Solução de problemas comuns de L2L e VPN IPsec de acesso remoto

Contents

Introdução

Informações de Apoio

Pré-requisitos

A configuração do IPSec VPN não funciona

Os VPN Clients não conseguem se conectar ao ASA

O cliente VPN interrompe a conexão com frequência na primeira tentativa ou "Conexão VPN segura encerrada pelo par. Motivo 433." ou do “conexão VPN seguro terminada pela Motivo Peer 433:(Motivo não especificado pelo peer)”

O acesso remoto e os usuários EZVPN conectam ao VPN mas não podem alcançar recursos externos

Incapaz de conectar mais de três usuários do cliente VPN

Incapaz de iniciar a sessão ou uma aplicação e de retardar transferência após o estabelecimento de túnel

Não é possível iniciar o túnel VPN no ASA

Incapaz de Passar o Tráfego Através do Túnel VPN

Configurar o par de backup para túnel VPN no mesmo mapa de criptografia

Desabilite/Reinicie o Túnel VPN

Alguns Túneis não Criptografados

Erro:- %ASA-5-713904: Group = DefaultRAGroup, IP = x.x.x.x, ...unsupported Transaction Mode v2 version.Tunnel terminated.

Erro:- %ASA-6-722036: Group client-group User xxxx IP x.x.x.x Transmitting large packet 1220 (threshold 1206)

Mensagem de Erro quando QoS for Habilitado em uma extremidade do Túnel VPN

AVISO: entrada do mapa de criptografia incompleta

Erro:- %ASA-4-400024: IDS:2151 Large ICMP packet from to on interface outside

Erro:- %ASA-4-402119: IPSEC: Received a protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP that failed anti-replay check.

Mensagem de erro – %ASA-4-407001: Deny traffic for local-host interface_name:inside_address, license limit of number exceeded

Mensagem de Erro - %VPN_HW-4-PACKET_ERROR:

Mensagem de erro: Command rejected: delete crypto connection between VLAN XXXX and XXXX, first.

Mensagem de erro – % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Dropped packet - Invalid Window Scale option for session x.x.x.x:27331 to x.x.x.x:23 [Initiator(flag 0,factor 0) Responder (flag 1, factor 2)]

%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse . Favor Atualizar o fluxo deste problema

%ASA-5-713068: Received non-routine Notify message: notify_type

%ASA-5-720012: (VPN-Secondary) Failed to update IPSec failover runtime data on the standby unit (or) %ASA-6-720012: (VPN-unit) Failed to update IPsec failover runtime data on the standby unit

Erro:- %ASA-3-713063: IKE Peer address not configured for destination 0.0.0.0

Erro: %ASA-3-752006: Tunnel Manager failed to dispatch a KEY_ACQUIRE message.

Erro: %ASA-4-402116: IPSEC: Received an ESP packet (SPI= 0x99554D4E, sequence number= 0x9E) from XX.XX.XX.XX (user= XX.XX.XX.XX) to YY.YY.YY.YY

Falha para iniciar o intalador 64-bit VA para habilitar o adaptador virtual devido ao erro 0xffffffff

O Cliente VPN Cisco não funciona com o cartão de dados em Windows 7

Alerta: "VPN functionality may not work at all"

Erro no preenchimento do IPSec

O túnel VPN é desconectado a cada 18 horas

O fluxo de tráfego não é mantido após a renegociação do túnel de LAN a LAN

A mensagem de erro indica que a largura de banda recorreu à funcionalidade de criptografia

Problema: o tráfego de criptografia de saída em um túnel IPsec falha, mesmo quando o tráfego de descriptografia de entrada funciona.

Diversos

Informações Relacionadas

Introdução

Este documento descreve as soluções mais comuns para os problemas de VPN IPsec.

Informações de Apoio

As soluções descritas aqui vêm diretamente das solicitações de serviço resolvidas pelo suporte técnico da Cisco.

Muitas dessas soluções são implementadas antes da solução de problemas detalhada de uma conexão VPN IPsec.

Este documento fornece um resumo dos procedimentos comuns a serem realizados antes de começar a solucionar problemas de conexão.

Embora os exemplos de configuração neste documento sejam para uso em roteadores e dispositivos de segurança, quase todos esses conceitos também são aplicáveis à VPN 3000.

Consulte Solução de problemas de segurança IP – Como entender e usar os comandos debug para obter uma explicação dos comandos debug comuns usados para solucionar problemas de IPsec no software Cisco IOS®.

Observação: o ASA não passa o tráfego multicast pelos túneis VPN IPsec.

Aviso: muitas das soluções apresentadas neste documento podem levar a uma perda temporária de toda a conectividade VPN IPsec em um dispositivo.

Recomenda-se que estas soluções estejam executadas com cuidado e de acordo com sua política do controle de alterações.

Pré-requisitos

Requisitos

A Cisco recomenda que você conheça a configuração da VPN IPsec nestes dispositivos da Cisco:

- Ferramenta de segurança do Cisco ASA 5500 Series
- Cisco IOS® Routers

Componentes Utilizados

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

- Ferramenta de segurança do Cisco ASA 5500 Series
- Cisco IOS®

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 as convenções do documento.

A configuração do IPSec VPN não funciona

Problema

Uma solução de VPN IPsec recém configurada ou modificada não funciona.

Uma configuração de VPN IPsec atual não funciona mais.

Soluções

Esta seção contém soluções para os problemas mais comuns de VPN IPsec.

Embora não estejam listadas em uma ordem específica, essas soluções podem ser usadas como uma lista de verificação de itens para verificar ou testar antes de você se envolver na correção detalhada.

Todas essas soluções vêm diretamente das solicitações de serviço do TAC e resolveram vários problemas.

- Permita NAT-Traversal (a edição #1 RA VPN)
- Teste a conectividade corretamente
- Habilitar ISAKMP
- Habilitar/Desabilitar do PFS
- Cancele associações de segurança velhas ou existentes (os túneis)
- Verificação do Tempo de Vida do ISAKMP
- Habilitar ou Desabilitar ISAKMP Keepalives
- Reinserção ou Recuperação de Chaves Pré-Compartilhadas
- Chave pré-compartilhada mal combinada
- Remoção e Reaplicação de Mapas de Criptografia
- Verificar se os comandos sysopt estão presentes (somente /ASA)
- Verificação da Identidade de ISAKMP
- Verificação do Timeout de Ociosidade/Sessão
- Verifique que os ACL estejam corretos e conectados ao Mapa de Criptografia
- Verificação das Políticas de ISAKMP
- Verifique que o Roteador esteja correto
- Verifique se o conjunto de transformação está correto
- Verificar os Números de Sequência e do Nome do Mapa de Criptografia
- Verificação da Correção do Endereço IP do Peer
- Verifique o grupo de túneis e os nomes do grupo
- Desabilite XAUTH para peers L2L
- Pool VPN se torna esgotado
- Problemas de latência no tráfego do cliente VPN

Nota:Alguns dos comandos nestas seções foram divididos em duas linhas devido a problemas de espaço.

Permita NAT-Traversal (a edição #1 RA VPN)

O NAT-Traversal (ou NAT-T) permite que o tráfego VPN passe pelos dispositivos NAT ou PAT,

como um roteador Linksys SOHO.

Caso o NAT-T não esteja ativado, geralmente parece que os usuários do VPN Client se conectam ao ASA sem problemas, mas eles não conseguem acessar a rede interna por trás do dispositivo de segurança.

Se você não ativar o NAT-T no dispositivo NAT/PAT, poderá receber a mensagem de erro **`regular translation creation failed for protocol 50 src inside:10.0.1.26 dst outside:10.9.69.4`** no ASA.

Da mesma forma, se você não conseguir fazer o login simultâneo no mesmo endereço IP, a **`conexão Secure VPN será encerrada localmente pelo cliente. A mensagem de erro Reason 412: The remote peer is no longer responding.`** será exibida.

Permitir o NAT-T no dispositivo da extremidade principal VPN a fim de resolver este erro.

Observação: com o software Cisco IOS® versão 12.2(13)T e posterior, o NAT-T é ativado por padrão no Cisco IOS®.

Está aqui o comando para permitir o NAT-T em um dispositivo do Cisco Security. O vinte (20) neste exemplo é o tempo de keepalive (padrão).

ASA

```
<#root>

securityappliance(config)#

crypto isakmp nat-traversal 20
```

Os clientes precisam ser modificados também para que tudo funcione.

No Cisco VPN Client, navegue até Connection Entries e clique em Modify. Essa ação abre uma nova janela em que você precisa escolher a guia Transport.

Nessa guia, clique em Enable Transparent Tunneling e no botão de rádio IPSec over UDP (NAT/PAT). Em seguida, clique em Salve e teste a conexão.

É importante permitir o UDP 4500 para portas NAT-T, UDP 500 e ESP pela configuração de uma ACL, pois o ASA atua como um dispositivo NAT.

Consulte Configuração de um túnel IPsec por meio de um firewall com NAT para obter mais informações sobre a configuração da ACL no ASA.

Teste a conectividade corretamente

O ideal é que a conectividade VPN seja testada nos dispositivos por trás dos dispositivos de endpoint que fazem a criptografia, mas muitos usuários testam a conectividade VPN com o comando ping nos dispositivos que fazem a criptografia.

Embora o ping geralmente funcione para essa finalidade, é importante que o ping seja executado na interface correta.

Caso o ping seja obtido de forma incorreta, pode parecer que a conexão VPN falhou, quando na verdade ela funciona. Este é um exemplo:

Roteador A ACL criptografado

```
access-list 110 permit ip 192.168.100.0 0.0.0.255 192.168.200.0 0.0.0.255
```

Roteador B ACL criptografado

```
access-list 110 permit ip 192.168.200.0 0.0.0.255 192.168.100.0 0.0.0.255
```

Nessa situação, um ping deve ser obtido da rede interna por trás de qualquer roteador. Isto é porque os ACLs criptografados são configurados somente para criptografar o tráfego com aqueles endereços de origem.

Um ping obtido das interfaces externas de um dos roteadores não é criptografado. Use as opções estendidas do comando ping no modo EXEC com privilégios para obter um ping na interface interna de um roteador:

<#root>

```
routerA#
ping
Protocol [ip]:
Target IP address: 192.168.200.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 192.168.100.1
Type of service [0]:
Set DF bit in IP header? [no]:
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, 100-byte ICMP Echos to 192.168.200.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.100.1
```

```
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = ½/4 ms
```

Imagine que os roteadores neste diagrama foram substituídos por dispositivos de segurança ASA. O ping que é usado para testar a conectividade também pode ser obtido da interface interna com a palavra-chave inside:

<#root>

```
securityappliance#
```

ping inside 192.168.200.10

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.200.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Não é recomendável direcionar o ping para a interface interna de um dispositivo de segurança.

Se você precisar direcionar o ping para a interface interna, ative o management-access nessa interface ou o dispositivo não responderá.

<#root>

```
securityappliance(config)#
```

management-access inside

Quando existe um problema com a conectividade, nem mesmo a fase um (1) da VPN funciona.

No ASA, se a conectividade falha, a saída SA é semelhante a este exemplo, que indica uma possível configuração incorreta do par de criptografia e/ou uma configuração incorreta da proposta de ISAKMP:

<#root>

```
Router#
```

show crypto isakmp sa

```
1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_WAIT_MSG2
```

O estado pode ser de MM_WAIT_MSG2 a MM_WAIT_MSG5, o que indica falha na troca de

estados em questão no Main Mode (MM).

A saída criptografada SA quando a fase 1 é up é similar a este exemplo:

<#root>

```
Router#
show crypto isakmp sa


1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

Habilitar ISAKMP

Se não há indicação de que um túnel VPN IPsec funciona, é possível que o ISAKMP não tenha sido ativado. Seja certo que você habilitou o ISAKMP em seus dispositivos.

Use um destes comandos para habilitar o ISAKMP em seus dispositivos:

Cisco IOS®

<#root>

```
router(config)#
crypto isakmp enable
```

Cisco ASA (substitua outside pela interface desejada)

<#root>

```
securityappliance(config)#
crypto isakmp enable outside
```

Você pode igualmente obter este erro quando você habilita o ISAKMP na interface externa:

```
UDP: ERROR - socket <unknown> 62465 in used
ERROR: IkeReceiverInit, unable to bind to port
```

A causa do erro pode ser que o cliente por trás do ASA recebe o PAT na porta UDP 500, antes

que o ISAKMP possa ser ativado na interface. Uma vez que essa tradução PAT é removida (clear xlate), o isakmp pode ser habilitado.

Verifique se os números de porta UDP 500 e 4500 estão reservados para a negociação das conexões ISAKMP com o par.

Quando o ISAKMP não é habilitado na interface, o cliente VPN mostra um Mensagem de Erro similar a esta mensagem:

```
Secure VPN connection terminated locally by client.
Reason 412: The remote peer is no longer responding
```

A fim resolver este erro, habilite o ISAKMP na interface criptografada do gateway de VPN.

Habilitar/Desabilitar do PFS

Nas negociações de IPsec, o Perfect Forward Secrecy (PFS) garante que cada nova chave criptográfica não tenha relação com nenhuma chave anterior.

Ative ou desative o PFS em ambos os pares de túnel. Caso contrário, o túnel IPsec de LAN-to-LAN (L2L) não será estabelecido no roteador ASA/Cisco IOS®.

O Perfect Forward Secrecy (PFS) é propriedade da Cisco e não é apoiado em dispositivos de terceiros.

ASA:

O PFS é desabilitado por padrão. Para ativar o PFS, use o comando pfs com a palavra-chave enable no modo de configuração de group-policy. Para desabilitar o PFS, insira a palavra-chave disable.

<#root>

```
hostname(config-group-policy)#
```

pfs {enable | disable}

Para remover o atributo PFS da configuração, insira a forma no deste comando.

Uma política de grupo pode herdar um valor para o PFS de outra política de grupo. Insira a forma no deste comando para evitar a transferência de um valor.

<#root>

hostname(config-group-policy)#

no pfs

Roteador Cisco IOS®:

Para especificar que o IPsec deve procurar o PFS quando novas associações de segurança são solicitadas para essa entrada do mapa de criptografia, use o comando set pfs no modo de configuração do mapa de criptografia.

Para especificar que o IPsec exige o PFS ao receber solicitações de novas associações de segurança, use o comando set pfs no modo de configuração do mapa de criptografia.

Para especificar que o IPsec não deva solicitar o PFS, use a forma no deste comando. Por padrão, o PFS não é solicitado. Se nenhum grupo for especificado com este comando, group1 será usado como o padrão.

```
set pfs [group1 | group2]
no set pfs
```

Para o comando set pfs:

- group1 — Especifica que o IPsec deve usar o grupo Diffie-Hellman prime modulus de 768 bits quando o novo intercâmbio Diffie-Hellman é executado.
- group2 — Especifica que o IPsec deve usar o grupo Diffie-Hellman prime modulus de 1024 bits quando o novo intercâmbio Diffie-Hellman é executado.

Exemplo:

<#root>

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#
```

set pfs group2

Apagar associações de segurança (túneis) antigas ou atuais

Se essa mensagem de erro ocorre no roteador Cisco IOS®®, o problema é que a SA expirou ou foi apagada.

O dispositivo final do túnel remoto não sabe que usa um AS expirado para enviar um pacote (não um pacote de estabelecimento de AS).

Quando um SA novo foi estabelecido, a comunicação recomeça, assim que inicie o tráfego interessante através do túnel para criar um SA novo e para restabelecer o túnel.

<#root>

%CRYPTO-4-IKMP_NO_SA: IKE message from x.x.x.x has no SA

Se você limpar o ISAKMP (associações de segurança da fase I) e do IPsec (fase II) (SA), é o mais simples e a melhor solução resolver frequentemente problemas do IPSec VPN.

Se você cancelar SA, você pode freqüentemente resolver uma ampla variedade de Mensagens de Erro e de comportamentos estranhos sem a necessidade de pesquisar defeitos.

Ao mesmo tempo que essa técnica pode ser facilmente usada em qualquer situação, é quase sempre um requisito limpar SAs após alterar ou adicionar a configuração de VPN IPsec atual.

Além disso, quando for possível cancelar somente associações de segurança específicas, o maior benefício pode vir de quando você limpa a SA global no dispositivo.

Uma vez que as associações de segurança foram canceladas, pode ser necessário enviar o tráfego através do túnel para restabelecê-las.

Aviso: a menos que você especifique quais associações de segurança devem ser apagadas, os comandos listados aqui podem apagar todas as associações de segurança no dispositivo. Prossiga com cuidado se houver outros túneis VPN IPsec em uso.

1. Veja as associações de segurança antes que você as cancele

    a. Cisco Cisco IOS®

    <#root>

    router#

    show crypto isakmp sa

    router#

    show crypto ipsec sa

    b. Dispositivos de segurança do Cisco ASA

    <#root>

    securityappliance#

    show crypto isakmp sa

    securityappliance#

```
show crypto ipsec sa
```

2. Cancele associações de segurança. Cada comando pode ser incorporado segundo as indicações em negrito ou serem incorporadas com as opções mostradas com elas.

    a. Cisco IOS®

        a. ISAKMP (Fase I)

```
<#root>

router#

clear crypto isakmp

 ?
  <0 - 32766>  connection id of SA
  <cr>
```

        b. IPsec (Fase II)

```
<#root>

router#

clear crypto sa

 ?
  counters  Reset the SA counters
  map       Clear all SAs for a given crypto map
  peer      Clear all SAs for a given crypto peer
  spi       Clear SA by SPI
  <cr>
```

    b. Dispositivos de segurança do Cisco ASA

        a. ISAKMP (Fase I)

```
<#root>

securityappliance#

clear crypto isakmp sa
```

        b. IPsec (Fase II)

```
<#root>

security appliance#

clear crypto ipsec sa

 ?

  counters  Clear IPsec SA counters
  entry     Clear IPsec SAs by entry
  map       Clear IPsec SAs by map
  peer      Clear IPsec SA by peer
  <cr>
```

Verificação do Tempo de Vida do ISAKMP

Se os usuários forem freqüentemente desconectados do túnel L2L, o problema pode ser um tempo de vida menor configurado na AS do ISAKMP.

Se houver discrepâncias na vida útil do ISAKMP, você poderá receber a mensagem de erro %ASA-5-713092: Group = x.x.x.x, IP = x.x.x.x, Failure during phase 1 rekey attempt due to collision no /ASA.

O padrão é 86.400 segundos (24 horas). Como regra geral, um tempo de vida menor proporciona negociações de ISAKMP mais seguras (até um ponto).sNo entanto, esses tempos mais curtos permitem que o Security Appliance configure mais rápido IPsec SAs mais rapidamente.

Uma correspondência é feita quando ambas as políticas dos dois peers contêm os mesmos valores de parâmetros de criptografia, hash, autenticação e Diffie-Hellman, e também quando a política do peer remoto especifica um tempo de vida menor ou igual ao tempo de vida especificado na política com a qual a comparação é feita.

Se os tempos de vida não forem idênticos, o tempo menor — da política do peer remoto — será usado. Se nenhuma correspondência aceitável for encontrada, o IKE recusará a negociação e a AS de IKE não será estabelecida.

Especifique a vida útil do SA. Este exemplo define uma vida útil de 4 horas (14.400 segundos). O padrão é 86400 segundos (24 horas).

ASA

```
<#root>

hostname(config)#

isakmp policy 2 lifetime  14400
```

Roteador Cisco IOS®

<#root>

```
R2(config)#
crypto isakmp policy 10
R2(config-isakmp)#
lifetime 86400
```

Se o tempo de vida configurada seja excedida, você recebe esta mensagem de erro quando a conexão de VPN é terminada:

Conexão do VPN segura terminada localmente pelo cliente. Reason 426: Maximum Configured Lifetime Exceeded.

Para resolver essa mensagem de erro, defina o valor lifetime como zero (0) para definir a vida útil de uma associação de segurança do IKE como infinita. A VPN deve estar sempre conectada e não deve ser encerrada.

```
hostname(config)#isakmp policy 2 lifetime 0
```

Você também pode executar disable re-xauth in the group-policy para resolver o problema.

Habilitar ou Desabilitar ISAKMP Keepalives

Se você configurar os keepalives de ISAKMP, eles ajudarão a impedir o descarte esporádico de VPNs LAN a LAN ou de acesso remoto, o que inclui clientes VPN, túneis e túneis que são descartados após um período de inatividade.

Esta característica deixa o endpoint de túnel monitorar a presença continuada de um peer remoto e relatar sua própria presença a esse peer.

Se o peer parar de responder, o endpoint irá remover a conexão.

Para que os keepalives de ISAKMP trabalhem, ambos os endpoints VPN devem suportá-los.

Configure os keepalives do ISAKMP no Cisco IOS® com este comando:

<#root>

```
router(config)#
crypto isakmp keepalive 15
```

Use estes comandos para configurar os keepalives do ISAKMP nos dispositivos de segurança do ASA:

Cisco ASA para o grupo de túneis chamado 10.165.205.222

<#root>

```
securityappliance(config)#

tunnel-group 10.165.205.222
   ipsec-attributes


securityappliance(config-tunnel-ipsec)#

isakmp keepalive
   threshold 15 retry 10
```

Em algumas situações, é necessário desabilitar este recurso para resolver o problema, por exemplo, se o cliente VPN estiver por trás de um firewall que impede a passagem de pacotes de DPD.

Cisco ASA para o grupo de túneis chamado 10.165.205.222

Desative o processamento de keepalive do IKE, que é ativado por padrão.

<#root>

```
securityappliance(config)#

tunnel-group 10.165.205.222
   ipsec-attributes


securityappliance(config-tunnel-ipsec)#

isakmp keepalive


disable
```

Desabilite o keepalive para o Cisco VPN Client 4.x

Navegue até %System Root% > Program Files > Cisco Systems >VPN Client > Profiles no PC Cliente que apresenta o problema, para desativar o keepalive do IKE, e edite o arquivo PCF, quando aplicável, para a conexão.

Altere o ForceKeepAlives=0 (padrão) para ForceKeepAlives=1.

Os keepalives são propriedade da Cisco e não são apoiados por dispositivos de terceira parte.

Reinserção ou Recuperação de Chaves Pré-Compartilhadas

Em muitos casos, um erro tipográfico simples pode ser o responsável quando um túnel VPN IPsec não funciona. Por exemplo, na ferramenta de segurança, as chaves pré-compartilhadas tornam-se escondidas uma vez que são incorporadas.

Esta ofuscação faz impossível considerar se uma chave está incorreta. Esteja certo que você incorporou todas as chaves-pré-compartilhadas corretamente em cada endpoint de VPN.

Insira uma chave novamente para ter certeza de que ela está correta. Essa solução simples pode evitar um troubleshooting mais detalhado.

Em uma VPN de acesso remoto, verifique se um nome de grupo válido e a chave pré-compartilhada correta foram inseridos no Cisco VPN Client.

Você poderá encontrar esse erro se o nome do grupo ou a chave pré-compartilhada não corresponder entre o VPN Client e o dispositivo de headend.

```
 1 12:41:51.900 02/18/06 Sev=Warning/3 IKE/0xE3000056
 The received HASH payload cannot be verified
 2 12:41:51.900 02/18/06 Sev=Warning/2 IKE/0xE300007D
Hash verification failed
3      14:37:50.562  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
4      14:37:50.593  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
5      14:44:15.937  10/05/06  Sev=Warning/2 IKE/0xA3000067
Received Unexpected InitialContact Notify (PLMgrNotify:888)
6      14:44:36.578  10/05/06  Sev=Warning/3 IKE/0xE3000056
The received HASH payload cannot be verified
7      14:44:36.593  10/05/06  Sev=Warning/2 IKE/0xE300007D
Hash verification failed... possibly be configured with invalid group password.
8      14:44:36.609  10/05/06  Sev=Warning/2 IKE/0xE3000099
Failed to authenticate peer (Navigator:904)
9      14:44:36.640  10/05/06  Sev=Warning/2 IKE/0xE30000A5
Unexpected SW error occurred while processing Aggressive Mode
negotiator:(Navigator:2202)
```

Aviso: caso você remova os comandos relacionados à criptografia, é provável que desative um ou todos os túneis VPN. Use esses comandos com cuidado e consulte a política de controle de alterações da empresa antes de remover os comandos relacionados à criptografia.

Use estes comandos para remover e reinserir a secretkey da chave pré-compartilhada do par 10.0.0.1 ou do grupo vpngroup no Cisco IOS®:

LAN para LAN VPN de Cisco

<#root>

```
router(config)#
```

```
no crypto isakmp key secretkey
```

```
   address 10.0.0.1

router(config)#

crypto isakmp key secretkey
   address 10.0.0.1
```

Acesso remoto VPN de Cisco

<#root>

```
router(config)#

crypto isakmp client configuration
   group vpngroup

router(config-isakmp-group)#

no key secretkey

router(config-isakmp-group)#

key secretkey
```

Use estes comandos para remover e reinserir a secretkey da chave pré-compartilhada do par 10.0.0.1 nos dispositivos de segurança do /ASA:

Cisco 6.x

<#root>

```
(config)#

no isakmp key secretkey address 10.0.0.1

(config)#

isakmp key secretkey address 10.0.0.1
```

Cisco/ASA 7.x e posterior

<#root>

```
securityappliance(config)#

tunnel-group 10.0.0.1
   ipsec-attributes

securityappliance(config-tunnel-ipsec)#

no ikev1 pre-shared-key

securityappliance(config-tunnel-ipsec)#
```

```
ikev1


pre-shared-key
   secretkey
```

Chave pré-compartilhada mal combinada

A iniciação do túnel VPN fica desconectada. Esse problema ocorre devido a uma chave pré-compartilhada incompatível durante as negociações da fase I.

A mensagem MM_WAIT_MSG_6 no comando show crypto isakimp sa indica uma chave pré-compartilhada incompatível, conforme mostrado neste exemplo:

```
<#root>

ASA#

show crypto isakmp sa


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

1         IKE Peer: 10.7.13.20
             Type : L2L                                Role : initiator
             Rekey : no                                State :

MM_WAIT_MSG_6
```

Para resolver esse problema, insira novamente a chave pré-compartilhada em ambos os dispositivos. A chave pré-compartilhada deve ser exclusiva e compatível. Consulte Reinserir ou recuperar chaves pré-compartilhadas para obter mais informações.

Remoção e Reaplicação de Mapas de Criptografia

Quando você apaga as associações de segurança e isso não resolve um problema de VPN IPsec, remova e reaplique o mapa de criptografia relevante para resolver uma ampla gama de problemas, que inclui descartes intermitentes do túnel VPN e falha de alguns sites VPN ao entrar em operação.

Aviso:se você remover um mapa de criptografia de uma interface, ele com certeza desativará todos os túneis IPsec associados a esse mapa de criptografia. Prossiga com cautela seguindo essas etapas e considere a política de controle de alterações da empresa antes de continuar.

Use estes comandos para remover e substituir um mapa de criptografia no Cisco IOS®:

Comece com a remoção do mapa de criptografia da relação. Use a forma no do comando crypto

map.

<#root>

```
router(config-if)#
no crypto map mymap
```

Continue a usar a forma no para remover um mapa de criptografia inteiro.

<#root>

```
router(config)#
no crypto map mymap 10
```

Substitua o mapa de criptografia na interface Ethernet0/0 para o peer 10.0.0.1. Este exemplo mostra a configuração exigida mínima do mapa de criptografia:

<#root>

```
router(config)#
crypto map mymap 10 ipsec-isakmp
router(config-crypto-map)#
match address 101
router(config-crypto-map)#
set transform-set mySET
router(config-crypto-map)#
set peer 10.0.0.1
router(config-crypto-map)#
exit
router(config)#
interface ethernet0/0
router(config-if)#
crypto map mymap
```

Use estes comandos para remover e substituir um mapa de criptografia no ASA:

Comece com a remoção do mapa de criptografia da relação. Use a forma no do comando crypto map.

<#root>

```
securityappliance(config)#

no crypto map mymap interface outside
```

Continue a usar a forma no para remover os outros comandos do mapa de criptografia.

<#root>

```
securityappliance(config)#

no crypto map mymap 10 match
   address 101

securityappliance(config)#

no crypto map mymap set
   transform-set mySET

securityappliance(config)#

no crypto map mymap set
   peer 10.0.0.1
```

Substitua o mapa de criptografia para o par 10.0.0.1. Este exemplo mostra a configuração exigida mínima do mapa de criptografia:

<#root>

```
securityappliance(config)#

crypto map mymap 10 ipsec-isakmp

securityappliance(config)#

crypto map mymap 10
   match address 101

securityappliance(config)#

crypto map mymap 10 set
   transform-set mySET

securityappliance(config)#

crypto map mymap 10 set
   peer 10.0.0.1

securityappliance(config)#

crypto map mymap interface outside
```

Se você remove e reaplica o mapa de criptografia, este igualmente resolve o problema de

conectividade se o endereço IP da extremidade principal foi mudado.

Verificar se os comandos sysopt estão presentes (somente ASA)

Os comandos sysopt connection permit-ipsec e sysopt connection permit-vpn permitem que pacotes de um túnel IPsec e os respectivos payloads ignorem as ACLs de interface no dispositivo de segurança.

Os túneis IPsec terminados no Security Appliance provavelmente falharão se um destes comandos não for habilitado.

No Security Appliance Software versão 7.0 e anterior, o comando sysopt relevante para essa situação é sysopt connection permit-ipsec.

No Security Appliance Software versão 7.1(1) e posterior, o comando sysopt relevante para essa situação é sysopt connection permit-vpn.

Na versão 6.x, essa funcionalidade está desativada por padrão. No /ASA 7.0(1) e posterior, essa funcionalidade está ativada por padrão. Use estes comandos show para determinar se o comando sysopt relevante está ativado no dispositivo:

Cisco ASA

<#root>

```
securityappliance#
```

show running-config all sysopt

```
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
```

sysopt connection permit-vpn

```
!--- sysopt connection permit-vpn is enabled !--- This device is running 7.2(2)
```

Use estes comandos para ativar o comando sysopt correto para o dispositivo:

Cisco ASA

<#root>

```
securityappliance(config)#
```

sysopt connection permit-vpn

Se você não quiser usar o comando sysopt connection, permita explicitamente o tráfego de interesse necessário da origem para o destino.

Por exemplo, da LAN remota para a LAN local do dispositivo remoto e "porta UDP 500" da interface externa do dispositivo remoto para a interface externa do dispositivo local, na ACL externa.

Verificação da Identidade de ISAKMP

Se o túnel VPN IPsec falhou na negociação do IKE, a falha pode ser devido à incapacidade do peer de reconhecer a identidade do peer.

Quando dois pares usam o IKE para instituir associações de segurança IPSec, cada par envia sua identidade de ISAKMP ao peer remoto.

Ele envia seu endereço IP ou nome de host dependendo de como a identidade de ISAKMP de cada um foi definida.

Por padrão, a identidade do ISAKMP da unidade de firewall é definida como o endereço IP.

Como regra geral, defina o Security Appliance e as identidades de seus peers da mesma forma para evitar uma falha de negociação de IKE.

Para definir a ID da fase 2 a ser enviada ao par, use o comando isakmp identity no modo de configuração global.

```
crypto isakmp identity address

!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with pre-shared key as authentication typ
```

OU

```
crypto isakmp identity auto

!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with ISAKMP negotiation by connection typ
```

OU

```
crypto isakmp identity hostname

!--- Uses the fully-qualified domain name of !--- the host exchange ISAKMP identity information (defaul
```

O túnel VPN não entra em operação após uma mudança de configuração no ASA com a ferramenta de migração de configuração do ASA. Estas mensagens aparecerão no registro:

[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Stale PeerTblEntry found, removing!

[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!

[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, construct_ipsec_delete(): No SPI to identify Phase 2 SA!

[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!

Verificação do Timeout de Ociosidade/Sessão

Se o timeout de ociosidade for definido como 30 minutos (padrão), o túnel será descartado após 30 minutos sem que tráfego passe por ele.

O VPN Client será desconectado após 30 minutos, independentemente do parâmetro de limite de tempo ocioso, e encontrará o erro **PEER_DELETE-IKE_DELETE_UNSPECIFIED**.

Configure idle timeout e session timeout como none para que o túnel esteja sempre ativo e nunca seja descartado, mesmo quando dispositivos de terceiros forem usados.

ASA

Digite o comando vpn-idle-timeout no modo de configuração de group-policy ou no modo de configuração de nome de usuário para configurar o período do limite de tempo do usuário:

<#root>

```
hostname(config)#
group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#
vpn-idle-timeout none
```

Configure um tempo máximo para conexões VPN com o comando vpn-session-timeout no modo de configuração de group-policy ou no modo de configuração do nome de usuário:

<#root>

```
hostname(config)#
group-policy DfltGrpPolicy attributes
hostname(config-group-policy)#
vpn-session-timeout none
```

Quando você configura o tunnel-all, não é necessário configurar o idle-timeout, porque mesmo se você configurar o limite de tempo ocioso da VPN, ele não funcionará, pois todo o tráfego passa pelo túnel (já que o tunnel-all foi configurado).

Portanto, o tráfego de interesse (ou mesmo o tráfego gerado pelo PC) é de interesse e não deixa que o Idle-timeout entre em ação.

Roteador Cisco IOS®

Use o comando crypto ipsec security-association idle-time no modo de configuração global ou no modo de configuração do mapa de criptografia para configurar o temporizador ocioso da SA do IPsec.

Por padrão, esses temporizadores estão desabilitados.

<#root>

crypto ipsec security-association idle-time

seconds

O tempo é medido em segundos, que o temporizador ocioso permite que um par inativo mantenha uma SA. Os valores válidos para o argumento seconds variam entre 60 e 86.400.

Verifique que os ACL são corretos e ativado ao mapa de criptografia

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 acesso define qual tráfego deve ser criptografado. Isso inclui uma ACL de criptografia em uma configuração de LAN para LAN ou uma ACL de split-tunnel em uma configuração de acesso remoto.

Quando essas ACLs estão configuradas de forma incorreta ou estão ausentes, o tráfego talvez flua em uma direção pelo túnel VPN ou não seja enviado pelo túnel.

Vincule a ACL de criptografia ao mapa de criptografia com o comando crypto map match address no modo de configuração global.

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 aspectos simples a serem verificados quando você suspeitar que uma ACL é a causa dos problemas com sua VPN IPsec.

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.

Certifique-se de que seu dispositivo está configurado para usar a isenção de NAT ACL. Em um roteador, isso significa que você usa o comando route-map.

No ASA, isso significa que você usa o comando nat (0). Uma isenção de NAT ACL é exigida para configurações do LAN para LAN e do acesso remoto.

Aqui, um roteador Cisco IOS® está configurado para isentar o tráfego enviado entre 192.168.100.0 /24 e 192.168.200.0 /24 ou 192.168.1.0 /24 no NAT. O tráfego destinado para qualquer outro lugar é sujeito à sobrecarga NAT:

```
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 deny ip 192.168.100.0 0.0.0.255
   192.168.1.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255 any

route-map nonat permit 10
  match ip address 110

ip nat inside source route-map nonat interface FastEthernet0/0 overload
```

A isenção de NAT ACL trabalha somente com o endereço IP ou as redes IP, tais como aqueles exemplos mencionados (da lista de acesso noNAT), e deve ser idêntica ao mapa de criptografia ACL.

As ACLs de isenção do NAT não funcionam com os números da porta (por exemplo, 23, 25, ...).

Em um ambiente VOIP, em que as chamadas de voz entre as redes são comunicadas pela VPN, as chamadas de voz não funcionarão se as ACLs do NAT 0 não estiverem configuradas corretamente.

Antes de solucionar problemas, sugerimos que verifique o status de conectividade da VPN, pois o problema pode estar na configuração incorreta das ACLs isentas do NAT.

Você pode receber o Mensagem de Erro como mostrado se há erro de configuração na isenção de NAT (nat 0) ACL.

```
%ASA-3-305005: No translation group found for
udp src Outside:x.x.x.x/p dst Inside:y.y.y.y/p
```

Exemplo incorreto:

<#root>

```
access-list noNAT extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
```

eq 25

Se a isenção do NAT (nat 0) não funcionar, tente removê-la e emitir o comando NAT 0 para que funcione.

Certifique-se de que seus ACL não estão para trás e de que são o tipo correto.

Criptofia e a excessão NAT de ACL para configurações LAN para LAN deve ser escrito da perspectiva do dispositivo em que o ACL é configurado.

Isso significa que as ACLs devem se espelhar. Neste exemplo, um túnel de LAN para LAN foi configurado entre 192.168.100.0 /24 e 192.168.200.0 /24.

Roteador A ACL criptografado

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
```

Roteador B ACL criptografado

```
access-list 110 permit ip 192.168.200.0 0.0.0.255
   192.168.100.0 0.0.0.255
```

Embora não apareça aqui, esse mesmo conceito se aplica aos dispositivos de segurança do ASA.

No ASA, as ACLs de split-tunnel para configurações de acesso remoto devem ser listas de acesso padrão que permitem o tráfego para a rede a qual os VPN Clients precisam acessar.

Os roteadores Cisco IOS® podem usar a ACL estendida para split-tunnel. Na lista de acesso estendida, usar 'any' na origem na ACL de split tunnel é semelhante a disable split tunnel.

Use apenas as redes de origem na ACL estendida para split tunnel.

Exemplo correto:

<#root>

access-list 140 permit ip

10.1.0.0 0.0.255.255

10.18.0.0 0.0.255.255

Exemplo incorreto:

<#root>

```
access-list 140 permit ip
```

any

```
 10.18.0.0 0.0.255.255
```

Cisco IOS®

<#root>

```
router(config)#
```

access-list 10 permit ip 192.168.100.0

```
router(config)#
```

crypto isakmp client configuration group MYGROUP

```
router(config-isakmp-group)#
```

acl 10

Cisco ASA

<#root>

securityappliance(config)#

access-list 10 standard
permit 192.168.100.0 255.255.255.0

securityappliance(config)#

group-policy MYPOLICY internal

securityappliance(config)#

group-policy MYPOLICY attributes

securityappliance(config-group-policy)#

split-tunnel-policy
tunnelspecified

securityappliance(config-group-policy)#

split-tunnel-network-list
value 10

Configuração da excessão de NAT na versão ASA 8.3 para o túnel do VPN de Site-para-Site:

Uma VPN site a site deve ser estabelecida entre HOASA e BOASA com ambos os ASAs na versão 8.3. A configuração da isenção de NAT em HOASA parece similar a esta:

```
object network obj-local
subnet 192.168.100.0 255.255.255.0
object network obj-remote
subnet 192.168.200.0 255.255.255.0
nat (inside,outside) 1 source static obj-local obj-local destination static obj-remote objremote
```

Verificação das Políticas de ISAKMP

Se o túnel IPsec não estiver ativado, verifique se as políticas de ISAKMP correspondem às dos peers remotos. Esta política de ISAKMP é aplicável à VPN site a site (L2L) e à VPN de acesso remoto.

Se os Cisco VPN Clients ou a VPN site a site não conseguir estabelecer o túnel com o dispositivo de remote-end, verifique se os dois pares contêm os mesmos valores de criptografia, hash, autenticação e parâmetro Diffie-Hellman.

Verifique quando a política de par remoto especifica uma vida útil inferior ou igual à vida útil na política que o iniciador enviou.

Se os tempos de vida não forem idênticos, o Security Appliance usará o menor. Se não houver uma correspondência aceitável, o ISAKMP recusará a negociação e a SA não será estabelecida.

```
"Error: Unable to remove Peer TblEntry, Removing peer from peer table
failed, no match!"
```

Está aqui o mensagem de registro detalhado:

```
4|Mar 24 2010 10:21:50|713903: IP = X.X.X.X, Error: Unable to remove PeerTblEntry
3|Mar 24 2010 10:21:50|713902: IP = X.X.X.X, Removing peer from peer table failed,
no match!
3|Mar 24 2010 10:21:50|713048: IP = X.X.X.X, Error processing payload: Payload ID: 1
4|Mar 24 2010 10:21:49|713903: IP = X.X.X.X, Information Exchange processing failed
5|Mar 24 2010 10:21:49|713904: IP = X.X.X.X, Received an un-encrypted
NO_PROPOSAL_CHOSEN notify message, drop
```

Essa mensagem geralmente é exibida devido a políticas de ISAKMP incompatíveis ou uma instrução NAT 0 ausente.

Além disso, esta mensagem aparece:

```
Error Message    %ASA-6-713219: Queueing KEY-ACQUIRE messages to be processed when
P1 SA is complete.
```

Essa mensagem indica que as mensagens da fase 2 estão na fila após a conclusão da fase 1. Essa mensagem de erro ocorre devido a um destes motivos:

- Má combinação na fase em alguns dos peers
- A ACL bloqueia os pares após a conclusão da fase 1

Essa mensagem geralmente é exibida após a mensagem de erro **`Removing peer from peer table failed, no match!`**.

Se o Cisco VPN Client não conseguir se conectar ao dispositivo headend, o problema pode ser a diferença na política de ISAKMP. O dispositivo de headend deve corresponder a uma das propostas de IKE do Cisco VPN Client.

Para a política de ISAKMP e o IPsec Transform-set usado no ASA, o Cisco VPN Client não pode usar uma política com uma combinação de DES e SHA.

Se você usa o DES, é necessário usar MD5 como o algoritmo de hash ou então as outras combinações, 3DES com SHA e 3DES com MD5.

Verifique que o Roteador esteja correto

Verifique se os dispositivos de criptografia, como os roteadores e os dispositivos de segurança do ASA, têm as informações de roteamento adequadas para enviar o tráfego pelo túnel VPN.

Se houver outros roteadores por trás do dispositivo de gateway, verifique se esses roteadores sabem como acessar o túnel e quais redes estão no outro lado.

Um componente-chave do roteamento em uma distribuição VPN é o Reverse Route Injection (RRI).

O RRI coloca entradas dinâmica para redes remotas ou clientes VPN na tabela de roteamento de um gateway de VPN.

Estas rotas são úteis ao dispositivo em que são instaladas, assim como aos outros dispositivos na rede porque as rotas instaladas pelo RRI podem ser redistribuídas com um protocolo de roteamento tal como o EIGRP ou o OSPF.

Em uma configuração de LAN para LAN, é importante para cada valor-limite ter uma rota ou umas rotas às redes para que se supor criptografar o tráfego.

Neste exemplo, Roteador A deve ter rotas às redes atrás de Roteador B com 10.89.129.2. o

Roteador B deve ter uma rota similar a 192.168.100.0 /24:

A primeira forma de garantir que cada roteador conheça as rotas apropriadas é configurar rotas estáticas para cada rede de destino. Por exemplo, o Roteador A pode ter estas declarações de rota configuradas:

```
ip route 0.0.0.0 0.0.0.0 172.22.1.1
ip route 192.168.200.0 255.255.255.0 10.89.129.2
ip route 192.168.210.0 255.255.255.0 10.89.129.2
ip route 192.168.220.0 255.255.255.0 10.89.129.2
ip route 192.168.230.0 255.255.255.0 10.89.129.2
```

Se o roteador A foi substituído por um ASA, a configuração pode ficar assim:

```
route outside 0.0.0.0 0.0.0.0 172.22.1.1
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
route outside 192.168.200.0 255.255.255.0 10.89.129.2
```

Se um grande número redes existem atrás de cada endpoint, a configuração das rotas estáticas torna-se difícil de manter.

Ao invés, recomenda-se que usar o Reverse Route Injection, como descrito. Lugares RRI nas rotas da tabela de roteamento para todas as redes remotas listadas no ACL criptografado.

Por exemplo, a criptografia ACL e o mapa de criptografia do Roteador A podem parecer como este:

<#root>

```
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.200.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.210.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.220.0 0.0.0.255
access-list 110 permit ip 192.168.100.0 0.0.0.255
   192.168.230.0 0.0.0.255

crypto map myMAP 10 ipsec-isakmp
 set peer 10.89.129.2
```

reverse-route

```
 set transform-set mySET
 match address 110
```

Se o roteador A foi substituído por um ASA, a configuração pode ficar assim:

<#root>

```
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.200.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.210.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.220.0 255.255.255.0
access-list cryptoACL extended permit ip 192.168.100.0
   255.255.255.0 192.168.230.0 255.255.255.0

crypto map myMAP 10 match address cryptoACL
crypto map myMAP 10 set peer 10.89.129.2
crypto map myMAP 10 set transform-set mySET
```

crypto map mymap 10 set reverse-route

Em uma configuração do acesso remoto, as mudanças de roteamento não são sempre necessárias.

Contudo, se outros roteadores existem atrás do gateway VPN ou ferramenta de segurança, aqueles roteadores precisam de alguma forma aprender o caminho cliente VPN.

Neste exemplo, suponha que os VPN Clients recebam endereços no intervalo de 10.0.0.0 /24 quando se conectam.

Se nenhum protocolo de roteamento está no uso entre o Gateway e o outro roteador, as rotas estáticas podem ser usadas em roteadores tais como Roteador 2:

```
ip route 10.0.0.0 255.255.255.0 192.168.100.1
```

Se um protocolo de roteamento tal como o EIGRP ou o OSPF está no uso entre o Gateway e outros roteadores, recomenda-se que o Reverse Route Injection esteja usado como descrito.

O RRI adiciona automaticamente rotas para o cliente VPN à tabela de roteamento do Gateway. Estas rotas podem então ser distribuídas às outras rotas na rede.

Roteador Cisco IOS®:

<#root>

```
crypto dynamic-map dynMAP 10
 set transform-set mySET
```

reverse-route

```
crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

Dispositivo de segurança do Cisco ASA:

<#root>

```
crypto dynamic-map dynMAP 10 set transform-set mySET
```

crypto dynamic-map dynMAP 10 set reverse-route

```
crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP
```

A questão de roteamento ocorre se o pool dos endereços IP atribuídos aos clientes VPN é sobrepostos com redes internas do dispositivo de extremidade principal. Para obter mais informações, consulte a seção Redes privadas sobrepostas.

Verifique se o conjunto de transformação está correto

Verifique se a criptografia de IPsec e os algoritmos de hash a serem usados pelo conjunto de transformação em ambos os pontos finais são os mesmos.

Consulte a seção Referência de comando do guia de configuração do Cisco Security Appliance para obter mais informações.

Para a política de ISAKMP e o IPsec Transform-set usado no ASA, o Cisco VPN Client não pode usar uma política com uma combinação de DES e SHA.

Se você usa o DES, é necessário usar MD5 como o algoritmo de hash ou então as outras combinações, 3DES com SHA e 3DES com MD5.

Verifique os números e nomes de seqüência do mapa de criptografia e também que o mapa de criptografia está aplicado na relação direita em que o começo/extremidade do túnel de IPsec

Se os pares estáticos e dinâmicos são configurados no mesmo mapa de criptografia, a ordem das entradas do mapa de criptografia é muito importante.

O número de sequência da entrada do mapa de criptografia dinâmico deve ser maior do que todas as outras entradas do mapa de criptografia estático.

Se as entradas estáticas tiverem uma numeração superior à da entrada dinâmica, as conexões com esses peers falharão e depurações como as mostradas aqui serão exibidas.

```
IKEv1]: Group = x.x.x.x, IP = x.x.x.x, QM FSM error (P2 struct &0x49ba5a0, mess id 0xcd600011)!
```

```
[IKEv1]: Group = x.x.x.x, IP = x.x.x.x, Removing peer from correlator table failed, no match!
```

Somente um mapa de criptografia dinâmico é permitido cada relação na ferramenta de segurança.

Aqui está um exemplo de um mapa de criptografia numerado corretamente que contenha uma entrada estática e uma entrada dinâmica. Note que a entrada dinâmica tem o número de seqüência mais alto e a sala foi adicionada à entrada adicional estática:

<#root>

```
crypto dynamic-map cisco 20 set transform-set myset
crypto map mymap 10 match address 100
crypto map mymap 10 set peer 172.16.77.10
crypto map mymap 10 set transform-set myset
crypto map mymap interface outside

crypto map mymap 60000 ipsec-isakmp dynamic ciscothe
```

Os nomes de mapa de criptografia diferencia entre maiúsculas e minúsculas.

Essa mensagem de erro também pode ser vista quando a sequência do mapa de criptografia dinâmico não está correta, o que faz com que o par acesse o mapa de criptografia errado.

Ela também é causada por uma lista de acesso de criptografia incompatível que define o tráfego de interesse:**%ASA-3-713042: IKE Initiator unable to find policy:**

Em um cenário em que vários túneis VPN devem ser encerrados na mesma interface, crie o mapa de criptografia com o mesmo nome (apenas um mapa de criptografia é permitido por interface), mas com um número de sequência diferente.

Isso vale para o roteador e o ASA.

Da mesma forma, consulte ASA: adicionar um novo túnel ou acesso remoto a uma VPN L2L atual – Cisco para obter mais informações sobre a configuração do mapa de criptografia para o cenário de VPN L2L e de acesso remoto.

Verificação da Correção do Endereço IP do Peer

Crie e gerencie o banco de dados de registros específicos da conexão para IPsec.

Para uma configuração de VPN IPsec de LAN para LAN (L2L) do ASA Security Appliance, especifique o <name> do grupo de túneis como o endereço IP do par remoto (extremidade do túnel remoto) no comando tunnel-group <name> type ipsec-l2l.

O endereço IP do par deve corresponder nos comandos tunnel group name e Crypto map set address.

Quando você configura a VPN com o ASDM, o número do grupo do túnel é gerado automaticamente com o endereço IP do peer correto.

Se o endereço IP do par não estiver configurado corretamente, os registros poderão conter essa mensagem, que pode ser resolvida pela configuração adequada do endereço IP do par.

```
[IKEv1]: Group = DefaultL2LGroup, IP = x.x.x.x,
ERROR, had problems decrypting packet, probably due to mismatched pre-shared key. Aborting
```

Quando o endereço IP do par não foi definido corretamente na configuração de criptografia do ASA, o ASA não consegue estabelecer o túnel VPN e fica travado apenas no estágio MM_WAIT_MSG4.

A fim resolver esta edição, corrija o endereço IP do peer na configuração.

Esta é a saída do comando show crypto isakmp sa, quando o túnel VPN fica travado no estado MM_WAIT_MSG4.

<#root>

```
hostname#
```

show crypto isakmp sa

```
1   IKE Peer: XX.XX.XX.XX
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_WAIT_MSG4
```

Verifique o grupo de túneis e os nomes do grupo

```
%ASA-3-713206: Tunnel Rejected: Conflicting protocols specified by
tunnel-group and group-policy
```

A mensagem aparece quando um túnel é deixado cair porque o túnel permitido especificado na política do grupo é diferente do que o túnel permitido na configuração do túnel-grupo.

<#root>

```
group-policy hf_group_policy attributes
  vpn-tunnel-protocol l2tp-ipsec

username hfremote attributes
  vpn-tunnel-protocol l2tp-ipsec
```

Both lines read:

```
  vpn-tunnel-protocol ipsec l2tp-ipsec
```

Permita na política do grupo padrão no IPSec já aos protocolos existentes na política padrão do grupo.

```
group-policy DfltGrpPolicy attributes
   vpn-tunnel-protocol L2TP-IPSec IPSec webvpn
```

Desabilite XAUTH para peers L2L

Se um túnel de LAN para LAN e um túnel VPN de acesso remoto estiverem configurados no mesmo mapa de criptografia, o par de LAN para LAN será solicitado a fornecer informações de XAUTH, e o túnel de LAN para LAN falhará com "CONF_XAUTH" na saída do comando show crypto isakmp sa.

Está aqui um exemplo do SA output:

<#root>

```
Router#
```

show crypto isakmp sa

```
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id  slot  status
X.X.X.X         Y.Y.Y.Y         CONF_XAUTH       10223    0   ACTIVE
X.X.X.X         Z.Z.Z.Z         CONF_XAUTH       10197    0   ACTIVE
```

Esse problema se aplica apenas ao Cisco IOS®, enquanto que o ASA não é afetado por esse problema, pois usa tunnel-groups.

Use a palavra-chave no-xauth ao inserir a chave isakimp, para que o dispositivo não solicite ao par as informações de XAUTH (nome de usuário e senha).

Esta palavra-chave desabilita o XAUTH para peers IPsec estáticos. Incorpore um comando similar a este no dispositivo que tem L2L e RA VPN configurados no mesmo mapa de critpografia:

<#root>

```
router(config)#
```

crypto isakmp key cisco123 address
**   172.22.1.164 no-xauth**

No cenário em que o ASA atua como o Easy VPN Server, o Easy VPN Client não consegue se conectar ao headend devido ao problema de Xauth.

Desative a autenticação do usuário no ASA para resolver o problema conforme mostrado:

```
<#root>

ASA(config)#

tunnel-group example-group type ipsec-ra

ASA(config)#

tunnel-group example-group ipsec-attributes

ASA(config-tunnel-ipsec)#

isakmp ikev1-user-authentication none
```

Consulte a seção Diversos deste documento para saber mais sobre o comando isakmp ikev1-user-authentication.

Pool VPN se torna esgotado

Quando a escala dos endereços IP atribuídos ao pool VPN não é suficiente, você pode estender a disponibilidade dos endereços IP de duas maneiras:

1. Remova a escala existente, e defina a escala nova. Aqui está um exemplo:

```
<#root>

CiscoASA(config)#

no ip local pool testvpnpool 10.76.41.1-10.76.41.254

CiscoASA(config)#

ip local pool testvpnpool 10.76.41.1-10.76.42.254
```

2. Quando as sub-redes descontínuas devem ser adicionadas ao pool VPN, você pode definir duas associações separadas VPN e para especificá-las então em ordem sob o “atributos grupo túnel”. Aqui está um exemplo:

```
<#root>

CiscoASA(config)#

ip local pool testvpnpoolAB 10.76.41.1-10.76.42.254

CiscoASA(config)#
```

```
ip local pool testvpnpoolCD 10.76.45.1-10.76.45.254
CiscoASA(config)#
tunnel-group test type remote-access
CiscoASA(config)#
tunnel-group test general-attributes
CiscoASA(config-tunnel-general)#
address-pool (inside) testvpnpoolAB testvpnpoolCD
CiscoASA(config-tunnel-general)#
exit
```

A ordem em que você especifica as associações é muito importante porque o ASA atribui endereços destas associações na ordem em que as associações aparecem neste comando.

A configuração dos pools de endereços no comando política de grupo de pools de endereço sempre sobrepõem as configurações de pool local no comando de pool de endereço.

Problemas de latência no tráfego do cliente VPN

Quando houver problemas de latência em uma conexão VPN, verifique estas condições para resolvê-los:

1. Verifique se o MSS do pacote pode ser mais reduzido.
2. Se IPsec/tcp for usado em vez de IPsec/udp, configure preserve-vpn-flow.
3. Recarregue o Cisco ASA.

Os VPN Clients não conseguem se conectar ao ASA

Problema

Os clientes da Cisco VPN não conseguem fazer a autenticação quando o X-AUTH é usado com o servidor Radius.

Solução

O problema pode ser o timeout do xauth. Aumente o valor do timeout do servidor AAA para resolver o problema.

Por exemplo:

```
<#root>
Hostname(config)#
```

```
aaa-server test protocol radius

hostname(config-aaa-server-group)#
aaa-server test host 10.2.3.4

hostname(config-aaa-server-host)#
timeout 10
```

Problema

Os clientes da Cisco VPN não conseguem fazer a autenticação quando o X-AUTH é usado com o servidor Radius.

Solução

Inicialmente, certifique-se de que a autenticação trabalha corretamente. Para reduzir o problema, verifique primeiramente a autenticação no banco de dados local no ASA.

```
tunnel-group tggroup general-attributes
               authentication-server-group none
               authentication-server-group LOCAL
        exit
```

Se isso funcionar, o problema estará relacionado à configuração do servidor Radius.

Verifique a conectividade do servidor Radius do ASA. Se o ping funcionar sem nenhum problema, verifique a seguir a configuração relacionada Radius no ASA e a configuração do banco de dados no servidor Radius.

Você pode usar o comando debug radius para solucionar problemas relacionados ao Radius. Para obter um exemplo de saída do debug radius, consulte este Exemplo de saída.

Antes de usar o comando debug no ASA, consulte esta documentação: Mensagem de aviso.

O cliente VPN interrompe a conexão com frequência na primeira tentativa ou "Conexão VPN segura encerrada pelo par. Motivo 433." ou do “conexão VPN seguro terminada pela Motivo Peer 433:(Motivo não especificado pelo peer)”

Problema

Os usuários do Cisco VPN Client recebem esse erro quando tentam fazer a conexão com o

dispositivo VPN de headend.

O VPN Client descarta a conexão com frequência na primeira tentativa

A conexão VPN de segurança é encerrada pelo par. Motivo 433.

A conexão VPN segura é encerrada pelo motivo do par 433: (motivo não especificado pelo par)

Tentativa de atribuir a rede ou o endereço IP de broadcast, removendo (xxxx) do pool

Solução 1

O problema pode estar na atribuição do pool IP por meio do ASA, servidor Radius, servidor DHCP ou servidor Radius que atua como servidor DHCP.

Use o comando debug crypto para verificar se a máscara de rede e os endereços IP estão corretos. Também, verifique que o pool não inclui o endereço de rede e o endereço de broadcast.

Os servidores Radius devem poder atribuir os endereços de IP apropriados aos clientes.

Solução 2

Esta edição igualmente ocorre devido à falha da autenticação extendida. Você deve verificar o servidor AAA para corrigir erros.

Verifique a senha de autenticação do servidor no servidor e no cliente. Recarregar o servidor AAA pode resolver esse problema.

Solução 3

Uma outra ação alternativa para esta edição é desabilitar a característica da detecção de riscos.

Quando há várias retransmissões para diferentes associações de segurança (SAs) incompletas, o ASA com o recurso de threat-detection ativado considera que ocorreu um ataque de verificação e as portas VPN são marcadas como o principal infrator.

Tente desabilitar a característica de detecção de ameaças uma vez que isto pode causar muitas despesas no processamento do ASA. Use estes comandos a fim desabilitar a detecção da ameaça:

```
no threat-detection basic-threat
no threat-detection scanning-threat shun
no threat-detection statistics
no threat-detection rate
```

Isto pode ser usado como uma ação alternativa para verificar se isto irá fixar o problema real.

Verifique se desativar a detecção de ameaças no Cisco ASA, na verdade, compromete vários recursos de segurança, como a mitigação das Tentativas de Verificação, DoS com SPI Inválido, pacotes que não passam na Inspeção da Aplicação e Sessões Incompletas.

Solução 4

Esta edição igualmente ocorre quando um grupo da transformação não é configurado corretamente. Uma configuração apropriada do grupo da transformação resolve a edição.

O acesso remoto e os usuários EZVPN conectam ao VPN mas não podem alcançar recursos externos

Problema

Os usuários de acesso remotos não têm nenhuma conectividade de Internet uma vez que conectam ao VPN.

Os usuários de acesso remotos não podem alcançar os recursos situados atrás de outros VPN no mesmo dispositivo.

Os usuários de acesso remotos podem acessar somente a rede local.

Soluções

Tente estas soluções a fim resolver esta edição:

- Não É Possível Acessar os Servidores na DMZ
- Os Clientes VPN Não Conseguem Resolver DNS
- Separação de Túneis - Não É Possível Acessar a Internet ou Redes Excluídas
- Acesso do LAN local
- Sobreposição de Redes Privadas

Não É Possível Acessar os Servidores na DMZ

Depois que o VPN Client estabeleceu o túnel IPsec com o dispositivo de headend VPN (ASA/roteador Cisco IOS®), os usuários do VPN Client podem acessar os recursos da rede INSID (10.10.10.0/24), mas não podem acessar a rede DMZ (10.1.1.0/24).

Diagrama

Verifique se a configuração NO NAT de separação de túneis foi adicionada ao dispositivo headend para permitir o acesso aos recursos da rede DMZ.

Exemplo:

Configuração do ASA:

Esta configuração mostra como configurar a isenção de NAT para a rede do DMZ a fim permitir os usuários VPN de alcançar a rede do DMZ:

```
object network obj-dmz
subnet 10.1.1.0 255.255.255.0
object network obj-vpnpool
subnet 192.168.1.0 255.255.255.0
nat (inside,dmz) 1 source static obj-dmz obj-dmz destination static obj-vpnpool obj-vpnpool
```

Após você adicionar uma nova entrada para a configuração de NAT, limpe a conversão de NAT.

```
Clear xlate
Clear local
```

Verifique:

Se o túnel foi estabelecido, acesse o Cisco VPN Client e escolha Status > Route Details para verificar se as rotas seguras aparecem nas redes DMZ e INSIDE.

Consulte ASA: adicionar um novo túnel ou acesso remoto a uma VPN L2L atual – Cisco para obter as etapas necessárias para adicionar um novo túnel VPN ou uma VPN de acesso remoto a uma configuração de VPN L2L que já existe.

Consulte ASA: exemplo de configuração de habilitação do tunelamento dividido para VPN Clients no ASA para obter instruções passo a passo sobre como permitir que VPN Clients acessem a Internet, enquanto estiverem encapsulados em um Cisco 5500 Series Adaptive Security Appliance (ASA).

Os Clientes VPN Não Conseguem Resolver DNS

Após o túnel ter sido estabelecido, se os VPN Clients não conseguirem resolver o DNS, o problema pode estar na configuração do servidor DNS no dispositivo de headend (ASA).

Verifique também a conectividade entre os clientes VPN e o servidor DNS. A configuração do servidor DNS deve ser definida na política de grupo e aplicada na política de grupo nos atributos gerais do tunnel-group, por exemplo:

<#root>

```
!--- Create the group policy named vpn3000 and !--- specify the DNS server IP address(172.16.1.1) !--- a

group-policy vpn3000 internal
```

```
group-policy vpn3000 attributes
 dns-server value 172.16.1.1
 default-domain value cisco.com


!--- Associate the group policy(vpn3000) to the tunnel group !--- with the default-group-policy.


tunnel-group vpn3000 general-attributes
 default-group-policy vpn3000
```

Os clientes VPN não conseguem se conectar a servidores internos pelo nome

O cliente VPN não é capaz de enviar pings para hosts ou servidores da rede interna remota ou headend pelo nome. É necessário habilitar a configuração de separação de DNS no ASA para resolver esse problema.

Separação de Túneis - Não É Possível Acessar a Internet ou Redes Excluídas

Split tunnel permite que clientes IPsec de acesso remoto direcionem condicionalmente os pacotes pelo túnel IPsec no formato criptografado ou para uma interface de rede no formato de texto simples, descriptografado, em que são encaminhados para um destino final.

Split-tunnel está desativado por padrão, que é o tráfego **tunnelall**.

```
split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}
```

A opção excludespecified é suportada somente para Cisco VPN Clients e não para EZVPN Clients.

```
ciscoasa(config-group-policy)#split-tunnel-policy excludespecified
```

Consulte estes documentos para obter exemplos de configuração detalhados do split-tunnel:

- ASA: exemplo de configuração de habilitação do tunelamento dividido para VPN Clients no ASA
- Exemplo de Configuração de Roteador que Permite Clientes VPN se Conectarem via IPsec e à Internet Usando a Separação de Túneis

Solução Hairpin

Esta característica é útil para o tráfego VPN que incorpora uma relação mas é então roteado fora

dessa mesma relação.

Por exemplo, em uma rede VPN hub e spoke, em que o dispositivo de segurança é o hub e as redes VPN remotas são os spokes, o tráfego de comunicação spoke a spoke deve entrar no dispositivo de segurança e depois sair novamente para o outro spoke.

Use a configuração same-security-traffic para permitir que o tráfego entre e saia da mesma interface.

<#root>

securityappliance(config)#

same-security-traffic permit intra-interface

Acesso do LAN local

Os usuários de acesso remotos conectam ao VPN e podem se conectar somente à rede local.

Para obter um exemplo de configuração mais detalhado, consulte ASA: permitir acesso à LAN local para VPN Clients.

Sobreposição de Redes Privadas

Problema

Se você não for capaz de acessar a rede interna após o estabelecimento do túnel, verifique o endereço IP atribuído ao cliente VPN que se sobrepõe com o da rede interna por trás do dispositivo headend.

Solução

Verifique se os endereços IP no pool a serem atribuídos aos VPN Clients, à rede interna do dispositivo de headend e à rede interna do VPN Client estão em redes diferentes.

É possível atribuir a mesma rede principal com sub-redes diferentes, mas algumas vezes pode haver problemas de roteamento.

Para obter mais exemplos, consulte o Diagrama e o Exemplo da seção Não é possível acessar os servidores no DMZ.

Incapaz de conectar mais de três usuários do cliente VPN

Problema

Apenas três VPN Clients podem se conectar ao ASA/. A conexão do quarto cliente falhará. Na ocasião da falha, esta mensagem de erro é exibida:

```
Secure VPN Connection terminated locally by the client.
     Reason 413: User Authentication failed.
```

```
tunnel rejected; the maximum tunnel count has been reached
```

Soluções

Na maioria dos casos, esse problema está relacionado a uma configuração de login simultâneo na política do grupo e ao limite máximo de sessões.

Tente estas soluções a fim resolver esta edição:

- Configuração de Logins Simultâneos
- Configure o ASA com a CLI
- Configurar Configurar

Configuração de Logins Simultâneos

Se a caixa de seleção Inherit no ASDM estiver marcada, apenas o número padrão de logins simultâneos será permitido para o usuário. O valor padrão de logins simultâneos é três (3).

Para resolver esse problema, aumente o número de logins simultâneos.

1. Inicie o ASDM e navegue até Configuration > VPN > Group Policy.
2. Escolha o Group apropriado e clique no botão Edit.
3. Na guia General, desmarque a caixa de seleção Inherit para Simultaneous Logins em Connection Settings. Escolha um valor apropriado no campo.

   O valor mínimo para este campo é zero (0), o que desativa o login e impede o acesso do usuário.

   Quando você faz login com a mesma conta de usuário em um PC diferente, a sessão atual (a conexão estabelecida de outro PC com a mesma conta de usuário) é encerrada, e uma nova sessão é estabelecida.

Este é o comportamento padrão e é independente aos inícios de uma logins de VPN simultâneos.

Configure o ASA com a CLI

Siga estas etapas para configurar o número desejado de logins simultâneos. Neste exemplo, vinte (20) foi escolhido como o valor desejado.

```
<#root>

ciscoasa(config)#

group-policy Bryan attributes

ciscoasa(config-group-policy)#

vpn-simultaneous-logins 20
```

Para saber mais sobre esse comando, consulte a Referência de comandos do Cisco Security Appliance.

Use o comando vpn-sessiondb max-session-limit no modo de configuração global para limitar as sessões VPN a um valor menor do que o permitido pelo dispositivo de segurança.

Use a versão **no** deste comando para remover o limite de sessão. Use o comando novamente para sobrescrever a configuração atual.

```
vpn-sessiondb max-session-limit {session-limit}
```

Este exemplo mostra como definir um limite máximo de 450 sessões de VPN:

```
<#root>

hostname#

vpn-sessiondb max-session-limit 450
```

Configurar

Mensagem de erro

```
20932 10/26/2007 14:37:45.430 SEV=3 AUTH/5 RPT=1863 10.19.187.229
Authentication rejected: Reason = Simultaneous logins exceeded for user
handle = 623, server = (none), user = 10.19.187.229, domain = <not
specified>
```

Solução

Conclua estes passos para configurar o número desejado de logins simultâneos. Você também pode tentar definir Simultaneous Logins como 5 para esta AS:

Escolha Configuration > User Management > Groups > Modify 10.19.187.229 > General > Simultaneous Logins e altere o número de logins para 5.

Incapaz de iniciar a sessão ou uma aplicação e de retardar transferência após o estabelecimento de túnel

Problema

Após o túnel IPsec ser estabelecido, o aplicativo ou a sessão não inicia pelo túnel.

Soluções

Use o comando ping para verificar a rede ou descobrir se o servidor de aplicações está acessível na rede.

Pode ser um problema com o tamanho máximo de segmento (MSS) para pacotes temporários que atravessam um roteador ou dispositivo /ASA, especificamente segmentos TCP com o bit SYN definido.

Cisco IOS® Router – Altere o valor de MSS na interface externa (Tunnel End Interface) do roteador

Execute estes comandos a fim mudar o valor MSS na interface externa (relação da extremidade do túnel) do roteador:

```
<#root>

Router>

enable

Router#

configure terminal

Router(config)#

interface ethernet0/1


Router(config-if)#ip tcp adjust-mss 1300

Router(config-if)#

end
```

Estas mensagens mostram a saída de depuração do MSS do TCP:

<#root>

```
Router#debug ip tcp transactions

Sep 5 18:42:46.247: TCP0: state was LISTEN -> SYNRCVD [23 -> 10.0.1.1(38437)]
Sep 5 18:42:46.247: TCP: tcb 32290C0 connection to 10.0.1.1:38437, peer MSS 1300, MSS is
1300
Sep 5 18:42:46.247: TCP: sending SYN, seq 580539401, ack 6015751
Sep 5 18:42:46.247: TCP0: Connection to 10.0.1.1:38437, advertising MSS 1300
Sep 5 18:42:46.251: TCP0: state was SYNRCVD -> ESTAB [23 -> 10.0.1.1(38437)]
```

O MSS é ajustado para 1300 no roteador conforme configurado.

Para obter mais informações, consulte ASA e Cisco IOS®: fragmentação de VPN.

ASA – Consulte a documentação do /ASA

Há uma incapacidade acessar corretamente a Internet ou retardar a transferência através do túnel por receber a Mensagem de Erro do tamanho do MTU e edições MSS.

Consulte este documento para resolver o problema:

- ASA e Cisco IOS®: fragmentação de VPN

Não é possível iniciar o túnel VPN no ASA

Problema

Você não consegue iniciar o túnel VPN na interface do ASA e, após o estabelecimento do túnel, a extremidade remota/VPN Client não consegue fazer ping na interface interna do ASA no túnel VPN.

Por exemplo, o cliente pn talvez não consiga iniciar uma conexão SSH ou HTTP com os ASAs dentro da interface pelo túnel VPN.

Solução

Não é possível fazer ping na interface interna na outra extremidade do túnel, a menos que o comando management-access esteja configurado no modo de configuração global.

<#root>

```
ASA-02(config)#

management-access inside


ASA-02(config)#

show management-access
```

```
management-access inside
```

Esse comando também ajuda na inicialização do SSH ou na conexão HTTP com a interface interna do ASA por um túnel VPN.

Esta informação também é verdadeira para a relação DMZ. Por exemplo, se você quiser fazer ping na interface DMZ do /ASA ou iniciar um túnel na interface DMZ, será necessário executar o comando management-access DMZ.

<#root>

```
ASA-02(config)#
```

management-access DMZ

Se o VPN Client não conseguir se conectar, verifique se as portas ESP e UDP estão abertas.

No entanto, se essas portas não estiverem abertas, tente se conectar no TCP 10000 selecionando essa porta na entrada de conexão do VPN Client.

Clique com o botão direito do mouse em modify > transport tab > IPsec over TCP.

Incapaz de Passar o Tráfego Através do Túnel VPN

Problema

Você é incapaz de passar o tráfego através de um túnel VPN.

Solução

Esse problema também pode ocorrer quando os pacotes ESP estão bloqueados. Para resolver esse problema, reconfigure o túnel VPN.

Esse problema pode ocorrer quando os dados não são criptografados, mas apenas descriptografados pelo túnel VPN, conforme mostrado nesta saída:

<#root>

```
ASA# sh crypto ipsec sa peer x.x.x.x
peer address: y.y.y.y
    Crypto map tag: IPSec_map, seq num: 37, local addr: x.x.x.x
      access-list test permit ip host xx.xx.xx.xx host yy.yy.yy.yy
      local ident (addr/mask/prot/port): (xx.xx.xx.xx/255.255.255.255/0/0)
      remote ident (addr/mask/prot/port): (yy.yy.yy.yy/255.255.255.255/0/0)
      current_peer: y.y.y.y
```

```
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
     #pkts decaps: 393, #pkts decrypt: 393, #pkts verify: 393

     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #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
     #send errors: 0, #recv errors: 0
```

Para resolver esse problema, verifique estas condições:

1. Se as listas de acesso criptografadas combinam com o local remoto, e estas listas de acesso NAT 0 estão corretas.
2. Se o roteamento estiver correto e o tráfego atingir a interface externa que passa pela interna. As saídas de exemplo mostram que a descriptografia está completa, mas a criptografia não ocorre.
3. Se o comando sysopt permit connection-vpn foi configurado no ASA. Caso contrário, configure esse comando, pois ele permite que o ASA isente o tráfego criptografado/VPN da verificação de ACL da interface.

Configurar o par de backup para túnel VPN no mesmo mapa de criptografia

Problema

Você quer usar múltiplos peers de backup para um único túnel vpn.

Solução

A configuração de vários pares é equivalente ao provisionamento de uma lista de fallback. Para cada túnel, a ferramenta de segurança tenta negociar com o primeiro peer da lista.

Se esse peer não responde, a ferramenta de segurança continua nos outros peers até que um peer responda ou até não houver mais peers na lista.

O ASA tem um mapa de criptografia já configurado como o par primário. O peer secundário pode ser adicionado após peer primário.

Este exemplo de configuração mostra o peer principal como X.X.X.X e o peer de backup como o Y.Y.Y.Y:

```
<#root>

ASA(config)#

crypto map mymap 10 set peer X.X.X.X Y.Y.Y.Y
```

Desabilite/Reinicie o Túnel VPN

Problema

A fim desabilitar temporariamente o túnel VPN e reiniciar o serviço, complete o procedimento descrito nesta seção.

Solução

Use o comando crypto map interface no modo de configuração global para remover um mapa de criptografia definido anteriormente para uma interface.

Use a forma no neste comando para remover o mapa de criptografia definido da interface.

<#root>

hostname(config)#

no crypto map

map-name

interface

interface-name

Este comando remove o mapa de criptografia definido a uma interface do dispositivo da segurança ativo fazendo o túnel VPN do IPSec inativo na interface.

Para reiniciar o túnel de IPsec em uma interface, você deve atribuir um mapa de criptografia ajustado a uma relação antes que a relação possa fornecer serviços IPSec.

<#root>

hostname(config)#

crypto map

map-name

interface

interface-name

Alguns Túneis não Criptografados

Problema

Quando um número enorme de túneis são configurado no gateway de VPN, alguns túneis não irão passar tráfego. O ASA não recebe pacotes criptografado para aqueles túneis.

Solução

Este problema ocorre porque o ASA não passa pacotes criptografado através dos túneis. As regras de criptografia duplicadas são criadas na tabela ASP.

Erro:- %ASA-5-713904: Group = DefaultRAGroup, IP = x.x.x.x, ...unsupported Transaction Mode v2 version.Tunnel terminated.

Problema

A mensagem de erro **`%ASA-5-713904: Group = DefaultRAGroup, IP = 192.0.2.0,... unsupported Transaction Mode v2 version.Tunnel terminated`** será exibida.

Solução

O motivo da mensagem de erro `Transaction Mode v2` é que o ASA é compatível apenas com a configuração do modo IKE V6 e não com a versão antiga do modo V2.

Use a versão do Modo Confdig IKE V6 a fim resolver este erro.

Erro:- %ASA-6-722036: Group client-group User xxxx IP x.x.x.x Transmitting large packet 1220 (threshold 1206)

Problema

A mensagem de erro **`%ASA-6-722036: Group < client-group > User < xxxx > IP < x.x.x.x> Transmitting large packet 1220 (threshold 1206)`** será exibida nos registros do ASA.

Que este registro significa e como isto podem ser resolvido?

Solução

Este mensagem de registro indica que um pacote grande foi enviado ao cliente. A fonte do pacote não está ciente do cliente MTU.

Isto pode igualmente ser devido à compressão de dados não-compressíveis. A solução alternativa é desativar a compactação de SVC usando o comando svc compression none, que resolve o problema.

Mensagem de Erro quando QoS for Habilitado em uma extremidade do Túnel VPN

Problema

Se você ativou a QoS em uma extremidade do túnel VPN, pode receber esta mensagem de erro:

```
IPSEC: Received an ESP packet (SPI= 0xDB6E5A60, sequence number= 0x7F9F) from
10.18.7.11 (user= ghufhi) to 172.16.29.23 that failed anti-replay check
```

Solução

Essa mensagem normalmente é causada quando uma extremidade do túnel executa a QoS. Isso acontece quando um pacote é detectado como fora de ordem.

É possível desabilitar a QoS para evitar que isso ocorra, mas você poderá ignorar esse fato desde que o tráfego atravesse o túnel.

AVISO: entrada do mapa de criptografia incompleta

Problema

Ao executar o comando crypto map mymap 20 ipsec-isakmp, você pode receber este erro:

AVISO: entrada do mapa de criptografia incompleta

Por exemplo:

<#root>

ciscoasa(config)#

crypto map mymap 20 ipsec-isakmp

WARNING: crypto map entry incomplete

Solução

Este é um alerta normal quando você define um novo mapa de criptografia; um lembrete de que parâmetros como a lista de acesso (endereço de correspondência), o conjunto de transformação e o endereço de par devem ser configurados antes que isso funcione.

Também é normal que a primeira linha digitada para definir o mapa de criptografia não seja mostrada na configuração.

Erro:- %ASA-4-400024: IDS:2151 Large ICMP packet from to on

interface outside

Problema

Incapaz de passar o grande pacote de ping através do túnel vpn. Quando tentamos transmitir pacotes de ping grandes, recebemos o erro **`%ASA-4-400024: IDS:2151 Large ICMP packet from to on interface outside.`**

Solução

Desative as assinaturas 2150 e 2151 para resolver esse problema. Depois que as assinaturas estiverem desativadas, o ping funcionará corretamente.

Use estes comandos a fim desabilitar as assinaturas:

Desabilitar assinatura 2151 do exame de ASA(config)#ip

Desabilitar assinatura 2150 do exame de ASA(config)#ip

Erro:- %ASA-4-402119: IPSEC: Received a protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP that failed anti-replay check.

Problema

Eu recebi este erro nos mensagens de registro do ASA:

`Erro:- %|ASA-4-402119: IPSEC: Received a protocol packet (SPI=spi, sequence number= seq_num) from remote_IP (username) to local_IP that failed anti-replay check.`

Solução

Para resolver esse erro, use o comando crypto ipsec security-association replay window-size para variar o tamanho da janela.

<#root>

`hostname(config)#`

`crypto ipsec security-association replay window-size 1024`

A Cisco recomenda que você use o tamanho de janela 1024 full para eliminar todos os problemas da anti-repetição.

Mensagem de erro – %ASA-4-407001: Deny traffic for local-host interface_name:inside_address, license limit of number exceeded

Problema

Poucos hosts são incapazes de conectar à Internet, e este mensagem de erro aparece no syslog:

Mensagem de erro – %ASA-4-407001: Deny traffic for local-host interface_name:inside_address, license limit of number exceeded

Solução

Este mensagem de erro é recebida quando o número de usuários excede o limite de licenças utilizadas. Para resolver esse erro, atualize a licença para um número maior de usuários.

A licença de usuário pode incluir 50, 100, ou usuários ilimitados conforme necessário.

Mensagem de Erro - %VPN_HW-4-PACKET_ERROR:

Problema

A mensagem de erro `Error Message - %VPN_HW-4-PACKET_ERROR:` indica que os pacotes ESP com HMAC enviados para o roteador apresentam incompatibilidade. Esse erro pode ser causado por estes problemas:

- Módulo VPN H/W defeituoso
- Pacote ESP corrompido

Solução

Para resolver este Mensagem de Erro:

- Ignore os Mensagens de Erro a menos que haja rompimento de tráfego.
- Se houver rompimento de tráfego, substitua o módulo.

Mensagem de erro: Command rejected: delete crypto connection between VLAN XXXX and XXXX, first.

Problema

Esta mensagem de erro será exibida quando você tentar adicionar uma VLAN permitida na porta de tronco em um switch: `Command rejected: delete crypto connection between VLAN XXXX and VLAN XXXX, first.`.

A borda do tronco WAN não pode ser alterado para permitir VLAN adicionais. Ou seja, você não pode adicionar VLANs no tronco IPSEC VPN SPA.

Este comando foi rejeitado porque resulta em uma VLAN de interface criptografada que pertence à lista de VLANs permitidas, o que representa uma possível violação de segurança IPSec.

Note que este comportamento se aplica a todas as portas de tronco.

Solução

Em vez do comando `no switchport trunk allowed vlan (vlanlist)`, use o comando `switchport trunk allowed vlan none` ou "`switchport trunk allowed vlan remove (vlanlist)`".

Mensagem de erro – % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Dropped packet - Invalid Window Scale option for session x.x.x.x:27331 to x.x.x.x:23 [Initiator(flag 0,factor 0) Responder (flag 1, factor 2)]

Problema

Este erro ocorre quando você tenta a telnet de um dispositivo na ponta oposta de um túnel VPN ou quando você tenta a telnet do próprio roteador:

`Mensagem de erro – % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Dropped packet - Invalid Window Scale option for session x.x.x.x:27331 to x.x.x.x:23 [Initiator(flag 0,factor 0) Responder (flag 1, factor 2)]`

Solução

A licença de usuário pode incluir 50, 100, ou usuários ilimitados conforme necessário. A função de escala de janela foi adicionada para permitir a rápida transmissão de dados em redes longas (LFN).

Estas são conexões típicas com ampla largura de banda, mas igualmente alta latência.

As redes com conexões via satélite são um exemplo de um LFN, uma vez que links por satélite possuem grande atraso de propagação mas têm tipicamente a largura de banda elevada.

Para ativar a função de escala de janela para oferecer suporte a LFNs, o tamanho da janela TCP deve ser superior a 65.535. Essa mensagem de erro poderá ser resolvida se você aumentar o tamanho da janela TCP para ter mais de 65.535.

%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse . Favor Atualizar o fluxo deste problema

Problema

Esta Mensagem de Erro aparece uma vez que o túnel VPN surge:

%ASA-5-305013: Asymmetric NAT rules matched for forward and reverse . Favor Atualizar o fluxo deste problema

Solução

Para resolver esse problema, quando não estiver na mesma interface que o host com NAT, use o endereço mapeado, em vez do endereço real, para se conectar ao host.

Além disso, ative o comando inspect se a aplicação incorporar o endereço IP.

%ASA-5-713068: Received non-routine Notify message: notify_type

Problema

Este Mensagem de Erro aparece se o túnel VPN não aparece:

%ASA-5-713068: Received non-routine Notify message: notify_type

Solução

Esta mensagem ocorre devido a uma falha de configuração (isto é, quando as políticas ou os ACL não são configurados para os mesmos peers).

Uma vez que as políticas e os ACL são combinados o túnel surge sem nenhum problema.

%ASA-5-720012: (VPN-Secondary) Failed to update IPSec failover runtime data on the standby unit (or) %ASA-6-720012: (VPN-unit) Failed to update IPsec failover runtime data on the standby unit

Problema

Uma destas Mensagens de Erro aparecem quando você tenta atualizar a Ferramenta de Segurança Adaptável da Cistos (ASA):

%ASA-5-720012: (VPN-Secondary) Failed to update IPSec failover runtime data on the standby unit.

%ASA-6-720012: (VPN-unit) Failed to update IPsec failover runtime data on the standby unit.

Solução

Estes Mensagens de Erro são erros informativos. As mensagens não impactam a funcionalidade do ASA ou do VPN.

Essas mensagens são exibidas quando o subsistema de failover da VPN não pode atualizar os dados de tempo de execução relacionados ao IPsec, pois o túnel IPsec relacionado foi excluído na unidade em standby.

Para resolvê-las, emita o comando wr standby na unidade ativa.

Erro:- %ASA-3-713063: IKE Peer address not configured for destination 0.0.0.0

Problema

A mensagem de erro **`%ASA-3-713063: IKE Peer address not configured for destination 0.0.0.0`** será exibida e o túnel não entrará em operação.

Solução

Esta mensagem aparece quando o endereço de peer IKE não está configurado para um túnel L2L.

Esse erro poderá ser resolvido se você alterar o número de sequência do mapa de criptografia e, em seguida, remover e reaplicar o mapa de criptografia.

Erro: %ASA-3-752006: Tunnel Manager failed to dispatch a KEY_ACQUIRE message.

Problema

A mensagem de erro `%ASA-3-752006: Tunnel Manager failed to dispatch a KEY_ACQUIRE message.Probable mis-configuration of the crypto map or tunnel-group."` será registrada no Cisco ASA.

Solução

Essa mensagem de erro pode ter sido causada pela configuração incorreta do mapa de criptografia ou do grupo de túneis. Certifique-se de que ambos estão configurados corretamente. Para obter mais informações sobre essa mensagem de erro, consulte o Erro 752006.

Abaixo, seguem algumas soluções corretivas:

- Remova a criptografia ACL (por exemplo, associada ao mapa dinâmico).

- Se existirem, remova as configurações de IKEv2 não utilizadas.
- Certifique-se de que a criptografia ACL coincidiu adequadamente.
- Se existirem, remova as entradas da lista de acesso em duplicidade.

Erro: %ASA-4-402116: IPSEC: Received an ESP packet (SPI= 0x99554D4E, sequence number= 0x9E) from XX.XX.XX.XX (user= XX.XX.XX.XX) to YY.YY.YY.YY

Em uma configuração de túnel VPN de LAN a LAN, a seguinte mensagem de erro é recebida no ASA de uma das extremidades:

```
O pacote interno desencapsulado não corresponde à política negociada na SA.

O pacote especifica o destino como 10.32.77.67, a origem como 10.105.30.1 e o protocolo como icmp.

A associação de segurança especifica o proxy local como 10.32.77.67/255.255.255.255/ip/0 e o proxy remoto como 10.105.42.192/255.255.255.224/ip/0.
```

Solução

É preciso verificar as listas de acesso de tráfego interessante definidas em ambas as extremidades do túnel VPN. Ambos devem corresponder como imagens espelhadas exatas.

Falha para iniciar o intalador 64-bit VA para habilitar o adaptador virtual devido ao erro 0xffffffff

Problema

A mensagem de registro `Failed to launch 64-bit VA installer to enable the virtual adapter due to error 0xffffffff` é recebida quando o AnyConnect não consegue se conectar.

Solução

Siga estes passos para resolver esse problema:

1. Acesse System > Internet Communication Management > Internet Communication settings e verifique se a opção Turn Off Automatic Root Certificates Update está desativada.
2. Se estiver desativada, desative toda a parte de Administrative Template do GPO atribuído ao computador afetado e teste novamente.

Consulte Turn off Automatic Root Certificates Update para obter mais informações.

O Cliente VPN Cisco não funciona com o cartão de dados em Windows 7

Problema

O Cliente VPN Cisco não funciona com o cartão de dados em Windows 7.

Solução

O Cliente VPN Cisco instalado em Windows 7 não funciona com conexões 3G uma vez que os cartões de dados não são apoiados nos clientes VPN instalados na máquina com Windows 7.

Alerta: "VPN functionality may not work at all"

Problema

Durante as tentativas de ativar o isakamp na interface externa do ASA, esta mensagem de alerta será recebida:

```
ASA(config)# crypto isakmp enable outside
WARNING, system is running low on memory.  Performance may start to degrade.
VPN functionality may not work at all.
```

Neste momento, acesse o ASA através do ssh. O HTTPS é parado e outros clientes SSL são afetados igualmente.

Solução

Este problema é causado pelos requisitos de memória dos diferentes módulos tais como o registador e a criptografia.

Verifique se você não tem o comando logging queue 0. Isso define o tamanho da fila como 8192 e a alocação de memória aumenta.

Em plataformas como o ASA5505 e o ASA5510, essa alocação de memória tende a esgotar a memória de outros módulos.

Erro no preenchimento do IPSec

Problema

A seguinte mensagem de erro é recebida:

```
%ASA-3-402130: CRYPTO: Received an ESP packet (SPI =
     0xXXXXXXX, sequence number= 0xXXXX) from x.x.x.x (user= user) to y.y.y.y with
     incorrect IPsec padding
```

Solução

O problema ocorre porque a VPN IPSec negocia sem um algoritmo de hash. O hash de pacotes garante a verificação de integridade do canal ESP.

Portanto, sem hash, os pacotes malformados são aceitos e não são detectados pelo Cisco ASA e ele tenta descriptografá-los.

No entanto, como esses pacotes estão malformados, o ASA encontra falhas durante a descriptografia de pacotes. Isso provoca as mensagens de erro no preenchimento verificadas.

A recomendação é incluir um algoritmo de hash no conjunto de transformação da VPN para garantir que o link entre os pares tenha o mínimo de pacotes malformados.

O túnel VPN é desconectado a cada 18 horas

Problema

Mesmo com o tempo de vida definido para 24 horas, o túnel VPN é desconectado a cada 18 horas.

Solução

A vida útil é o tempo máximo em que a SA pode ser usada para rechaveamento. O valor configurado para o tempo de vida é diferente do tempo de rechaveamento da associação de segurança.

Desse modo, é necessário negociar uma nova associação de segurança (ou par de associação de segurança, no caso do IPsec) antes que a atual expire.

O tempo de rechaveamento deve ser sempre mais curto do que o tempo de vida, para permitir várias tentativas, caso o primeiro rechaveamento falhe.

Os RFCs (Requests for Comment ou Pedidos de comentários) não especificam como calcular o tempo do rechaveamento. Isso é deixado a critério dos responsáveis pela implementação.

Portanto, o tempo varia de acordo com a plataforma. Algumas implementações usam um fator aleatório para calcular o tempo de rechaveamento.

Por exemplo, se o ASA inicia o túnel, é normal que seja rechaveado em 64.800 segundos = 75% de 86.400.

Se é o roteador que inicia, então o ASA pode esperar mais tempo, disponibilizando mais tempo

para que o par inicie o rechaveamento.

Portanto, é normal que a sessão VPN seja desconectada a cada 18 horas, para usar outra chave na negociação VPN. Isso não deve causar nenhum problema ou cancelamento de VPN.

O fluxo de tráfego não é mantido após a renegociação do túnel de LAN a LAN

Problema

O fluxo de tráfego não é mantido após a renegociação do túnel de LAN a LAN.

Solução

O ASA monitora cada conexão que passa por ele e mantém uma entrada na tabela de estados de acordo com o recurso de inspeção da aplicação.

Os detalhes sobre o tráfego criptografado que passam pela VPN são mantidos como um banco de dados de associações de segurança (Security Association ou SA). Para as conexões VPN de LAN a LAN, ele mantém dois fluxos de tráfego diferentes.

Um é o tráfego criptografado entre os gateways de VPN. O outro é o fluxo de tráfego entre o recurso de rede do gateway de VPN e o usuário final da outra extremidade.

Quando a VPN é encerrada, os detalhes do fluxo dessa SA específica são excluídos.

Contudo, a entrada na tabela de estados mantida pelo ASA para essa conexão TCP torna-se obsoleta por inatividade, o que dificulta o download.

Isso significa que o ASA ainda mantém a conexão TCP para esse fluxo específico, enquanto a aplicação do usuário é encerrada.

No entanto, as conexões TCP ficam dispersas e, eventualmente, o limite de tempo é atingido após a expiração do temporizador ocioso do TCP.

Esse problema foi resolvido ao implementar um recurso chamado Fluxos persistentes com túnel IPSec.

Um comando novo, sysopt connection preserve-vpn-flows, foi integrado ao Cisco ASA para reter as informações da tabela de estados na renegociação do túnel VPN.

Por padrão, esse comando está desativado. Para ativar esse recurso, o Cisco ASA mantém as informações da tabela de estados do TCP quando a VPN L2L se recupera da interrupção e restabelece o túnel.

A mensagem de erro indica que a largura de banda recorreu à funcionalidade de criptografia

Problema

O roteador 2900 Series recebeu a seguinte mensagem de erro:

Erro: Mar 20 10:51:29: %CERM-4-TX_BW_LIMIT: Maximum Tx Bandwidth limit of 85000 Kbps reached for Crypto functionality with securityk9 technology package license.

Solução

Esse é um problema já conhecido que ocorre devido às rígidas diretrizes impostas pelo Governo dos Estados Unidos da América.

De acordo, a licença securityk9 só pode permitir uma criptografia de payload até taxas próximas a 90 Mbps e limitar o número de túneis/sessões TLS criptografadas para o dispositivo.

Para obter mais informações sobre as restrições de exportação de criptografia, consulte Cisco ISR G2 SEC e HSEC Licensing.

No caso de dispositivos Cisco, calcula-se que o tráfego unidirecional seja menor do que 85 Mbps de entrada ou saída do roteador ISR G2, com um total bidirecional de 170 Mbps.

Essa exigência aplica-se às plataformas Cisco ISR G2 1900, 2900 e 3900. Este comando ajuda a visualizar estas limitações:

<#root>

```
Router#
```

show platform cerm-information

```
Crypto Export Restrictions Manager(CERM) Information:
CERM functionality: ENABLED
 ---------------------------------------------------------------
 Resource                      Maximum Limit          Available
 ---------------------------------------------------------------
 Tx Bandwidth(in kbps)         85000                  85000
 Rx Bandwidth(in kbps)         85000                  85000
 Number of tunnels               225                    225
 Number of TLS sessions         1000                   1000
---Output truncated----
```

Para evitar esse problema, compre uma licença HSECK9. Uma licença de recurso "hseck9" disponibiliza uma funcionalidade aprimorada de criptografia de payload, com contagens maiores de túneis VPN e sessões de voz seguras.

Para obter mais informações sobre o licenciamento do roteador Cisco ISR, consulte Ativação de software.

Problema: o tráfego de criptografia de saída em um túnel

IPsec falha, mesmo quando o tráfego de descriptografia de entrada funciona.

Solução

Este problema tem sido observado em conexões IPsec após vários rechaveamentos, mas não está claro qual é a condição desencadeadora.

A presença desse problema poderá ser estabelecida se você verificar a saída do comando show asp drop e se o contador de contexto da VPN expirada aumentar para cada pacote de saída enviado.

Diversos

A mensagem AG_INIT_EXCH aparece em “mostrar criptografia isakmp sa” e nos Comandos de Saída “debug"

Se o túnel não for iniciado, a mensagem AG_INIT_EXCH será exibida na saída do comando show crypto isakmp sa e na saída do debug.

O motivo pode ser uma incompatibilidade de políticas de isakamp ou um bloqueio da porta UDP 500 no caminho.

Debugar a mensagem “Você recebeu um mensagem IPC durante o estado inválido” aparece

Esta mensagem é um mensagem informativa e não não tem relação com a desconexão do túnel VPN.

Informações Relacionadas

- ASA e Cisco IOS®: fragmentação de VPN
- Ferramentas de segurança do Cisco ASA 5500 Series
- Negociação IPsec/Protocolos IKE
- 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.

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.