.0.1/0.0.0.0/0/0 (type=1),
    src_proxy= 10.32.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xd532efbd(3576885181), conn_id= 2, keysize= 0, flags= 0x4
IPSEC(
```

initialize_sas

```
): ,
  (key eng. msg.) src=10.1.0.1, dest= 10.1.0.2,
    src_proxy= 10.1.0.1/0.0.0.0/0/0 (type=1),
    dest_proxy= 10.32.8.1/0.0.0.0/0/0 (type=1),
    protocol= ESP, transform= esp-3des esp-md5-hmac ,
    lifedur= 0s and 0kb,
    spi= 0xa3dc0fc8(2749108168), conn_id= 1, keysize= 0, flags= 0x4
return status is IKMP_NO_ERROR
```

Problemas comuns de roteador para VPN Client

Incapacidade de acessar sub-redes fora do túnel VPN: túnel dividido

Este exemplo de saída da configuração do roteador mostra como ativar um túnel dividido para as conexões VPN.

O **split tunnel**comando é associado ao grupo conforme configurado no**crypto isakmp client configuration group hw-client-**

groupnamecomando.

Isso permite queCisco VPN Client o use o roteador para acessar uma sub-rede adicional que não seja parte do túnel VPN.

Isso é feito sem comprometer a segurança da conexão IPsec. O túnel é formado na rede 192.0.2.18.

O tráfego flui sem criptografia para dispositivos não definidos no**access list 150**comando, como a Internet.

<#root>

!

crypto isakmp client configuration group hw-client-groupname

 key hw-client-password
 dns 192.0.2.20 198.51.100.21
 wins 192.0.2.22 192.0.2.23
 domain cisco.com
 pool dynpool

acl 150

!
!

access-list 150 permit ip 192.0.2.18 0.0.0.127 any

!

Problemas comuns de PIX para VPN Client

Os assuntos nesta seção endereçam os problemas comuns que você encontra quando você configura o PIX ao IPsec com a ajuda do cliente VPN 3.x. As configurações de amostra para o PIX são baseadas na versão 6.x.

O tráfego não flui depois que o túnel é estabelecido: não é possível fazer ping dentro da rede atrás do PIX

Esse é um problema comum associado ao roteamento. Assegure-se de que o PIX tenha uma rota para as redes que estão no interno e são conectadas não diretamente à mesma sub-rede.

Também, a rede interna precisa de ter uma rota de volta ao PIX para os endereços no pool do endereço de cliente.

Esta saída mostra um exemplo.

```
!--- Address of PIX inside interface.

ip address inside 10.1.1.1 255.255.255.240

!--- Route to the networks that are on the inside segment. !--- The next hop is the router on the inside

route inside 172.16.0.0 255.255.0.0 10.1.1.2 1

 !--- Pool of addresses defined on PIX from which it assigns !--- addresses to the VPN Client for the I

ip local pool mypool 10.1.2.1-10.1.2.254

!--- On the internal router, if the default gateway is not !--- the PIX inside interface, then the route

ip route 10.1.2.0 255.255.255.0 10.1.1.1
```

Depois que o túnel estiver ativado, o usuário não poderá navegar na Internet: Túnel dividido

O motivo mais comum para este problema é que, com o túnel de IPsec do cliente VPN ao PIX, todo o tráfego está enviado através do túnel ao PIX Firewall.

A funcionalidade PIX não permite que o tráfego seja enviado para a interface onde foi recebida. Portanto, o tráfego destinado à Internet não funciona.

Para corrigir esse problema, use**split tunnel**o comando. A ideia atrás deste reparo é que somente um envia o tráfego específico através do túnel e o resto do tráfego vai diretamente para a Internet, não através do túnel.

<#root>

vpngroup vpn3000 split-tunnel 90

```
access-list 90 permit ip 10.1.1.0 255.255.255.0 10.1.2.0 255.255.255.0
access-list 90 permit ip 172.16.0.0 255.255.0.0 10.1.2.0 255.255.255.0
```

vpngroup vpn3000 split-tunnel 90O comando ativa o túnel dividido comaccess-list number 90.

access-list number 90O comando define qual tráfego flui pelo túnel, o resto do qual é negado no final da lista de acesso.

A lista de acesso precisa ser a mesma paraNetwork Address Translation (NAT)negar o PIX.

Depois que o túnel é ativado, certos aplicativos não funcionam: ajuste de MTU no cliente

Após o túnel ser estabelecido, embora você possa fazer ping nas máquinas na rede atrás do PIX Firewall, você não pode usar certos aplicativos como o Microsoft

Outlook

Um problema comum é o tamanho máximo da unidade de transferência (MTU) dos pacotes. O cabeçalho IPSec pode ter de 50 a 60 bytes, que são adicionados ao pacote original.

Se o tamanho do pacote for maior que 1500 (o padrão para a Internet), a seguir os dispositivos precisam ser fragmentados. Depois que este adiciona o cabeçalho IPSec, o tamanho está ainda abaixo de 1496, que é o máximo para o IPsec.

O **show interface**comando mostra a MTU dessa interface específica nos roteadores que estão acessíveis ou nos roteadores em suas próprias instalações.

Para determinar a MTU de todo o caminho da origem para o destino, os datagramas de vários tamanhos são enviados comDo Not Fragment (DF)o conjunto de bits de modo que, se o datagrama enviado for maior que a MTU, esta mensagem de erro seja enviada de volta à origem:

```
frag. needed and DF set
```

Esta saída mostra um exemplo de como encontrar o MTU do trajeto entre os hosts com endereços IP 10.1.1.2 e 172.16.1.56.

<#root>

```
Router#
debug ip icmp
ICMP packet debugging is on

!--- Perform an extended ping.

Router#
ping
Protocol [ip]:
Target IP address:
172.16.1.56
Repeat count [5]:
Datagram size [100]:
1550
Timeout in seconds [2]:

!--- Make sure you enter y for extended commands.

Extended commands [n]:
y
```

```
Source address or interface:
10.1.1.2
Type of service [0]:


!--- Set the DF bit as shown.


Set DF bit in IP header? [no]:
y
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1550-byte ICMP Echos to 172.16.1.56, timeout is 2 seconds:

2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
2w5d: ICMP: dst (172.16.1.56): frag. needed and DF set.
Success rate is 0 percent (0/5)


!--- Reduce the datagram size further and perform extended ping again.

Router#
ping
Protocol [ip]:
Target IP address:
172.16.1.56
Repeat count [5]:
Datagram size [100]:
1500
Timeout in seconds [2]:
Extended commands [n]:
y
Source address or interface:
10.1.1.2
Type of service [0]:
Set DF bit in IP header? [no]:
y
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 172.16.1.56, timeout is 2 seconds:
!!!!!
```

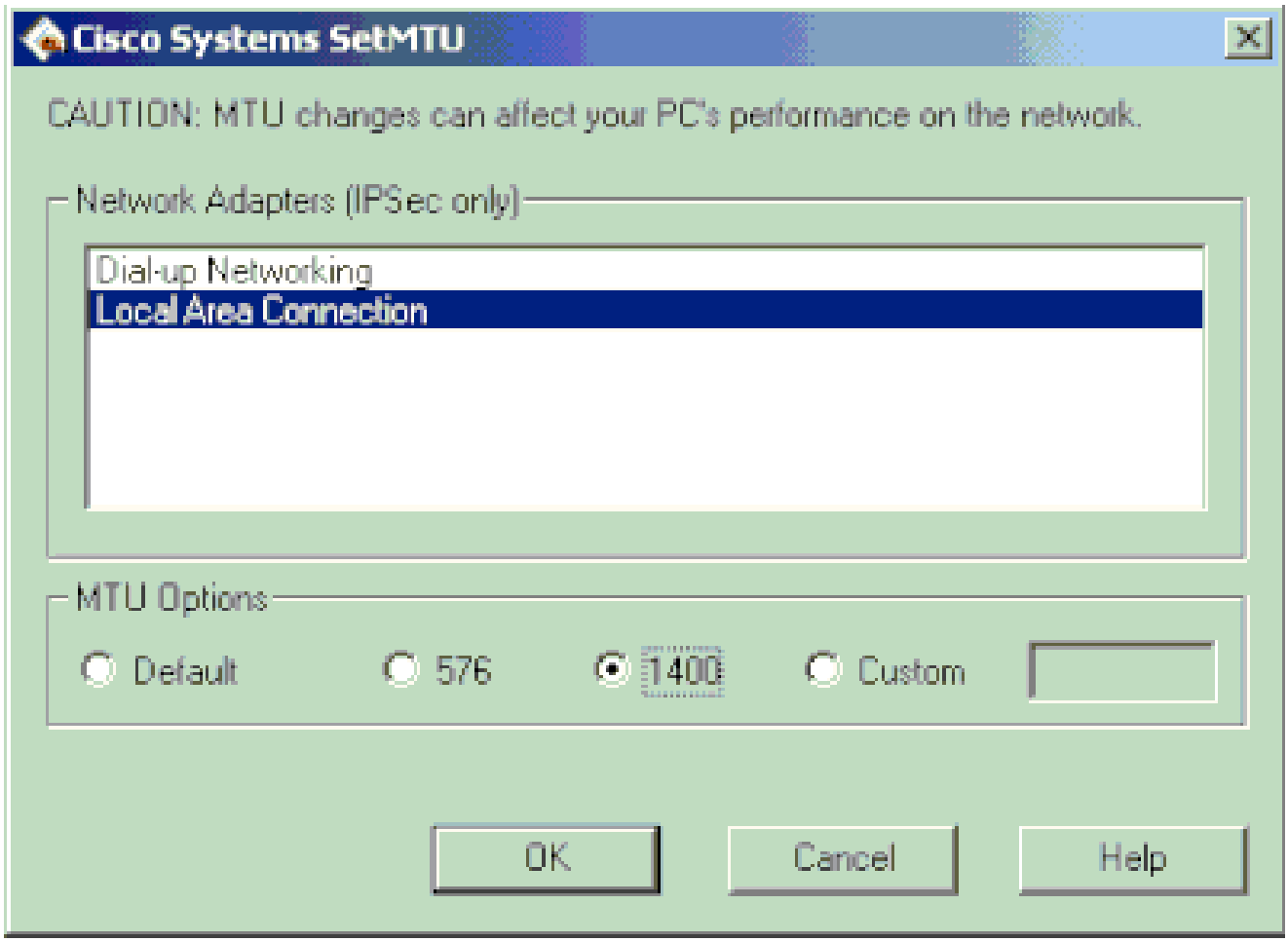
```
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2
2w5d: ICMP: echo reply rcvd, src 172.16.1.56, dst 10.1.1.2

Success rate is 100 percent (5/5), round-trip min/avg/max = 380/383/384 ms
```

O cliente VPN vem com uma utilidade de ajuste de MTU que permite que o usuário ajuste o MTU para o Cisco VPN Client.

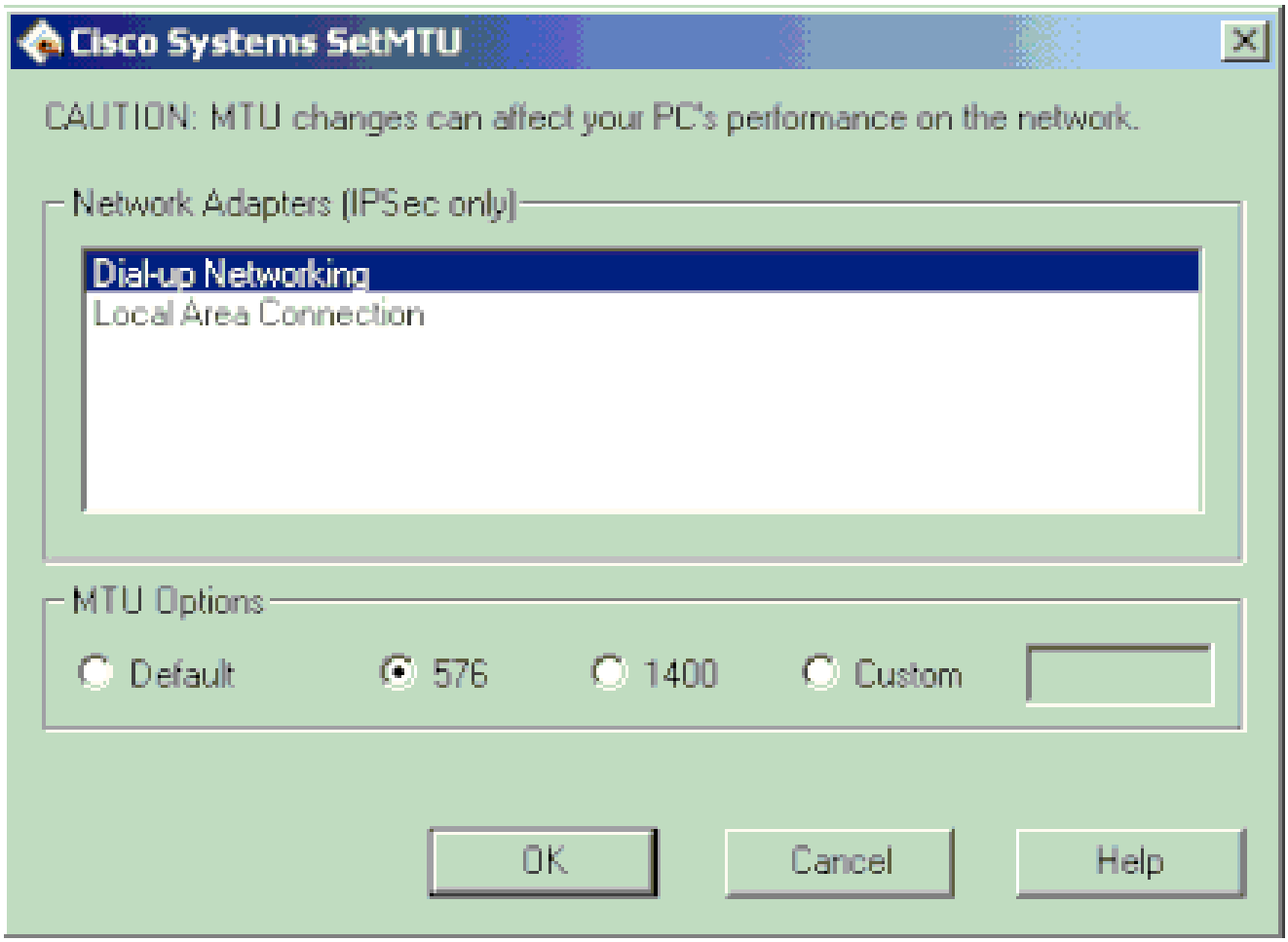
No caso dos usuários cliente do PPP over Ethernet (PPPoE), ajuste o MTU para o adaptador PPPoE.

Termine estas etapas a fim ajustar o utilitário MTU para o cliente VPN.

1. Escolher **Start** > **Programs** > **Cisco System VPN Client** > **Set MTU**.
2. Selecione**Local Area Connection**e clique no botão de opção 1400.
3. Clique em**OK**.



4. Repita a etapa 1 e selecione**Dial-up Networking**.
5. Clique no 576botão de opção e clique em**OK**.



Perca o comando sysopt

Use o **sysopt connection permit-ipsec**comando nas configurações de IPsec no PIX para permitir que o tráfego de IPsec passe pelo PIX Firewall sem uma verificação**conduitaccess-list**ou instruções de comando.

Por padrão, qualquer sessão de entrada deve ser explicitamente permitida por uma instrução de **conduit** comando ou de **access-list**comando. Com tráfego protegido de IPSec, a verificação de lista de acesso secundária pode ser redundante.

Para permitir que sessões de entrada de IPsec autenticadas/cifradas sempre sejam permitidas, use**sysopt connection permit-ipsec**o comando.

Verifique as listas de controle de acesso (ACL)

Há duas listas de acesso usadas em uma configuração de VPN IPsec típica. Uma lista de acessos é usada para isentar o tráfego que é destinado para o túnel VPN do processo NAT.

A outra lista de acessos define que tráfego a criptografar. Isso inclui uma ACL criptografada em uma configuração de LAN para LAN ou uma ACL de túnel dividido em uma configuração de acesso remoto.

Quando essas ACLs são configuradas incorretamente ou perdidas, o tráfego possivelmente flui apenas em uma direção pelo túnel VPN ou não foi enviado pelo túnel.

Certifique-se de ter configurado todas as listas de acesso necessárias para concluir sua configuração de VPN IPsec e de que essas listas de acesso definem o tráfego correto.

Esta lista contém artigos para verificar quando você suspeita que um ACL é a causa dos problemas com seu IPSec VPN.

- Certifique-se de que seus isenção de NAT e ACLs cript. especificam o tráfego correto.
- Se você tem túneis múltiplos VPN e ACLs cript. múltiplos, certifique-se de que estes ACL não se sobrepõe.
- Não use o ACL duas vezes. Mesmo se sua isenção de NAT ACL e ACL criptografado especifica o mesmo tráfego, use duas listas de acessos diferentes.
- Certifique-se de que seu dispositivo está configurado para usar a isenção de NAT ACL. Ou seja, use**route-map**o comando no roteador; use**nat (0)**o comando no PIX ou no ASA. Uma isenção de NAT ACL é exigida para configurações do LAN para LAN e do acesso remoto.

Para aprender mais sobre como verificar as instruções da ACL, consulte a seção Verificar se as ACLs estão corretas nasSoluções de Troubleshooting de VPN IPsec de Acesso Remoto e L2L Mais Comuns.

Informações Relacionadas

- Página do suporte de protocolo do IPsec Negotiation/IKE
- Página de suporte do PIX
- Notas técnicas
- 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.