GETVPN 문제 해결 가이드

목차

소개

이 문서는 GETVPN(Group Encrypted Transport VPN) 문제를 식별 및 격리하고 가능한 솔루션을 제공하는 데 도움이 되는 체계적인 문제 해결 방법론과 유용한 도구를 제공하기 위한 것입니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- GETVPN
  공식 GETVPN 컨피그레이션 가이드
  공식 GETVPN 설계 및 구현 가이드

- Syslog 서버 사용

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

GETVPN 문제 해결 방법론

복잡한 기술 문제의 대부분의 트러블슈팅과 마찬가지로, 이 키에서는 문제를 특정 기능, 하위 시스템 또는 구성 요소로 격리할 수 있습니다.GETVPN 솔루션은 다음과 같은 다양한 기능 구성 요소로 구성됩니다.

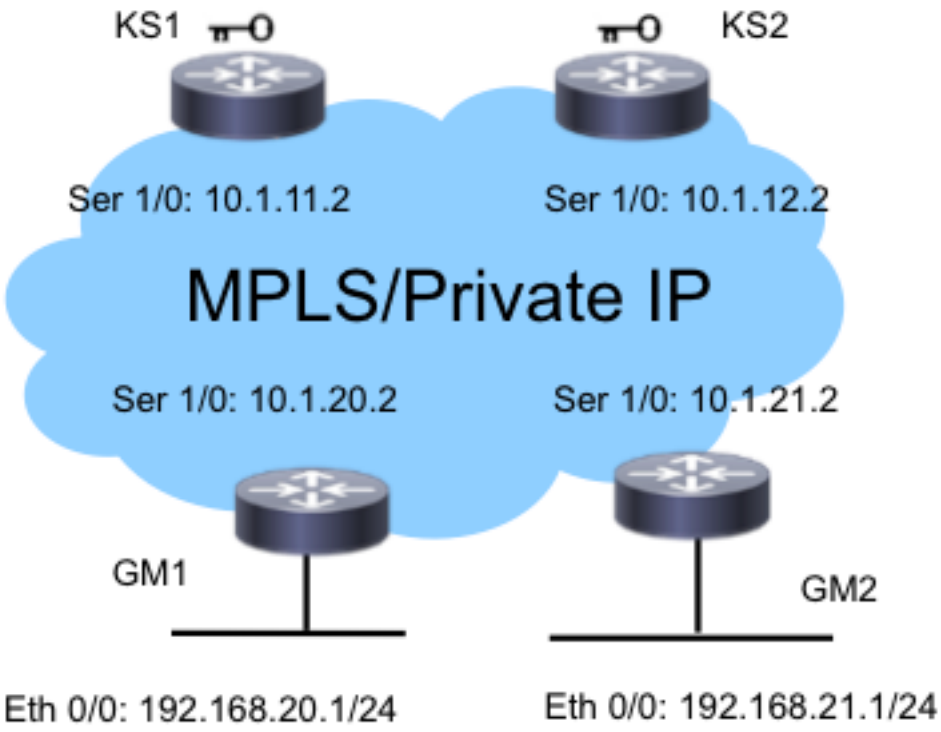
- IKE(Internet Key Exchange) - 컨트롤 플레인을 인증하고 보호하기 위해 GM(Group Member)과 KS(Key Server)와 COOP(Cooperative Protocol) KS 간에 사용됩니다.
- GDOI(Group Domain of Interpretation) - 그룹 키를 배포하고 모든 GM에 키 리키와 같은 키 서비스를 제공하기 위해 KS에 사용되는 프로토콜입니다.
- COOP - KS가 서로 통신하고 이중화를 제공하기 위해 사용되는 프로토콜입니다.
- 헤더 보존 - 엔드 투 엔드 트래픽 전달을 위해 원래 데이터 패킷 헤더를 보존하는 터널 모드의 IPsec
- TBAR(Time Based Anti-Replay) - 그룹 키 환경에서 사용되는 재생 탐지 메커니즘입니다.

또한 문제 해결 프로세스를 쉽게 수행할 수 있도록 다양한 문제 해결 도구를 제공합니다.이러한 툴 중 어떤 툴을 사용할 수 있는지, 각 문제 해결 작업에 적합한 시기를 파악하는 것이 중요합니다.문제 해결 시, 가장 적게 간섭하는 방법으로 시작하여 생산 환경이 부정적인 영향을 받지 않도록 하는 것이 좋습니다.이 정형 트러블슈팅의 핵심은 제어 또는 데이터 플레인 문제로 문제를 해결할 수 있다

는 것입니다.프로토콜 또는 데이터 플로우를 따르고 여기에 제시된 다양한 툴을 사용하여 검사하면 이를 수행할 수 있습니다.

참조 토폴로지

이 GETVPN 토폴로지 및 주소 지정 체계는 이 문제 해결 문서의 나머지 부분에서 사용됩니다.



참조 구성

- 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
```

참고:KS2 및 GM2 컨피그레이션은 여기에 포함되어 있지 않습니다.

용어

- **KS** - 키 서버
- **GM** - 그룹 멤버
- **COOP** - 협력 프로토콜
- **TBAR** - 시간 기반 재전송 방지
- **KEK** - 키 암호화 키
- **TEK** - 트래픽 암호화 키

로깅 시설 준비 및 기타 모범 사례

트러블슈팅을 시작하기 전에 여기에 설명된 대로 로깅 기능을 준비했는지 확인하십시오.다음은 몇 가지 모범 사례입니다.

- 라우터의 사용 가능한 메모리 양을 확인하고 로깅 버퍼링된 **디버깅**을 큰 값(가능한 경우 10MB 이상)으로 구성합니다.
- 콘솔, 모니터 및 syslog 서버에 대한 로깅을 비활성화합니다.
- 버퍼 재사용으로 인한 로그 손실을 방지하기 위해 **show log** 명령을 정기적으로 20분~1시간 간격으로 검색하여 로깅 버퍼 내용을 검색합니다.
- 어떤 일이 발생하든 영향을 받는 GM 및 KS에서 **show tech** 명령을 입력하고 필요한 경우 글로벌 및 관련된 각 VRF(Virtual Routing and Forwarding)에서 **show ip route** 명령의 출력을 검사합니다.
- 디버깅된 모든 디바이스 간에 클록을 동기화하려면 NTP(Network Time Protocol)를 사용합니다.디버그 및 로그 메시지 모두에 대해 밀리초(밀리초) 타임스탬프를 활성화합니다.

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

- show 명령 출력이 타임스탬프인지 확인합니다.

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

- 컨트롤 플레인 이벤트 또는 데이터 플레인 카운터에 대한 show 명령 출력을 수집하는 경우 항상 동일한 출력의 여러 이터레이션을 수집합니다.

GETVPN 컨트롤 플레인 문제 해결

컨트롤 플레인은 GM에서 정책 및 SA(Security Association)가 생성되어 데이터 플레인 트래픽을 암호화하고 해독할 준비가 된 모든 프로토콜 이벤트를 의미합니다.GETVPN 제어 평면의 일부 주요 검사점은 다음과 같습니다.

컨트롤 플레인 디버깅 모범 사례

이러한 트러블슈팅 모범 사례는 GETVPN에 국한되지 않습니다.거의 모든 컨트롤 플레인 디버깅에 적용됩니다.가장 효과적인 문제 해결을 위해 이러한 모범 사례를 따르는 것이 중요합니다.

- 콘솔 로깅을 끄고 로깅 버퍼 또는 syslog를 사용하여 디버그를 수집합니다.
- 디버깅되는 모든 디바이스에서 라우터 클럭을 동기화하려면 NTP를 사용합니다.
- 디버그 및 로그 메시지에 대해 msec 타임스탬프를 활성화합니다.

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

- show 명령 출력이 디버그 출력과 상호 연결될 수 있도록 타임스탬프가 지정되어야 합니다.

```
terminal exec prompt timestamp
```

- 가능한 경우 확장 환경에서 조건부 디버깅을 사용합니다.

GETVPN 컨트롤 플레인 문제 해결 도구

GETVPN Show 명령

일반적으로 이러한 명령은 거의 모든 GETVPN 문제에 대해 수집해야 하는 명령 출력입니다.

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 Syslog 메시지

GETVPN은 중요한 프로토콜 이벤트 및 오류 조건을 위해 광범위한 syslog 메시지 집합을 제공합니다.GETVPN 트러블슈팅을 수행할 때 항상 syslog가 가장 먼저 확인해야 합니다.

공통 KS Syslog 메시지

Syslog 메시지	설명
COOP_CONFIG_MISMATCH	기본 키 서버와 보조 키 서버 간의 구성이 일치하지 않습니다.

COOP_KS_선택	로컬 키 서버가 그룹의 선택 프로세스를 시작했습니다.
COOP_KS_REACH	구성된 협력 키 서버 간의 연결이 복원됩니다.
COOP_KS_TRANS_TO_PRI	**로컬 키 서버가 그룹의 보조 서버가 되는 기본 역할로 전환되었습니다.**
COOP_KS_UNAUTH	권한 있는 원격 서버가 그룹의 로컬 키 서버에 연결하려고 했습니다. 이는 우 이벤트로 간주될 수 있습니다.
COOP_KS_UNREACH	**구성된 협력 키 서버 간의 연결이 끊기며, 이는 적대적인 이벤트로 간주될 수 습니다.**
KS_GM_폐기됨	키 재설정 프로토콜 동안, 권한이 없는 구성원이 그룹에 가입하려고 시도했 이는 적대적으로 간주될 수 있습니다.
KS_SEND_MCAST_REKEY	**멀티캐스트 다시 키를 보내는 중입니다.**
KS_SEND_UNICAST_REKEY	**유니캐스트 다시 키를 보내는 중입니다.**
KS_승인되지 않음	GDOI 등록 프로토콜 동안, 승인되지 않은 회원이 그룹에 가입하려고 시도했 , 그것은 적대적으로 여겨질 수 있다.
승인되지 않은_IPADDR	요청한 장치에 그룹에 가입할 권한이 없기 때문에 등록 요청이 삭제되었습니

일반적인 GM Syslog 메시지

Syslog 메시지	설명
GM_CLEAR_REGISTER	**clear crypto gdoi** 명령이 로컬 그룹 구성원에 의해 실행되었습니다.
GM_CM_첨부	로컬 그룹 구성원에 대한 암호화 맵이 첨부되었습니다.
GM_CM_분리	로컬 그룹 구성원에 대해 암호화 맵이 분리되었습니다.&
GM_RE_등록	**한 그룹에 대해 생성된 IPsec SA가 만료되었거나 지워졌을 수 있습니다. 버에 다시 등록해야 합니다.**
GM_RECV_REKEY	**다시 키를 받았습니다.**
GM_REGS_COMPL	**등록이 완료되었습니다.**
GM_REKEY_TRANS_2_MULTI	그룹 멤버가 유니캐스트 키 리키 메커니즘을 사용하는 것에서 멀티캐스트 커니즘을 사용하는 것으로 전환되었습니다.
GM_REKEY_TRANS_2_UNI	그룹 멤버가 멀티캐스트 키 리키 메커니즘을 사용하는 것에서 유니캐스트 커니즘 사용으로 전환되었습니다.
의사_시간_큼	그룹 구성원이 자체 의사 시간과 크게 다른 값으로 의사 시간을 받았습니
재생 실패	그룹 구성원 또는 키 서버에서 재생 방지 확인에 실패했습니다.

참고:빨간색으로 강조 표시된 메시지는 GETVPN 환경에서 가장 자주 또는 중요한 메시지입니다.

전역 암호화 및 GDOI 디버그

GETVPN 디버그는 다음과 같이 구분됩니다.

1. 먼저 문제 해결 중인 디바이스에서 수행합니다.

```
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. 두 번째로 문제 해결 중인 문제 유형입니다.

```
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. 세 번째로 활성화해야 하는 디버깅 수준입니다.버전 15.1(3)T 이상에서는 모든 GDOI 기능 디버그가 이러한 디버그 수준을 갖도록 표준화되었습니다.이는 충분한 디버깅 세분화로 대규모 GETVPN 환경의 문제를 해결할 수 있도록 설계되었습니다.GETVPN 문제를 디버깅할 때는 적절한 디버그 수준을 사용하는 것이 중요합니다.일반적으로 가장 낮은 디버그 레벨인 오류 레벨로 시작하고 필요한 경우 디버깅 세분성을 높입니다.

```
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 조건부 디버깅

Cisco IOS® 버전 15.1(3)T 이상에서는 대규모 환경에서 GETVPN 문제를 해결하는 데 도움이 되도록 GDOI 조건부 디버깅이 추가되었습니다.따라서 이제 모든 ISAKMP(Internet Security Association and Key Management Protocol) 및 GDOI 디버그를 그룹 또는 피어 IP 주소를 기반으로 하는 조건부 필터로 트리거할 수 있습니다.대부분의 GETVPN 문제에서는 GDOI 디버그에만 GDOI 관련 작업이 표시되므로 적절한 조건부 필터로 ISAKMP 및 GDOI 디버그를 활성화하는 것이 좋습니다 .ISAKMP 및 GDOI 조건부 디버그를 사용하려면 다음 두 단계를 완료하십시오.

1. 조건부 필터를 설정합니다.
2. 평소와 같이 관련 ISAKMP 및 GDOI를 활성화합니다.

예:

```
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)
```

참고:ISAKMP 및 GDOI 조건부 디버그를 사용하여 조건 필터 정보가 없을 수 있는 디버그 메시지(예: 디버그 경로의 IP 주소)를 catch하기 위해 일치하지 않는 플래그를 활성화할 수 있습니다.그러나 많은 양의 디버그 정보를 생성할 수 있으므로 주의하여 사용해야 합니다.

GDOI 이벤트 추적

이는 버전 15.1(3)T에 추가되었습니다.이벤트 추적은 상당한 GDOI 이벤트 및 오류를 위해 항상 켜져 있는 가벼운 추적 기능을 제공합니다.또한 예외 조건에 대해 traceback이 활성화된 exit-path 추적도 있습니다.이벤트 추적은 기존 syslog보다 더 많은 GETVPN 이벤트 기록 정보를 제공할 수 있습니다.

GDOI 이벤트 추적은 기본적으로 활성화되어 **show monitor even-trace** 명령을 사용하여 추적 버퍼에서 검색할 수 있습니다.

```
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
```

exit path trace는 기본적으로 traceback 옵션을 활성화하여 종료 경로(예외 및 오류 조건)에 대한 자세한 정보를 제공합니다.그런 다음 tracebacks를 사용하여 종료 경로 조건으로 이동한 정확한 코드 시퀀스를 디코딩할 수 있습니다.추적 버퍼에서 역추적을 검색하려면 detail 옵션을 사용합니다.

```
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
```

기본 추적 버퍼 크기는 512개 항목이며, 문제가 간헐적으로 발생하는 경우에는 충분하지 않을 수 있습니다.이 기본 추적 항목 크기를 늘리려면 다음과 같이 이벤트 추적 구성 매개변수를 변경할 수 있습니다.

```
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
```

GETVPN 컨트롤 플레인 체크포인트 및 공통 문제

다음은 GETVPN에 대한 몇 가지 일반적인 컨트롤 플레인 문제입니다.다시 반복하기 위해 제어 평면은 GM에서 데이터 플레인 암호화 및 암호 해독을 활성화하는 데 필요한 모든 GETVPN 기능 구성 요소로 정의됩니다.높은 수준의 경우 GM 등록, 보안 정책 및 SA 다운로드/설치, 후속 KEK/TEK 키 재설정이 필요합니다.

COOP 설정 및 정책 생성

KS가 보안 정책 및 관련 KEK/TEK을 성공적으로 생성했는지 확인하고 확인하려면 다음을 입력합니다.

```
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
```

KS 정책 설정의 일반적인 문제 중 하나는 기본 KS와 보조 KS 간에 서로 다른 정책이 구성되어 있는 경우입니다.이렇게 하면 예측할 수 없는 KS 동작이 발생할 수 있으며 다음 오류가 보고됩니다.

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

현재 기본 및 보조 KS 간에 자동 컨피그레이션 동기화가 없으므로 수동으로 수정해야 합니다.

COOP는 GETVPN의 중요한(거의 항상 필수) 구성이므로 COOP가 올바르게 작동하고 COOP KS 역할이 올바른지 확인하는 것이 중요합니다.

```
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
```

기능적 COOP 설정에서 이 프로토콜 플로우를 관찰해야 합니다.

IKE Exchange > ANN with COOP priorities 교환 > COOP Selection > ANN from primary to secondary KS (정책, GM 데이터베이스 및 키)

COOP가 제대로 작동하지 않거나 여러 KS가 기본 KS가 되는 등의 COOP 분할이 있는 경우 문제 해결을 위해 이러한 디버그를 수집해야 합니다.

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

IKE 설정

후속 정책 및 SA 다운로드를 위한 제어 채널을 보호하려면 GETVPN에 성공적인 IKE 교환이 필요합니다.성공적인 IKE 교환이 끝나면 GDOI_REKEY sa가 생성됩니다.

Cisco IOS 15.4(1)T 이전 버전에서는 **show crypto isakmp sa** 명령과 함께 GDOI_REKEY를 표시할 수 있습니다.

```
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#
```

Cisco IOS 15.4(1)T 이상에서는 이 GDOI_REKEY sa가 show crypto gdoi rekey sa 명령과 함께 표시됩니다.

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

참고:초기 IKE 교환이 완료되면 GDOI_REKEY SA를 사용하여 KS에서 GM으로 후속 정책과 키가 푸시됩니다.따라서 GDOI_IDLE SA가 만료될 때 키 재설정이 없습니다.수명이 다 되면

사라집니다.그러나 GM에서 키 다시 입력을 받으려면 항상 GDOI_REKEY SA가 있어야 합니다.

GETVPN에 대한 IKE 교환은 기존의 포인트-투-포인트 IPsec 터널에 사용된 IKE와 다르지 않으므로 문제 해결 방법은 동일하게 유지됩니다.IKE 인증 문제를 해결하려면 이러한 디버그를 수집해야 합니다.

```
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)
```

등록, 정책 다운로드 및 SA 설치

IKE 인증이 성공하면 GM은 KS에 등록합니다.이러한 syslog 메시지는 이 문제가 올바르게 발생할 때 표시됩니다.

```
%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
```

다음 명령을 사용하여 정책 및 키를 확인할 수 있습니다.

```
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#
```

참고:GETVPN에서는 인바운드 및 아웃바운드 SA가 동일한 SPI를 사용합니다.

GETVPN 등록 및 정책 설치 유형의 문제를 해결하려면 다음 디버그가 필요합니다.

```
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)
```

참고:이러한 출력의 결과에 따라 추가 디버그가 필요할 수 있습니다.

일반적으로 GETVPN 등록은 GM 다시 로드 직후 발생하므로 이 EEM 스크립트는 다음 디버그를 수집하는 데 도움이 될 수 있습니다.

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

키 재설정

GM이 KS에 등록되고 GETVPN 네트워크가 올바르게 설정되면 기본 KS는 등록된 모든 GM에 키 재설정 메시지를 보낼 책임이 있습니다.키 재설정 메시지는 GM의 모든 정책, 키 및 의사 시간을 동기화하는 데 사용됩니다.리키 메시지는 유니캐스트 또는 멀티캐스트 방법을 통해 전송할 수 있습니다.

이 syslog 메시지는 키 재설정 메시지가 전송될 때 KS에 표시됩니다.

```
%GDOI-5-KS_SEND_UNICAST_REKEY: Sending Unicast Rekey for group G1 from address
10.1.11.2 with seq # 11
```
GM에서 이것은 rekey를 수신할 때 표시되는 syslog입니다.

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

KS에서 키 재설정을 위한 RSA 키 쌍 요구 사항

키 재설정 기능을 사용하려면 KS에 RSA 키가 있어야 합니다. KS는 등록 중에 이 보안 채널을 통해 RSA 키 쌍의 공개 키를 GM에 제공합니다.그런 다음 KS는 GDOI SIG 페이로드에서 개인 RSA 키를 사용하여 GM에 전송되는 GDOI 메시지에 서명합니다.GM은 GDOI 메시지를 수신하고 공용 RSA 키를 사용하여 메시지를 확인합니다.KS와 GM 간의 메시지는 KEK로 암호화되며, GM에 등기시 분배된다.등록이 완료되면 후속 키 다시 키는 KEK로 암호화되어 개인 RSA 키로 서명됩니다.

GM 등록 중 KS에 RSA 키가 없는 경우 다음 메시지가 syslog에 나타납니다.

```
%GDOI-1-KS_NO_RSA_KEYS: RSA Key - get : Not found, Required for group G1
```
키가 KS에 없으면 GM이 처음으로 등록되지만 다음 키 재설정은 KS에서 실패합니다.결국 GM의 기존 키가 만료되고 다시 등록됩니다.

```
%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.
```
RSA 키 쌍은 키 재설정 메시지에 서명하기 위해 사용되므로 기본 KS와 모든 보조 KS 간에 동일해야 **합니다**.이렇게 하면 기본 KS 장애 시 보조 KS(새 기본 KS)에서 전송하는 키 리키가 GM에서 올바르게 검증될 수 있습니다.기본 KS에서 RSA 키 쌍을 생성할 때 이 요구 사항을 충족하기 위해 모든 보조 KS로 내보낼 수 있도록 키 쌍을 내보낼 수 있는 옵션으로 생성해야 합니다.

재키 문제 해결

KEK/TEK 키 재설정 실패는 고객 구축에서 발생하는 가장 일반적인 GETVPN 문제 중 하나입니다 .리키 문제 해결 방법은 다음과 같이 리키 단계를 따라야 합니다.

1. KS에서 재키를 보냈나요?

   이 명령은 %GDOI-5-KS_SEND_UNICAST_REKEY syslog 메시지 또는 이 명령을 사용하여 보다 정확하게 확인할 수 있습니다.

```
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
```

   재전송된 키 수는 KS에서 수신하지 못한 키 재확인 패킷 및 가능한 키 재지정 문제를 나타냅니

다.GDOI rekey는 UDP를 신뢰할 수 없는 전송 메커니즘으로 사용하므로 기본 전송 네트워크의 신뢰성에 따라 일부 키 재전송이 예상될 수 있지만, 키 재전송 증가 추세를 항상 조사해야 합니다.

GM당 보다 자세한 리키 통계도 얻을 수 있습니다.이 경우 일반적으로 재키 문제가 발생할 수 있습니다.

```
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. 키 재설정 패킷이 기본 인프라 네트워크에서 전달되었습니까?

   KS와 GM 간의 트랜짓 네트워크에서 리키 패킷이 삭제되지 않도록 키 재전송 경로를 따라 표준 IP 트러블슈팅을 수행해야 합니다.여기에서 사용되는 몇 가지 일반적인 문제 해결 도구는 전송 네트워크의 입력/출력 ACL(Access Control List), Netflow 및 패킷 캡처입니다.

3. 키 재설정 패킷이 키 재처리를 위해 GDOI 프로세스에 도달했습니까?

   GM 키 재설정 통계를 확인합니다.

```
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. 키 확인 패킷이 KS로 돌아갔습니까?

   GM에서 KS로 다시 키 확인 패킷을 추적하려면 1~3단계를 수행합니다.

멀티캐스트 키

멀티캐스트 rekey는 다음과 같은 측면에서 유니캐스트 rekey와 다릅니다.

- KS에서 GM으로 이러한 키 재설정 패킷을 전송하기 위해 멀티캐스트가 사용되므로 KS는 키 재설정 패킷 자체를 복제할 필요가 없습니다.KS는 키 재설정 패킷의 복사본 하나만 전송하고 멀티캐스트 지원 네트워크에서 복제됩니다.
- 멀티캐스트 키 재설정에 대한 승인 메커니즘이 없으므로 GM이 키 재전송 패킷을 받지 않을 경우 KS는 이를 알지 못하므로 GM 데이터베이스에서 GM을 제거하지 않습니다.그리고 확인 메시지가 없으므로 KS는 항상 키 재전송 컨피그레이션을 기반으로 키 재전송 패킷을 재전송합니다.

멀티캐스트 키 재설정 문제는 GM에서 키 리키가 수신되지 않을 때 발생합니다.다음과 같은 여러 가지 가능한 원인이 있을 수 있습니다.

- 멀티캐스트 라우팅 인프라 내의 패킷 전달 문제
- 엔드 투 엔드 멀티캐스트 라우팅이 네트워크 내에서 활성화되지 않음

멀티캐스트 키 재설정 문제를 해결하는 첫 번째 단계는 멀티캐스트에서 유니캐스트 방법으로 전환할 때 리키가 작동하는지 확인하는 것입니다.

문제가 멀티캐스트 키 재지정과 관련이 있음을 확인한 후 KS가 지정된 멀티캐스트 주소로 리키를 전송하는지 확인합니다.

```
%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
```

멀티캐스트 주소에 대한 ICMP(Internet Control Message Protocol) 요청을 사용하여 KS와 GM 간의 멀티캐스트 연결을 테스트합니다.멀티캐스트 그룹에 속한 모든 GM은 ping에 응답해야 합니다 .ICMP가 이 테스트의 KS 암호화 정책에서 제외되었는지 확인합니다.

```
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
```

멀티캐스트 ping 테스트가 실패하면 멀티캐스트 문제 해결을 수행해야 합니다. 이 문제는 이 문서의 범위를 벗어납니다.

컨트롤 플레인 릴레이 확인

증상

고객이 GM을 새로운 Cisco IOS 버전으로 업그레이드할 때 syslog에 표시되는 이 메시지와 함께 KEK 키 재설정 오류가 발생할 수 있습니다.

```
%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
```

이 동작은 컨트롤 플레인 메시지에 추가된 재전송 방지 확인과 함께 도입된 상호 운용성 문제로 인해 발생합니다.특히 이전 코드를 실행하는 KS는 KEK 키 재설정 시퀀스 번호를 1로 재설정하며, 이 값은 다시 재생된 키 패킷으로 해석될 때 새 코드를 실행하는 GM이 삭제합니다.자세한 내용은 Cisco 버그 ID CSCta05809(GETVPN:재생에 적합한 GETVPN 컨트롤 플레인) 및 GETVPN 구성 제한.

배경

GETVPN을 사용하면 컨트롤 플레인 메시지가 시간 기반 재전송 방지 확인 서비스를 제공하기 위해 시간에 민감한 정보를 전달할 수 있습니다.따라서 이러한 메시지는 시간 정확성을 보장하기 위해 재전송 방지 보호가 필요합니다.다음 메시지는 다음과 같습니다.

- **KS**에서 GM으로 메시지 키 재설정
- **KS** 간 COOP **알림 메시지**

이 재전송 방지 보호 구현의 일부로서, TBAR가 활성화된 경우 유사 시간 확인뿐만 아니라 재생된 메시지를 보호하기 위해 시퀀스 번호 검사가 추가되었습니다.

솔루션

이 문제를 해결하려면 컨트롤 플레인 재생 확인 기능 이후에 GM과 KS를 Cisco IOS 버전으로 업그레이드해야 합니다.새 Cisco IOS 코드를 사용하는 경우 KS는 KEK 리키에 대해 시퀀스 번호를 다시 1로 재설정하지 않고, 대신 현재 시퀀스 번호를 계속 사용하고 TEK 리키에 대한 시퀀스 번호만 재설정합니다.

이러한 Cisco IOS 버전에는 Replay Check 기능이 있습니다.

- 12.4(15)T10
- 12.4(22)T3
- 12.4(24)T2
- 15.0(1)M 이상

기타 재생 관련 문제

- ANN 메시지 재전송 확인 실패(Cisco 버그 ID CSCtc52655)로 인해 COOP 실패

디버그 컨트롤 플레인 재생 실패

다른 컨트롤 플레인 재생 실패 시 이 정보를 수집하고 시간이 KS와 GM 간에 동기화되었는지 확인합니다.

- GM과 KS 모두의 Syslog
- ISAKMP 디버그
- KS와 GM의 GDOI 디버그(키 재설정 및 재생)

컨트롤 플레인 패킷 조각화 문제

GETVPN을 사용하면 컨트롤 플레인 패킷 단편화가 일반적인 문제이며, 컨트롤 플레인 패킷이 충분히 커서 IP 프래그먼트화가 필요할 때 이 두 시나리오 중 하나에서 자신을 나타낼 수 있습니다.

- GETVPN COOP 알림 패킷

- GETVPN 키 재설정 패킷

COOP 알림 패킷

COOP Announcement 패킷은 GM 데이터베이스 정보를 전달하므로 대규모 GETVPN 구축에서 크게 증가할 수 있습니다.과거 경험에서 1,500개 이상의 GM으로 구성된 GETVPN 네트워크는 1,8024바이트보다 큰 알림 패킷을 생성하는데, 이는 Cisco IOS의 기본 Huge 버퍼 크기입니다.이 경우 KS는 다음 오류로 인해 ANN 패킷을 전송할 수 있을 만큼 큰 버퍼를 할당하지 못합니다.

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

이 조건을 수정하려면 이 버퍼 조정을 권장합니다.

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

패킷 키 재설정

암호화 정책이 큰 경우 암호화 ACL에서 8개 이상의 ACE(Access Control Entries) 행으로 구성된 정책과 같이 GETVPN 키 재설정 패킷은 일반적인 1500 IP MTU(Maximum Transition Unit) 크기를 초과할 수도 있습니다.

조각화 문제 및 식별

이전 두 시나리오에서 COOP 또는 GDOI rekey가 제대로 작동하려면 GETVPN이 프래그먼트된 UDP 패킷을 올바르게 전송하고 수신할 수 있어야 합니다.일부 네트워크 환경에서는 IP 단편화가 문제가 될 수 있습니다.예를 들어, ECMP(Equal Cost Multi Path) 포워딩 플레인으로 구성된 네트워크와 포워딩 플레인의 일부 디바이스에서는 VFR(Virtual Fragmentation Reassembly)과 같은 프래그먼트된 IP 패킷의 가상 재어셈블리가 필요합니다.

문제를 식별하려면 프래그먼트된 UDP 848 패킷이 제대로 수신되지 않은 것으로 의심되는 디바이스에서 리어셈블리 오류를 확인합니다.

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

리어셈블리 시간 제한이 계속 증가하면 debug ip error 명령을 사용하여 드롭이 rekey/COOP 패킷 흐름의 일부인지 확인합니다.확인된 후에는 패킷을 삭제했을 수 있는 전달 평면에서 정확한 디바이스를 격리하기 위해 일반 IP 포워딩 트러블슈팅을 수행해야 합니다.일반적으로 사용되는 일부 도구는 다음과 같습니다.

- 패킷 캡처
- 트래픽 전달 통계
- 보안 기능 통계(방화벽, IPS)
- VFR 통계

GDOI 상호 운용성 문제

여러 해 동안 GETVPN에서 다양한 상호 운용성 문제가 발견되었으며, 상호 운용성 문제를 위해 KS와 GM 간의 Cisco IOS 릴리스 버전과 KS 간의 Cisco IOS 릴리스 버전을 확인하는 것이 중요합니다.

기타 잘 알려진 GETVPN 상호 운용성 문제는 다음과 같습니다.

- 컨트롤 플레인 릴레이 확인
- GETVPN KEK 키 재설정 동작 변경
- Cisco 버그 ID CSCub42920(GETVPN:KS가 이전 GM 버전에서 키 재설정 ACK에서 해시의 유효성을 검사하지 못함)
- Cisco 버그 ID CSCuw48400(GetVPN GM이 등록하거나 키 재설정을 수행할 수 없음 - sig-hash > 기본 SHA-1)
- Cisco 버그 ID CSCvg19281(새 KS 쌍으로 마이그레이션한 후 다중 GETVPN GM 충돌)GM 버전이 3.16 이전이고 KS가 이전 코드에서 3.16 이상으로 업그레이드된 경우 이 문제가 발생할 수 있습니다.)

GETVPN IOS 업그레이드 절차

GETVPN 환경에서 Cisco IOS 코드 업그레이드를 수행해야 하는 경우 다음 Cisco IOS 업그레이드 절차를 따라야 합니다.

1. 먼저 보조 KS를 업그레이드하고 COOP KS 선택이 완료될 때까지 기다립니다.
2. 모든 보조 KS에 대해 1단계를 반복합니다.
3. 기본 KS를 업그레이드합니다.
4. GM 업그레이드

GETVPN 데이터 플레인 문제 해결

컨트롤 플레인 문제와 비교했을 때 GETVPN 데이터 플레인 문제는 GM에 데이터 플레인 암호화 및 암호 해독을 수행하는 정책 및 키가 있지만, 어떤 이유로 엔드 투 엔드 트래픽 흐름이 작동하지 않는 문제입니다.GETVPN에 대한 대부분의 데이터 플레인 문제는 일반 IPsec 포워딩과 관련되며 GETVPN에 특정하지 않습니다.따라서 여기에서 설명하는 대부분의 문제 해결 방식은 일반적인 IPsec 데이터 플레인 문제에도 적용됩니다.

암호화 문제(그룹 기반 또는 쌍 방식 터널 모두)에서는 문제를 해결하고 데이터 경로의 특정 부분으로 문제를 격리하는 것이 중요합니다.특히, 여기에서 설명하는 문제 해결 접근 방식은 다음과 같은 질문에 답변하는 데 도움이 됩니다.

- 라우터 암호화 또는 라우터 해독 등 어떤 디바이스가 원인입니까?
- 인그레스(ingress) 또는 이그레스(egress) 중 어느 방향으로 문제가 발생합니까?

GETVPN 데이터 플레인 문제 해결 도구

IPsec 데이터 플레인 문제 해결은 컨트롤 플레인에 대한 문제 해결과 매우 다릅니다.데이터 플레인을 사용하면 일반적으로 실행할 수 있는 디버그가 없거나 적어도 프로덕션 환경에서 안전하게 실행할 수 있습니다.따라서 문제 해결은 전달 경로를 따라 패킷을 추적하는 데 도움이 되는 서로 다른 카운터와 트래픽 통계에 크게 의존합니다.다음과 같이 패킷이 삭제되는 위치를 격리하기 위해 체크포인트 세트를 개발할 수 있습니다.

다음은 몇 가지 데이터 플레인 디버깅 도구입니다.

- 액세스 목록
- IP 우선 순위 어카운팅
- Netflow
- 인터페이스 카운터
- 암호화 카운터
- IP CEF(Cisco Express Forwarding) 글로벌 및 기능별 삭제 카운터
- EPC(Embedded Packet Capture)
- 데이터 플레인 디버깅(IP 패킷 및 CEF 디버깅)

이전 이미지의 데이터 경로에 있는 검사점은 다음 툴을 사용하여 검증할 수 있습니다.

GM 암호화

- 인그레스 LAN 인터페이스
  입력 ACL
  인그레스 netflow
  임베디드 패킷 캡처
  입력 우선 순위 계정

- 암호화 엔진
  crypto ipsec sa 표시
  show crypto ipsec sa detail(암호화 ipsec sa 세부 정보 표시)
  암호화 엔진 가속기 통계 표시

- 이그레스 WAN 인터페이스
  이그레스 네트워크 흐름
  임베디드 패킷 캡처
  출력 우선 순위 계정

GM 암호 해독

- 인그레스 WAN 인터페이스
  입력 ACL
  인그레스 netflow
  임베디드 패킷 캡처
  입력 우선 순위 계정

- 암호화 엔진
  crypto ipsec sa 표시
  crypto ipsec sa detail 표시
  암호화 엔진 가속기 통계 표시

- 이그레스 LAN 인터페이스
  이그레스 네트워크 흐름
  포함된 패킷 캡처

반환 경로는 동일한 트래픽 흐름을 따릅니다.다음 섹션에서는 사용 중인 이러한 데이터 플레인 도구의 몇 가지 예를 소개합니다.

암호화/암호 해독 카운터

라우터의 암호화/암호 해독 카운터는 IPsec 흐름을 기반으로 합니다.그러나 GETVPN은 일반적으로 모든 것을 암호화하는 "permit ip any any" 암호화 정책을 구축하기 때문에 GETVPN에서는 이 기능이 제대로 작동하지 않습니다.따라서 일부 플로우에 대해서만 문제가 발생하고 전부는 아닌 일부 플로우에 대해서만 문제가 발생할 경우, 제대로 작동하는 상당한 백그라운드 트래픽이 있을 때 패킷이 암호화되거나 해독되는지 정확하게 평가하기 위해 이러한 카운터를 사용하기가 다소 어려울 수 있습니다.

```
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

Netflow를 사용하여 두 GM의 인그레스 및 이그레스 트래픽을 모두 모니터링할 수 있습니다 .GETVPN permit ip any any policy를 사용하면 암호화된 트래픽은 집계되며 흐름별 정보를 제공하지 않습니다.그런 다음 나중에 설명한 DSCP/우선 순위 표시와 함께 흐름별 정보를 수집해야 합니다.

이 예에서는 다양한 체크포인트에 GM1 뒤의 호스트에서 GM2 뒤의 호스트로 100 카운트 ping에 대한 netflow가 표시됩니다.

GM 암호화

Netflow 컨피그레이션:

```
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 출력:

```
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#
```

참고:이전 출력에서 *는 이그레스 트래픽을 나타냅니다.첫 번째 행은 WAN 인터페이스에서 나가는 이그레스 암호화 트래픽(프로토콜 0x32 = ESP)과 LAN 인터페이스를 통과하는 두 번째 라인 인그레스 ICMP 트래픽을 보여줍니다.

GM 암호 해독

구성:

```
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 출력:

```
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 우선순위 표시

암호화 문제를 해결하는 데 있어 문제는 패킷이 암호화되면 페이로드에 대한 가시성이 상실되며, 이는 암호화가 수행해야 하는 작업입니다. 따라서 특정 IP 흐름에 대한 패킷을 추적하기가 어려워진다는 것입니다.IPsec 문제 해결에 있어서 이 제한을 해결하는 방법에는 두 가지가 있습니다.

- IPsec 변환으로 ESP-NULL을 사용합니다.IPsec은 여전히 ESP 캡슐화를 수행하지만 페이로드에 적용되는 암호화가 없으므로 패킷 캡처에 표시됩니다.
- L3/L4 특성에 따라 고유한 DSCP(Differentiated Services Code Point)/우선 순위 표시와 함께 IP 흐름을 표시합니다.

ESP-NULL은 두 터널 엔드포인트를 모두 변경해야 하며 고객 보안 정책에 따라 허용되지 않는 경우가 많습니다.따라서 Cisco는 일반적으로 DSCP/우선 순위 표시를 대신 사용하는 것이 좋습니다.

DSCP/우선 순위 참조 차트

ToS(16진수)	ToS(십진수)	IP 우선 순위	DSCP	이진
0xE0	224	7 네트워크 제어	56개 CS7	11100000
0xC0	192	6 네트워크 간 제어	CS6 48개	11000000
0xB8	184	5 중요	46EF	10111000
0xA0	160		40개 CS5	10100000
0x88	136	4 플래시 재정의	34AF41	10001000
0x80	128		CS4 32개	10000000
0x68	104	3 플래시	26AF31	01101000

0x60	96		CS3 24개	01100000
0x48	72	2 즉시	18AF21	01001000
0x40	64		CS2 16개	01000000
0x20	32	1 우선 순위	CS1 8개	00100000
0x00	0	0 루틴	0 플트	00000000

DSCP/우선 순위로 패킷 표시

이러한 방법은 일반적으로 특정 DSCP/우선순위 표시와 함께 패킷을 표시하기 위해 사용됩니다.

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
```

라우터 Ping

```
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>
```

> **참고:**마킹을 적용하기 전에 일반 트래픽 흐름과 DSCP/우선 순위 프로필을 모니터링하여 표시된 트래픽 흐름이 고유하도록 하는 것이 좋습니다.

표시된 패킷 모니터링

IP 우선 순위 어카운팅

```
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
```

인터페이스 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
```

임베디드 패킷 캡처

EPC(Embedded Packet Capture)는 패킷이 특정 디바이스에 도달했는지 확인하기 위해 인터페이스 레벨에서 패킷을 캡처하는 데 유용한 툴입니다.EPC는 일반 텍스트 트래픽에서 잘 작동하지만 캡처된 패킷이 암호화되면 문제가 될 수 있습니다.따라서 문제를 더 효과적으로 해결하기 위해 앞서 설명한 DSCP/우선 순위 표시와 같은 기술이나 IP 패킷의 길이와 같은 기타 IP 문자를 EPC와 함께 사용해야 합니다.

Cisco IOS-XE 패킷 추적

이 기능은 CSR1000v, ASR1000 및 ISR4451-X와 같이 Cisco IOS-XE를 실행하는 모든 플랫폼에서 기능 전달 경로를 추적하는 데 유용합니다.

GETVPN 데이터 플레인 공통 문제

GETVPN에 대한 IPsec 데이터 플레인의 트러블슈팅은 주로 GETVPN의 고유한 데이터 플레인 속성으로 인한 2가지 예외를 제외하고 전통적인 포인트-투-포인트 IPsec 데이터 플레인 문제를 해결하는 것과 다릅니다.

시간 기반 재생 방지 실패

GETVPN 네트워크에서는 더 이상 쌍으로 작동하는 터널이 없으므로 TBAR 장애를 해결하기 어려울 수 있습니다.GETVPN TBAR 오류를 해결하려면 다음 단계를 완료하십시오.

1. TBAR 장애로 인해 삭제되는 패킷을 식별한 후 암호화 GM을 식별합니다.

   Version 15.3(2)T 이전의 TBAR 실패 syslog는 실패한 패킷의 소스 주소를 인쇄하지 않았으므로 어떤 패킷이 실패했는지 식별하기가 매우 어렵습니다.이는 Cisco IOS에서 다음을 인쇄하는 버전 15.3(2)T 이상에서 크게 향상되었습니다.

```
%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
```

TBAR 기록은 이 버전에서도 구현되었습니다.

```
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
```

참고:이전에 언급한 향상된 기능은 Cisco IOS-XE에서 Cisco 버그 ID CSCun49335 및 Cisco IOS에서 Cisco 버그 ID CSCub91811로 구현되었습니다.
이 기능이 없는 Cisco IOS 버전의 경우 **debug crypto gdoi gm replay detail**도 이 정보를 제공할 수 있습니다. 그러나 이 디버그는 모든 트래픽에 대한 TBAR 정보(TBAR 오류로 인해 삭제된 패킷만 아님)를 인쇄하므로 프로덕션 환경에서 실행할 수 없습니다.

```
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. 패킷의 소스가 식별되면 암호화 GM을 찾을 수 있어야 합니다.그런 다음 GM의 암호화 및 암호 해독 모두에 대한 의사 타임스탬프를 모니터링하여 잠재적인 의사 시간 표출을 확인해야 합니다.GM과 KS를 모두 NTP에 동기화하고, GM의 클럭 기울이로 인해 문제가 발생하는지 확인하기 위해 모든 NTP의 참조 시스템 클럭과 함께 의사 시간 정보를 정기적으로 수집하는 것이 가장 좋은 방법입니다.

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
```

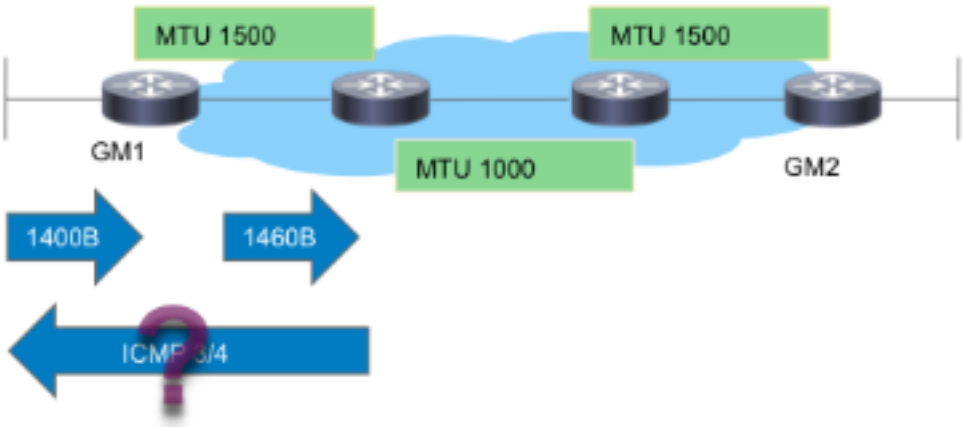
```
Anti-replay Information For Group G1:
Timebased Replay:
Replay Value              : 625866.51 secs
Input Packets : 4 Output Packets : 4
Input Error Packets : 2 Output Error Packets : 0
Time Sync Error : 0 Max time delta : 0.00 secs
```

이전 예에서 재생 값에 표시된 것처럼 의사 시간이 GM 간에 상당히 다른 경우, 동일한 참조 시간으로 출력을 캡처하면 클럭 기울이기 때문에 문제가 발생할 수 있습니다.

> **참고:**Cisco Aggregated Services Router 1000 Series 플랫폼에서는 플랫폼 아키텍처로 인해 QFP(Quantum Flow Processor)의 데이터 경로가 실제로 pseudotime 틱 수를 계산하기 위한 벽시계를 가리킵니다.이로 인해 NTP 동기화로 인해 벽면 시계 시간이 변경될 때 TBAR에 문제가 발생했습니다.이 문제는 Cisco 버그 ID CSCum37911에 설명되어 있습니다.

PMTUD 및 GETVPN 헤더 보존

GETVPN을 사용하면 PMTUD(Path MTU Discovery)가 GM의 암호화 및 암호 해독 간에 작동하지 않으며 DF(Don't Fragment) 비트 집합이 있는 큰 패킷은 블랙홀링될 수 있습니다.이 작업이 작동하지 않는 이유는 데이터 소스/대상 주소가 ESP 캡슐화 헤더에 보존되는 GETVPN Header Preservation 때문입니다.이 이미지는 다음과 같습니다.



이 그림에서 볼 수 있듯이 PMTUD는 GETVPN과 함께 다음과 같이 분할됩니다.

1. 대용량 데이터 패킷이 암호화 GM1에 도착합니다.
2. 사후 암호화 ESP 패킷은 GM1에서 전달되어 목적지로 전달됩니다.
3. IP MTU가 1400바이트인 트랜짓 링크가 있으면 ESP 패킷이 삭제되고 ICMP 3/4 패킷이 데이터 패킷의 소스인 패킷 소스로 전송됩니다.
4. ICMP3/4 패킷은 GETVPN 암호화 정책에서 제외되지 않은 ICMP로 인해 삭제되거나, ESP 패킷(인증되지 않은 페이로드)에 대해 아무것도 모르기 때문에 엔드 호스트가 삭제합니다.

요약하면, PMTUD는 현재 GETVPN에서 작동하지 않습니다.이 문제를 해결하기 위해 Cisco는 다음 단계를 권장합니다.

1. 전송 네트워크에서 암호화 오버헤드 및 최소 경로 MTU를 수용하기 위해 TCP 패킷 세그먼트 크기 주석 크기를 줄이기 위해 "ip tcp adjust-mss"를 구현합니다.
2. PMTUD를 방지하기 위해 데이터 패킷에서 DF 비트가 암호화 GM에 도착하면 지웁니다.

일반 IPsec 데이터 플레인 문제

대부분의 IPsec 데이터 플레인 문제 해결은 기존의 포인트 투 포인트 IPsec 터널 문제 해결과 같습니다.일반적인 문제 중 하나는 %CRYPTO-4-RECVD_PKT_MAC_ERR입니다.자세한 문제 해결 정보는 Syslog "%CRYPTO-4-RECVD_PKT_MAC_ERR:" Ping Loss Over IPsec 터널 문제 해결을 참조하십시오.

알려진 문제

이 메시지는 SADB의 SPI와 일치하지 않는 IPsec 패킷이 수신될 때 생성될 수 있습니다.pkt가 일치하지 않는 플로우에 대해 보고된 Cisco 버그 ID CSCtd47420 - GETVPN - CRYPTO-4-RECVD_PKT_NOT_IPSEC을 참조하십시오.예를 들면 다음과 같습니다.

```
%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
```

이 메시지는 %CRYPTO-4-RECVD_PKT_INV_SPI여야 합니다. 이 메시지는 기존 IPsec과 ASR과 같은 일부 하드웨어 플랫폼에 대해 보고됩니다.이 코스메틱 문제는 Cisco 버그 ID CSCup80547에 의해 수정되었습니다.ESP pak용 CRYPTO-4-RECVD_PKT_NOT_IPSEC을 보고하는 동안 오류가 발생했습니다.

> **참고:**이러한 메시지는 다른 GETVPN 버그 CSCup34371 때문에 나타날 수 있습니다 .GETVPN GM은 TEK 키 재설정 후 트래픽 해독을 중지합니다.

이 경우 GM은 SADB에 유효한 IPsec SA가 있지만 GETVPN 트래픽은 해독할 수 없습니다(SA가 키 재지정됨). SA가 만료되면 문제가 즉시 사라지고 SADB에서 제거됩니다.이 문제는 TEK rekey가 미리 수행되기 때문에 상당한 가동 중단을 초래합니다.예를 들어, TEK 수명이 7200초인 경우 가동 중단은 22분이 될 수 있습니다.이 버그를 발생시키기 위해 충족해야 하는 정확한 조건에 대해서는 버그 설명을 참조하십시오.

Cisco IOS-XE를 실행하는 플랫폼에서 GETVPN 문제 해결

문제 해결 명령

Cisco IOS-XE를 실행하는 플랫폼에는 플랫폼별 구현이 있으며, GETVPN 문제에 대해 플랫폼별 디버깅이 필요한 경우가 많습니다.다음은 이러한 플랫폼에서 GETVPN을 트러블슈팅하기 위해 일반적으로 사용되는 명령 목록입니다.

crypto eli all 표시

플랫폼 소프트웨어 ipsec 정책 통계 표시

플랫폼 소프트웨어 ipsec fp 활성 인벤토리 표시

show platform hardware qfp active feature ipsec spd all

플랫폼 하드웨어 qfp 활성 통계 삭제 지우기

show platform hardware qfp active feature ipsec 데이터 삭제 지우기

crypto ipsec sa 표시

crypto gdoi 표시

내부 암호화 ipsec 표시

디버그 암호화 ipsec

디버그 암호화 ipsec 오류

디버그 암호화 ipsec 상태

debug crypto ipsec 메시지

debug crypto ipsec hw-req

debug crypto gdoi gm infra detail

debug crypto gdoi gm rekey detail

ASR1000 공통 문제

IPsec 정책 설치 실패(연속 재등록)

암호화 엔진이 수신한 IPsec 정책 또는 알고리즘을 지원하지 않는 경우 ASR1000 GM이 계속해서 키 서버에 등록될 수 있습니다.예를 들어, Nitrox 기반 ASR 플랫폼(예: ASR1002)에서 Suite-B 또는 SHA2 정책은 지원되지 않으므로 연속 재등록 증상이 발생할 수 있습니다.

일반적인 마이그레이션/업그레이드 문제

ASR1000 TBAR 제한

ASR1000 플랫폼에서 Cisco 버그 ID CSCum37911 수정은 20초 미만의 TBAR 시간이 지원되지 않는 이 플랫폼에 대한 제한을 도입했습니다.IOS-XE의 GETVPN 제한을 참조하십시오.

이 확장 버그가 열려 이 제한을 들어올립니다. Cisco 버그 ID CSCuq25476 - ASR1k는 20초 미만의 GETVPN TBAR 창 크기를 지원해야 합니다.

업데이트:이 제한은 Cisco 버그 ID CSCur57558 수정과 함께 해제되었으며 더 이상 XE3.10.5, XE3.13.2 및 이후 코드에서 제한이 없습니다.

또한 Cisco IOS-XE 플랫폼(ASR1k 또는 ISR4k)에서 실행되는 GM의 경우 TBAR가 활성화된 경우 디바이스에서 이 문제에 대한 수정 사항과 함께 버전을 실행하는 것이 좋습니다.Cisco 버그 ID CSCut91647 - IOS-XE의 GETVPN:GM에서 TBAR 장애로 인해 패킷을 잘못 삭제합니다.

ISR4x00 분류 문제

거부 정책이 무시되는 ISR4x00 플랫폼에서 회귀를 발견했습니다.자세한 내용은 Cisco 버그 ID CSCut14355 - GETVPN - ISR4300 GM에서 거부 정책을 무시합니다.

관련 정보

- GET VPN(Group Encrypted Transport VPN) - Cisco Systems
- 기술 지원 및 문서 – Cisco Systems