Troubleshooting de IPSec: Compreendendo e usando comandos debug

Índice

Introdução

Este documento descreve os **comandos debug** comuns usados para pesquisar defeitos edições do IPsec em ambo o Cisco IOS? Software e PIX/ASA. Este original supõe que você configurou o IPsec. Refira às Mensagens de Erro do IPSec comum e edições do IPSec comum para mais detalhes.

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. Contém uma lista de verificação dos procedimentos comuns que você pôde tentar antes que você comece a troubleshoot uma conexão e chamar o Suporte Técnico Cisco.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- **Cisco IOS Software**Conjunto de recursos do IPsec.56i - Indica a única característica da criptografia padrão de dados (DES) (no Cisco IOS Software Release 11.2 e Mais Recente).k2 - Indica a característica do DES triplo (no Cisco IOS Software Release 12.0 e Mais Recente). 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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Depurações do Cisco IOS Software

Os assuntos nesta seção descrevem os comandos debug do Cisco IOS Software. Refira às Mensagens de Erro do IPSec comum e edições do IPSec comum para mais detalhes.

show crypto isakmp sa

Este comando mostra as associações de segurança do protocolo internet security association management (ISAKMP) (SA) construídas entre peers.

```
dst      src        state     conn-id     slot
12.1.1.2  12.1.1.1   QM_IDLE    1           0
```

show crypto ipsec sa

Este comando mostra o IPsec SAs construído entre peers. O túnel criptografado é construído entre 12.1.1.1 e 12.1.1.2 para o tráfego que vai entre redes 20.1.1.0 e 10.1.1.0. Você pode ver as duas SAs de Payload de Segurança de Encapsulamento (ESP) desenvolvidas interna e externamente. O cabeçalho de autenticação (AH) não é usado, pois não há SAs de AH.

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

```
  interface: FastEthernet0
    Crypto map tag: test, local addr. 12.1.1.1 local ident (addr/mask/prot/port):
(20.1.1.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.1.1.0/255.255.255.0/0/0)
current_peer: 12.1.1.2 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.: 12.1.1.1,
remote crypto endpt.: 12.1.1.2 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. Desde que a fase 2 (associações de segurança) do SA é unidirecional, cada SA mostra o tráfego em somente um sentido (as criptografias são de saída e decifragens são de entrada).

debug crypto isakmp

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

```
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 fonte e o destino dos pontos finais de túnel de IPSec. Src_proxy e dest_proxy são as sub-redes cliente. Duas mensagens “sa criadas” aparecem com uma em cada sentido. (Quatro mensagens aparecem se você executa o ESP e o AH.)

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

```
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= 12.1.1.2,
SRC= 12.1.1.1, dest_proxy= 10.1.1.0/0.0.0.0/0/0, src_proxy= 20.1.1.0/0.0.0.16/0/0, 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 12.1.1.2 to 12.1.1.1 for prot 2 IPSEC(spi_response): getting spi 194838793 for SA
from 12.1.1.2 to 12.1.1.1 for prot 3 IPSEC(key_engine): got a queue event...
IPSEC(initialize_sas): , (key eng. msg.) dest= 12.1.1.2, SRC= 12.1.1.1, dest_proxy=
10.1.1.0/255.255.255.0/0/0, src_proxy= 20.1.1.0/255.255.255.0/0/0, 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= 12.1.1.2, dest= 12.1.1.1,
src_proxy= 10.1.1.0/255.255.255.0/0/0, dest_proxy= 20.1.1.0/255.255.255.0/0/0, 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= 12.1.1.2,
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= 12.1.1.2, 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 erro "Replay Check Failed”:

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

Este erro é um resultado da requisição no meio de transmissão (especialmente se existem caminhos paralelos), ou trajetos desiguais do pacote que processam o Cisco IOS interno para grande contra a carga inferior positiva dos pacotes pequenos. Mude o conjunto de transformação para refletir isto. A *verificação da resposta* somente é considerada quando o conjunto de transformação esp-md5-hmac está habilitado. Para suprimir esta mensagem de erro, desabilite o

esp-md5-hmac e faça somente a criptografia. Refira à identificação de bug Cisco CSCdp19680 (somente clientes registrados).

Para obter informações sobre de como configurar a janela IPsec Anti-Replay, refira a como configurar a janela do IPsec Anti-Replay: Expansão e desabilitação.

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 a identificação do proxy, tais como o tráfego interessante, a lista de controle de acesso (ACL) ou cripto ACL, não combinam em ambas as extremidades. Verifique a configuração em ambos os dispositivos, e certifique-se de que os crypto ACLs combinam.

Uma outra razão possível é a combinação errônea dos parâmetros ajustados da transformação. Certifique-se de que em ambas as extremidades, os gateways de VPN usam os mesmos grupos de transformação com os mesmos parâmetros.

Endereço local inválido

Esta saída mostra um exemplo da Mensagem de Erro:

```
IPSEC(validate_proposal): invalid local address 12.2.6.2
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:

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

O mensagem IKE de X.X.X.X falhou sua verificação de sanidade ou é deformado

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 150.150.150.1 failed its
 sanity check or is malformed
```

O processamento do Modo Principal Falhou com o correspondente

Este é um exemplo do Mensagem de Erro do *Modo Principal*. 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 150.150.150.1
```

O **comando show crypto isakmp sa** mostra ISAKMP SA em MM_NO_STATE. 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 espelhar-se em si mesmas (todas as entradas precisam de 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 15.15.15.1 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 15.15.15.1
```

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 150.150.150.2
```

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

Esta Mensagem de Erro aparece normalmente com a mensagem correspondente do Mensagem de Erro do VPN 3000 concentrator: Nenhuma proposta foi escolhida(14). Isto é resultado das conexões serem 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= 194.70.240.150, src= 198.174.236.6,
    dest_proxy= 10.0.0.76/255.255.255.255/0/0 (type=1),
    src_proxy= 198.174.238.203/255.255.255.255/0/0 (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 198.174.236.6 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 de IPsec recebido especifica um deslocamento predeterminado dos parâmetros de segurança (SPI) que não exista na base de dados das associações de segurança (SADB). Esta pode ser uma condição temporária devido a:

- Pequenas diferenças no envelhecimento das associações de segurança (SA) entre os ipsec peers
- Os SA locais que estão sendo cancelados
- Pacotes incorreto enviados pelo ipsec peer

Isto pode igualmente ser um ataque.

Ação recomendada: O peer não pode reconhecer que os SA locais estiveram cancelados. Se uma nova conexão é estabelecida do roteador local, os dois peers podem então restabelecer com sucesso. Se não, se o problema ocorre por mais do que um breve período, tente estabelecer uma nova conexão ou contatar o administrador do peer.

IPSEC(initialize_sas): IDs do proxy inválido

O erro 21:57:57: `IPSEC(initialize_sas):` o ID proxy inválido indica que a identidade de proxy recebida não combina a identidade de proxy configurada conforme a lista de acessos. A fim assegurar-se de que ambos combinam, verifique a saída do **comando debug**.

No **comando debug** do pedido da proposta, o IP correspondente 10.1.1.0 0.0.0.255 20.1.1.0 0.0.0.255 da licença da lista de acesso 103 não combina. 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= 192.1.1.1, src= 192.1.1.2,
    dest_proxy= 10.1.1.1/255.255.255.0/0/0 (type=4),
    src_proxy= 20.1.1.1/255.255.255.0/0/0 (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 ou o algoritmo de hash oferecido não combina a política! ou o algoritmo de criptografia oferecido não combina a política! Mensagem de Erro nos roteadores.

```
=RouterA=
3d01h: ISAKMP (0:1): processing SA payload. message ID = 0
3d01h: ISAKMP (0:1): found peer pre-shared key matching 209.165.200.227
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 do código da autenticação de mensagem Hash (HMAC) no pacote de IPsec. Isto acontece geralmente quando o pacote é corrompido de alguma maneira.

```
Sep 22 11:02:39 131.203.252.166 2435:
Sep 22 11:02:39: %MOTCR-1-ERROR:motcr_crypto_callback() motcr return failure Sep 22 11:02:39
131.203.252.166 2436: Sep 22 11:02:39: %MOTCR-1-PKTENGRET_ERROR: MOTCR PktEng Return Value =
0x20000, PktEngReturn_MACMiscompare
```

Se você encontra ocasionalmente este Mensagem de Erro você pode ignorá-la. Contudo se este se torna mais freqüente, você precisa de investigar o que está realmente corrompendo o 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. Assegure-se de a combinação transforme grupos configurados em ambos os peers.

Todas as propostas IPsec SA encontraram inaceitável

Este Mensagem de Erro ocorre quando os parâmetros IPSec da fase 2 são combinados mal entre as sites e local remoto. A fim resolver esta edição, especifique os mesmos parâmetros na transformação ajustada de modo que combinem e o VPN bem sucedido estabeleça.

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 pode ser 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. Isto efetivamente desabilita a autenticação/proteção anti-replay, que (por sua vez) impede os erro de queda de pacote desordenados (misturado) ao tráfego de IPSec *%HW_VPN-1-HPRXERR: Hardware VPN0/2: Pacote de criptografia/Erro de descriptografia, status=4615*.
2. Uma ação alternativa que se aplica realmente à razão mencionada no artigo #1 acima é ajustar o tamanho da unidade de transmissão máxima (MTU) de córregos de entrada a 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. A fim remover o interruptor que rápido você pode usar este comanda no modo de configuração da 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 de IPsec recebidos pelo roteador de descriptografia estão fora de serviço devido à ordem de pacote no 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.`Router(config-if)#`**`crypto ipsec fragmentation before-encryption`**

3. Ajuste o valor MTU a um tamanho que não tenha que ser fragmentado.`Router(config)#`**`interface type [slot_#/]port_#`** `Router(config-if)#`**`ip mtu MTU_size_in_bytes`**
4. Promova a imagem IOS à imagem estável mais recente neste trem.

Nota: Mudar o tamanho do MTU em toda a interface do roteador causará todos os túneis terminados nessa relação a ser rasgada. Você deve planejar terminar esta ação alternativa durante um tempo ocioso da máquina 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 apoiada no 7600 Series Router. 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
12.1.1.2  12.1.1.1   QM_IDLE    1           0
```

Na saída **show cripto isakmp sa**, o estado deve sempre ser 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.

```
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 12.1.1.1 e 12.1.1.2 para o tráfego que vai entre redes 20.1.1.0 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 **comando show crypto ipsec sa** é mostrado nesta saída.

```
interface: outside
    Crypto map tag: vpn, local addr. 12.1.1.1
   local  ident (addr/mask/prot/port): (20.1.1.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (12.1.1.2/255.255.255.255/0/0) current_peer: 10.2.1.1 dynamic allocated
peer ip: 12.1.1.2 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.: 12.1.1.1, remote crypto endpt.: 12.1.1.2 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 combinar (para tentar o 3DES em vez do DES e do [SHA] do algoritmo de mistura segura) é aceitável, e ISAKMP SA é construído. 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 **comando debug crypto isakmp**.

```
crypto_isakmp_process_block: src 12.1.1.1, dest 12.1.1.2
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 12.1.1.2 OAK_QM exchange ISAKMP
(0:0): Need config/address ISAKMP (0:0): initiating peer config to 12.1.1.2. ID = 2607270170
(0x9b67c91a) return status is IKMP_NO_ERROR crypto_isakmp_process_block: src 12.1.1.2, dest
12.1.1.1 ISAKMP_TRANSACTION exchange ISAKMP (0:0): processing transaction payload from 12.1.1.2.
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 12.1.1.1
prot 0 port 0 INITIAL_CONTACTIPSEC(key_engine): got a queue event...
```

debug crypto ipsec

Este comando indica informações de **debug** sobre conexões IPSec.

```
IPSEC(key_engine): got a queue event...
IPSEC(spi_response): getting spi 0xd532efbd(3576885181) for SA
        from  12.1.1.2  to  12.1.1.1  for prot 3
return status is IKMP_NO_ERROR
crypto_isakmp_process_block: src 12.1.1.2, dest 12.1.1.1
OAK_QM exchange
oakley_process_quick_mode:
OAK_QM_AUTH_AWAIT
ISAKMP (0): Creating IPSec SAs inbound SA from 12.1.1.2 to 12.1.1.1 (proxy 10.32.8.1 to
12.1.1.1.) has spi 3576885181 and conn_id 2 and flags 4 outbound SA from 12.1.1.1 to 12.1.1.2
(proxy 12.1.1.1 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= 12.1.1.1, src= 12.1.1.2,
dest_proxy= 12.1.1.1/0.0.0.0/0/0 (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= 12.1.1.1, dest=
12.1.1.2, src_proxy= 12.1.1.1/0.0.0.0/0/0 (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

A incapacidade alcançar sub-redes fora do VPN escava um túnel: Divisão de túnel

Mostras destas saídas de configuração da amostra de roteador como permitir o split tunneling para as conexões de VPN. O **comando access list 150** é associado ao grupo como configurado no **comando crypto isakmp client configuration group hw-client-groupname**. Isto permite que o Cisco VPN Client use o roteador a fim alcançar uma sub-rede adicional que não seja parte do túnel VPN. Isto é feito sem compromizing à segurança da conexão IPSec. O túnel é formado na rede 172.168.0.128. Fluxos de tráfego não criptografados aos dispositivos não definidos no **comando access list 150**, tal como a Internet.

```
!
crypto isakmp client configuration group hw-client-groupname key hw-client-password dns
172.168.0.250 172.168.0.251 wins 172.168.0.252 172.168.0.253 domain cisco.com pool dynpool acl
150 ! ! access-list 150 permit ip 172.168.0.128 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 pode 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 IPsec session. 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 router needs to have route !--- for 10.1.2.0/24 network with next hop
as the PIX inside interface !--- (as in Cisco IOS routers). ip route 10.1.2.0 255.255.255.0
10.1.1.1
```

Depois que o túnel está aberto, o usuário é incapaz de navegar na Internet: Divisão de túnel

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. Conseqüentemente o tráfego destinado à Internet não funciona. Para fixar este problema, use o **comando split tunneling**. 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.

```
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
```

Nota: O **comando vpngroup vpn3000 split-tunnel 90** ativa o tunelamento dividido com o **access-list number 90**. O **comando access-list 90** define qual tráfego corre através do túnel, o resto do qual é negado na extremidade da lista de acessos. A lista de acessos precisa ser a mesma para negar a tradução de endereço de rede (NAT) no PIX.

Depois que o túnel está aberto, determinados aplicativos não funcionam: Ajuste MTU no cliente

Às vezes depois que o túnel é estabelecido, você pôde poder sibilar as máquinas na rede atrás do PIX Firewall, mas você é incapaz de usar determinados aplicativos como o Microsoft outlook. Um problema comum é o tamanho máximo da unidade de transferência (MTU) dos pacotes. O cabeçalho IPSec pode ser até 50 pés a 60 bytes, que é adicionado 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 **comando show interface** mostra o MTU desta interface particular nos roteadores que são acessíveis ou nos roteadores em seus próprios locais. A fim de determinar o MTU do caminho inteiro da fonte ao destino, as datagramas de vários tamanhos são enviados com não fragmentar (DF) o jogo de bit de modo que, se a datagrama enviado for mais do que o MTU, este Mensagem de Erro seja enviada de volta à fonte:

```
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.

```
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
```

Nota: 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.

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

1. Escolha o **Start > Programs > Cisco System VPN Client > set MTU**.
2. Selecione a **conexão de área local**, e clique então o botão de rádio **1400**.
3. Clique em **OK**.
4. Repita etapa 1, e selecione a **rede de comunicação dial-up**.
5. Clique o botão de rádio **576**, e clique então em **OK**.

Perca o comando sysopt

Use o **comando sysopt connection permit-ipsec nas** configurações IPSec no PIX a fim permitir que o tráfego de IPSec passe pelo PIX Firewall sem uma verificação de indicações do **comando conduit or access-list**. Por padrão, toda a sessão de entrada deve explicitamente ser permitida por uma indicação do **comando conduit oru access-list**. Com tráfego protegido de IPSec, a verificação de lista de acesso secundária pode ser redundante. A fim permitir o IPsec autenticado/cifrar sessões de entrada a ser permitidas sempre, use o **comando sysopt connection permit-ipsec**.

Verifique as lista de controle de acesso (os 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. Isto inclui um ACL criptogafado em uma instalação do LAN para LAN ou em um split-tunneling ACL em uma configuração do acesso remoto. Quando estes ACL são configurados incorretamente ou faltando, o tráfego pode fluir somente em um sentido através do túnel VPN, ou não pode ser enviado através do 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 cripto especifica o mesmo tráfego, use duas Listas de acesso diferentes.
- Certifique-se de que seu dispositivo está configurado para usar a isenção de NAT ACL. Isto é, use o **comando route-map** no roteador; use o comando **nat (0)** no PIX ou no ASA. Uma isenção de NAT ACL é exigida para o LAN para LAN e as configurações do Acesso remoto.

A fim aprender mais sobre como verificar as indicações ACL, refira à seção verifique se os ACLs estão corretos no mais frequente L2L e acesso remoto que IPsec VPN soluções de problemas.

Informações Relacionadas

- Página do suporte de protocolo do IPsec Negotiation/IKE
- Uma introdução à criptografia do protocolo de segurança IP (IPSEC)

- Página de suporte do PIX
- Referências de comando PIX
- Solicitações de Comentários (RFCs)
- Suporte Técnico e Documentação - Cisco Systems