GETVPN pesquisam defeitos o guia

Índice

Introdução

Este documento é pretendido apresentar uma metodologia de Troubleshooting estruturada e ferramentas úteis para ajudar a identificar e isolar problemas cifrados grupo do transporte VPN (GETVPN) e a fornecer soluções possíveis.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- GETVPN
  Manual de configuração oficial GETVPN
  Guia de implementação e projeto oficial GETVPN

- Uso do servidor de SYSLOG

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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.

Metodologia de Troubleshooting GETVPN

Como com a maioria de Troubleshooting de problemas da tecnologia complexa, a chave é poder isolar o problema a uma característica, a um subsistema, ou a um componente específico. A solução GETVPN é compreendida de um número de componentes da característica, especificamente:

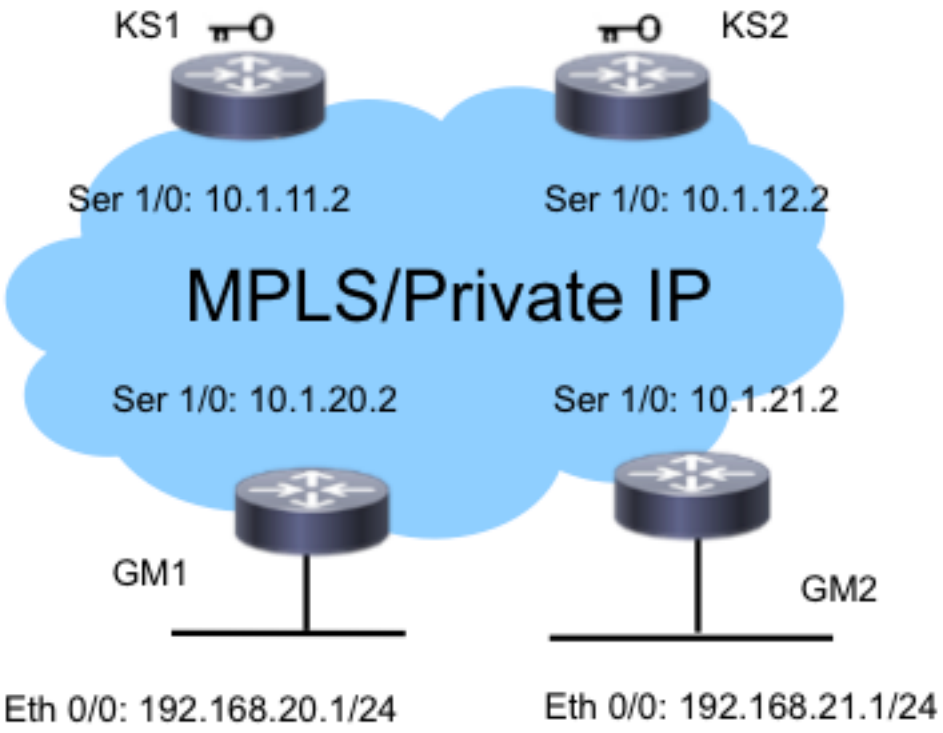
- Internet Key Exchange (IKE) - Usado entre o membro do grupo (GM) e o server chave (KS), e entre o protocolo cooperativo (CAPOEIRA) KSs a fim autenticar e proteger o plano do controle.
- Agrupe o domínio da interpretação (GDOI) - protocolo usado para o KS a fim distribuir chaves do grupo e para proporcionar o serviço chave como rekey a todo o GMs.
- CAPOEIRA - Protocolo usado para o KSs a fim comunicar-se um com o otro e fornecer a Redundância.
- Preservação do encabeçamento - IPsec no modo de túnel que preserva o encabeçamento de pacote de dados originais para a entrega do tráfego de ponta a ponta.

- O tempo baseou a Anti-repetição (TBAR) - Mecanismo de detecção da repetição usado em um ambiente da chave do grupo.

Igualmente fornece um grupo extensivo de ferramentas de Troubleshooting a fim facilitar o processo da pesquisa de defeitos. É importante compreender quais destas ferramentas estão disponíveis, e quando são apropriados para cada tarefas de Troubleshooting. Ao pesquisar defeitos, é sempre uma boa ideia começar com menos métodos intrusivos de modo que o ambiente de produção não seja impactado negativamente. A chave a esta Troubleshooting estruturado é poder quebrar para baixo o problema a um controle ou à edição plana dos dados. Você pode fazer este se você segue o protocolo ou o fluxo de dados e usa as várias ferramentas apresentadas aqui ponto de verificação as.

Topologia da referência

Esta topologia e o método de endereçamento GETVPN são usados durante todo o resto deste documento de Troubleshooting.



Configurações de referência

- KS1

```
crypto gdoi group G1
identity number 3333
server local
rekey authenmypubkeyrsa get
rekey transport unicast
sa ipsec 1
profile gdoi-p
match address ipv4ENCPOL
address ipv4 10.1.11.2
redundancy
local priority 10
```

```
peer address ipv4 10.1.12.2
```

- **GM1**

```
crypto gdoi group G1
identity number 3333
server address ipv4 10.1.11.2
server address ipv4 10.1.12.2
!
crypto map gm_map 10 gdoi
set group G1
!
interface Serial1/0
crypto map gm_map
```

Note: As configurações KS2 e GM2 não são incluídas aqui para a brevidade.

Terminologia

- **KS** - Server chave
- **GM** - Membro do grupo
- **CAPOEIRA** - Protocolo cooperativo
- **TBAR** - O tempo baseou a Anti-repetição
- **KEK** - Chave de criptografia chave
- **TEK** - Chave de criptografia de tráfego

Preparação da facilidade de registro e outros melhores prática

Antes que você comece a pesquisar defeitos, assegure-se de que você prepare a facilidade de registro como descrita aqui. Alguns melhores prática são alistados igualmente aqui:

- Verifique a quantidade de memória livre do roteador, e configurar o **logging buffered debugging a um** grande valor (10 MB ou mais se possível).

- Desabilite o registro ao console, ao monitor, e aos servidores de SYSLOG.

- Recupere o índice do logging buffer com o **comando show log** em intervalos regulares, cada 20 minutos a uma hora, a fim impedir a perda do log devendo proteger a reutilização.

- O que quer que acontece, inscreva o **comando show tech de** GMs e de KSs afetados, e examine a saída do **comando show ip route em** global e cada roteamento virtual e transmissão (VRF) envolveram, se alguns são exigidos.

- Use a sincronização do Network Time Protocol (NTP) o pulso de disparo entre todos os dispositivos que são debugados. Permita timestamps do milissegundo (milissegundo) para ambos debugam e mensagens de registro:

```
service timestamps debug datetime msec
service timestamps log datetime msec
```

- Certifique-se que os show command outputs (resultado do comando show) são timestamped.

```
Router#terminal exec prompt timestamp
```

- Quando você recolhe os show command outputs (resultado do comando show) para o controle aplanam eventos ou os contadores planos dos dados, recolhem sempre interações múltiplas da mesma saída.

Pesquise defeitos edições do plano do controle GETVPN

Controle o plano significa todos os eventos do protocolo que conduziram à política e à criação da associação de segurança (SA) no GM de modo que estivessem prontos para cifrar e decifrar o tráfego plano dos dados. Alguns dos pontos de verificação chaves no plano do controle GETVPN são:

Controle melhores prática planos da eliminação de erros

Estes melhores prática do Troubleshooting não são específico GETVPN; aplicam-se a quase toda a eliminação de erros do plano do controle. É crítico seguir estes melhores prática a fim assegurar a maioria de Troubleshooting efetivo:

- Desligue o logging de console e use o logging buffer ou o Syslog a fim recolher debuga.
- Use relógios do roteador da sincronização NTP em todos os dispositivos que são debugados.
- Permita o milissegundo que timestamping para debugam e mensagens de registro:

```
service timestamp debug datetime msec
service timestamp log datetime msec
```

- Certifique-se que os show command outputs (resultado do comando show) são timestamped de modo que possam ser correlacionados com o resultado do debug:

```
terminal exec prompt timestamp
```

- Use o debugging condicional em um ambiente da escala se possível.

Ferramentas de Troubleshooting do plano do controle GETVPN

Comandos show GETVPN

Em regra geral, estes são o comando outputs o devem recolher para quase todos os problemas GETVPN.

KS

```
show crypto gdoi
show crypto gdoi ks coop
show crypto gdoi ks members
show crypto gdoi ks rekey
show crypto gdoi ks policy
```

GM

```
show crypto eli
show crypto gdoi rekey sa
show crypto gdoi
show crypto gdoi gm
show crypto gdoi gm rekey
```

Mensagens do syslog GETVPN

GETVPN fornece um grupo extensivo de mensagens do syslog para eventos e condições de erro significativos do protocolo. O Syslog deve sempre ser o primeiro lugar a olhar quando você executa o Troubleshooting GETVPN.

Mensagens do syslog comuns KS

Mensagens de syslog	Explicação
COOP_CONFIG_MISMATCH	A configuração entre o server do chave principal e o server da chave secundária é combinada mal.
COOP_KS_ELECTION	O server chave local incorporou o processo de eleição a um grupo.
COOP_KS_REACH	A alcançabilidade entre os server chaves cooperativos configurados é restaurada.
COOP_KS_TRANS_TO_PRI	O concluiu a transição chave local do server a um papel principal de ser u servidor secundário em um grupo.
COOP_KS_UNAUTH	Um servidor remoto autorizado tentou contactar o server chave local em u grupo, que poderia ser considerado um evento hostil.
COOP_KS_UNREACH	A alcançabilidade entre os server chaves cooperativos configurados é per que poderiam ser considerados um evento hostil.
KS_GM_REVOKED	Durante rekey o protocolo, um membro desautorizado tentado juntar-se a grupo, que poderia ser considerado um evento hostil.
KS_SEND_MCAST_REKEY	Enviando o Multicast rekey.
KS_SEND_UNICAST_REKEY	Enviando o unicast rekey.
KS_UNAUTHORIZED	Durante o protocolo de registro GDOI, um membro desautorizado tentou ju se a um grupo, que poderia ser considerado um evento hostil.
UNAUTHORIZED_IPADDR	A requisição de registro foi deixada cair porque o dispositivo de pedido nã autorizado para se juntar ao grupo.

Mensagens do syslog comuns GM

Mensagens de syslog	Explicação
GM_CLEAR_REGISTER	O comando **cripto claro do gdoi** foi executado pelo membro do grupo loc
GM_CM_ATTACH	Um crypto map foi anexado para o membro do grupo local.
GM_CM_DETACH	Um crypto map foi destacado para o grupo local member.&
GM_RE_REGISTER	IPsec SA criado para um grupo pôde ter sido expirado ou cancelado. Necessidade de registrar-se novamente ao server chave.
GM_RECV_REKEY	Rekey recebeu.
GM_REGS_COMPL	Registro completo.
GM_REKEY_TRANS_2_MULTI	O membro do grupo tem o concluiu a transição de usar um unicast para rekey o mecanismo a usar um mecanismo do Multicast.
GM_REKEY_TRANS_2_UNI	O membro do grupo tem o concluiu a transição de usar um Multicast pa rekey o mecanismo a usar um mecanismo do unicast.
PSEUDO_TIME_LARGE	Um membro do grupo recebeu um pseudotime com um valor que fosse maior parte diferente de seu próprio pseudotime.

REPLAY_FAILED	Um membro do grupo ou um server da chave falharam uma verificação anti-repetição.

Note: As mensagens destacadas no vermelho são as mensagens as mais comuns ou as mais significativas consideradas em um ambiente GETVPN.

Cripto e GDOI globais debugam

GETVPN debuga é dividido:

1. Primeiramente pelo dispositivo em que você está pesquisando defeitos.
```
F340.06.15-2900-18#debug cry gdoi ?
 all-features  All features in GDOI
 condition     GDOI Conditional Debugging
 gm            Group Member
 ks            Key Server
```
2. Em segundo pelo tipo de problema você está pesquisando defeitos.
```
GM1#debug cry gdoi gm ?
 all-features    All Group Member features
 infrastructure  GM Infrastructure
 registration    GM messages related to registration
 rekey           GM messagese related to Re-Key
 replay          Anti Replay
```
3. Terço pelo nível da eliminação de erros que precisa de ser permitida. Na versão 15.1(3)T e mais recente, toda a característica GDOI debuga foi estandardizada para ter estes níveis de debug. Isto foi projetado a fim ajudar a pesquisar defeitos ambientes em grande escala GETVPN com bastante granularidade da eliminação de erros. Quando você debuga problemas GETVPN, é importante usar o nível de debug apropriado. Em regra geral, o começo com o mais baixo nível de debug, isso é o nível de erro, e aumenta a granularidade da eliminação de erros quando necessário.
```
GM1#debug cry gdoi gm all-features ?
 all-levels  All levels
 detail      Detail level
 error       Error level
 event       Event level
 packet      Packet level
 terse       Terse level
```

Debugging condicional GDOI

Na versão 15.1(3)T e mais recente do ® do Cisco IOS, o debugging condicional GDOI foi adicionado a fim ajudar a pesquisar defeitos GETVPN em um ambiente em grande escala. Tão todo o Internet Security Association and Key Management Protocol (ISAKMP) e GDOI debugam podem agora ser provocados com um filtro condicional baseado no grupo ou no endereço IP do peer. Para a maioria de problemas GETVPN, é bom permitir o ISAKMP e o GDOI debuga com o filtro condicional apropriado, desde que GDOI debuga somente operações GDOI-específicas da mostra. A fim usar o ISAKMP e o GDOI condicionais debuga, terminam estas duas etapas simples:

1. Ajuste o filtro condicional.
2. Permita o ISAKMP e o GDOI relevantes como de costume.

Por exemplo:

```
KS1# debug crypto gdoi condition peer add ipv4 10.1.20.2
% GDOI Debug Condition added.

KS1#
KS1# show crypto gdoi debug-condition
GDOI Conditional Filters:
Peer Address 10.1.20.2
Unmatched NOT set

KS1#debug crypto gdoi ks registration all-levels
GDOI Key Server Registration Debug level: (Packet, Detail, Event, Terse, Error)
```

> **Note**: Com o ISAKMP e o GDOI condicionais debuga, a fim travar debugam as mensagens que não puderam ter a informação condicional do filtro, por exemplo o endereço IP de Um ou Mais Servidores Cisco ICM NT no trajeto debugar, a bandeira **ímpar** pode ser permitido. Contudo, isto deve ser usado com cuidado porque pode produzir uma grande quantidade de debuga a informação.

Traços do evento GDOI

Isto foi adicionado na versão 15.1(3)T. O rastreamento de evento oferece o peso leve, sempre-no seguimento para eventos significativos e erros GDOI. Há igualmente saída-PATH que segue com o retorno de monitoramento permitido para condições de exceção. Os traços do evento podem fornecer mais informação de história do evento GETVPN do que Syslog tradicionais.

Os traços do evento GDOI são permitidos à revelia e podem ser recuperados da trace buffer com o comando do uniforme-**traço do monitor da mostra**.

```
GM1#show monitor event-trace gdoi ?
all Show all the traces in current buffer
back Show trace from this far back in the past
clock Show trace from a specific clock time/date
coop GDOI COOP Event Traces
exit GDOI Exit Traces
from-boot Show trace from this many seconds after booting
infra GDOI INFRA Event Traces
latest Show latest trace events since last display
merged Show entries in all event traces sorted by time
registration GDOI Registration event Traces
rekey GDOI Rekey event Traces

GM1#show monitor event-trace gdoi rekey all
*Nov 6 15:55:16.117: GDOI_REKEY_EVENT: ACK_SENT: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 15:55:16.117: GDOI_REKEY_EVENT: REKEY_RCVD: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 16:11:01.125: GDOI_REKEY_EVENT: ACK_SENT: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
*Nov 6 16:11:01.125: GDOI_REKEY_EVENT: REKEY_RCVD: From 10.1.12.2 to 10.1.13.2
with seq no 1 for the group G1
```

O rastreamento de caminho da saída fornece a informação detalhada sobre o trajeto da saída, isso é exceção e condições de erro, com a opção do retorno de monitoramento permitida à revelia. Os retornos de monitoramento podem então ser usados a fim descodificar a sequência exata do código que conduziu à condição do trajeto da saída. Use a opção do **detalhe** a fim recuperar os retornos de monitoramento da trace buffer:

```
GM1#show monitor event-trace gdoi exit all detail
*Nov 6 15:15:25.611: NULL_VALUE_FOUND:Invalid GROUP Name
-Traceback= 0xCA51318z 0xCA1F4DBz 0xC9B2707z 0xCA1ED4Ez 0x97EB018z
0x97EA960z 0x97E8D62z 0x97F3706z 0x97F3361z 0xA02684Ez
*Nov 6 15:15:25.611: MAP_NOT_APPLIED_IN_ANY_INTERFACE:
-Traceback= 0xCA51318z 0xCA46718z 0xCA1EF79z 0x97EB018z 0x97EA960z
0x97E8D62z 0x97F3706z 0x97F3361z 0xA02684Ez 0xA01FD52z
*Nov 6 15:15:25.650: NULL_VALUE_FOUND:NULL Parameters passed idb or ipaddress
when idb ipaddress is changed
-Traceback= 0xCA51318z 0xCA22430z 0xA09A8DCz 0xA09D8F6z 0xA0F280Fz
0xBA1D1F4z 0xBA1CACCz 0xBA1C881z 0xBA1C5BBz 0xA0F494Az
```

O tamanho de trace buffer do padrão é 512 entradas, e este não pôde ser bastante se o problema é intermitente. A fim aumentar este tamanho da entrada do traço do padrão, os parâmetros de configuração do traço do evento podem ser mudados como mostrado aqui:

```
GM1#show monitor event-trace gdoi rekey parameters
Trace has 512 entries
Stacktrace is disabled by default

GM1#
GM1#config t
Enter configuration commands, one per line. End with CNTL/Z.
GM1(config)#monitor event-trace gdoi rekey size ?
<1-1000000> Number of entries in trace
```

Pontos de verificação e problemas comuns do plano do controle GETVPN

Estão aqui algumas das edições do plano do controle comum para GETVPN. Para reiterar, o plano do controle é definido como todos os componentes da característica GETVPN exigidos a fim permitir a criptografia e a descriptografia do dataplane no GMs. Em um nível alto, isto exige o registro bem sucedido GM, a política de segurança e a transferência SA/instalam, e KEK/TEK subsequentes rekey.

Criação da instalação e da política da CAPOEIRA

A fim verificar e verificar que o KS criou com sucesso a política de segurança e o KEK/TEK associado, entre:

```
KS1#show crypto gdoi ks policy
Key Server Policy:
For group G1 (handle: 2147483650) server 10.1.11.2 (handle: 2147483650):

For group G1 (handle: 2147483650) server 10.1.12.2 (handle: 2147483651):

# of teks : 1 Seq num : 10
KEK POLICY (transport type : Unicast)
spi : 0x18864836BA888BCD1126671EEAFEB4C7
management alg : disabled encrypt alg : 3DES
crypto iv length : 8 key size : 24
orig life(sec): 1200 remaining life(sec): 528
sig hash algorithm : enabled sig key length : 162
sig size : 128
sig key name : key1

TEK POLICY (encaps : ENCAPS_TUNNEL)
spi : 0x91E3985A
```

```
access-list : ENCPOL
transform : esp-null esp-sha-hmac
alg key size : 0 sig key size : 20
orig life(sec) : 900 remaining life(sec) : 796
tek life(sec) : 2203 elapsed time(sec) : 1407
override life (sec): 0 antireplay window size: 4

Replay Value 442843.29 secs
```

Um problema comum com a instalação da política KS é quando há umas políticas diferentes configuradas entre o KSs preliminar e secundário. Isto pode conduzir ao comportamento imprevisível KS e este erro será relatado:

```
KS1#show crypto gdoi ks policy
Key Server Policy:
For group G1 (handle: 2147483650) server 10.1.11.2 (handle: 2147483650):

For group G1 (handle: 2147483650) server 10.1.12.2 (handle: 2147483651):

# of teks : 1 Seq num : 10
KEK POLICY (transport type : Unicast)
spi : 0x18864836BA888BCD1126671EEAFEB4C7
management alg : disabled encrypt alg : 3DES
crypto iv length : 8 key size : 24
orig life(sec): 1200 remaining life(sec): 528
sig hash algorithm : enabled sig key length : 162
sig size : 128
sig key name : key1

TEK POLICY (encaps : ENCAPS_TUNNEL)
spi : 0x91E3985A
access-list : ENCPOL
transform : esp-null esp-sha-hmac
alg key size : 0 sig key size : 20
orig life(sec) : 900 remaining life(sec) : 796
tek life(sec) : 2203 elapsed time(sec) : 1407
override life (sec): 0 antireplay window size: 4

Replay Value 442843.29 secs
```

Atualmente não há nenhuma sincronização da configuração automática entre KSs preliminar e secundário, assim que estes devem manualmente ser retificados.

Porque a CAPOEIRA é uma configuração crítica (e quase sempre imperativa) para GETVPN, é chave certificar-se que trabalhos da CAPOEIRA corretamente e os papéis da CAPOEIRA KS está correta:

```
KS1#show crypto gdoi ks coop
Crypto Gdoi Group Name :G1
Group handle: 2147483650, Local Key Server handle: 2147483650

Local Address: 10.1.11.2
Local Priority: 200
 Local KS Role: Primary   , Local KS Status: Alive
Local KS version: 1.0.4
Primary Timers:
Primary Refresh Policy Time: 20
Remaining Time: 10
Antireplay Sequence Number: 40

Peer Sessions:
```

```
Session 1:
Server handle: 2147483651
Peer Address: 10.1.12.2
Peer Version: 1.0.4
Peer Priority: 100
Peer KS Role: Secondary , Peer KS Status: Alive
Antireplay Sequence Number: 0

IKE status: Established
Counters:
Ann msgs sent: 31
Ann msgs sent with reply request: 2
Ann msgs recv: 64
Ann msgs recv with reply request: 1
Packet sent drops: 7
Packet Recv drops: 0
Total bytes sent: 20887
Total bytes recv: 40244
```

Em uma instalação funcional da CAPOEIRA, este fluxo do protocolo deve ser observado:

A troca IKE > o ANN com prioridades da CAPOEIRA trocaram > eleição da CAPOEIRA > ANN de preliminar a KS secundário (política, base de dados GM, e as chaves)

Quando a CAPOEIRA não funciona corretamente, ou se há uma separação da CAPOEIRA, tal como KSs múltiplo tornam-se os KS preliminares, estes debugam devem ser recolhidos pesquisando defeitos:

```
debug crypto isakmp
debug crypto gdoi ks coop all-levels
show crypto isakmp sa
show crypto gdoi ks coop
```

Instalação IKE

A troca bem sucedida IKE é exigida para GETVPN a fim fixar o canal de controle para a política subsequente e a transferência SA. No fim da troca bem sucedida IKE, GDOI_REKEY sa é criado.

Nas versões mais cedo do que o Cisco IOS 15.4(1)T, o GDOI_REKEY pode ser mostrado com o **comando show crypto isakmp sa**:

```
GM1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
10.1.13.2 10.1.11.2 GDOI_REKEY        1075 ACTIVE
10.1.11.2 10.1.13.2 GDOI_IDLE         1074 ACTIVE

IPv6 Crypto ISAKMP SA

GM1#
```

No Cisco IOS 15.4(1)T e mais tarde, este GDOI_REKEY sa é mostrado com a **mostra que o gdoi cripto rekey o** comando **sa**:

```
GM1#show crypto gdoi rekey sa
GETVPN REKEY SA
dst             src             conn-id         status
10.1.13.2       10.1.11.2       1114            ACTIVE
```

Note: Uma vez que a troca inicial IKE termina, as políticas subsequentes e as chaves **estarão empurradas do** KS ao GM com o uso GDOI_REKEY SA. Tão há nenhum rekey para GDOI_IDLE SA quando expiram; desaparecem quando suas vidas expiram. Contudo, deve sempre haver GDOI_REKEY SA no GM para que receba rekeys.

A troca IKE para GETVPN é não diferente do IKE usado em túneis de IPsec pontos a ponto tradicionais, assim que o método de Troubleshooting permanece o mesmo. Estes debugam devem ser recolhidos a fim pesquisar defeitos edições da autenticação de IKE:

```
debug crypto isakmp
debug crypto isakmp error
debug crypto isakmp detail (hidden command, if detailed isakmp exchange information
is needed)
debug crypto isakmp packet (hidden command, if packet level isakmp information is needed)
```

O registro, a transferência da política, e o SA instalam

Uma vez que a autenticação de IKE sucede, o GM registra-se com o KS. Estes mensagens do syslog estão esperados ser considerados quando este ocorre corretamente:

```
%GDOI-5-GM_REKEY_TRANS_2_UNI: Group G1 transitioned to Unicast Rekey.
%GDOI-5-SA_KEK_UPDATED: SA KEK was updated
%GDOI-5-SA_TEK_UPDATED: SA TEK was updated
%GDOI-5-GM_REGS_COMPL: Registration to KS 10.1.12.2 complete for group G1 using
address 10.1.13.2
%GDOI-5-GM_INSTALL_POLICIES_SUCCESS: SUCCESS: Installation of Reg/Rekey policies
from KS 10.1.12.2 for group G1 & gm identity 10.1.13.2
```

A política e as chaves podem ser verificadas com este comando:

```
GM1#show crypto gdoi
GROUP INFORMATION

Group Name : G1
Group Identity : 3333
Crypto Path : ipv4
Key Management Path : ipv4
Rekeys received : 1
IPSec SA Direction : Both

Group Server list : 10.1.11.2
10.1.12.2

Group member : 10.1.13.2 vrf: None
Version : 1.0.4
Registration status : Registered
Registered with : 10.1.12.2
Re-registers in       : 139 sec
Succeeded registration: 1
Attempted registration: 1
Last rekey from : 10.1.11.2
Last rekey seq num : 0
Unicast rekey received: 1
Rekey ACKs sent : 1
Rekey Rcvd(hh:mm:ss)  : 00:05:20
allowable rekey cipher: any
```

```
allowable rekey hash : any
allowable transformtag: any ESP

Rekeys cumulative
Total received : 1
After latest register : 1
Rekey Acks sents : 1

ACL Downloaded From KS 10.1.11.2:
access-list deny icmp any any
access-list deny eigrp any any
access-list deny ip any 224.0.0.0 0.255.255.255
access-list deny ip 224.0.0.0 0.255.255.255 any
access-list deny udp any port = 848 any port = 848
access-list permit ip any any

KEK POLICY:
Rekey Transport Type : Unicast
Lifetime (secs) : 878
Encrypt Algorithm : 3DES
Key Size : 192
Sig Hash Algorithm : HMAC_AUTH_SHA
Sig Key Length (bits) : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
Serial1/0:
IPsec SA:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac
sa timing:remaining key lifetime (sec): (200)
Anti-Replay(Time Based) : 4 sec interval


GM1#
GM1#
GM1#show crypto ipsec sa

interface: Serial1/0
Crypto map tag: gm1map, local addr 10.1.13.2

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 0.0.0.0 port 848
PERMIT, flags={}
#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 10.1.13.2, remote crypto endpt.: 0.0.0.0
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
current outbound spi: 0x0(0)
PFS (Y/N): N, DH group: none

local crypto endpt.: 10.1.13.2, remote crypto endpt.: 0.0.0.0
path mtu 1500, ip mtu 1500, ip mtu idb Serial1/0
current outbound spi: 0x8BF147EF(2347845615)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8BF147EF(2347845615)
```

```
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 1, flow_id: SW:1, sibling_flags 80000040, crypto map: gm1map
sa timing: remaining key lifetime (sec): (192)
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: Y replay window size: 4
Status: ACTIVE(ACTIVE)

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x8BF147EF(2347845615)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel, }
conn id: 2, flow_id: SW:2, sibling_flags 80000040, crypto map: gm1map
sa timing: remaining key lifetime (sec): (192)
Kilobyte Volume Rekey has been disabled
IV size: 8 bytes
replay detection support: Y replay window size: 4
Status: ACTIVE(ACTIVE)

outbound ah sas:

outbound pcp sas:
GM1#
```

Note: Com GETVPN, os SA de entrada e de partida usam o mesmo SPI.

Com GETVPN o registro e a política instalam o tipo de problema, estes debugam são precisados a fim pesquisar defeitos:

```
debug crypto isakmp (KS and GM)
debug crypto gdoi ks registration all-levels (KS)
debug crypto gdoi gm registration all-level (GM)
debug crypto engine (GM only)
show crypto eli detail (multiple iterations on GM)
```

Note: Adicional debuga pode ser exigido segundo o resultado destas saídas.

Desde que o registro GETVPN ocorre tipicamente imediatamente depois do reload GM, este script EEM pôde ser útil a fim recolher estes debuga:

```
debug crypto isakmp (KS and GM)
debug crypto gdoi ks registration all-levels (KS)
debug crypto gdoi gm registration all-level (GM)
debug crypto engine (GM only)
show crypto eli detail (multiple iterations on GM)
```

Rekey

Uma vez que o GMs está registrado ao KS e a rede GETVPN se estabelece corretamente, o KS preliminar é responsável para enviar rekey mensagens a todo o GMs registrado a ele. As mensagens do rekey são usadas a fim sincronizar todas as políticas, chaves, e pseudotimes no GMs. As mensagens do rekey podem ser enviadas com um unicast ou um método do Multicast.

Este mensagem do syslog está considerado no KS quando a mensagem do rekey é enviada:

```
debug crypto isakmp (KS and GM)
debug crypto gdoi ks registration all-levels (KS)
debug crypto gdoi gm registration all-level (GM)
debug crypto engine (GM only)
show crypto eli detail (multiple iterations on GM)
```

No GMs, este é o Syslog que é visto quando recebe o rekey:

```
debug crypto isakmp (KS and GM)
debug crypto gdoi ks registration all-levels (KS)
debug crypto gdoi gm registration all-level (GM)
debug crypto engine (GM only)
show crypto eli detail (multiple iterations on GM)
```

A exigência do par de chaves RSA para Rekey em KS

Rekey a funcionalidade exige a presença de chaves RSA no KS. O KS fornece a chave pública do par de chaves RSA ao GM através deste canal seguro durante o registro. O KS assina então as mensagens GDOI enviadas ao GM com a chave privada RSA no payload GDOI SIG. O GM recebe as mensagens GDOI e usa a chave do público RSA a fim verificar a mensagem. As mensagens entre o KS e o GM são cifradas com o KEK, que é distribuído igualmente ao GM durante o registro. Uma vez que o registro está completo, subsequente rekeys estão cifrados com o KEK e assinados com a chave privada RSA.

Se a chave RSA está não atual no KS durante o registro GM, esta mensagem aparece no Syslog:

```
debug crypto isakmp (KS and GM)
debug crypto gdoi ks registration all-levels (KS)
debug crypto gdoi gm registration all-level (GM)
debug crypto engine (GM only)
show crypto eli detail (multiple iterations on GM)
```

Quando as chaves não estão atuais no KS, o GM registra-se pela primeira vez, mas o seguintes rekey falham do KS. Eventualmente as chaves existentes no GM expiram, e registra-se novamente outra vez.

```
debug crypto isakmp (KS and GM)
debug crypto gdoi ks registration all-levels (KS)
debug crypto gdoi gm registration all-level (GM)
debug crypto engine (GM only)
show crypto eli detail (multiple iterations on GM)
```

Desde que o par de chaves RSA é usado a fim assinar as mensagens do rekey, **DEVEM** ser as mesmas entre KSs preliminar e todo o secundário. Isto assegura-se de que durante uma falha preliminar KS, rekeys enviado por um KS secundário (o KS preliminar novo) possa ainda corretamente ser validado pelo GMs. Quando gerencie o par de chaves RSA no KS preliminar, o par de chaves deve ser criado com a opção **exportable** de modo que possam ser exportados para todo o KSs secundário a fim cumprir esta exigência.

Rekey o Troubleshooting

KEK/TEK rekey a falha são um dos problemas os mais comuns GETVPN encontrados nos desenvolvimentos de cliente. Pesquisar defeitos rekey edições deve seguir as etapas do rekey

como esboçadas aqui:

1. Fez rekeys obtêm enviado pelo KS?

   Isto pode ser verificado por um observion do mensagem do syslog %GDOI-5-KS_SEND_UNICAST_REKEY ou mais exatamente com este comando:

```
KS1#show crypto gdoi ks rekey
Group G1 (Unicast)
Number of Rekeys sent               : 341
Number of Rekeys retransmitted      : 0
KEK rekey lifetime (sec) : 1200
Remaining lifetime (sec) : 894
Retransmit period : 10
Number of retransmissions : 5
IPSec SA 1 lifetime (sec) : 900
Remaining lifetime (sec) : 405
```

   O número de rekeys retransmitido é indicativo de rekey os pacotes de reconhecimento não recebidos pelo KS e consequentemente possível rekey edições. Mantenha na mente que os GDOI rekey os usos UDP como um mecanismo de transporte incerto, assim que alguns rekey gotas puderam ser esperados segundo a confiança da rede de transporte subjacente, mas uma tendência do aumento rekey retransmissões deve sempre ser investigada.

   Um por-GM mais detalhado rekey estatísticas pode igualmente ser obtido. Este é tipicamente o primeiro lugar para procurar o potencial rekey edições.

```
KS1#show crypto gdoi ks members

Group Member Information :

Number of rekeys sent for group G1 : 346

Group Member ID : 10.1.14.2 GM Version: 1.0.4
Group ID : 3333
Group Name : G1
Key Server ID : 10.1.11.2
 Rekeys sent       : 346
Rekeys retries : 0
Rekey Acks Rcvd : 346
Rekey Acks missed : 0

Sent seq num : 2 1 2 1
Rcvd seq num : 2 1 2 1

Group Member ID : 10.1.13.2 GM Version: 1.0.4
Group ID : 3333
Group Name : G1
Key Server ID : 10.1.12.2
 Rekeys sent       : 340
Rekeys retries : 0
Rekey Acks Rcvd : 340
Rekey Acks missed : 0

Sent seq num : 2 1 2 1
Rcvd seq num : 2 1 2 1
```

2. Rekey pacotes obtêm entregado na rede de infraestrutura subjacente?

   O Troubleshooting de IP padrão ao longo do trajeto de encaminhamento do rekey deve ser seguido a fim assegurar-se de que os pacotes do rekey não estejam deixados cair no transit network entre KS e GM. Algumas ferramentas de Troubleshooting comuns usadas aqui são Access Control Lists (ACLs), Netflow, e captura de pacote de informação do entrada/saída no transit network.

3. Rekey o alcance que dos pacotes o processo GDOI para rekey o processamento?

   Verifique o GM rekey estatísticas:

```
GM1#show crypto gdoi gm rekey
Group G1 (Unicast)
Number of Rekeys received (cumulative) : 340
Number of Rekeys received after registration : 340
Number of Rekey Acks sent : 340
```

4. Rekey o retorno do pacote do reconhecimento ao KS?

   Siga etapas 1 a 3 a fim seguir o pacote do reconhecimento do rekey do GM de volta ao KS.

Muticast Rekey

O Multicast rekey é diferente do unicast rekey nestes aspectos:

- Desde que o Multicast é usado a fim transportar estes rekey pacotes do KS ao GMs, o KS não precisam de replicate os pacotes do rekey próprio. O KS envia somente uma cópia do pacote do rekey, e replicated na rede Multicast-permitida.
- Não há nenhum mecanismo do reconhecimento para o Multicast rekey, assim que se um GM não era receber o pacote do rekey, o KS não teria nenhum conhecimento dele, e consequentemente nunca removerá um GM de seu base de dados GM. E porque não há nenhum reconhecimento, o KS retransmitirá sempre os pacotes do rekey baseados no seu rekey a configuração da retransmissão.

O mais geralmente - o Multicast considerado rekey o problema é quando o rekey não é recebido no GM. Podia haver um número de causas possíveis para esta, como:

- Edição da entrega de pacotes dentro do infra-estruturo de roteamento de transmissão múltipla
- O roteamento de transmissão múltipla fim-a-fim não é permitido dentro da rede

A primeira etapa para pesquisar defeitos uma edição com Multicast rekey é considerar se rekey trabalhos quando comutado do Multicast ao método do unicast.

Uma vez que você identifica que a edição é específica ao Multicast rekey, verifique que KS envia o rekey ao endereço de multicast especificado.

```
GM1#show crypto gdoi gm rekey
Group G1 (Unicast)
Number of Rekeys received (cumulative) : 340
Number of Rekeys received after registration : 340
```

```
Number of Rekey Acks sent : 340
```

Teste a Conectividade do Multicast entre o KS e o GM com um pedido do Internet Control Message Protocol (ICMP) ao endereço de multicast. Todo o GMs que é parte do grupo de transmissão múltipla deve responder ao sibilo. Assegure-se de que o ICMP esteja excluído da política de criptografia KS para este teste.

```
KS1#ping 226.1.1.1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 226.1.1.1, timeout is 2 seconds:

Reply to request 0 from 10.1.21.2, 44 ms
```

Se o teste de ping do Multicast falha, a seguir o Troubleshooting do Multicast deve ser executado, que é fora do espaço deste documento.

Controle a verificação plana do relé

Sintoma

Quando os clientes promovem seu GM a uma versão do Novo Cisco IOS, puderam experimentar o KEK rekey falhas com esta mensagem observada no Syslog:

```
KS1#ping 226.1.1.1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 226.1.1.1, timeout is 2 seconds:

Reply to request 0 from 10.1.21.2, 44 ms
```

Este comportamento é causado por uma questão de interoperabilidade introduzida com a verificação da anti-repetição que é adicionada para mensagens do plano do controle. Especificamente, um KS que execute o código mais velho restaurará o KEK rekey o número de sequência a 1, e este será deixado cair pelo GM que executa o código novo quando interpreta que como replayed rekey o pacote. Para mais detalhes, veja a identificação de bug Cisco CSCta05809 (GETVPN: Controle plano GETVPN apreciável à repetição), e restrições de configuração GETVPN.

Background

Com GETVPN, as mensagens do plano do controle podem levar a informação sensível ao tempo a fim proporcionar o serviço com base no período da verificação da anti-repetição. Consequentemente, estas mensagens exigem a proteção anti-replay elas mesmas a fim assegurar o accruracy do tempo. Estas mensagens são:

- **Rekey mensagens de** KS ao GM
- **PRENDA mensagens de anúncio** entre KSs

Como parte desta aplicação da proteção anti-replay, as verificações do número de sequência estiveram adicionadas a fim proteger mensagens replayed, assim como uma verificação do pseudotime quando TBAR é permitido.

Solução

A fim resolver esta edição, o GM e KS devem ser promovidos às versões do Cisco IOS depois que a característica da verificação da repetição do plano do controle. Com o código do Novo Cisco IOS, KS não restaura o número de sequência de volta a 1 para um KEK rekey, mas pelo contrário continua a usar o número de sequência atual e restaura somente o número de sequência para o TEK rekeys.

Estas versões do Cisco IOS têm as características da verificação da repetição:

- 12.4(15)T10
- 12.4(22)T3
- 12.4(24)T2
- 15.0(1)M e mais atrasado

Outros problemas relacionados da repetição

- CAPOEIRA falha devido às mensagens ANN que falham a verificação da repetição (identificação de bug Cisco CSCtc52655)

Debugar falhas planas da repetição do controle

Para outras falhas da repetição do plano do controle, recolha esta informação e certifique-se que os tempos são sincronizados entre o KS e o GM.

- Syslog do GM e do KS
- O ISAKMP debuga
- GDOI debuga (rekey e repetição) de KS e de GM

Controle edições planas da fragmentação de pacote de informação

Com GETVPN, a fragmentação de pacote de informação plana do controle é um problema comum, e pode manifestar-se em uma destas duas encenações quando os pacotes do plano do controle são grandes bastante que exigirão a fragmentação de IP:

- Pacotes do anúncio da CAPOEIRA GETVPN
- GETVPN rekey pacotes

Pacotes do anúncio da CAPOEIRA

Os pacotes do anúncio da CAPOEIRA levam a informação de base de dados GM, e assim podem crescer grandes em um grande desenvolvimento GETVPN. Da experiência anterior, uma rede GETVPN que consista em 1500+ GMs produza os pacotes do anúncio maiores de 18024 bytes, que é o tamanho de buffer enorme do padrão do Cisco IOS. Quando isto acontece, o KS não atribui um buffer grande bastante para transmitir os pacotes ANN com este erro:

```
KS1#ping 226.1.1.1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 226.1.1.1, timeout is 2 seconds:

Reply to request 0 from 10.1.21.2, 44 ms
```

A fim retificar esta circunstância, este ajuste do buffer é recomendado:

```
KS1#ping 226.1.1.1

Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 226.1.1.1, timeout is 2 seconds:

Reply to request 0 from 10.1.21.2, 44 ms
```

Rekey pacotes

GETVPN rekey pacotes podem igualmente exceder o tamanho máximo típico da unidade da transição IP 1500 (MTU) quando a política de criptografia é grande, como uma política que consista nas linhas 8+ das entradas de controle de acesso (ACE) na criptografia ACL.

Problema de fragmentação e identificação

Em ambos os cenários anteriores, GETVPN deve poder transmitir corretamente e para receber os pacotes de UDP fragmentados para que a CAPOEIRA ou o GDOI rekey para trabalhar corretamente. A fragmentação de IP pode ser um problema em alguns ambientes de rede. Por exemplo, uma rede que consista plano da transmissão do trajeto dos custos iguais no multi (ECMP), e alguns dispositivos no plano da transmissão exigem a remontagem virtual dos pacotes IP fragmentados, tais como a remontagem virtual da fragmentação (VFR).

A fim identificar o problema, verifique os erros da remontagem no dispositivo onde se suspeita que os pacotes fragmentados UDP 848 não estão recebidos corretamente:

```
KS1#show ip traffic | section Frags
Frags: 10 reassembled, 3 timeouts, 0 couldn't reassemble
0 fragmented, 0 fragments, 0 couldn't fragment
```

Se os timeouts de remontagem continuam a incrementar, use o **comando error debugar IP** a fim confirmar se a gota é parte do fluxo de pacote de informação rekey/COOP. Uma vez que confirmado, o Troubleshooting normal do encaminhamento de IP deve ser executado a fim isolar o dispositivo exato no plano da transmissão que pôde ter deixado cair os pacotes. Algumas ferramentas de uso geral incluem:

- Captura de pacote de informação
- Estatísticas do encaminhamento de tráfego
- Estatísticas dos recursos de segurança (Firewall, IPS)
- Estatísticas VFR

Questões de interoperabilidade GDOI

As várias questões de interoperabilidade foram encontradas com GETVPN ao longo dos anos, e é crítico observar as versões do Cisco IOS Release entre KS e GM e entre o KSs para questões de interoperabilidade.

Outras questões de interoperabilidade conhecidas GETVPN são:

- Controle a verificação plana do relé
- GETVPN KEK Rekey a mudança do comportamento
- Identificação de bug Cisco CSCub42920 (GETVPN: KS não valida a mistura rekey dentro o ACK das versões precedentes GM)

- Identificação de bug Cisco CSCuw48400 (o GM de GetVPN incapaz de se registrar ou rekey falha - a SIG-mistura > o padrão SHA-1)
- Identificação de bug Cisco CSCvg19281 (o GM múltiplo GETVPN causa um crash após a migração aos pares novos KS; se uma versão GM está mais adiantada de 3.16, e KS está promovido de um código inicial a 3.16 ou mais atrasado, esta edição pode acontecer)

Procedimento da upgrade de IOS GETVPN

Este procedimento do upgrade do Cisco IOS deve ser seguido quando uma elevação do código do IOS Cisco precisa de ser executada em um ambiente GETVPN:

1. Promova um KS secundário primeiramente e espere até que a eleição da CAPOEIRA KS esteja terminada.
2. Repita Step1 para todo o KSs secundário.
3. Promova o KS preliminar.
4. Promova GMs.

Pesquise defeitos edições do plano dos dados GETVPN

Comparado para controlar problemas planos, as edições do plano dos dados GETVPN são os problemas onde o GM tem a política e as chaves para executar a criptografia e a descriptografia do dataplane, mas por qualquer motivo o fluxo de tráfego de ponta a ponta não trabalha. A maioria das edições do dataplane para GETVPN relacionam-se à transmissão genérica do IPsec, e não se são específico GETVPN. Assim a maioria do abordagem de Troubleshooting descrito aqui aplica-se às edições genéricas do dataplane do IPsec também.

Com problemas da criptografia (Grupo-baseado ou por pares túneis), é importante pesquisar defeitos o problema e isolar o problema a uma parte particular do datapath. Especificamente, o abordagem de Troubleshooting descrito aqui é pretendido ajudá-lo a responder a estas perguntas:

- Que dispositivo é o culpado - roteador de criptografia ou roteador de descriptografia?
- Em que sentido é o problema que acontece - ingresso ou saída?

Os dados GETVPN aplanam ferramentas de Troubleshooting

O Troubleshooting do dataplane do IPsec é muito diferente daquele para o plano do controle. Com o dataplane, há geralmente nenhum debuga que você pode ser executado, ou é executado pelo menos com segurança em um ambiente de produção. Assim o Troubleshooting confia pesadamente nos contadores e nas estatísticas de tráfego diferentes que podem ajudar a seguir o pacote ao longo de um trajeto de encaminhamento. A ideia é poder desenvolver um grupo de pontos de verificação a fim ajudar a isolar-se onde os pacotes puderam ser deixados cair como mostrado aqui:

Estão aqui as ferramentas para debug do plano de alguns dados:

- Listas de acesso
- Explicar da Precedência IP
- Netflow
- Contadores de interface
- Contadores criptos
- Cisco Express Forwarding (CEF) IP global e contadores de queda da Por-característica
- Captura de pacote de informação encaixada (EPC)
- O plano dos dados debuga (o pacote IP e o CEF debugam)

Os pontos de verificação no datapath na imagem anterior podem ser validados com estas ferramentas:

GM de criptografia

- Interface de LAN do ingresso
  - Entrada ACL
  - Netflow do ingresso
  - Captura de pacote de informação encaixada
  - Conta de precedência da entrada

- Crypto-engine
  - **show crypto ipsec sa**
  - **mostre o detalhe cripto IPsec sa**
  - **estatísticas do acelerador do show crypto engine**

- Interface WAN da saída
  - Netflow da saída
  - Captura de pacote de informação encaixada
  - Conta de precedência da saída

GM de descriptografia

- Interface WAN do ingresso
  - Entrada ACL
  - Netflow do ingresso
  - Captura de pacote de informação encaixada
  - Conta de precedência da entrada

- Crypto-engine
  - **show crypto ipsec sa**
  - **mostre o detalhe cripto IPsec sa**

estatísticas do acelerador do show crypto engine

- Interface de LAN da saída
  Netflow da saída
  Captura de pacote de informação encaixada

O caminho de retorno segue o mesmo fluxo de tráfego. As próximas seções têm alguns exemplos destas ferramentas do dataplane no uso.

Contadores da criptografia /descriptografia

Os contadores da criptografia /descriptografia em um roteador são baseados em um fluxo do IPsec. Infelizmente isto não trabalha bem com GETVPN desde que GETVPN distribui tipicamente uma “licença IP toda a qualquer” política de criptografia que cifrar tudo. Assim se o problema acontece somente para alguns dos fluxos e não de tudo, estes contadores podem ser um tanto difíceis de usar-se a fim avaliar corretamente se os pacotes estão cifrados ou decifrados quando há bastante tráfego de background significativo que trabalha.

```
GM1#show crypto ipsec sa | in encrypt|decrypt
#pkts encaps: 100, #pkts encrypt: 100, #pkts digest: 100
#pkts decaps: 100, #pkts decrypt: 100, #pkts verify: 100
```

Netflow

O Netflow pode ser usado a fim monitorar o ingresso e o tráfego de saída em ambos GMs. Note com a **licença IP** GETVPN **toda a qualquer** política, o tráfego enrypted será agregado e não fornece a informação do por-fluxo. a informação do Por-fluxo deverá então ser recolhida com a marcação DSCP/precedence descrita mais tarde.

Neste exemplo, o Netflow para um sibilo de 100 contagens de um host atrás de GM1 a um host atrás de GM2 é mostrado nos vários pontos de verificação.

GM de criptografia

Configuração Netflow:

```
interface Ethernet0/0
description LAN
ip address 192.168.13.1 255.255.255.0
ip flow ingress
ip pim sparse-dense-mode
!
interface Serial1/0
description WAN interface
ip address 10.1.13.2 255.255.255.252
ip flow egress
ip pim sparse-dense-mode
crypto map gm1map
```

Netflow output:

```
GM1#show ip cache flow | be SrcIf
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Et0/0 192.168.13.2 Se1/0* 192.168.14.2 32 8DE1 6523   100
```

```
Et0/0 192.168.13.2 Se1/0 192.168.14.2 01 0000 0800   100
GM1#
```

Note: Na saída precedente, * denota o tráfego de saída. A primeira linha mostra o tráfego criptografado da saída (com protocolo 0x32 = ESP) fora da interface WAN, e a segunda linha tráfego do ingresso ICMP que bate a interface de LAN.

GM de descriptografia

Configuração:

```
interface Ethernet0/0
description LAN interface
ip address 192.168.14.1 255.255.255.0
ip flow egress
ip pim sparse-dense-mode
!
interface Serial1/0
description WAN interface
ip address 10.1.14.2 255.255.255.252
ip flow ingress
ip pim sparse-dense-mode
crypto map gm1map
```

Netflow output:

```
GM2#show ip cache flow | be SrcIf
SrcIf SrcIPaddress DstIf DstIPaddress Pr SrcP DstP Pkts
Se1/0 192.168.13.2 Et0/0 192.168.14.2 32 8DE1 6523   100
Se1/0 192.168.13.2 Et0/0* 192.168.14.2 01 0000 0800   100
GM2#
```

Marcação da precedência DSCP/IP

O desafio com pesquisa de defeitos de um problema da criptografia é que uma vez que o pacote é cifrado você perde a visibilidade no payload, que é o que a criptografia é suposta para fazer, e aquela faz difícil seguir o pacote para um fluxo particular IP. Há duas maneiras de endereçar esta limitação quando se trata de pesquisar defeitos um problema do IPsec:

- O uso ESP-NULL como o IPsec transforma. O IPsec ainda executa o encapsulamento ESP mas o no encryption é aplicado ao payload, assim que são visíveis em uma captura de pacote de informação.
- Marque um fluxo IP com uma marcação original do Differentiated Services Code Point (DSCP) /precedence baseada em suas características L3/L4.

ESP-NULL exigem mudanças em ambos os pontos finais do túnel e não são reservados frequentemente baseado na política de segurança do cliente. Consequentemente, Cisco recomenda tipicamente o uso de DSCP/precedence que marca pelo contrário.

Gráfico de referência DSCP/Precedence

ToS (encantar)	ToS(Decimal)	Precedência de IP	DSCP	Binário
0xE0	224	Controle de rede 7	56 CS7	11100000
0xC0	192	Controle da rede interna 6	48 CS6	11000000
0xB8	184	5 crítico	46 EF	10111000

0xA0	160		40 CS5	10100000
0x88	136	Cancelamento flash 4	34 AF41	10001000
0x80	128		32 CS4	10000000
0x68	104	Flash 3	26 AF31	01101000
0x60	96		24 CS3	01100000
0x48	72	2 imediato	18 AF21	01001000
0x40	64		16 CS2	01000000
0x20	32	1 prioridade	8 CS1	00100000
0x00	0	0 rotinas	0 Dflt	00000000

Marque pacotes com DSCP/Precedence

Estes métodos são usados tipicamente a fim marcar pacotes com as marcações específicas DSCP/Precedence.

PBR

```
interface Ethernet1/0
ip policy route-map mark
!
access-list 150 permit ip host 172.16.1.2 host 172.16.254.2
!
route-map mark permit 10
match ip address 150
set ip precedence flash-override
```

MQC

```
class-map match-all my_flow
match access-group 150
!
policy-map marking
class my_flow
set ip precedence 4
!
interface Ethernet1/0
service-policy input marking
```

Sibilo do roteador

```
GM1-host#ping ip
Target IP address: 192.168.14.2
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]: 136
...
<snip>
```

> **Note**: É sempre uma boa ideia monitorar o fluxo de tráfego normal e perfil DSCP/precedence antes que você aplique a marcação de modo que o fluxo de tráfego marcado seja original.

Monitore pacotes marcados

Explicar da Precedência IP

```
interface Ethernet0/0
ip address 192.168.1.2 255.255.255.0
ip accounting precedence input
```

```
middle_router#show interface precedence
Ethernet0/0
Input
Precedence 4: 100 packets, 17400 bytes
```

Relação ACL

```
middle_router#show access-list 144
Extended IP access list 144
10 permit ip any any precedence routine
20 permit ip any any precedence priority
30 permit ip any any precedence immediate
40 permit ip any any precedence flash
50 permit ip any any precedence flash-override (100 matches)
60 permit ip any any precedence critical
70 permit ip any any precedence internet (1 match)
80 permit ip any any precedence network
```

Captura de pacote de informação encaixada

A captura de pacote de informação encaixada (EPC) é uma ferramenta útil para capturar pacotes a nível de interface a fim identificar se um pacote alcançou um dispositivo específico. Recorde que os trabalhos do EPC bem para o tráfego do texto claro, mas podem ser um desafio quando os pacotes capturados forem cifrados. Consequentemente as técnicas como a marcação DSCP/precedence discutida previamente ou outros caráteres IP, tais como o comprimento do pacote IP, têm que ser usados junto com o EPC a fim fazer a pesquisa de defeitos de mais eficaz.

Rastreamento de pacotes do Cisco IOS XE

Este é uns recursos úteis para seguir o trajeto de encaminhamento da característica em todas as Plataformas que executam o Cisco IOS XE, tal como CSR1000v, ASR1000, e em ISR4451-X.

Os dados GETVPN aplanam problemas comuns

Pesquisar defeitos o dataplane do IPsec para GETVPN é na maior parte não diferente de pesquisar defeitos edições pontos a ponto tradicionais do dataplane do IPsec, com as duas exceções devido a estas propriedades originais do dataplane de GETVPN.

O tempo baseou a falha da Anti-repetição

Em uma rede GETVPN, as falhas TBAR podem frequentemente ser difíceis de pesquisar defeitos desde que há já não por pares uns túneis. A fim pesquisar defeitos falhas GETVPN TBAR, termine estas etapas:

1. Identifique que pacote é deixado cair devido à falha TBAR e identifique subseqüentemente o GM de criptografia.

   Antes da versão 15.3(2)T, o Syslog da falha TBAR não imprimiu o endereço de origem do pacote falhado, assim que este faz muito difícil identificar que o pacote falhou. Isto foi melhorado significativamente na versão 15.3(2)T e mais recente, onde o Cisco IOS imprime este:

```
middle_router#show access-list 144
Extended IP access list 144
10 permit ip any any precedence routine
20 permit ip any any precedence priority
30 permit ip any any precedence immediate
40 permit ip any any precedence flash
50 permit ip any any precedence flash-override (100 matches)
60 permit ip any any precedence critical
70 permit ip any any precedence internet (1 match)
80 permit ip any any precedence network
```

   Uma história TBAR foi executada igualmente nesta versão:

```
GM2#show crypto gdoi gm replay
Anti-replay Information For Group G1:
Timebased Replay:
Replay Value : 621388.66 secs
Input Packets : 0 Output Packets : 0
Input Error Packets : 2 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs

TBAR Error History (sampled at 10pak/min):
19:29:32.081 EST Wed Nov 13 2013: src=192.168.13.2; my_pst=620051.84 secs;
peer_pst=619767.09 secs; win=4
```

   Note: Os realces mencionados previamente têm sido executados desde no Cisco IOS XE pela identificação de bug Cisco CSCun49335 e no Cisco IOS pela identificação de bug Cisco CSCub91811.
   Para as versões do Cisco IOS que não tiveram esta característica, o **detalhe da repetição gm do gdoi do debug crypto** pode igualmente fornecer esta informação, embora esta debugue cópias a informação TBAR para todo o tráfego (não somente deixado cair pacotes devido à falha TBAR), assim que não pôde ser praticável ser executado em um ambiente de produção.

```
GM2#show crypto gdoi gm replay
Anti-replay Information For Group G1:
Timebased Replay:
Replay Value : 621388.66 secs
Input Packets : 0 Output Packets : 0
Input Error Packets : 2 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs

TBAR Error History (sampled at 10pak/min):
```

```
19:29:32.081 EST Wed Nov 13 2013: src=192.168.13.2; my_pst=620051.84 secs;
peer_pst=619767.09 secs; win=4
```

2. A fonte do pacote é identificada uma vez, você deve poder encontrar o GM de criptografia. Então, o pseudotimestamp no GMs de criptografia e de descriptografia deve ser monitorado para toda a tração potencial do pseudotime. A melhor maneira de fazer isto seria sincronizar GMs e o KS ao NTP e recolher periodicamente a informação do pseudotime com um relógio de sistema de referência em todo a fim determinar se o problema é causado pelo enviesamento do pulso de disparo no GMs.

GM1

```
GM1#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.469 EST Wed Nov 13 2013

Anti-replay Information For Group G1:
Timebased Replay:
Replay Value              : 625866.26 secs
Input Packets : 0 Output Packets : 0
Input Error Packets : 0 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs
```

GM2

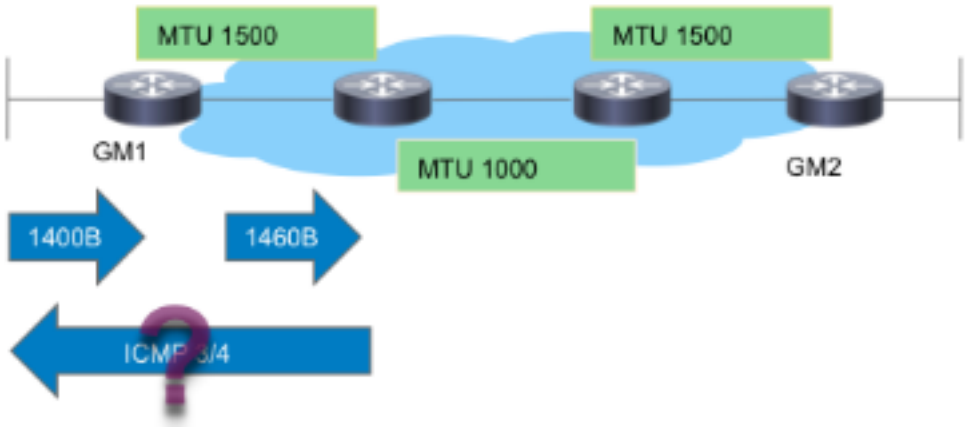
```
GM2#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.743 EST Wed Nov 13 2013

Anti-replay Information For Group G1:
Timebased Replay:
Replay Value              : 625866.51 secs
Input Packets : 4 Output Packets : 4
Input Error Packets : 2 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs
```

No exemplo anterior, se o pseudotime (como indicado pelo valor da repetição) é significativamente diferente entre o GMs quando as saídas estão capturadas com o mesmo tempo da referência, a seguir o problema pode ser atribuído para cronometrar o enviesamento.

> **Note**: Na plataforma agregada Cisco do 1000 Series do roteador dos serviços, devido à arquitetura da plataforma, o datapath no processador do fluxo do quantum (QFP) refere realmente o pulso de disparo de parede contando tiquetaques do pseudotime. Isto criar problemas com o TBAR quando as mudanças do tempo da parede devido à sincronização de NTP. Este problema é documentado com a identificação de bug Cisco CSCum37911.

Preservação do encabeçamento PMTUD e GETVPN

Com GETVPN, o Path MTU Discovery (PMTUD) não trabalha entre o GMs de criptografia e de descriptografia, e grandes pacotes com don't fragment (DF) o jogo do bit pode obter blackholed. A razão que esta não trabalha é devido à preservação do encabeçamento GETVPN onde a origem de dados/endereços de destino é preservada no ESP que encapsula o encabeçamento. Isto é descrito nesta imagem:



Enquanto a imagem mostra, o PMTUD divide com o GETVPN com este fluxo:

1. O grande pacote de dados chega no GM1 de criptografia.
2. O pacote ESP da cargo-criptografia é enviado fora de GM1 e entregado para o destino.
3. Se há um enlace de trânsito com o IP MTU de 1400 bytes, o pacote ESP estará deixado cair, e uma mensagem demasiado grande do pacote ICMP 3/4 será enviada para o origem do pacote, que é a fonte do pacote de dados.
4. O pacote ICMP3/4 é para o fim host devido ao ICMP não excluído da política de criptografia GETVPN, ou deixado cair deixado cair desde que não sabe qualquer coisa sobre o pacote ESP (payload não-autenticado).

Em resumo, o PMTUD não trabalha com GETVPN hoje. A fim trabalhar em torno desta edição, Cisco recomenda estas etapas:

1. O implementar “IP tcp ajusta-mss” a fim reduzir a ordem o da lata do tamanho do segmento do pacote de TCP acomoda o MTU de caminho das despesas gerais e do mínimo da criptografia no transit network.
2. Cancele o bit DF no pacote de dados como chegam no GM de criptografia a fim evitar o PMTUD.

Edições genéricas de Dataplane do IPsec

A maioria do Troubleshooting do dataplane do IPsec é como a pesquisa de defeitos de túneis de IPsec pontos a ponto tradicionais. Um dos problemas comuns é %CRYPTO-4-RECVD_PKT_MAC_ERR. Veja o Mensagem de Erro do Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR:" com perda do sibilo sobre o Troubleshooting do túnel de IPsec para mais detalhes do Troubleshooting.

Problemas conhecidos

Esta mensagem pode ser gerada quando um pacote de IPsec é recebido que não combine um SPI no SADB. Veja a identificação de bug Cisco CSCtd47420 - GETVPN - CRYPTO-4-RECVD_PKT_NOT_IPSEC relatado para o pkt que não combina o fluxo. Um exemplo é:

```
GM2#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.743 EST Wed Nov 13 2013
```

```
Anti-replay Information For Group G1:
Timebased Replay:
Replay Value              : 625866.51 secs
Input Packets : 4 Output Packets : 4
Input Error Packets : 2 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs
```

Esta mensagem deve ser %CRYPTO-4-RECVD_PKT_INV_SPI, que é o que obtém relatado para o IPsec tradicional assim como em algumas plataformas de hardware tais como o ASR. Este problema cosmético foi fixado pela identificação de bug Cisco CSCup80547: Erro em relatar CRYPTO-4-RECVD_PKT_NOT_IPSEC para ESP pak.

> **Note**: Estas mensagens podem às vezes parecer devido a um outro erro CSCup34371 GETVPN: O GM GETVPN para de decrytping o tráfego depois que o TEK rekey.

Neste caso, o GM não pode decifrar o tráfego GETVPN, embora tenha IPsec válido SA no SADB (o SA que está sendo rekeyed). O problema desaparece assim que o SA expirar e for removido do SADB. Esta edição causa a indisponibilidade significativa, porque o TEK rekey é executado adiantado. Por exemplo, a indisponibilidade pode ser 22 minutos no caso de uma duração de TEK de 7200 segundos. Veja a descrição do erro para a condição exata que deve ser estada conforme a fim encontrar este erro.

Pesquise defeitos GETVPN nas Plataformas que executam o Cisco IOS XE

Comandos para Troubleshooting

As Plataformas que executam o Cisco IOS XE têm aplicações específicos da plataforma, e exigem frequentemente a eliminação de erros específico da plataforma para edições GETVPN. Está aqui uma lista de comandos usados tipicamente a fim pesquisar defeitos GETVPN nestas Plataformas:

show crypto eli todo

mostre estatísticas da política do IPsec do software de plataforma

mostre o inventário do active fp do IPsec do software de plataforma

mostre a qfp do hardware da plataforma o IPsec ativo spd todo da característica

mostre a qfp do hardware da plataforma a gota das estatísticas ativas clara

mostre a qfp do hardware da plataforma a gota ativa dos dados do IPsec da característica clara

show crypto ipsec sa

mostre o gdoi cripto

mostre o IPsec cripto interno

debug crypto ipsec

erro do IPsec do debug crypto

estados do IPsec do debug crypto

mensagem IPSec do debug crypto

HW-req do IPsec do debug crypto

do debug crypto do gdoi gm detalhe infra

o gm do gdoi do debug crypto rekey o detalhe

Problemas comuns ASR1000

A política de IPsec instala a falha (o Re-registro contínuo)

Um GM ASR1000 pôde continuar a registrar-se ao server chave se a crypto-engine não apoia a política de IPsec ou o algoritmo recebida. Por exemplo, no Nitrox baseou Plataformas ASR (tais como ASR1002), série-b ou as políticas SHA2 não são apoiadas e esta pode causar os sintomas contínuos do re-registro.

Edições comuns da migração/elevação

Limitação ASR1000 TBAR

Na plataforma ASR1000, o reparo da identificação de bug Cisco CSCum37911 introduziu uma limitação nesta plataforma onde o tempo TBAR de menos de 20 segundos não é apoiado. Veja limitações para GETVPN em IOS-XE.

Este erro do realce foi aberto para levantar esta limitação, a identificação de bug Cisco CSCuq25476 - ASR1k precisa de apoiar um tamanho de janela GETVPN TBAR de menos de 20 segundos.

Atualização: Esta limitação tem sido levantada desde com o reparo para a identificação de bug Cisco CSCur57558, e é já não uma limitação em XE3.10.5, em XE3.13.2 e em código mais recente.

Igualmente note-o, para um GM que seja executado em Plataformas do Cisco IOS XE (ASR1k ou ISR4k), é altamente recomendado que o dispositivo executa uma versão com o reparo para esta edição se TBAR é permitido; Identificação de bug Cisco CSCut91647 - GETVPN em IOS-XE: O GM deixa cair incorretamente pacotes devido à falha TBAR.

Edição da classificação ISR4x00

Uma regressão foi encontrada na plataforma ISR4x00 onde as políticas da negação são ignoradas. Para detalhes, veja a identificação de bug Cisco CSCut14355 - GETVPN - O GM ISR4300 ignora nega a política.

Informações Relacionadas

- Transporte cifrado grupo VPN (GET VPN) - Cisco Systems
- Suporte Técnico e Documentação - Cisco Systems