A maioria de IPSec VPN comum L2L e de Acesso remoto que pesquisa defeitos soluções

Índice

Introdução

Este documento contém as soluções mais comuns para problemas de VPN IPsec. Essas soluções foram obtidas diretamente das solicitações de atendimento resolvidas pelo Suporte Técnico da Cisco. Muitas dessas soluções podem ser implementadas antes de um troubleshooting profundo de uma conexão de VPN IPsec. Em conseqüência, este documento fornece uma lista de verificação de procedimentos comuns a serem testados antes de ligar para o Suporte Técnico Cisco.

Se você precisa originais do exemplo de configuração para o VPN de Site-para-Site e para o acesso remoto VPN, refira o *acesso remoto VPN, Site-para-Site VPN (L2L) com PIX, Site-para-Site VPN (L2L) com IOS,* e o *Site para Site VPN (L2L) com VPN3000*seções de Exemplos de Configuração e TechNotes.

Nota: Mesmo que os exemplos de configuração neste documento sejam para o uso em roteadores e em ferramentas de segurança, quase todos estes conceitos são igualmente aplicáveis ao VPN 3000 concentrator.

Nota: Refira o Troubleshooting de Segurança IP - Compreendendo e usando comandos debug fornecer os comandos debug de uma explicação comun que são usados para pesquisar defeitos edições do IPsec no Cisco IOS ® Software e no PIX.

Nota: ASA/PIX não passará o tráfego multicast sobre túneis do IPSec VPN.

Nota: Você pode olhar acima para qualquer comando usado neste documento com a ferramenta de consulta de comandos (somente clientes registrados).

aviso: Muitas das soluções apresentadas neste original podem conduzir a uma perda temporária de toda a conectividade do IPSec VPN 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

Cisco recomenda que você tenha conhecimento da configuração do IPSec VPN nestes dispositivos Cisco:

- Ferramenta de segurança do Cisco PIX 500
- Ferramenta de segurança do Cisco ASA 5500 Series
- Roteadores do Cisco IOS

- Cisco VPN 3000 Series Concentrators (*opcional*)

Componentes Utilizados

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

- Ferramenta de segurança do Cisco ASA 5500 Series
- Ferramenta de segurança do Cisco PIX 500
- 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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

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 sejam listados em nenhum pedido específico, estas soluções podem ser usadas como uma lista de verificação dos artigos para serem verificados ou tentados antes que você contate o Troubleshooting detalhado e chame o TAC. Todas estas soluções vêm diretamente dos pedidos do serviço TAC e resolveram os problemas de diversos clientes.

- 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
- Verifique que os comandos sysopt estam presente (PIX/ASA somente)
- 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
- Edições com latência para o tráfego do cliente VPN

Nota: Alguns dos comandos nestas seções foram derrubados a uma segunda linha devido à considerações espaciais.

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

NAT-Traversal ou o NAT-T permitem que o tráfego VPN passe através dos dispositivos NAT ou PAT, tais como um roteador Linksys SOHO. Se o NAT-T não for ativado, os usuários do cliente VPN conectam-se frequentemente ao PIX ou ao ASA sem nenhum problema, mas são incapazes de acessar a rede interna atrás da ferramenta de segurança.

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

Similarmente, se você é incapaz de fazer o início de uma sessão simultâneo do mesmo endereço IP, a conexão do VPN seguro terminada localmente pelo cliente. `Motivo 412: O peer remoto não está mais respondendo.` é exibida a mensagem de erro. Permitir o NAT-T no dispositivo da extremidade principal VPN a fim de resolver este erro.

Nota: Com Cisco IOS Software Versão 12.2(13)T e Mais Recente, o NAT-T é permitido por padrão no Cisco IOS.

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

PIX/ASA 7.1 e mais recente

```
pix(config)#isakmp nat-traversal 20
```

PIX/ASA 7.2(1) e mais recente

```
securityappliance(config)#crypto isakmp nat-traversal 20
```

Os clientes precisam ser modificados também para que tudo funcione.

No Cisco VPN Client, selecione **Connection Entries** e clique em **Modify**. Uma nova janela será aberta. Selecione a guia **Transport**. Nessa guia, selecione **Enable Transparent Tunneling** e o botão de opção **IPSec over UDP (NAT / PAT)**. Clique em **Save** e teste a conexão.

Nota: Este comando é o mesmo para o PIX 6.x e o PIX/ASA 7.x.

Nota: É importante permitir o UDP 4500 para portas NAT-T, UDP 500 e ESP pela configuração de um ACL porque o PIX/ASA actua como um dispositivo NAT. Consulte Configurando um Túnel

IPsec Através de um Firewall com NAT para obter mais informações sobre a configuração de ACLs em um PIX/ASA.

Concentrador de VPN

Escolha **Configuration > Tunneling and Security > IPSEC > NAT Transparency > Enable:** ***IPsec sobre o NAT-T*** a fim de permitir o NAT-T no concentrador VPN.

Nota: O NAT-T igualmente conecta múltiplos clientes VPN ao mesmo tempo através de um dispositivo PAT a toda a extremidade principal seja ele PIX, Roteador ou Concentrador.

Teste a conectividade corretamente

Idealmente, a conectividade de VPN é testada de dispositivos por trás de dispositivos de ponto final que fazem a criptografia, ainda que muitos usuários testem a conectividade de VPN com o comando **ping** nos dispositivos que fazem a criptografia. Enquanto o **ping** geralmente funciona para esse motivo, é importante buscar a fonte seu ping da interface correta. Se a origem do **ping** estiver incorreta, pode parecer que a conexão de VPN falhou quando na realidade ela funciona. Tome este cenário como 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
```

Nesta situação, um **ping** deve ser originado da rede “interna” atrás de um ou outro roteador. Isto é porque os ACLs criptografados são configurados somente para criptografar o tráfego com aqueles endereços de origem. Um **ping** proveniente da interface da Internet de qualquer um dos roteadores não é criptografado. Use as opções estendidas do comando **ping** no modo EXEC privilegiado para gerar um ping da interface "interna" de um roteador.

```
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 pelos dispositivos de segurança PIX ou ASA. O **ping** usado para testar a conectividade também pode ser gerado pela interface interna com a palavra-chave **interna**:

```
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
```

Nota: Não se recomenda que você vise a interface interna de uma ferramenta de segurança com seu **ping**. Se você deve visar a interface interna com seu **ping**, você deve permitir a gestão de **acesso n**na interface, ou o dispositivo não responde.

```
securityappliance(config)#management-access inside
```

Nota: Quando existe um problema com a conectividade, mesmo a fase 1 de VPN não carrega. No ASA, se a conectividade falhar, a saída SA é similar a este exemplo, o que indica possivelmente uma configuração incorreta da criptografia peer e/ou a configuração incorreta da proposta

ISAKMP:

```
Router#show crypto isakmp sa 1 IKE Peer: XX.XX.XX.XX Type : L2L Role : initiator Rekey : no
State : MM_WAIT_MSG2
```

Nota: O estado poderia ser de MM_WAIT_MSG2 a MM_WAIT_MSG5, o que denota a falha de troca interessada do estado no modo principal (MM).

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

```
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 houver indicação alguma de que um túnel VPN IPsec foi ativado, é possível que o ISAKMP não tenha sido habilitado. Seja certo que você habilitou o ISAKMP em seus dispositivos. Use um destes comandos para habilitar o ISAKMP em seus dispositivos:

- Cisco IOS`router(config)#`**`crypto isakmp enable`**
- Cisco PIX 7.1 e mais recente (substitua a **parte externa** com a interface desejada)`pix(config)#`**`isakmp enable outside`**
- Cisco PIX/ASA 7.2(1) e mais recente (substitua a **parte externa** com sua interface desejada)`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 atrás de ASA/PIS obtem PAT'd à porta 500 UDP antes que o isakmp possa ser habilitado na interface. Uma vez que essa tradução PAT é removida (clear xlate), o isakmp pode ser habilitado.

Nota: Certifique-se sempre de que os números de porta UDP 500 e 4500 estejam reservados para a negociação das conexões ISAKMP com o peer.

Nota: 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
```

Nota: 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. Habilite ou desabilite o PFS em ambos os tuneis peer; se não, o túnel de LAN-to-LAN (L2L) IPsec não é estabelecido no roteador PIX/ASA/IOS.

PIX/ASA:

O PFS é desabilitado por padrão. Para habilitá-lo, use o comando **pfs** com a palavra-chave enable no modo de configuração de política de grupo. Para desabilitar o PFS, insira a palavra-chave disable.

```
hostname(config-group-policy)#pfs {enable | disable}
```

Para remover o atributo de PFS da configuração em execução, 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 impedir que um valor seja herdado.

```
hostname(config-group-policy)#no pfs
```

IOS Router:

Para especificar que o IPsec peça o PFS quando novas associações de segurança forem solicitadas para esta entrada do mapa de criptografia, ou que o IPsec exija 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:

```
Router(config)#crypto map map 10 ipsec-isakmp
Router(config-crypto-map)#set pfs group2
```

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

Cancele associações de segurança velhas ou existentes (os túneis)

Se esta mensagem de erro ocorrer no IOS Router, o problema é que a AS expirou ou foi limpa. 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.

```
%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.

Nota: 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 as associações de segurança a serem canceladas, os comandos listados aqui podem cancelar 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**Cisco IOS**`router#show crypto isakmp sa router#show crypto ipsec sa` **Dispositivos de segurança Cisco PIX/ASA**`securityappliance#show crypto isakmp sa securityappliance#show crypto ipsec sa` **Nota:** Estes comandos são os mesmos para Cisco PIX 6.x e PIX/ASA 7.x
2. Cancele associações de segurança. Cada comando pode ser incorporado segundo as indicações em negrito ou serem incorporadas com as opções mostradas com elas.**Cisco IOSISAKMP (Fase I)**`router#clear crypto isakmp ? <0 - 32766> connection id of SA <cr>`**IPsec (Fase II)**`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>`**Dispositivos de segurança Cisco PIX/ASAISAKMP (Fase I)**`securityappliance#clear crypto isakmp sa` **IPsec (Fase II)**`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 ocorrer alguma discrepância na duração de ISAKMP, você pode receber o **%PIX|ASA-5-713092: Grupo = x.x.x.x, IP= x.x.x.x, falha durante a tentativa rekeying da fase 1 devido à mensagem do erro de colisão no** PIX/ASA. Para o FWSM, você pode receber o %FWSM-5-713092: `Grupo = x.x.x.x, IP= x.x.x.x, falha durante a tentativa rekeying da fase 1 devido à mensagem do erro de colisão.` Configure o mesmo valor em ambos os peers para corrigir o problema.

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).

PIX/ASA

```
hostname(config)#isakmp policy 2 lifetime 14400
```

Roteador IOS

```
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. Motivo 426:` Tempo de vida configurada excedida.

A fim resolver este Mensagem de Erro, ajuste o valor do ***tempo de vida*** *0* a fim ajustar o tempo de vida de uma associação de segurança IKE ao infinito. O VPN sempre será conexão e não terminará.

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

Você pode igualmente **desabilitar re-xauth na grupo-política** a fim resolver a edição.

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.

- Configurar os ISAKMP keepalives no Cisco IOS com este comando:`router(config)#` **`crypto isakmp keepalive 15`**
- Use estes comandos para configurar os ISAKMP keepalives nos dispositivos de segurança PIX/ASA:Cisco PIX 6.x`pix(config)#` **`isakmp keepalive 15`** Cisco PIX/ASA 7.x ou posterior para o grupo de túnel chamado **10.165.205.222**`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 PIX/ASA 7.x ou posterior para o grupo de túnel chamado **10.165.205.222**Desabilita o processamento de keepalives do IKE, o qual é habilitado por padrão.`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**Selecione **%System Root% > Program Files > Cisco Systems > VPN Client > Profiles** no PC cliente que está experimentando o problema para desabilitar o keepalive do IKE e edite o **PCF file** onde aplicável para a conexão.Altere **'ForceKeepAlives=0'** (padrão) para **'ForceKeepAlives=1'**.

Nota: 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 simples erro de digitação pode ser a causa de um túnel VPN IPsec não ser ativado. 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.** Re-entre a chave para garantir que está correta; esta é uma solução simples que possa ajudar a evitar o Troubleshooting 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. Esse erro poderá ocorrer se o nome do grupo/chave pré-compartilhada não coincidir entre o cliente VPN e o dispositivo 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... may 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)
```

Você também pode recuperar uma chave pré-compartilhada sem nenhuma alteração de configuração PIX/ASA Security Appliance. Refira ao PIX/ASA 7.x: Recuperação de chave pré-compartilhada.

aviso: Se você remover os comandos criptografados-relacionados, você provavelmente irá derrubar um ou todos seus túneis VPN. Use estes comandos com cuidado e refira à política do controle de alterações de sua organização antes que você siga estas etapas.

- Use estes comandos para remover e inserir novamente a chave pré-compartilhada **secretkey** para o peer **10.0.0.1** ou o grupo **vpngroup** no IOS:LAN para LAN VPN de Cisco`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`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 inserir novamente a chave pré-compartilhada **secretkey** para o peer **10.0.0.1** em PIX/ASA Security Appliances:Cisco PIX 6.x`pix(config)#no isakmp key secretkey address 10.0.0.1 pix(config)#isakmp key secretkey address 10.0.0.1` Cisco PIX/ASA 7.x ou posterior`securityappliance(config)#tunnel-group 10.0.0.1 ipsec-attributes securityappliance(config-tunnel-ipsec)#no pre-shared-key securityappliance(config-tunnel-ipsec)#pre-shared-key secretkey`

Chave pré-compartilhada mal combinada

A iniciação do túnel VPN fica desconectada. Esta edição pôde ocorrer devido a uma chave-pré-compartilhada malcombinada durante a fase I de negociações.

A **mensagem MM_WAIT_MSG_6** no **comando show cryptografado isakmp sa** indica uma chave-pré-compartilhada malcombinada segundo as indicações deste exemplo:

```
ASA#show crypto isakmp sa Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: 10.7.13.20 Type : L2L Role : initiator Rekey : no State : MM_WAIT_MSG_6
```

A fim resolver esta edição, entre novamente a chave pré-compartilhada em ambos os dispositivos; a chave-pré-compartilhada deve ser única e combinada. VejaRe-Entre ou recupere a chave-pré-compartilhada para mais informação.

Remoção e Reaplicação de Mapas de Criptografia

Quando você cancela associações de segurança, e isto não resolve uma edição do IPSec VPN, remova e reaplique o mapa de criptografia relevante a fim resolver uma ampla variedade de edições que inclua uma queda intermitente do túnel VPN e a falha de alguns locais VPN para vir acima.

aviso: Se você remover o mapa de criptografia de uma relação, isto **definitivamente** derruba todos os túneis de IPsec associados com este mapa de criptografia. Siga estas etapas com cuidado e considere a política do controle de alterações de sua organização antes que você continue.

- Use estes comandos para remover e substituir um mapa de criptografia no Cisco IOS:Comece com a remoção do mapa de criptografia da relação. Não use nenhum formulário do **comando mapa de criptografia**.`router(config-if)#no crypto map mymap` Continue a usar o formulário **no** para remover um mapa de criptografia inteiro.`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:`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 remover e substituir um mapa de criptografia no PIX ou no ASA:Comece com a remoção do mapa de criptografia da relação. Não use nenhum formulário do **comando mapa de criptografia**.`securityappliance(config)#no crypto map mymap interface outside` Continue a usar o formulário **no** para remover os outros comandos de mapa de criptografia.`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:`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`

Nota: 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.

Verifique que os comandos sysopt estam presente (PIX/ASA somente)

Os comandos **sysopt connection permit-ipsec** e **sysopt connection permit-vpn** permitem que os pacotes de um túnel IPsec e suas payloads desviem das ACLs da interface no Security Appliance. Os túneis IPsec terminados no Security Appliance provavelmente falharão se um destes comandos não for habilitado.

Na versão de software 7,0 da ferramenta de segurança e mais adiantado, o comando sysopt relevante para esta situação é **sysopt connection permit-ipsec**.

Na versão de software da ferramenta de segurança 7.1(1) e mais atrasado, o comando sysopt relevante para esta situação é licença-**VPN da conexão do sysopt**.

Em PIX 6.x, esta funcionalidade é **deficiente** à revelia. No PIX/ASA 7.0(1) ou posterior, a funcionalidade é **habilitada** por padrão. Use estes comandos show para determinar se o comando **sysopt** relevante está habilitado em seu dispositivo:

- Cisco PIX 6.x`pix# show 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 no sysopt uauth allow-http-cache no sysopt connection permit-ipsec !--- sysopt connection permit-ipsec is disabled no sysopt connection permit-pptp no sysopt connection permit-l2tp no sysopt ipsec pl-compatible`
- Cisco PIX/ASA 7.x`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 habilitar o comando **sysopt** correto para seu dispositivo:

- Cisco PIX 6.x e PIX/ASA 7,0`pix(config)#sysopt connection permit-ipsec`
- Cisco PIX/ASA 7.1(1) ou posterior`securityappliance(config)#sysopt connection permit-vpn`

Nota: Se você não deseja usar o **comando connection do sysopt**, a seguir você deve explicitamente permitir o tráfego exigido, que é tráfego interessante da fonte ao destino, por exemplo, do LAN do dispositivo remoto à LAN do dispositivo local e “da porta 500" UDP para a interface externa do dispositivo remoto à interface externa do dispositivo local, no ACL exterior.

Verificação da Identidade de ISAKMP

Se o túnel do IPSec VPN falhou dentro da negociação de IKE, a falha pode ser devido ao PIX ou à incapacidade de seu par reconhecer a identidade de seu par. 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 de ISAKMP da unidade PIX 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 fazer com que o ID da Fase 2 seja enviado para o peer, 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 type
```

OU

```
crypto isakmp identity auto
!--- If the RA or L2L (site-to-site) VPN tunnels connect !--- with ISAKMP negotiation by
connection type; IP address for !--- preshared key or cert DN for certificate authentication.
```

OU

```
crypto isakmp identity hostname
!--- Uses the fully-qualified domain name of !--- the host exchanging ISAKMP identity
information (default). !--- This name comprises the hostname and the domain name.
```

O túnel VPN não vem acima após configuração movente do PIX ao ASA usando a ferramenta da migração da configuração PIX/ASA; estas mensagens aparecem no registro:

```
[IKEv1]: O grupo = x.x.x.x, IP= x.x.x.x, Stale PeerTblEntry encontrado, removendo! [IKEv1]:
Grupo = x.x.x.x, IP= x.x.x.x, removendo o par da tabela do correlator falhada, sem
correspondência! [IKEv1]: Grupo = x.x.x.x, IP= x.x.x.x, construct_ipsec_delete(): Nenhum SPI
para identificar a fase 2 SA! [IKEv1]: Grupo = x.x.x.x, IP= x.x.x.x, removendo o par da tabela
do correlator falhada, sem correspondência!
```

Esta edição acontece desde que o PIX é configurado por padrão para identificar a conexão como

o **hostname** onde o ASA identifica como o **IP**. A fim resolver esta edição, use o **comando de identidade de criptografia isakmp**no modo de configuração global como mostrado abaixo:

```
crypto isakmp identity hostname !--- Use the fully-qualified domain name of !--- the host exchanging ISAKMP identity information (default). !--- This name comprises the hostname and the domain name.
```

Quando você recebe a Mensagem de Erro INVALID_COOKIE das un-criptografia recebidas, emita o **comando endereço de criptografia da identidade do isakmp** a fim resolver a edição.

Nota: O comando da **identidade do isakmp** foi fornecido da versão de software 7.2(1). Consulte a Referência de Comandos do Cisco Security Appliance Versão 7.2 para obter mais informações.

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 cliente VPN será desconectado após 30 minutos, independentemente da configuração do timeout de ociosidade e receberá o erro PEER_DELETE-IKE_DELETE_UNSPECIFIED.

Configurar o **idle timeout** e o **timeout de sessão** porque **nenhuns** a fim fazer sempre **acima o** túnel, e de modo que o túnel seja deixado cair nunca mesmo quando usando dispositivos de terceira parte.

PIX/ASA 7.x ou posterior

Insira o comando **vpn-idle-timeout** no modo de configuração de política de grupo ou no modo de configuração de nome de usuário para configurar o período de timeout do usuário.

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

Configure o tempo máximo para as conexões de VPN com o comando **vpn-session-timeout** no modo de configuração de política de grupo ou no modo de configuração de nome de usuário:

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

Nota: Quando você tem configurado **túnel-todo**, você não precisa de configurar o **idle-timeout** porque, mesmo se você configurar o VPN-idle-timeout, não funcionará porque todo o tráfego está atravessando o túnel (desde que túnel-todo esteja configurado). Conseqüentemente, o tráfego interessante (ou mesmo o tráfego gerado pelo PC) será interessante e não deixará o Idle-timeout entrar a ação.

Cisco IOS Router

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 de ociosidade da AS IPsec. Por padrão, esses temporizadores estão desabilitados.

```
crypto ipsec security-association idle-time seconds
```

O tempo é expresso em *segundos*, e representa o período no qual o temporizador de ociosidade permite que um peer 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 acessos define que tráfego a criptografado; isto inclui um ACL criptografado em uma instalação do LAN para LAN ou em um split-tunneling ACL em uma configuração do acesso remoto. Quando estes ACL são configurados incorretamente ou de faltas, o tráfego pôde somente fluir em um sentido através do túnel VPN, ou não pôde ser enviado através de todo túnel.

Nota: Certifique-se ligar o ACL criptografia com o mapa de criptografia usando o comando address do coincidente do mapa de criptografia 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.**Nota:** No concentrador VPN, você pôde ver um registro como este:`Túnel Rejeitado: O par IKE não combina o peer remoto como definido na política L2L`A fim evitar esta mensagem e a fim trazer acima o túnel, certifique-se de que os ACLs cript. não sobrepor e o mesmo tráfego interessante não está sendo usado por nenhum outro túnel VPN configurado.
- Não use o ACL duas vezes. Mesmo se sua isenção de NAT ACL e ACL criptografado especifica o mesmo tráfego, use duas listas de acessos diferentes.
- Na configuração de acesso remoto, não use lista de acesso para o tráfego de interesse com o mapa de criptografia dinâmica. Isso poderá fazer com que o cliente VPN seja incapaz de se conectar ao dispositivo headend. Se você configurou equivocadamente o ACL criptografado para o acesso remoto VPN, você pode obter o %ASA-3-713042: `Iniciador IKE incapaz de encontrar a política:` Mensagem de Erro do intf2.**Nota:** Se este é um túnel de site para site VPN, certifique-se combinar a lista de acessos com o par. Eles devem estar na ordem reversa no peer.Consulte Exemplo de Configuração do PIX/ASA 7.x e do Cisco VPN Client 4.x com Autenticação IAS RADIUS (contra Active Directory) do Windows 2003 para obter um exemplo de configuração que mostra como estabelecer a conexão de VPN de acesso remoto entre um Cisco VPN Client e o PIX/ASA.
- 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 PIX ou no ASA, isto 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 IOS Router é configurado para isentar o tráfego que é enviado entre **192.168.100.0 /24** e **192.168.200.0 /24** ou **192.168.1.0 /24** do 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
```

Aqui, um PIX é

configurado para isentar o tráfego que é enviado entre **192.168.100.0 /24** e **192.168.200.0 /24** ou **192.168.1.0 /24** do NAT. Por exemplo, todo tráfego restante é sujeito à sobrecarga NAT:`access-list **noNAT** extended permit ip 192.168.100.0 255.255.255.0 192.168.200.0 255.255.255.0 access-list **noNAT** extended permit ip 192.168.100.0 255.255.255.0 192.168.1.0 255.255.255.0 nat (inside) 0 access-list **noNAT** nat (inside) 1 0.0.0.0 0.0.0.0 global (outside) 1 interface` **Nota:** 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 exceção de NAT não funcionam com os números de porta (por exemplo, 23, 25, etc.).**Nota:** Em um ambiente VoIP, onde as chamadas de voz entre redes estejam sendo comunicadas com o VPN, as chamadas de voz não trabalham se o NAT 0 ACL não é configurado corretamente. Antes de atravessar profundamente o Troubleshooting de VoIP, sugere-se para verificar o estado da conectividade de VPN porque o problema poderia ser com o erro de configuração de NAT ACL isentos.**Nota:** Você pode receber o Mensagem de Erro como mostrado se há erro de configuração na isenção de NAT (nat 0) ACL.`%PIX-3-305005: **No translation group** found for icmp src outside:192.168.100.41 dst inside:192.168.200.253 (type 8, code 0) %ASA-3-305005: No translation group found for`

`udp src Outside:x.x.x.x/p dst Inside:y.y.y.y/p`**Nota: Exemplo incorreto:**`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 excessão de NAT (0 nat) não funciona, tente removê-la a seguir 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. Isto significa que os ACL devem **se espelhar**um ao outro. Neste exemplo, um túnel LAN a LAN é estabelecido 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`**Nota:** Embora não se ilustre aqui, este mesmo conceito também aplica-se às ferramentas de segurança PIX e ASA.No PIX/ASA, o separação-túnel ACL para configurações do acesso remoto deve ser as lista de **acesso padrão** que permitem o tráfego à rede a que os clientes VPN precisam do acesso. Os IOS Router podem usar o ACL extendido para o túnel-separado.**Nota:** Na lista de acesso extendida, usar **"qualquer"** na fonte no split tunneling ACL é similar desabilitar o split tunneling. Use somente as redes de origem na ACL estendida para a separação de túneis.**Nota: Exemplo correto:**`access-list 140 permit ip **10.1.0.0 0.0.255.255** 10.18.0.0 0.0.255.255` **Nota: Exemplo incorreto:**`access-list 140 permit ip **any** 10.18.0.0 0.0.255.255` Cisco IOS`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 PIX 6.x`pix(config)#**access-list 10 permit** 192.168.100.0 255.255.255.0 pix(config)#**vpngroup MYGROUP split-tunnel 10**` Cisco PIX/ASA 7.x`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**`

Este erro ocorre em ASA 8.3 se NO NAT ACL estiver desconfigurado ou não configurado no ASA:

```
%ASA-5-305013: Regras assimétricas NAT combinadas para fluxo para frente e para trás; Conexão para a parte externa do udp src: interior do dst x.x.x.x/xxxxx: x.x.x.x/xx negado devido à falha do caminho reverso NAT
```

A fim resolver esta edição, verifique se a configuração está correta ou reconfigure se os ajustes estão incorretos.

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

Um VPN de Site-para-Site tem que ser estabelecido entre HOASA e BOASA com ambos os ASA usando a 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 clientes VPN de Cisco ou o VPN de Site-para-Site não podem estabeleça o túnel com o dispositivo remoto-final, certific dos **dois pares contenham a mesmos cifragem, mistura, autenticação, e valores de parâmetro de Diffie-Hellman** e quando a política do peer remoto especifica uma vida inferior ou igual à vida 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, dropping
```

Esta mensagem parece geralmente devido às políticas de ISAKMP combinadas mal ou a uma indicação faltante NAT 0.

Além disso, esta mensagem aparece:

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

Esta mensagem indica que as mensagens da fase 2 estão sendo enviadas à fila após a fase 1 estar completa. Esta Mensagem de Erro pode ser devido a uma destas razões:

- Má combinação na fase em alguns dos peers
- O ACL está obstruindo os peers para completar a fase 1

Esta mensagem vem geralmente depois que o peer de remoção da tabela do peer que falhou, sem correspondência! mensagem de erro.

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

de IKE do Cisco VPN Client.

Nota: Para o conjunto de transformação da política de ISAKMP e do IPsec que é usado no PIX/ASA, o Cisco VPN Client não pode usar uma política com uma combinação de DES e de 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

O roteamento é uma parte crítica de quase todas as implementações de VPN IPsec. Esteja certo que seus dispositivos da criptografia tais como roteadores e ferramentas de segurança PIX ou ASA têm a informação de roteamento apropriada para enviar o tráfego por seu túnel VPN. Além disso, se outros roteadores existem atrás de seu dispositivo de gateway, seja certo que aqueles roteadores saibam como alcançar o túnel e que 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 Roteador A foi substituído com um PIX ou um ASA, a configuração pode olhar como esta:`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:`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 Roteador A foi substituído por um PIX ou por um ASA, a configuração pode parecer como esta:`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 clientes VPN estão dados endereços na escala de **10.0.0.0 /24** quando conectados.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.Cisco IOS Router:`crypto dynamic-map dynMAP 10 set transform-set mySET` **`reverse-route`** `crypto map myMAP 60000 ipsec-isakmp dynamic dynMAP`Cisco PIX ou ferramenta de segurança ASA:`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`

Nota: 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 informações adicionais, consulte a seção Sobreposição de Redes Privadas.

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 Comandos do Guia de Configuração do Cisco Security Appliance para obter mais informações.

Nota: Para o conjunto de transformação da política de ISAKMP e do IPsec que é usado no PIX/ASA, o Cisco VPN Client não pode usar uma política com uma combinação de DES e de 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 seqüência da entrada do mapa de criptografia dinâmico **deve ser** mais alto do que todas as outras entradas do mapa estático de criptografia. 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!
```

Nota: 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:

```
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 cisco
```

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

Nota: Este Mensagem de Erro pode igualmente ser considerado quando a sequência cripto dinâmica do homem não está correta que faz com que o par bata o crypto map errado, e igualmente por uma lista de acessos cripto combinada mal que defina o tráfego interessante:

```
%ASA-3-713042: Iniciador IKE incapaz de encontrar a política:
```

Nos cenários em que vários túneis VPN são terminados na mesma interface, precisamos criar um mapa de criptografia com o mesmo nome (somente um mapa de criptografia é permitido por interface), mas com um número de seqüência diferente. Isso é verdadeiro para o roteador, PIX e ASA.

Consulte Configurando o IPsec Entre PIXs Hub e Remotos com Clientes VPN e Autenticação Estendida para obter mais informações sobre a configuração de um PIX hub para o mesmo mapa de criptografia com números de seqüência diferentes na mesma interface. Similarmente, refira ao PIX/ASA 7.X: Adicionar um túnel ou um acesso remoto novo a um L2L existente VPN para mais informação a fim aprender mais sobre a configuração do mapa de criptografia para encenações L2L e de acesso remoto VPN.

Verificação da Correção do Endereço IP do Peer

Para uma configuração de VPN LAN a LAN (L2L) de um PIX/ASA Security Appliance 7.x, você deve especificar o **<name>** do grupo do túnel e o **Remote peer IP Address** (extremidade remota do túnel) no comando **tunnel-group <name> type ipsec-l2l** para a criação e o gerenciamento do banco de dados de registros específicos de conexão do IPsec. O endereço IP do peer deve coincidir 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 peer não é configurado corretamente, os registros podem conter esta mensagem, que pode ser resolvida pela configuração apropriada do **endereço IP do peer**.

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

Para uma configuração de VPN LAN a LAN (L2L) de um PIX 6.x, o endereço IP do peer (extremidade remota do túnel) deve coincidir com os comandos **isakmp key address** e **set peer** no mapa de criptografia para uma conexão de VPN IPsec bem sucedida.

Quando o endereço IP do peer não foi configurado corretamente na configuração de criptografia ASA, o ASA não pode estabelecer o túnel VPN e pendurar somente na fase *MM_WAIT_MSG4* . A fim resolver esta edição, corrija o endereço IP do peer na configuração.

Está aqui a saída do **comando show crypto isakmp sa** quando o túnel VPN pendura no estado MM_WAIT_MSG4.

```
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

```
%PIX|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.

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

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

Both lines should 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 do acesso remoto VPN são configurados no mesmo mapa de criptografia, o par do LAN para LAN soar um alerta para a informação XAUTH, e o túnel de LAN para LAN falha com o "***CONF_XAUTH***" na saída do **comando show crypto isakmp sa**.

Está aqui um exemplo do SA output:

```
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
```

Nota: Esta edição aplica-se somente ao Cisco IOS e ao PIX 6.x visto que o PIX/ASA 7.x não é afetado por esta edição desde que use o grupo túnel.

Use a palavra-chave **no-xauth** quando você incorpora a chave do isakmp, assim que o dispositivo não alerta o par para a informação 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:

```
router(config)#crypto isakmp key cisco123 address 172.22.1.164 no-xauth
```

Na encenação onde o PIX/ASA 7.x actua como o Easy VPN Server, o cliente VPN fácil é incapaz de conectar à extremidade principal devido à edição de Xauth. Desabilite a autenticação de usuários no PIX/ASA para resolver o problema conforme mostrado:

```
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:`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:`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.

Nota: 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.

Edições com latência para o tráfego do cliente VPN

Quando há umas edições da latência sobre uma conexão de VPN, verifique o seguinte a fim resolver isto:

1. Verifique se o MSS do pacote pode ser reduzido mais.
2. Se o IPsec/tcp é usado em vez do IPsec/UDP, a seguir configurar o conserva-VPN-fluxo.
3. Recarregue Cisco ASA.

Os clientes VPN são incapazes de conectar com o ASA/PIX

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:

```
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 isto funcionar bem, o problema deve ser relacionado à configuração deve ser relacionada ao 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 poderia usar o **comando debug radius** para pesquisar defeitos problemas relacionados ao raio. Para a amostra **faça o debug do radius** saída, refira a estas saídas de exemplo.

Nota: Antes que você use o **comando debug** no ASA, refira a esta documentação: Mensagem de advertência.

A conexão das gotas do cliente VPN frequentemente na primeira conexão de VPN da tentativa ou da “Segurança terminou pelo par. Motivo 433." ou do “conexão VPN seguro terminada pela Motivo Peer 433:(Motivo não especificado pelo peer)”

Problema

Os usuários do Cliente VPN da Cisco podem receber este erro quando tentam a conexão com a extremidade principal do dispositivo VPN.

Do “a *conexão das gotas cliente VPN frequentemente na primeira tentativa*” ou da “na *conexão de VPN Segurança terminou pelo par. Motivo 433."* ou “*Conexão de VPN Seguro terminada pelo motivo 433:(Motivo Não Especificada pelo Peer)*” ou “*Tentada atribuir a rede ou transmitir o endereço IP, removendo (x.x.x.x) do pool”*

Solução 1

O problema pode ser com a atribuição do pool do IP com ASA/PIX, servidor Radius, servidor DHCP ou através do servidor Radius que actua como o servidor DHCP. Use o comando **debug crypto** a fim de verificar que o netmask 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. Verificar a senha da autenticação de servidor no Servidor e no cliente e recarregar o servidor AAA pude resolver esta edição.

Solução 3

Uma outra ação alternativa para esta edição é desabilitar a característica da detecção de riscos. Às vezes quando há umas múltiplas retransmissões para diferentes Associações de Ssegurança incompletas (SA), o ASA com a característica da detecção de ameaça permitida pensa que um ataque da exploração está ocorrendo e as portas VPN estão marcadas como o principal ofensor. 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
```

Para mais informações sobre esta característica, refira à detecção de ameaças.

Nota: Isto pode ser usado como uma ação alternativa para verificar se isto irá fixar o problema real. Certifique-se se ao desabilitar a detecção de ameaças do Cisco ASA irá comprometer os diversos recursos de segurança tais como o abrandamento das tentativas da exploração, DoS com SPI inválido, os pacotes que falham a Inspeção de Aplicativo 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

- Hairpinning
- Acesso do LAN local
- Sobreposição de Redes Privadas

Não É Possível Acessar os Servidores na DMZ

Uma vez que o cliente VPN está estabelecido o túnel de IPsec com o dispositivo de extremidade principal VPN (roteador PIX/ASA/IOS), os usuários de cliente VPN podem alcançar os 10.10.10.0/24) recursos da rede interna (, mas são incapazes de alcançar a rede do 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

ASA/PIX
ciscoasa#**show running-config** *!--- Split tunnel for the **inside network** access* access-list vpnusers_spitTunnelAcl permit ip 10.10.10.0 255.255.0.0 any *!--- Split tunnel for the **DMZ network** access* access-list vpnusers_spitTunnelAcl permit ip 10.1.1.0 255.255.0.0 any *!--- Create a pool of addresses from which IP addresses are assigned !--- dynamically to the remote VPN Clients.* ip local pool vpnclient 192.168.1.1-192.168.1.5 *!--- This access list is used for a nat zero command that prevents !--- traffic which matches the access list from undergoing NAT. !--- No Nat for the **DMZ network.*** access-list nonat-dmz permit ip 10.1.1.0 255.255.255.0 192.168.1.0 255.255.255.0 *!--- No Nat for the **Inside network**.* access-list nonat-in permit ip 10.10.10.0 255.255.255.0 192.168.1.0 255.255.255.0 *!--- NAT 0 prevents NAT for networks specified in the **ACL nonat** .* nat (DMZ) 0 access-list nonat-dmz nat (inside) 0 access-list nonat-in

Configuração da versão ASA 8.3:

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 tiver sido estabelecido, vá para o **Cisco VPN Client** e selecione **Status > Route Details** para verificar se as rotas seguras são mostradas para as redes DMZ e INSIDE.

Refira ao PIX/ASA 7.x: Acesso do mail server no exemplo da configuração DMZ para obter mais informações sobre como estabelecer o PIX Firewall para o acesso a um mail servidor situado na rede da Zona Desmilitarizada (DMZ).

Refira ao PIX/ASA 7.x: Adicionar um túnel ou um acesso remoto novo a um L2L existente VPN a fim fornecer as etapas exigidas adicionar um túnel novo VPN ou um acesso remoto VPN a uma configuração de VPN L2L que já exista.

Refira ao PIX/ASA 7.x: Permita que o split tunneling para clientes VPN no exemplo de configuração ASA a fim fornecer instruções passo a passo em como permitir a clientes VPN o acesso ao Internet quando forem em túnel em uma ferramenta de segurança adaptável da ferramenta de segurança da Cisco (ASA) 5500 Series.

Consulte Exemplo de Configuração do PIX/ASA 7.x e do Cisco VPN Client 4.x com Autenticação IAS RADIUS (contra Active Directory) do Windows 2003 para obter mais informações de como estabelecer a conexão de VPN de acesso remoto entre um Cisco VPN Client (4.x para Windows) e o PIX 500 Series Security Appliance 7.x.

Os Clientes VPN Não Conseguem Resolver DNS

Após o túnel ser estabelecido, se os clientes VPN não conseguirem resolver o DNS, o problema pode estar na configuração do servidor DNS no dispositivo headend (ASA/PIX). Verifique também a conectividade entre os clientes VPN e o servidor DNS. A configuração do servidor DNS deve ser configurada sob a política do grupo e ser aplicada sob o a política do grupo nos atributos gerais do túnel-grupo; por exemplo:

```
!--- Create the group policy named vpn3000 and !--- specify the DNS server IP
address(172.16.1.1) !--- and the domain name(cisco.com) in the group policy. 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 !--- using 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

A separação de túneis permite que os clientes IPsec de acesso remoto direcionem condicionalmente pacotes para o túnel IPsec na forma criptografada ou enviem pacotes diretamente para uma interface de rede na forma de texto não criptografado, onde eles são roteados para um destino final. A separação de túneis é desabilitada por padrão, o que representa o tráfego tunnelall.

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

Nota: A opção *excludespecified* é apoiada somente para clientes VPN da Cisco, não clientes EZVPN.

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

Consulte estes documentos para obter exemplos de configuração detalhados da separação de

túneis:

- PIX/ASA 7.x: **Exemplo de Configuração de Habilitação do Tunelamento Dividido for 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
- Exemplo de Configuração da Separação de Túneis para Clientes VPN no VPN 3000 Concentrator

Hairpinning

Esta característica é útil para o tráfego VPN que incorpora uma relação mas é então roteado fora dessa mesma relação. Por exemplo, se você tem uma rede VPN do hub and spoke, onde a ferramenta de segurança seja o cubo e as redes VPN remotas sejam spokes, para que um spoke se comunique com um outro spoke, o tráfego deve sair na ferramenta de segurança e então outra vez ao outro spoke.

Use a configuração do **same-security-traffic** para permitir que o tráfego incorpore e retire a mesma relação.

```
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 mais exemplos de configuração detalhada, refira ao PIX/ASA 7.x: Permita o acesso do LAN local para clientes VPN.

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

Certifique-se sempre de que os endereços IP do pool que será atribuído aos clientes VPN, a rede interna do dispositivo headend e a rede interna do cliente VPN pertençam a redes diferentes. É possível atribuir a mesma rede principal com sub-redes diferentes, mas algumas vezes pode haver problemas de roteamento.

Para mais exemplos, veja o *Diagrama* e o *Exemplo* do Incapaz de Acessar os Servidores DMZ seção DMZ.

Incapaz de conectar mais de três usuários do cliente VPN

Problema

Somente três clientes VPN podem conectar ao ASA/PIX; a conexão para o quarto cliente irá falhar. 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
- Configuração do ASA/PIX com a CLI
- Configurar o concentrador Configura o Concentrador

Para obter mais informações, consulte a seção Configuração de Políticas de Grupo de Procedimentos de Configuração de VPN no ASDM Selecionados para a Cisco ASA 5500 Series Versão 5.2.

Configuração de Logins Simultâneos

Se a caixa de verificação **herdada no** ASDM é verificada, apenas o número padrão de inícios de uma sessão simultâneos está permitido o usuário. O valor padrão para os logins simultâneos é três.

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

1. Inicie o ASDM e navegue para **Configuration > VPN > Group Policy**.
2. Selecione o valor de **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.**Nota:** O valor mínimo para este campo é 0, o qual desabilita o login e impede o acesso de usuários.**Nota:** Quando você entra usando a mesma conta de usuário de um PC diferente, a sessão atual (a conexão estabelecida de um outro PC usando a mesma conta de usuário) está terminada, e a nova sessão está estabelecida. Este é o comportamento padrão e é independente aos inícios de uma logins de VPN simultâneos.

Configuração do ASA/PIX com a CLI

Conclua estes passos para configurar o número desejado de logins simultâneos. Neste exemplo, 20 foi escolhido como o valor desejado.

```
ciscoasa(config)#group-policy Bryan attributes ciscoasa(config-group-policy)#vpn-simultaneous-
logins 20
```

Para aprender mais sobre este comando, consulte a Referência de Comandos do Cisco Security Appliance Versão 7.2.

Use o comando **vpn-sessiondb max-session-limit** no modo de configuração global para limitar as sessões de VPN a um valor menor do que o permitido pelo Security Appliance. Use a versão no deste comando para remover o limite de sessões. 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:

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

Configuração do Concentrador

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 o **Configuration > User Management > Groups > Modify 10.19.187.229 > General > Simultaneous Logins**, e mude 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 aplicativos pode ser alcançado de sua rede. A causa pode ser um problema com o tamanho máximo do segmento (MSS) para os pacotes transientes que atravessam um roteador ou dispositivo PIX/ASA, especialmente segmentos de TCP com o bit SYN definido.

Cisco IOS Router - Mude o valor MSS na interface externa (relação da extremidade do túnel) de Roteador

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

```
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:

```
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 mais informação, refira ao PIX/ASA 7.x e IOS: Fragmentação VPN.

PIX/ASA 7.X - Refira à documentação PIX/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. Refira a estes originais a fim resolver a edição:

- PIX/ASA 7.x e IO: Fragmentação VPN
- Problema PIX/ASA 7.0: MSS Excedido - Os Clientes HTTP não Podem Consultar Alguns Web Sites

Incapaz de iniciar o túnel VPN de ASA/PIX

Problema

Você não consegue iniciar o túnel VPN da interface do ASA/PIX e, após o túnel ser estabelecido, o ponto remoto/cliente VPN não é capaz de enviar um ping para a interface interna do ASA/PIX no túnel VPN. Por exemplo, o cliente VPN não é capaz de iniciar uma conexão de SSH ou HTTP para a interface interna do ASA via túnel VPN.

Solução

A interface interna do PIX não poderá responder a pings enviados pela outra extremidade do túnel a menos que o comando **management-access** seja configurado no modo de configuração global.

```
PIX-02(config)#management-access inside PIX-02(config)#show management-access management-access
inside
```

Nota: Este comando também ajuda a iniciar um ssh ou a conexão HTTP à interface interna do ASA através de um túnel VPN.

Nota: Esta informação também é verdadeira para a relação DMZ. Por exemplo, se você quer ping a interface DMZ do PIX/ASA ou a querer iniciar um túnel da interface DMZ, então o **gerenciamneot de acesso DMZ** é exigido.

```
PIX-02(config)#management-access DMZ
```

Nota: Se o cliente VPN é incapaz de conectar, certifique-se que portas ESP e UDP estão abertas, contudo se aquelas portas não estão abertas então tente conectar em TCP 10000 com a seleção desta porta sob a entrada da conexão de cliente de VPN. O Clique com o botão direito **modify > transport tab > IPsec over TCP**. Refira ao PIX/ASA 7.x para dar suporte ao IPsec sobre o TCP em qualquer Exemplo da Configuração de Porta para mais informações a respeito do IPsec sobre TCP.

Incapaz de Passar o Tráfego Através do Túnel VPN

Problema

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

Solução

Esta edição ocorre devido ao problema descrito na identificação de bug Cisco CSCtb53186 (somente clientes registrados). A fim resolver esta edição, recarregue o ASA. Refira o erro para mais informação.

Este problema também pode ocorrer quando os pacotes ESP são bloqueados. A fim resolver esta edição, reconfigurando o túnel VPN.

Esta edição pôde ocorrer quando os dados não são criptografados, mas somente descriptografados pelo túnel VPN segundo as indicações desta saída:

```
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
```

A fim de resolver esta edição, verifique o seguinte:

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 está correto e o tráfego condiz com a interface externa passando completamente para dentro. As saídas de exemplo mostram que a descriptografia está completa, mas a criptografia não ocorre.
3. Se o comando da licença conexão-VPN do sysopt foi configurado no ASA. Se não configurado, configurar este comando porque permite que o ASA isente o tráfego encrypted/VPN da verificação da relação ACL.

Configurando o peer de backup para o túnel vpn no mesmo mapa de criptografia

Problema

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

Solução

Configurar múltiplos peers é equivalente a fornecer uma lista de reserva. 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 deve ter um mapa de criptografia já configurado como o peer principal. 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:

```
ASA(config)#crypto map mymap 10 set peer X.X.X.X Y.Y.Y.Y
```

Para mais informação, refira ao Mapa de criptografia da seção de peer na *Comando de Referência do Cisco Security Appliance, versão 8.0*.

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 command**no modo de configuração global para remover um mapa de criptografia previamente ajustado a uma interface. Não use a forma**no** deste comando a fim remover o mapa de criptografia definido na interface.

```
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.

```
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. Este é um problema conhecido e o Bug ID CSCtb53186 (somente clientes registrados) foi arquivado para endereçar este problema. A fim resolver este problema, recarregue o ASA ou atualize o software para uma versão em que este erro é fixado.

Erro: -- %ASA-5-713904: O grupo = DefaultRAGroup, IP= x.x.x.x, cliente estão usando uma versão não suportada no modo de transação v2. Túnel terminado.

Problema

O %ASA-5-713904: `Group = DefaultRAGroup, IP= 99.246.144.186, o cliente está usando uma versão não suportada do do Modo de Transação v2.` O mensagem de erro Túnel terminado aparece.

Solução

O motivo para o Mensagem de Erro Modo de Transação V2 é que o ASA suporta somente o Modo de Configuração IKE V6 e não 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 que transmitem o pacotes maiores 1220 (ponto inicial 1206)

Problema

O %ASA-6-722036: Group < client-group > User < xxxx > IP < x.x.x.x> Transmite pacotes maiores 1220 (ponto inicial 1206) mensagens de erro aparece 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 ação alternativa é desligar a compressão SVC com o comando de não compressão svc, o que resolve o problema.

Erro: O comando none do grupo de autenticação do servidor foi depreciado

Problema

Se você transferir a configuração de VPN do PIX/ASA versão 7.0.x para o outro Security Appliance versão 7.2.x, a seguinte mensagem de erro será recebida:

```
ERROR: The authentication-server-group none command has been deprecated.
The "isakmp ikev1-user-authentication none" command in the ipsec-attributes should be used
instead.
```

Solução

Não há mais suporte ao comando **authentication-server-group** na versão 7.2(1) ou posterior. Este comando foi substituído e movido para o modo de configuração de atributos gerais do grupo do

túnel.

Consulte a seção isakmp ikev1-user-authentication da referência de comandos para obter mais informações sobre esse comando.

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

Problema

Se você habilitou o QoS em uma extremidade do Túnel VPN, você poderá 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 checking
```

Solução

Normalmente, essa mensagem é causada quando uma extremidade do túnel está executando QoS. Isso acontece quando um pacote é detectado 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: a entrada do mapa de criptografia estará incompleta

Problema

Quando você executa o comando do IPSEC-**ISAKMP do mymap 20 do mapa de criptografia**, você poderá receber este erro:

```
AVISO: a entrada do mapa de criptografia estará incompleta
```

Por exemplo:

```
ciscoasa(config)#crypto map mymap 20 ipsec-isakmp WARNING: crypto map entry will be incomplete
```

Solução

Este é um aviso normal quando um novo mapa de criptografia é definido, um lembrete que parâmetros como access-list (endereço correspondente), transform set e peer address devem ser configurados para que ele possa funcionar. Também é normal que a primeira linha digitada para definir o mapa de criptografia não seja mostrada na configuração.

Erro: -- %ASA-4-400024: Grande pacote ICMP IDS:2151 na interface externa

Problema

Incapaz de passar o grande pacote de ping através do túnel vpn. Quando nós tentamos passar

grandes pacotes de ping nós obtemos o erro %ASA-4-400024: `Grande pacote ICMP IDS:2151 na interface externa`

Solução

Desabilite as assinaturas 2150 e 2151 a fim resolver este problema. Uma vez que as assinaturas são desabilitadas o ping funciona muito bem.

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: - %PIX|ASA-4-402119: IPSEC: Recebeu um pacote de protocolo (SPI=spi, número de sequência = seq_num) do remote_IP (username) ao local_IP que falhou a verificação da anti-repetição.

Problema

Eu recebi este erro nos mensagens de registro do ASA:

```
Erro: - %PIX|ASA-4-402119: IPSEC: Recebeu um pacote de protocolo (SPI=spi, número de sequência =
seq_num) do remote_IP (username) ao local_IP que falhou a verificação da anti-repetição.
```

Solução

A fim resolver este erro, use o comando crypto ipsec security-association replay windows size para variar o tamanho da janela.

```
hostname(config)#crypto ipsec security-association replay window-size 1024
```

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

Mensagem de Erro - %PIX|ASA-4-407001: Negue o tráfego para o local-host interface_name: inside_address, limite de número de licenças excedido

Problema

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

```
Mensagem de Erro - %PIX|ASA-4-407001: Negue o tráfego para o local-host interface_name:
inside_address, limite de número de licenças excedido
```

Solução

Este mensagem de erro é recebida quando o número de usuários excede o limite de licenças utilizadas. Este erro pode ser resolvido fazendo um upgrade aumentando o número 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 - %VPN_HW-4-PACKET_ERROR: A Mensagem de Erro indica que o pacote ESP com o HMAC recebido pelo roteador está mal combinado. Este erro pôde 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: Comando rejeitado: apague primeiro a conexão criptografada entre VLAN XXXX e XXXX.

Problema

Este Mensagem de Erro aparece quando você tenta adicionar um VLAN permitida na porta tronco de um interruptor: `Comando rejeitado:` conexão criptografada da supressão entre VLAN XXX e VLAN XXXX, primeiramente.

A borda do tronco WAN não pode ser alterado para permitir VLAN adicionais. Isto é, você é incapaz de adicionar VLANs no tronco dos **IPSEC VPN SPA**.

Este comando é rejeitado porque permiti-lo conduzirá a uma interface criptografada conectada VLAN que pertence à lista de VLAN habilitada da relação, que levanta uma ruptura potencial da segurança IPSec. Note que este comportamento se aplica a todas as portas de tronco.

Solução

Em vez do comando nenhum interruptor vlan (vlanlist) permitido no tronco , use o comandointerruptor vlan none permitido no tronco ou o comando interruptor remover vlan (vlanlist) no tronco.

Mensagem de Erro - % FW-3-RESPONDER_WND_SCALE_INI_NO_SCALE: Pacote deixando cair - Opção inválida da escala do indicador para a sessão

x.x.x.x:27331 a 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: Pacote deixando cair - Opção
inválida da escala do indicador para a sessão x.x.x.x:27331 a 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 escamação do indicador foi adicionada para permitir a transmissão rápida dos dados nas longas redes fat (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 habilitar a escamação da janela para dar suporte a LFNs, o tamanho da janela TCP deve ser superior a 65.535. Esta Mensagem de Erro pode ser resolvida aumentando o tamanho da janela TCP para além de 65.535.

%ASA-5-305013: Regras assimétricas NAT se combinam para avante e para trás. Favor Atualizar o fluxo deste problema

Problema

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

```
%ASA-5-305013: Regras assimétricas NAT se combinam para avante e para trás. Favor Atualizar o
fluxo deste problema
```

Solução

A fim de resolver este problema quando não na mesma relação que o host usando NAT, use o endereço mapeado ao vez do endereço real para se conectar ao host. Além disso, permita o **comando inspect** se a aplicação encaixa o endereço IP.

%PIX|ASA-5-713068: Mensagem de notificação recebida fora da rotina: notify_type

Problema

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

```
%PIX|ASA-5-713068: Mensagem de notificação recebida fora da rotina: 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-Secundário) Falha na atualização do tempo de execução do IPSec na unidade em espera (ou) %ASA-6-720012: ((VPN-unidade) Falha na atualização do tempo de execução de dados na unidade em espera

Problema

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

```
%ASA-5-720012: (VPN-Secundário) Falha na atualização do tempo de execução do failover do IPSec
na unidade em espera.

%ASA-6-720012: (VPN-unidade) Falha na atualização do tempo de execução do failover do IPsec na
unidade em espera.
```

Solução

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

Estas mensagens aparecem quando o subsistema do failover VPN não pode atualizar os dados do tempo de execução do IPSEC relacionados ao túnel de IPsec correspondente que foi apagado da unidade em pespera. A fim resolver estes, emita o **comando wr standby** na unidade ativa.

Dois erros foram arquivados para endereçar este comportamento e atualizar a versão de software do ASA onde estes erros são fixos. Refira ao Cisco bug IDs CSCtj58420 (somente clientes registrados) e CSCtn56517 (somente clientes registrados) para mais informação.

Erro: -- %ASA-3-713063: Endereço de peer IKE não configurado para o destino 0.0.0.0

Problema

O %ASA-3-713063: Endereço de peer IKE não configurado para o destino 0.0.0.0 a mensagem de erro surge e o túnel não surge .

Solução

Esta mensagem aparece quando o endereço de peer IKE não está configurado para um túnel L2L. Este erro pode ser resolvido mudando o número de seqüência do mapa de criptografia, então removendo e reaplicando o mapa de criptografia.

Erro: %ASA-3-752006: O gerente do túnel não despachou uma mensagem KEY_ACQUIRE.

Problema

`O %ASA-3-752006: Escave um túnel o gerente não são despachados uma mensagem KEY_ACQUIRE. Configuração incorreta provável do crypto map ou do grupo de túneis.”` o Mensagem de Erro é entrado Cisco ASA.

Solução

Este Mensagem de Erro pode ser causado por um misconfiguration do crypto map ou do grupo de túneis. Assegure-se de que ambos estejam configurados corretamente. Para obter mais informações sobre deste Mensagem de Erro, refira o erro 752006.

Estão aqui algumas das ações corretiva:

- Remova o ACL cripto (por exemplo, associado ao mapa dinâmico).
- Remova a configuração relacionada IKEv2 não utilizada, se existerem.
- Verifique que o ACL cripto combinou corretamente.
- Remova as entradas de lista de acesso duplicadas, se exister.

Erro: %ASA-4-402116: IPSEC: Recebeu um pacote ESP (SPI= 0x99554D4E, number= 0x9E da sequência) de XX.XX.XX.XX (user= XX.XX.XX.XX) a YY.YY.YY.YY

Em uma instalação do Túnel VPN de Lan para Lan, este erro é recebido em uma extremidade ASA:

```
O pacote interno do descapsulado não combina a política negociada no SA.

O pacote especifica seu destino como 10.32.77.67, sua fonte como 10.105.30.1, e seu protocolo como o ICMP.

O SA especifica seu proxy local como 10.32.77.67/255.255.255.255/ip/0 e seu remote_proxy como 10.105.42.192/255.255.255.224/ip/0.
```

Solução

Você precisa de verificar as listas de acesso do tráfego interessante definidas no ambas as extremidades do túnel VPN. Ambos devem combinar como imagens espelhadas exatas.

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

Problema

A Falha para lançar o 64-bit VA installer para habilitar o adaptador vitrual devido ao erro erro 0xffffffff mensagem de registro recebida quando o Any Connect falha para se conectar.

Solução

Siga estes passos para resolver esse problema:

1. Vá a **System > Internet Communication management > Internet Communication settings** e certifique-se que **Turn Off Automatic Root Certificates Update** esteja desabilitado.
2. Se desabilitado, a seguir desabilite o **Administrative Template** do GPO atribuído à máquina e teste outra vez.

Consulte Turn off Automatic Root Certificates Update para mais informação.

Erro 5: Nenhum hostname existe para esta entrada de conexão. Incapaz de fazer a conexão de VPN.

Problema

O erro 5: `Nenhum hostname existe para esta entrada de conexão.` A mensagem de erro Incapaz de fazer a conexão VPN é recebida durante uma nova instalação PC.

Solução

Este problema é devido à identificação de erro Cisco CSCso94244 (somente clientes registrados). Consulte este bug 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.

Mensagem de advertência: "A “funcionalidade de VPN pode não funcionar”

Problema

Ao tentar permitir o isakmp na interface externa do ASA, este mensagem de advertência é 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. Certifique-se que você não tem o **comando logging queue 0**. Este configura o tamanho da fila para 8192 e a aumenta a alocação de memória.

Nas plataformas tais como ASA5505 e ASA5510, esta alocação de memória tende a deixar os outros módulos sem memória (IKE e etc.). A identificação de erro Cisco CSCtb58989 (somente clientes registrados) foi registrada para endereçar um tipo de comportamento similar. A fim resolver isto, configurar a fila de registo em um valor inferior, tal como 512.

Erro do estofamento do IPsec

Problema

Este Mensagem de Erro é recebido:

```
%PIX|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

A edição ocorre porque o IPSec VPN negocia sem um algoritmo de hashing. O hashing do pacote assegura a verificação de integridade para o canal ESP. Consequentemente, sem picar, os pacotes malformado são indetectados aceitado por Cisco ASA e tenta decifrar estes pacotes. Contudo, porque estes pacotes são deformados, o ASA encontra falhas ao decifrar o pacote. Isto causa os Mensagens de Erro do estofamento que são considerados.

A recomendação é incluir um algoritmo de hash no grupo da transformação para o VPN e assegurar-se de que o link entre os pares tenha a malformação mínima do pacote.

Tempo de retardo da interrupção em telefones do local remoto

Problema

O tempo de retardo da interrupção é experimentado em telefones do local remoto. Como isto é resolvido?

Solução

Desabilite inspeção magro e do sorvo a fim resolver este problema:

```
asa(config)# no inspect sip asa(config)# no inspect skinny
```

O túnel VPN obtém desligado após cada 18 horas

Problema

O túnel VPN obtém desligado após cada 18 horas mesmo que a vida seja ajustada por 24 horas.

Solução

A vida é o tempo máximo onde o SA pode ser usado rekeying. O valor que você incorpora à configuração porque a vida é diferente da época do rekey do SA. Consequentemente, é necessário negociar um par novo SA (ou SA no caso do IPsec) antes que atual expire. O tempo do rekey deve sempre ser menor do que a vida a fim permitir tentativas múltiplas caso que as primeiras rekey a tentativa falha. Os RFC não especificam como calcular o tempo do rekey. Isto é deixado à discreção dos aplicadores. Consequentemente, o tempo variará segundo a plataforma usada, que versão de software, etc.

Algumas aplicações podem usar um fator aleatório para calcular o temporizador do rekey. Por exemplo, se o ASA inicia o túnel, a seguir é normal que rekey em 64800 segundos = 75% de 86400. Se os novatos do roteador, então o ASA podem esperar mais por muito tempo para dar ao par mais hora de iniciar o rekey. Assim, é normal que a sessão de VPN obtém desligou cada 18 horas para usar uma outra chave para a negociação VPN. Isto não deve causar nenhuma gota ou problema VPN.

O fluxo de tráfego não é mantido depois que o LAN ao túnel LAN é renegociado

Problema

O fluxo de tráfego não é mantido depois que o LAN ao túnel LAN é renegociado.

Solução

O ASA monitora cada conexão que as passagens com ele e mantêm uma entrada em sua tabela de estado de acordo com a característica da inspeção de aplicativo. Os detalhes do tráfego criptografado que passam com o VPN são mantidos sob a forma de um base de dados da associação de segurança (SA). Para o LAN às conexões de VPN LAN, mantém dois fluxos de tráfego diferentes. Um é o tráfego criptografado entre os gateways de VPN. O outro é o fluxo de tráfego entre os recursos de rede atrás do gateway de VPN e o utilizador final atrás da outra extremidade. Quando o VPN é terminado, os detalhes do fluxo para este SA particular estão suprimidos. Contudo, a entrada de tabela do estado mantida pelo ASA para esta conexão de TCP torna-se velha devido a nenhuma atividade, que impede da transferência. Isto significa que o ASA ainda reterá a conexão de TCP para esse fluxo particular quando o aplicativo de usuário terminar. Contudo, as conexões de TCP transformar-se-ão estática e eventualmente intervalo depois que o temporizador de ociosidade TCP expira.

Este problema foi resolvido introduzindo uma característica chamada fluxos escavados um túnel IPsec de Persistente. Um comando new, conserva-VPN-fluxos da conexão do sysopt, foi integrado em Cisco ASA a fim reter a informação da tabela de estado na negociação nova do túnel VPN. À revelia, este comando é desabilitado. Permitindo isto, Cisco ASA manterá a

informação da tabela de estado TCP quando o L2L VPN recupera do rompimento e restabelece o túnel.

O Mensagem de Erro indica que a largura de banda alcançou para a funcionalidade cripto

Problema

Este Mensagem de Erro é recebido no 2900 Series Router:

```
Erro: 20 de março 10:51:29: %CERM-4-TX_BW_LIMIT: Limite máximo da largura de banda de Tx de
85000 kbps alcançados para a funcionalidade cripto com a licença do pacote da tecnologia
securityk9.
```

Solução

Este é um problema conhecido que ocorra devido às diretrizes restritas emitidas pelo governo dos estados unidos. De acordo com isto, a licença securityk9 pode somente permitir uma criptografia de payload até taxas perto de 90Mbps e limitar o número de sessões cifradas tunnels/TLS ao dispositivo. Para obter mais informações sobre das restrições de exportação criptos, refira Cisco ISR G2 SEC e licenciar HSEC.

Em caso dos dispositivos Cisco, é derivado para ser menos do que o tráfego unidirecional 85Mbps ou fora do roteador ISR G2, com um total bidirecional de 170 Mbps. Esta exigência aplica-se para Plataformas ISR G2 de Cisco 1900, 2900, e as 3900. Este comando ajuda-o em ver estas limitações:

```
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----
```

Há um erro arquivado para endereçar este comportamento. Refira a identificação de bug Cisco CSCtu24534 (clientes registrados somente) para mais informação.

A fim evitar este problema, você precisa de comprar uma licença HSECK9. Uma licença de recurso de "hseck9" fornece a funcionalidade aumentada da criptografia de payload as contagens aumentadas do túnel VPN e fixa sessões da Voz. Para obter mais informações sobre do roteador de Cisco ISR que licencia, refira a ativação de software.

Problema: O tráfego de partida da criptografia em um túnel de IPsec pode falhar, mesmo se o tráfego de entrada da descriptografia está trabalhando.

Solução

Esta edição esteve observada em uma conexão IPSec depois que o múltiplo rekeys, mas a condição do disparador não é clara. A presença desta edição pode ser estabelecida verificando a saída do comando da **gota asp da mostra** e verificando que o contador expirado do contexto VPN aumenta para cada pacote externo enviado. Refira a identificação de bug Cisco CSCtd36473

(clientes registrados somente) para mais informação.

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 aparece na saída do **comando show crypto isakmp sa** e também no **resultado do debug**. O motivo pode ser devido à má combinação das políticas isakmp ou se a porta udp 500 for bloqueada 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

- Problema PIX/ASA 7.0: MSS Excedido - Os Clientes HTTP não Podem Consultar Alguns Web Sites
- PIX/ASA 7.x e IO: Fragmentação VPN
- Ferramentas de segurança do Cisco ASA 5500 Series
- Cisco PIX 500 Series Security Appliances
- Negociação IPsec/Protocolos IKE
- Cisco VPN 3000 Series Concentrators
- Suporte Técnico e Documentação - Cisco Systems