Handleiding voor probleemoplossing in VPN

Inhoud

Inleiding

Dit document is bedoeld om een gestructureerde methodologie voor probleemoplossing en handige tools te bieden om problemen op het gebied van groepsversleuteld transport (GETVPN) te identificeren en te isoleren, en om mogelijke oplossingen te bieden.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- GETVPN
  Officiële GETVPN-configuratiegids
  Officiële gids voor ontwerpen en implementeren van VPN

- SLB: servergebruik

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Methodologie voor GETVPN-probleemoplossing

Zoals bij de meeste problemen met ingewikkelde technologieën is de sleutel in staat om het probleem te isoleren van een bepaalde functie, subsysteem of component. De GETVPN-oplossing bestaat uit een aantal functieonderdelen, met name:

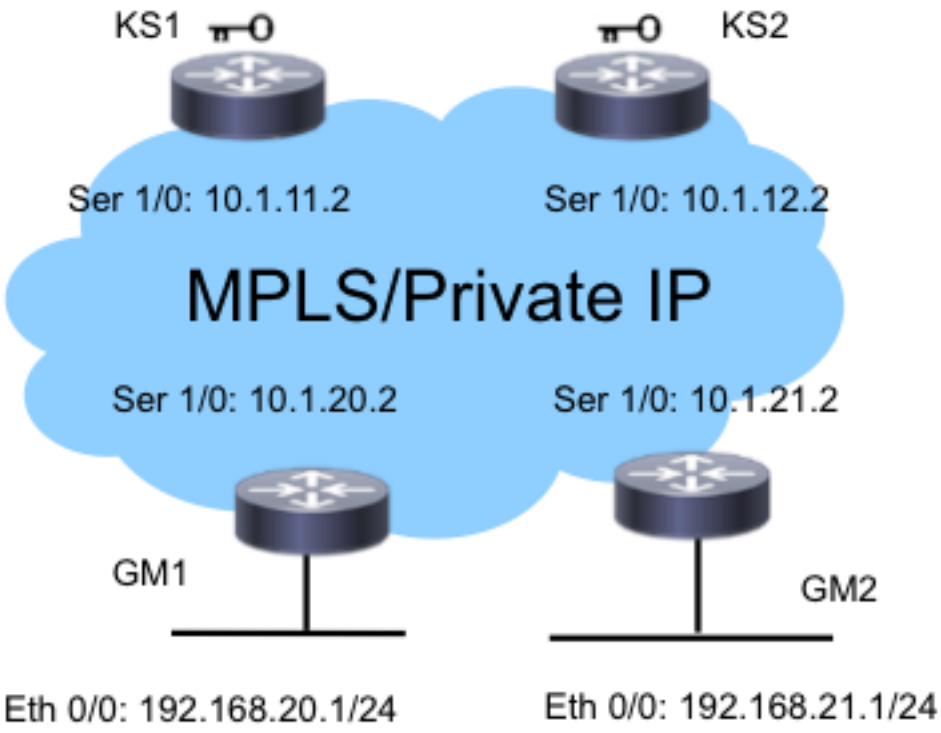
- Internet Key Exchange (IKE) - gebruikt tussen groepslid (GM) en Key Server (KS), en tussen COOP (Cooperative Protocol) KSs om het besturingsplane te authentiseren en te beschermen.
- Group Domain of Interpretation (GDOI) - Protocol dat voor de KS wordt gebruikt om groepsleutels te verdelen en sleuteldiensten zoals rekey aan alle GM's te leveren.
- COOP - Protocol gebruikt voor de KS's om met elkaar te communiceren en redundantie te bieden.
- Bewaren van header - IPsec in tunnelmodus die de oorspronkelijke pakketheader voor levering van end-to-end verkeer bevestigt.
- Time Based Anti-Replay (TBAR) - Replay-detectiemechanisme, gebruikt in een

groepssleutelomgeving.

Het biedt ook een uitgebreide reeks gereedschappen voor het oplossen van problemen om het proces van probleemoplossing te vergemakkelijken. Het is belangrijk om te begrijpen welke van deze gereedschappen beschikbaar zijn en wanneer ze geschikt zijn voor elke taak om een oplossing te vinden. Wanneer u problemen oplost, is het altijd een goed idee om met de minste opdringerige methoden te beginnen zodat de productieomgeving niet negatief wordt beïnvloed. De sleutel tot deze gestructureerde probleemoplossing is om het probleem af te breken tot een probleem met een controle of een datalevak. U kunt dit doen als u het protocol of de gegevensstroom volgt en de verschillende hier gepresenteerde gereedschappen gebruikt om ze te controleren.

Referentietechnologie

Deze GETROKKEN VPN topologie en het adresschema worden gebruikt door de rest van dit het oplossen van problemen document.



Naslagconfiguraties

- 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
```

Opmerking: De KS2- en GM2-configuraties zijn hier niet opgenomen voor de beknoptheid.

Terminologie

- **KS** - sleutelserver
- **GM** - groepslid
- **COOP** - samenwerkingsprotocol
- **TBAR** - Tijdgebaseerde antireplay
- **KEK** - sleutel voor encryptie
- **TEK** - Verkeersencryptie-toets

Voorbereiding van de opslagfaciliteit en andere beste praktijken

Voordat u begint met het oplossen van problemen, zorg er dan voor dat u de loginstallatie hebt voorbereid zoals hier beschreven. Hieronder worden ook een aantal optimale werkwijzen genoemd:

- Controleer de routerhoeveelheid vrij geheugen en stel de **houtkap** op **gebufferd** voor **het foutoptreden** tot een grote waarde (10 MB of meer indien mogelijk).

- Uitschakelen van loggen op de console-, monitor- en syslogservers.

- Retourneert de houtbufferinhoud met de opdracht log **tonen**, met regelmatige tussenpozen, elke 20 minuten tot een uur, om logverlies door hergebruik van de buffer te voorkomen.

- Wat er ook gebeurt, voer de **show tech-**opdracht van de getroffen GM's en KSs in en onderzoek de output van de opdracht **ip** wereldwijd en elke Virtual Routing and Forwarding (VRF) die nodig is.

- Gebruik Network Time Protocol (NTP) om de kloktijd te synchroniseren tussen alle apparaten die worden gezuiverd. Tijd van milliseconde (msec) toe te passen voor zowel debug- als logberichten:

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

- Zorg ervoor dat de uitvoer van het showcommando op tijd wordt geplaatst.

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

- Wanneer u showcommando outputs verzamelt voor besturingsplangebeurtenissen of tellers van het gegevensvliegtuig, verzamelt u altijd meerdere iteraties van dezelfde output.

Probleemoplossing voor problemen met VPN-besturingsplane

besturingsplane: alle protocolgebeurtenissen die hebben geleid tot de oprichting van de beleids- en beveiligingsassociatie (SA) op de GM, zodat deze klaar zijn om het gegevensverkeer te versleutelen en te decrypteren. Enkele van de belangrijkste controlepunten in het GETVPN-besturingsplane zijn:

Besturingssysteem: beste praktijken afluisteren

Deze optimale werkwijzen voor probleemoplossing zijn niet specifiek voor VPN; zij zijn van toepassing op bijna elk besturingsplandebug . Het is van cruciaal belang om deze beste praktijken te volgen om de meest effectieve oplossing te garanderen:

- Schakel de houtkap uit en gebruik de houtkapbuffer of het slingermiddel om de defecten te verzamelen.
- Gebruik NTP om routerklokken te synchroniseren op alle apparaten die worden gezuiverd.
- Laat msec timestamping voor debug en logberichten toe:

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

- Zorg ervoor dat de uitvoer van het showcommando voorzien is van een tijdelijke stempel zodat ze gecorreleerd kunnen worden met de debug uitvoer:

```
terminal exec prompt timestamp
```

- Gebruik indien mogelijk voorwaardelijke debugging in een schaalomgeving.

Tools voor probleemoplossing in VPN-besturingsplane

Opdrachten voor VPN-weergave

In het algemeen, zijn dit de opdrachtoutput die u zou moeten verzamelen voor bijna alle GETVPN problemen.

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
```

GETVPN-signaleringsberichten

GETVPN biedt een uitgebreide reeks syfilosofische berichten voor belangrijke protocolgebeurtenissen en foutvoorwaarden. De oplossing moet altijd de eerste plaats zijn om te kijken wanneer u een oplossing voor GETVPN uitvoert.

Common KS Syslog Messaging

Syslog-berichten	verklaring
COOP_CONFIG_MISMATCH	De configuratie tussen de primaire en de secundaire sleutelserver is niet aangepast.
COOP_KS_ELECTION	De lokale sleutelserver heeft het verkiezingsproces in een groep ingevoerd
COOP_KS_REACH	De bereikbaarheid tussen de geconfigureerde coöperatieve sleutelservers hersteld.
COOP_KS_TRANS_TO_PRI	De lokale sleutelserver ging over naar een primaire rol van een secundaire server in een groep.
COOP_KS_UNAUTH	Een geautoriseerde externe server probeerde contact op te nemen met de lokale sleutelserver in een groep, wat als een vijandige gebeurtenis kon wo gezien.
COOP_KS_ONREACH	De bereikbaarheid tussen de geconfigureerde coöperatieve sleutelservers verloren, wat als een vijandige gebeurtenis kan worden beschouwd.
KS_GM_REVOKED	Tijdens het protocol probeerde een ongeautoriseerd lid zich aan te sluiten een groep, die als een vijandig evenement kon worden beschouwd.
KS_SEND_MCAST_REKEY	Verzenden van multicast opnieuw.
KS_SEND_UNICAST_REKEY	Verzenden van eenhoorapparaat.
KS_ONBEVOEGD	Tijdens het registratie protocol van GDOI probeerde een niet-geautoriseerd zich aan te sluiten bij een groep, die als een vijandige gebeurtenis kon wor gezien.
ONBEVOEGD_IPADDR	Het registratieverzoek is ingetrokken omdat het verzoekende apparaat niet gemachtigd om zich bij de groep aan te sluiten.

GGM-systeemmeldingen

Syslog-berichten	verklaring
GM_CLEAR_REGISTER	De **duidelijke crypto gdoi** opdracht is uitgevoerd door het lokale groepsli
GM_CM_ATTACH	Een crypto kaart is aangesloten voor het lokale groepslid.
GM_CM_DETACH	Een crypto kaart is losgekoppeld voor het lokale groepslid&.
GM_RE_REGISTER	IPsec SA, gemaakt voor één groep, is mogelijk verlopen of gewist. Moet opnieuw worden geregistreerd op de sleutelserver.
GM_RECV_REKEY	Rekey heeft ontvangen.
GM_REGS_COMPL	Registratie voltooid.
GM_REKEY_TRANS_2_MULTI	Groepslid is overgestapt van het gebruik van een unicast rekey mechan naar het gebruik van een multicast mechanisme.

GM_REKEY_TRANS_2_UNI	Groepslid is overgestapt van het gebruik van een multicast rekey mechanisme naar het gebruik van een unicast mechanisme.
PSEUDO_TIME_GROOT	Een groepslid heeft een pseudotijd ontvangen met een waarde die grotendeels afwijkt van zijn eigen pseudotijd.
REPLAY_FAILLE	Een groepslid of een sleutelserver heeft een anti-replay controle mislukt

Opmerking: De rood gemarkeerde berichten zijn de meest voorkomende of belangrijke berichten die in een GETVPN-omgeving worden gezien.

Wereldwijde encryptie en GDOI-uitvindingen

GETVPN-afstanden zijn verdeeld:

1. Eerst door het apparaat waarop u een oplossing wilt vinden.
```
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. Ten tweede, het type probleem dat u wilt oplossen.
```
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. Ten derde door het niveau van het debuggen dat moet worden ingeschakeld. In versie 15.1(3)T en later zijn alle GDOI-functies standaard standaard ontwikkeld om deze debug-niveaus te hebben. Dit werd ontworpen om problemen op te lossen in grote GETVPN-omgevingen met genoeg debugging granularity. Wanneer u GETVPN-problemen reinigt, is het belangrijk om het juiste debug-niveau te gebruiken. Als algemene regel, begin met het laagste debug niveau, dat is het foutenniveau, en verhoog de het debuggen granularity wanneer nodig.
```
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
```

GDOI-conditionering voor afluisteren

In Cisco IOS® versie 15.1(3)T en hoger werd GDOI voorwaardelijke debugging toegevoegd om probleemoplossing te ondersteunen bij VPN in een grootschalige omgeving. Dus alle versies van Internet Security Association en Key Management Protocol (ISAKMP) en GDOI kunnen nu worden geactiveerd met een voorwaardelijk filter op basis van de groep of peer IP-adres. Voor de meeste problemen met GETVPN is het goed om zowel ISAKMP als GDOI uitzettingen met het juiste voorwaardelijke filter mogelijk te maken, omdat GDOI-uitzettingen alleen GDOI-specifieke operaties tonen. Voltooi de volgende twee eenvoudige stappen om voorwaardelijke bijdragen van ISAKMP en GDOI te gebruiken:

1. Stel het voorwaardelijke filter in.

2. Schakel zoals gewoonlijk het betreffende ISAKMP en GDOI in.

Bijvoorbeeld:

```
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)
```

> Opmerking: Met zowel ISAKMP als GDOI voorwaardelijke deposito's, om debug-berichten te vangen die niet de voorwaardelijke filterinformatie hebben, bijvoorbeeld het IP-adres in het debug-pad, kan de **ongeëvenaarde** vlag worden ingeschakeld. Dit moet echter met de nodige voorzichtigheid worden gebruikt omdat het een grote hoeveelheid debug-informatie kan veroorzaken.

GDOI-Event Traces

Dit is toegevoegd in versie 15.1(3)T. Event Tracering biedt licht gewicht, altijd-on tracering voor belangrijke GDOI-gebeurtenissen en fouten. Er is ook exit-path-tracering die is ingeschakeld voor uitzonderingen. De sporen van de gebeurtenis kunnen meer informatie over de gekregen van de gebeurtenis van VPN dan traditionele syslogs verstrekken.

De GDOI gebeurtenis sporen worden door gebrek in staat gesteld en kunnen van de spoorbuffer met de **show monitor gelijkspooropdracht** worden teruggewonnen.

```
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
```

Het spoor van het uitgang verstrekt gedetailleerde informatie over exit pad, dat uitzondering en foutvoorwaarden is, met de traceeroptie die standaard ingeschakeld is. De tracbacks kunnen dan

worden gebruikt om de exacte codevolgorde te decoderen die tot de voorwaarde van het exit pad heeft geleid. Gebruik de optie **detail** om de sporen van de spoorbuffer op te halen:

```
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
```

De standaard buffergrootte is 512 items, en dit zou niet genoeg kunnen zijn als het probleem intermitterend is. Om deze standaard opties grootte te verhogen, kan de configuratie van de gebeurtenis spoorconfiguratie worden gewijzigd zoals hier wordt getoond:

```
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
```

Controleer VPN-besturingsplane en problemen

Hier zijn een aantal gemeenschappelijke problemen met betrekking tot het besturingsplane voor GETVPN. Om te kunnen herhalen, wordt het besturingsplane gedefinieerd als alle onderdelen van de GETVPN-functie die vereist zijn om dataplane-encryptie en decryptie op de GM's mogelijk te maken. Op een hoog niveau vereist dit succesvolle GM-registratie, veiligheidsbeleid en het downloaden/installeren van SA, en de daaropvolgende KEK/TEK rekey.

COOP-instellingen en beleidsvorming

Om na te gaan en te controleren of de KS het beveiligingsbeleid en de daarmee verbonden KEK/TEK succesvol heeft opgezet, dient u:

```
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
```

Eén gemeenschappelijk probleem met de instelling van het KS-beleid is wanneer er verschillende beleidsvormen zijn ingesteld tussen de primaire en secundaire KS. Dit kan leiden tot onvoorspelbaar KS-gedrag en deze fout wordt gerapporteerd:

```
%GDOI-3-COOP_CONFIG_MISMATCH: WARNNING: replay method configuration between
Primary KS and Secondary KS are mismatched
```

Momenteel is er geen automatische configuratie-sync tussen primaire en secundaire KS, zodat deze handmatig moeten worden gecorrigeerd.

Omdat COOP een kritieke (en vrijwel altijd verplichte) configuratie is voor GETVPN, is het van essentieel belang om ervoor te zorgen dat COOP correct werkt en dat de COOP KS-rollen correct zijn:

```
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
```

Bij een functionele COOP-instelling dient deze protocolstroom te worden gevolgd:

IKE Exchange > ANN met uitgewisselde COOP-prioriteiten > COOP-verkiezingen > ANN van primair naar secundair KS (beleid, GM-database en sleutels)

Wanneer COOP niet correct werkt, of als er een COOP-splitsing is, zoals meerdere KS's de primaire KS worden, moeten deze debugs worden verzameld om een oplossing te vinden:

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

IKE instellen

Voor GETVPN is een succesvolle IKE-uitwisseling vereist om het controlekanaal voor het daaropvolgende beleid en de SA-download te kunnen beveiligen. Aan het eind van de succesvolle IKE-uitwisseling wordt een GDOI_REKEY gecreëerd.

In versies eerder dan Cisco IOS 15.4(1)T, kan GDOI_REKEY met de opdracht **Show crypto isakmp als** opdracht worden getoond:

```
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#
```

In Cisco IOS 15.4(1)T en later wordt deze GDOI_REKEY SA getoond met de **show crypto gdoi rekey sa** opdracht:

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

> Opmerking: Nadat de eerste IKE-uitwisseling is voltooid, worden het daaropvolgende beleid en de sleutels van de KS naar de GM gestuurd met behulp van GDOI_REKEY SA. Dus er is geen rekey voor GDOI_IDLE SA wanneer ze verlopen; zij verdwijnen wanneer hun leven verstrijkt . Er moet echter altijd GDOI_REKEY SA op de GM staan om rekeys te kunnen ontvangen.

De IKE-uitwisseling voor GETVPN is niet anders dan de IKE die in traditionele point-to-point IPsec-tunnels wordt gebruikt, zodat de methode om problemen op te lossen hetzelfde blijft. Deze details moeten worden verzameld om IKE-authenticatie problemen op te lossen:

```
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)
```

Registratie, beleidsdownloads en end-of-life details

Zodra IKE-verificatie slaagt, registreert GM bij de KS. Deze syslogberichten worden verwacht wanneer ze op de juiste manier worden weergegeven:

```
%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
```

Het beleid en de toetsen kunnen met deze opdracht worden geverifieerd:

```
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#
```

Opmerking: Met GETVPN gebruiken inkomende en uitgaande SA's dezelfde SPI.

Met de registratie van GETVPN en de installatie van het beleid type problemen, zijn deze problemen nodig om een oplossing te vinden:

```
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)
```

Opmerking: Afhankelijk van het resultaat van deze uitgangen kunnen extra uitzettingen nodig zijn.

Aangezien GETVPN registratie normaal gesproken direct na het GGM-herladen optreedt, kan dit EEM-script behulpzaam zijn bij het verzamelen van deze gegevens:

```
event manager applet debug
event syslog pattern "RESTART"
action 1.0 cli command "enable"
action 2.0 cli command "debug crypto gdoi all all"
```

Rekey

Zodra de GGM's bij de KS zijn geregistreerd en het GETVPN-netwerk correct is opgezet, is de primaire KS verantwoordelijk voor het versturen van aanplakberichten naar alle GG's die er bij zijn geregistreerd. De rekey-berichten worden gebruikt om alle beleid, sleutels en pseudotijden op de GM's te synchroniseren. De rekey boodschappen kunnen worden verstuurd via een unicast of een multicast methode.

Dit syslogbericht wordt op de KS gezien wanneer het rekey bericht wordt verstuurd:

```
%GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey for group G1 from address
10.1.11.2 with seq # 11
```

Bij de GM's is dit de syslog die gezien wordt als hij de rekey krijgt:

```
%GDOI-5-GM_RECV_REKEY: Received Rekey for group G1 from 10.1.11.2 to 10.1.20.2
with seq # 11
```

RSA Key Pair-vereiste voor Rekey op KS

Rekey-functionaliteit vereist de aanwezigheid van RSA-toetsen op de KS. De KS verschaft de

openbare sleutel van de RSA-sleutelpaar aan de GM door middel van dit beveiligde kanaal tijdens de registratie. De KS tekent vervolgens de GDOI-berichten die naar de GM zijn gestuurd met de particuliere RSA-toets in de GDOI SIG-lading. De GM ontvangt de GDOI-berichten en gebruikt de openbare RSA-toets om het bericht te controleren. De berichten tussen de KS en de GM worden versleuteld met de KEK, die ook tijdens de registratie aan de GM wordt verspreid. Nadat de registratie is voltooid, worden de volgende exemplaren versleuteld met de KEK en getekend met de particuliere RSA-toets.

Als de RSA-toets niet aanwezig is op de KS tijdens GM-registratie, verschijnt dit bericht op de syslog:

```
%GDOI-1-KS_NO_RSA_KEYS: RSA Key - get : Not found, Required for group G1
```

Wanneer de sleutels niet op de KS staan, registreert de GM voor het eerst, maar de volgende rekey valt niet op de KS. Uiteindelijk verlopen de bestaande toetsen op het GM en herregistreert het opnieuw.

```
%GDOI-4-GM_RE_REGISTER: The IPSec SA created for group G1 may have expired/been
cleared, or didn't go through. Re-register to KS.
```

Aangezien het RSA-sleutelpaar wordt gebruikt om de rekey-berichten te tekenen, **MOET** het tussen het primaire en alle secundaire KS hetzelfde zijn. Dit zorgt ervoor dat bij een primaire KS-storing de rekys die door een secundaire KS (de nieuwe primaire KS) worden verstuurd, nog steeds naar behoren door de GM's kunnen worden gevalideerd. Wanneer het RSA-sleutelpaar op de primaire KS genereert, moet het sleutelpaar met de **uitvoerbare** optie gecreëerd worden zodat ze naar alle secundaire KS's kunnen worden geëxporteerd om aan deze eis te voldoen.

Rekey Troubleshooter

KEK/TEK rekstoffout is een van de meest voorkomende GETVPN-problemen die bij klantenimplementaties zijn ondervonden. De volgende stappen moeten worden gevolgd bij het oplossen van problemen:

1. Waren de rekeys verstuurd door de KS?

   Dit kan worden gecontroleerd door een observatie van het %GDOI-5-KS_SEND_UNICAST_REKEY syslog bericht of preciezer met deze opdracht:

```
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
```

   Het aantal rekeys dat opnieuw wordt doorgegeven, is een indicatie van rekruteringsontvangstpakketten die niet door de KS zijn ontvangen en dus van mogelijke rekey-kwesties. Houd in gedachten dat de GDOI rekey UDP als een onbetrouwbaar

transportmechanisme gebruikt, zodat sommige druppels verwacht kunnen worden afhankelijk van de betrouwbaarheid van het onderliggende transportnetwerk, maar een trend van toenemende wederopnames moet altijd worden onderzocht.

Er kunnen ook gedetailleerdere cijfers worden verkregen per GGM. Dit is meestal de eerste plaats om op zoek te gaan naar mogelijke problemen.

```
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. Worden de rekey-pakketten afgeleverd in het onderliggende infrastructuurnetwerk?

   Er moet worden gevolgd hoe IP-probleemoplossing langs het pad voor het doorsturen van de formulieren kan worden toegepast om te voorkomen dat de pakketten in het transitnetwerk tussen KS en GM worden gedropt. Sommige gemeenschappelijke probleemoplossing die hier worden gebruikt, zijn invoer/uitvoer van toegangscontrolelijsten (ACL's), NetFlow en pakketvastlegging in het transitnetwerk.

3. Hebben de rekey-pakketten het GDOI-proces bereikt voor rekey-verwerking?

   Controleer de GGM-cijfers:

```
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. Kwam het nieuwe ontvangstpakket terug naar de KS?

Volg stap 1 tot en met 3 om het zeer belangrijke ontvangstpakket van de GM terug naar de KS te traceren.

Muticast Rekey

Multicast rekey onderscheidt zich in deze opzichten van unicast rekey:

- Aangezien multicast wordt gebruikt om deze rekey pakketten van de KS naar de GM's te transporteren, hoeven de KS de rekey pakketten zelf niet te reproduceren. De KS stuurt slechts één kopie van het rekenset en zij worden gerepliceerd in het multicast-enabled netwerk.
- Er is geen erkenningsmechanisme voor multicast rekey, dus als een GM niet het rekey-pakje zou ontvangen, zouden de KS er geen kennis van hebben en zal hij daarom nooit een GM uit zijn GM-database verwijderen. En omdat er geen erkenning is, zullen de KS altijd de rekey pakketten opnieuw verzenden op basis van de rekey retransmission configuratie.

Het meest voorkomende multicast rekey-probleem is wanneer de rekey niet op de GM wordt ontvangen. Hiervoor zouden een aantal mogelijke oorzaken kunnen bestaan, zoals:

- Packet-leveringsprobleem in de multicast-routinginfrastructuur
- End-to-end multicast routing is niet ingeschakeld binnen het netwerk

De eerste stap naar het oplossen van een probleem met multicast rekey is om te zien of rekey werkt wanneer men van de multicast naar de unicast methode overschakelt.

Zodra u hebt vastgesteld dat het probleem specifiek is voor multicast rekey, controleert u of KS de rekey naar het multicast adres dat is opgegeven.

```
%GDOI-5-KS_SEND_MCAST_REKEY: Sending Multicast Rekey for group G1 from address
10.1.11.2 to 226.1.1.1 with seq # 6
```

Test multicast connectiviteit tussen de KS en GM met een ICMP-verzoek (Internet Control Message Protocol) naar het multicast-adres. Alle GM's die deel uitmaken van de multicast groep moeten op het ping reageren. Zorg ervoor dat ICMP voor deze test is uitgesloten van het KS-encryptiebeleid.

```
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
```

Als de multicast ping-test mislukt, moet de multicast-probleemoplossing worden uitgevoerd, wat niet binnen het bereik van dit document valt.

Relay-controle van besturingsplane

Symptoom

Wanneer klanten hun GM naar een nieuwe Cisco IOS versie upgraden, kunnen zij KEK rekey defecten ervaren met dit bericht dat in de syslog wordt waargenomen:

```
%GDOI-3-GDOI_REKEY_SEQ_FAILURE: Failed to process rekey seq # 1 in seq payload for
group G1, last seq # 11
%GDOI-3-GDOI_REKEY_FAILURE: Processing of REKEY payloads failed on GM 10.1.13.2 in the group G1,
with peer at 10.1.11.2
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of GDOI mode failed with peer at 10.1.11.2
```

Dit gedrag wordt veroorzaakt door een interoperabiliteitsprobleem dat wordt geïntroduceerd met de terugspeelcontrole die wordt toegevoegd voor de communicatie van het besturingsplane. Met name een KS die de oudere code runt zal het KEK rekey sequentienummer terugstellen naar 1, en dit zal worden laten vallen door de GM die de nieuwe code runt wanneer hij dat interpreteert als een gerespeeld rekey pakket. Voor meer informatie, zie Cisco bug-ID CSCta05809 (GETVPN: GETVPN-besturingsplane (geschikt om opnieuw af te spelen) en VPN-configuratierestricties.

Achtergrond

Met GETVPN kunnen de berichten van het besturingsplane tijdgevoelige informatie bij zich hebben om de tijdgebaseerde antireplay-controle te kunnen leveren. Daarom zijn deze berichten op zichzelf gericht tegen herhalingsbescherming om te garanderen dat de tijd werkelijk gegroeid is. Deze berichten zijn:

- **Rekey Messages** van KS naar GM
- **COOP-berichten** tussen KS

Als onderdeel van deze anti-replay security implementatie werden sequentienummer controles toegevoegd om weergegeven berichten te beschermen, evenals een pseudotime controle wanneer TBAR werd geactiveerd.

Oplossing

Om dit probleem op te lossen, moeten zowel GM als KS naar Cisco IOS-versies worden bijgewerkt nadat de herspeeloptie van het besturingsplane is ingeschakeld. Met de nieuwe Cisco IOS code, stelt KS het sequentienummer niet terug naar 1 voor een KEK rekey, maar in plaats daarvan blijft het het huidige sequentienummer gebruiken en stelt alleen het sequentienummer voor TEK rekeys in.

Deze Cisco IOS-versies hebben de functies Replay Control:

- 12.4(15)T10
- 12.4(22)T3
- 12.4(24)T2
- 15,0(1)M en later

Overige kwesties in verband met terugspelen

- COOP-storing door ANN-berichten bij niet-terugspeelcontrole (Cisco bug-ID CSCtc52655)

Standaardinstellingen van besturingsplane terugspelen

Verzamel deze informatie voor andere fouten in het besturingsplane en zorg ervoor dat de tijd wordt samengevat tussen de KS en GM.

- Syslog van zowel GM als KS

- ISAKMP-uitvindingen
- GDOI debugs (rekey and replay) van zowel KS als GM

Problemen met pakketfragmentatie bij besturingsplane

Met GETVPN is de fragmentatie van pakketten van het besturingsplane een gemeenschappelijk probleem en kan het zich in een van deze twee scenario's manifesteren wanneer de pakketten van het besturingsplane groot genoeg zijn dat ze IP-fragmentatie nodig hebben:

- Packet van GETVPN COOP-aankondiging
- Packet over GETVPN

COOP-aankondigingen

De aankondigingen van COOP bevatten de informatie over de GM-database en kunnen dus groot worden in een grote versie van GETVPN. Op basis van eerdere ervaringen zal een netwerk van GETVPN dat uit 1500+ GM's bestaat aankondigingen van meer dan 18024 bytes produceren, wat de grootte van de buffer van Cisco IOS is. Wanneer dit gebeurt, wijzen de KS geen buffer toe die groot genoeg is om de ANN-pakketten met deze fout te verzenden:

```
%SYS-2-GETBUF: Bad getbuffer, bytes= 18872 -Process= "Crypto IKMP", ipl= 0, pid= 183
```

Om deze conditie te corrigeren, wordt deze bufferafstemming aanbevolen:

```
buffers huge permanent 10
buffers huge size 65535
```

Rekey Packets

GETVPN-pakketten kunnen ook de typische grootte van 1500 IP Max Transition Unit (MTU) overschrijden wanneer het encryptiebeleid groot is, zoals een beleid dat uit 8+ lijnen van Access Control Entries (ACE's) in de encryptie ACL bestaat.

Fragmentation Probleem en identificatie

In beide van de vorige scenario's moet GETVPN de gefragmenteerde UDP-pakketten correct kunnen verzenden en ontvangen om COOP of GDOI goed te kunnen laten werken. IP-fragmentatie kan een probleem zijn in bepaalde netwerkomgevingen. Een netwerk dat bestaat uit het ECMP-verzendvlak (equal Cost Multi Path) en sommige apparaten in het verzendvlak vereisen een virtuele hermontage van de gefragmenteerde IP-pakketten, zoals Virtual Fragmentation Reassembleren (VFR).

Om het probleem te identificeren, controleer de herassemblagefouten op het apparaat waar men vermoedt dat de gefragmenteerde UDP 848 pakketten niet goed worden ontvangen:

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

Als de tijdelijke instellingen voor hermontage blijven toenemen, gebruikt u de opdracht **ip-fout** debug om te bevestigen of de druppel deel uitmaakt van de rekey/COOP-pakketstroom. Zodra het is bevestigd, moet de normale IP-doorvoeroplossing worden uitgevoerd om het exacte apparaat in het doorvoervliegtuig te isoleren dat de pakketten kan hebben laten vallen. Enkele meest

gebruikte gereedschappen zijn:

- PacketCapture
- Statistieken voor verkeersgeleiding
- Statistieken voor beveiligingsfuncties (Firewall, IPS)
- VFR-statistieken

GDOI-interoperabiliteitsproblemen

In de loop der jaren zijn er diverse interoperabiliteitsproblemen gevonden met GETVPN, en het is van cruciaal belang om de Cisco IOS release versies tussen KS en GM op te merken, en tussen de KS's voor interoperabiliteitsproblemen.

Andere bekende interoperabiliteitskwesties van GETVPN zijn:

- Relay-controle van besturingsplane
- GETVPN KEK gedragsverandering
- Cisco bug-ID CSCub42920 (GETVPN: KS heeft hash in rekey ACK van eerdere GM-versies niet gevalideerd)
- Cisco bug-ID CSCuw48400 (GetVPN GM niet kan registreren of aanvullen met fouten - SIG-shash > standaard SHA-1)
- Cisco bug-ID CSCvg19281 (Multiple GETVPN GM-crashes na migratie naar nieuwe KS-paren; als een GM-versie eerder dan 3.16 is en KS van een eerdere code naar 3.16 of later is bijgewerkt, kan dit probleem zich voordoen)

GETVPN IOS-upgrade-procedure

Deze Cisco IOS-upgradeprocedure moet worden gevolgd wanneer een Cisco IOS-codeupgrade in een VPN-omgeving moet worden uitgevoerd:

1. upgrade eerst bij een tweede KS en wacht tot de COOP KS-verkiezing is voltooid.
2. Herhaal Stap 1 voor alle secundaire KSs.
3. upgrade van de primaire KS.
4. GGM's upgrade.

Probleemoplossing voor problemen met VPN-datacenter

Vergeleken met problemen in het besturingsplane is GETVPN-datavliegtuigprobleem een probleem waarbij de GM het beleid en de sleutels heeft om dataplane-encryptie en decryptie uit te voeren, maar om de een of andere reden werkt de end-to-end verkeersstroom niet. De meeste dataplane-problemen voor GETVPN hebben betrekking op generisch IPsec-verzenden en zijn niet specifiek voor VPN. Dus het meeste van de benadering voor het oplossen van problemen die hier wordt beschreven is ook van toepassing op generieke IPsec dataplane kwesties.

Met encryptieproblemen (zowel op groep gebaseerde als op paar gebaseerde tunnels) is het belangrijk om het probleem op te lossen en het probleem aan een bepaald deel van de datapath te isoleren. Met name de hier beschreven probleemoplossing is bedoeld om u te helpen deze vragen te beantwoorden:

- Welk apparaat is de schuldige - het versleutelen van router of het decrypteren van router?
- In welke richting gebeurt het probleem - toegang of stress?

Tools voor probleemoplossing in VPN-datacenters

Het oplossen van IPsec-dataplane is heel anders dan die voor het besturingsplane. Bij de dataplane zijn er gewoonlijk geen uitwerpselen die je kunt gebruiken, of op z'n minst veilig kunnen rennen in een productieomgeving. Dus de oplossing voor het probleem is zwaar afhankelijk van verschillende tellers en verkeersstatistieken die kunnen helpen het pakket langs een door:sturen pad te traceren. Het idee is om een verzameling checkpoints te ontwikkelen om zo te voorkomen dat pakketten zoals hieronder wordt aangegeven, worden verzonden:

Hier zijn een paar gereedschappen voor het fouilleren van datacenters:

- Toegangslijsten
- IP-prioriteitsaccounting
- NetFlow
- Interfacetellers
- Crypto-tellers
- IP Cisco Express Forwarding (CEF) wereldwijde en Drop Per-optie tellers
- Ingesloten pakketvastlegging (EPC)
- Debugs van datacenters (IP-pakketten en CEF-debugs)

De checkpoints in de datapath in de vorige afbeelding kunnen met deze tools worden gevalideerd:

GGM versleutelen

- Invoersignaal LAN-interface
  - Invoer ACL
  - Ingoesstroomtoevoer
  - Ingesloten pakketvastlegging
  - Boekhoudkundige voorkeuren

- Cryptomotor
  - **show crypto ipsec sa**
  - **Laat crypto ipsec als detail zien**
  - **statistieken van cryptomotorversnellers**

- IP-interface
  - Bron:
  - Ingesloten pakketvastlegging
  - Boekhouding uitvoervoorrang

decryptie GM

- Ingreress WAN-interface
    Invoer ACL
    Ingoesstroomtoevoer
    Ingesloten pakketvastlegging
    Boekhoudkundige voorkeuren

- Crypto Engine
    show crypto ipsec sa
    crypto ipsec als detail weergeven
    statistieken van cryptomotorversnellers

- Uitgebreide LAN-interface
    Bron:
    Ingesloten pakketvastlegging

Het retourpad volgt dezelfde verkeersstroom. De volgende secties hebben een paar voorbeelden van deze dataplanetools in gebruik.

Encryptie/decryptie-telers

De encryptie/decryptie tellers op een router zijn gebaseerd op een stroom van IPsec. Helaas werkt dit niet goed bij GETVPN omdat GETVPN doorgaans een 'soepele' encryptie-beleid implementeert dat alles versleutelt. Dus als het probleem alleen optreedt voor een deel van de stromen en niet alle, kunnen deze tellers ietwat moeilijk te gebruiken zijn om te oordelen of de pakketten versleuteld of ontsleuteld zijn wanneer er genoeg belangrijk achtergrondverkeer is dat werkt.

```
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

NetFlow kan worden gebruikt voor de controle van zowel het ingangsverkeer als het toegangsverkeer op beide GM's. Let op dat de GETVPN-**vergunning om het even welk** beleid **ip** heeft, het versleutelde verkeer is geaggregeerd en geeft niet de per-flow informatie. Informatie per stroom moet dan worden verzameld met de DSCP/prioriteitsmarkering die later wordt beschreven.

In dit voorbeeld wordt de netflow voor een pingelen van 100 pingelen van een gastheer achter GM1 aan een gastheer achter GM2 op de verschillende controlepunten getoond.

GGM versleutelen

Netwerkconfiguratie:

```
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-uitvoer:

```
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#
```

> Opmerking: In de vorige uitvoer * staat het drukverkeer. De eerste lijn toont zwaar versleuteld verkeer (met protocol 0x32 = ESP) uit de WAN-interface en het tweede lijn ICMP-verkeer dat de LAN-interface raakt.

decryptie GM

Configuratie:

```
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-uitvoer:

```
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#
```

DSCP/IP-prioriteitsmarkering

De uitdaging met het oplossen van een encryptie probleem is dat wanneer het pakket versleuteld is, u zicht in de lading verliest, wat de encryptie moet doen, en dat maakt het moeilijk om het pakket voor een bepaalde IP-stroom te traceren. Er zijn twee manieren om deze beperking aan te pakken wanneer het op het oplossen van een IPsec-probleem aankomt:

- Gebruik ESP-NULL als de IPsec-transformatie. IPsec voert nog steeds ESP-insluiting uit maar er wordt geen encryptie op de lading toegepast, zodat ze in een pakketvastlegging zichtbaar zijn.
- Merk een IP-stroom op met een uniek gedifferentieerd servicescodepunt (DSCP)/prioriteitsmarkering op basis van hun L3/L4-kenmerken.

ESP-NULL vereist wijzigingen op zowel tunneleindpunten als is vaak niet toegestaan op basis van

het klantenbeveiligingsbeleid. Daarom raadt Cisco doorgaans het gebruik van DSCP/prioriteitsmarkering aan.

DSCP/referentieschema

Naar S (hex)	ToS(decimal)	IP-voorrang	DSCP	Binair
0xE0	224	7 Netwerkcontrole	56 CS7	11100000
0xC0	192	6 Internetwork Control	48 CS6	11000000
0xB8	184	5 Cruciaal	46 EF	10111000
0xA0	160		40 CS5	10100000
0x88	136	4 Flash negeren	34 AF. 41	10001000
0x80	128		32 CS4	10000000
0x68	104	3 Flitser	26 AF31	01101000
0x60	96		24 CS3	01100000
0x48	72	2 Onmiddellijk	18 AF21	01001000
0x40	64		16 CS2	01000000
0x20	32	1 Prioriteit	8 CS1	00100000
0x00	0	0 Routine	0 Dflt.	00000000

Packet met DSCP/voorrang markeren

Deze methoden worden doorgaans gebruikt om pakketten te markeren met de specifieke DSCP/Precision markeringen.

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
```

Routerping

```
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>
```

Opmerking: Het is altijd een goed idee om de normale verkeersstroom en het DSCP/prioriteitsprofiel te controleren voordat u markering toepast, zodat de gemarkeerde verkeersstroom uniek is.

Monitorgemarkeerde pakketten

IP-prioriteitsaccounting

```
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
```

Interface 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
```

Ingesloten pakketvastlegging

Embedded Packet Capture (EPC) is een handig gereedschap om pakketten op het interfaceniveau op te nemen om te identificeren of een pakket een specifiek apparaat bereikt heeft. Onthoud dat EPC goed werkt voor duidelijk tekstverkeer, maar het kan een uitdaging zijn wanneer de opgenomen pakketten worden versleuteld. Daarom moeten technieken zoals DSCP/priorence-markering die eerder of andere IP-tekens zijn besproken, zoals de lengte van het IP-pakket, samen met EPC worden gebruikt om de probleemoplossing efficiënter te maken.

Cisco IOS XE-pakkettracering

Dit is een bruikbare optie om het pad voor het verzenden van functies te overtrekken op alle platforms die Cisco IOS-XE gebruiken, zoals CSR1000v, ASR1000 en ISR4451-X.

VPN-datacenter - gemeenschappelijke problemen

Problemen oplossen met de IPsec-dataplane voor GETVPN is meestal niet anders dan problemen

oplossen met traditionele point-to-point IPsec-dataplane, met twee uitzonderingen als gevolg van deze unieke dataplaneeigenschappen van GETVPN.

Tijdgebaseerde antireplay-fout

In een GETVPN-netwerk kunnen TBAR-fouten vaak moeilijk worden opgelost omdat er niet langer paarsgewijze tunnels zijn. Voltooi de volgende stappen om problemen op te lossen met VPN-TBAR-fouten:

1. Identificeer welk pakje wegens TBAR-storing is gevallen en identificeer vervolgens de versleuteling GM.

   Vóór versie 15.3(2)T is de TBAR-mislukkingscode niet het bronadres van het mislukte pakket afgedrukt, zodat het zeer moeilijk is om te identificeren welk pakket is mislukt. Dit is aanzienlijk verbeterd in versie 15.3(2)T en later, waar Cisco IOS dit afdrukt:

   ```
   %CRYPTO-4-PKT_REPLAY_ERR: decrypt: replay check failed
   connection id=13, sequence number=1

   %GDOI-4-TIMEBASED_REPLAY_FAILED: An anti replay check has failed in group G1:
   my_pseudotime = 620051.84 secs, peer_pseudotime = 619767.09 secs, replay_window =
   4 (sec), src_ip = 192.168.13.2, dst_ip = 192.168.14.2
   ```

   Een TBAR-geschiedenis is ook in deze versie geïmplementeerd:

   ```
   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
   ```

   Opmerking: De eerder genoemde verbeteringen zijn sindsdien geïmplementeerd in Cisco IOS-XE door Cisco bug-ID CSCun4935 en in Cisco IOS door Cisco bug-id CSC91811. Voor Cisco IOS versies die deze optie niet hebben gehad, **debug crypto gdoi gm replay details** kunnen ook deze informatie leveren, hoewel dit debug de informatie van de TBAR voor al verkeer (niet alleen pakketten die wegens TBAR mislukking zijn gevallen), zodat het niet mogelijk is om in een productieomgeving te lopen.

   ```
   GDOI:GM REPLAY:DET:(0):my_pseudotime is 621602.30 (secs), peer_pseudotime is 621561.14
   (secs), replay_window is 4 (secs), src_addr = 192.168.14.2, dest_addr = 192.168.13.2
   ```

2. Zodra de bron van het pakket is geïdentificeerd, moet u de versleutelde GM kunnen vinden. Vervolgens moet de pseudotimestamp op zowel de versleutel als de decryptie van GM's worden gecontroleerd op elke mogelijke pseudotime-verschuiving. De beste manier om dit te

doen zou het synchroniseren van zowel GM's als de KS naar NTP zijn en periodiek de pseudotime informatie verzamelen met een referentiesysteem klok op alle, om te bepalen of het probleem wordt veroorzaakt door klokscheefheid op de GM's.

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

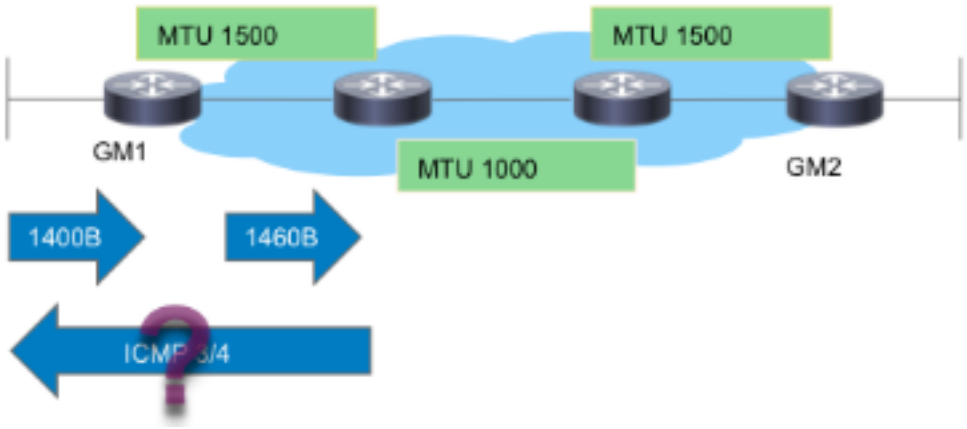
```
GM2#show crypto gdoi gm replay
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *21:06:26.743 EST Wed Nov 13 2013

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
```

In het vorige voorbeeld, als de pseudotijd (zoals aangegeven door Replay Value) aanzienlijk verschilt tussen de GM's wanneer de uitvoer wordt opgenomen met dezelfde referentietijd, kan het probleem worden toegeschreven aan klokscheefheid.

> Opmerking: Op het Cisco Aggregated Services Router 1000 Series platform, dankzij de platform architectuur, verwijst de datapath op de Quantum Flow Processor (QFP) feitelijk naar de wandklok voor het tellen van pseudotime ticks. Dit heeft problemen met TBAR veroorzaakt wanneer de tijd voor de muurkap verandert door NTP-sync. Dit probleem is gedocumenteerd voor Cisco bug-ID CSCum37911.

behoud van een PMTUD- en GETVPN-header

Met GETVPN werkt Pad MTU Discovery (PMTUD) niet tussen het versleutelen en decrypteren van GM's en grote pakketten met de optie Don't Fragment (DF)-bit kunnen worden geblokkeerd. De reden dat dit niet werkt, is vanwege GETVPN Header Conservation, waar de gegevensbron/doeladressen bewaard worden in de ESP-inkapselende header. Dit wordt in deze afbeelding getoond:



Zoals de afbeelding toont, valt PMTUD met GETVPN uit bij deze stroom:

1. Grote gegevenspakketten worden ingevoerd bij het versleutelen van GM1.
2. Het post-encryptie ESP-pakket wordt verzonden van GM1 en aan de bestemming geleverd.
3. Als er een doorvoerlink is met IP MTU van 1400 bytes, wordt het ESP-pakket verwijderd en wordt een ICMP 3/4-pakket dat te groot is, naar de pakketbron verzonden, wat de bron van het gegevenspakket is.
4. Het pakket ICMP3/4 wordt niet ingetrokken door ICMP niet uitgesloten van het encryptiebeleid van GETVPN, of door de eindhost laten vallen omdat deze niets weet over het ESP-pakket (onecht bevonden lading).

Samengevat werkt PMTUD vandaag de dag niet voor GETVPN. Om rond dit probleem te werken, raadt Cisco de volgende stappen aan:

1. Voer "ip tcp adaptieve mss" in om de grootte van het TCP-pakketsegment te verminderen om encryptie overhead en minimum pad MTU in het transitnetwerk op te nemen.
2. Schakel het PDF-bit in het gegevenspakket uit zodra ze op het coderende GM arriveren, om PMTUD te voorkomen.

Generic IPsec Dataplane-problemen

Het meeste oplossen van IPsec-dataplane is als het oplossen van traditionele point-to-point IPsec-tunnels. Een van de gebruikelijke problemen is %CRYPTO-4-RECVD_PKT_MAC_ERR. Zie Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR:" foutmelding met Ping Loss over IPsec Tunnel probleemoplossing voor meer informatie over probleemoplossing.

Bekende problemen

Dit bericht kan worden gegenereerd wanneer een IPsec-pakket wordt ontvangen dat niet overeenkomt met een SPI in de SADB. Zie Cisco bug-ID CSCtd47420 - GETVPN - CRYPTO-4-RECVD_PKT_NOT_IPSEC, gerapporteerd voor markten die niet overeenkomen met stroom. Een voorbeeld is:

```
%CRYPTO-4-RECVD_PKT_NOT_IPSEC: Rec'd packet not an IPSEC packet. (ip)
vrf/dest_addr= /192.168.14.2, src_addr= 192.168.13.2, prot= 50
```

Dit bericht moet %CRYPTO-4-RECVD_PKT_INV_SPI zijn, wat wordt gerapporteerd voor traditionele IPsec en op sommige hardwareplatforms zoals ASR. Dit cosmetische probleem is

opgelost door Cisco bug-ID CSCup80547: Fout in rapporteren van CRYPTO-4-RECVD_PKT_NOT_IPSEC voor ESP pak.

> Opmerking: Deze berichten kunnen soms verschijnen door een ander GETVPN-bug CSCup34371: GETVPN stopt met het stelen van verkeer na TEK.

In dit geval kan GM geen GETVPN-verkeer decrypteren, alhoewel het een geldig IPsec SA in de SADB heeft (de SA die wordt opgewaardeerd). Het probleem verdwijnt zodra de SA vervalt en uit de SADB wordt verwijderd. Deze kwestie veroorzaakt een aanzienlijke onderbreking, omdat TEK rekey van tevoren wordt uitgevoerd. Het bereik kan bijvoorbeeld 22 minuten zijn bij een TEK levensduur van 7200 seconden. Zie de beschrijving van de bug voor de exacte conditie waaraan moet worden voldaan om deze bug te kunnen tegenkomen.

Probleemoplossing via VPN op platforms die Cisco IOS-XE uitvoeren

Opdrachten voor probleemoplossing

Platforms die Cisco IOS-XE lopen hebben platform-specifieke implementaties en vereisen vaak platform-specifieke het zuiveren voor GETVPN kwesties. Hier is een lijst met opdrachten die doorgaans worden gebruikt om problemen met GETVPN op deze platforms op te lossen:

show crypto eli

statistieken over het ipsec-softwarebeleid tonen

actieve inventaris van platform software ipsec

show platform hardware qfp actieve optie ipsec spd

actieve statistieken van platform hardware qfp tonen

tonen het platform hardware qfp actieve optie ipsec-gegevens

show crypto ipsec sa

show crypto gdoi

toon crypto ipsec intern

crypto ipsec debug

fout van crypto ipsec

debug van crypto ipsec-statussen

crypto ipsec-bericht debug

debug van crypto ipsec hw-req

debug van crypto gdoi - grominfra - details

debug van crypto gdoi rekey - details

ASR1000 gemeenschappelijke problemen

IPsec Policy Install (continue herregistratie)

Een ASR1000 GM kan zich blijven registreren bij de Key Server als de cryptomotor het ontvangen IPsec-beleid of -algoritme niet ondersteunt. Bijvoorbeeld, op Nitrox-gebaseerde ASR-platforms (zoals ASR1002), worden Suite-B of SHA2-beleid niet ondersteund en dit kan de continue herregistratiesymptomen veroorzaken.

Gemeenschappelijke migratie-/upgrade-kwesties

ASR 1000 TBAR-beperking

Op het ASR1000-platform, introduceert Cisco bug-ID CSCum37911 een beperking op dit platform waar de TBAR-tijd van minder dan 20 seconden niet wordt ondersteund. Zie Beperkingen voor GETVPN op IOS-XE.

Dit verbeteringsfout is geopend om deze beperking op te heffen, moet Cisco bug-ID CSCuq25476 - ASR1k een venstergrootte van minder dan 20 seconden voor GETVPN TBAR ondersteunen.

Update: Deze beperking is sindsdien opgeheven met de oplossing voor Cisco bug-ID CSCur5758 en is niet langer een beperking in XE3.10.5, XE3.13.2 en latere code.

Let ook op, voor een GM die op Cisco IOS-XE platforms (ASR1k of ISR4k) draait, dat het apparaat een versie met de oplossing voor dit probleem runt als TBAR is ingeschakeld. Cisco bug-ID CSCut91647 - GETVPN op IOS-XE: wegens TBAR-storing worden pakketten onjuist verlaagd.

ISR4x00-indelingsprobleem

Er werd een regressie gevonden op het ISR4x00-platform waar het ontkenningsbeleid wordt genegeerd. Zie Cisco bug-ID CSCut14355 - GETVPN - ISR4300 GM-negers ontkennen beleid.

Gerelateerde informatie

- Group Encrypted Transport VPN (Get VPN) - Cisco Systems
- Technische ondersteuning en documentatie – Cisco Systems