일반적인 GETVPN 문제 해결

목차

소개
사전 요구 사항
요구 사항
사용되는 구성 요소
배경 정보 - GETVPN 문제 해결 도구
컨트롤 플레인 디버깅 도구
명령 표시
Syslog
GDOI(Group Domain of 해석) 이벤트 추적
GDOI 조건부 디버깅
전역 암호화 및 GDOI 디버그
데이터 플레인 디버깅 도구
문제 해결
로깅 시설 준비 및 기타 모범 사례
IKE 설정 문제 해결
초기 등록 문제 해결
정책 관련 문제 해결
등록 전에 정책 문제 발생(실패 닫기 정책과 관련)
정책 문제는 POST 등록 후 발생하며 푸시되는 글로벌 정책과 관련이 있습니다.
정책 문제가 POST 등록 후 발생하며 글로벌 정책 및 로컬 재정의 병합과 관련이 있습니다.
키 재설정 문제 해결
TBAR(Time-based Anti-replay) 문제 해결
KS 이중화 문제 해결
FAQ
하나의 GETVPN 그룹에 대해 KS로 구성된 라우터가 동일한 그룹에 대해 GM으로 작동할 수 있습니까?
관련 정보

소개

이 문서에서는 대부분의 일반적인 GETVPN(Group Encrypted Transport VPN) 문제에 대해 수집할 디버그에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- GETVPN
- 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.

배경 정보 - GETVPN 문제 해결 도구

GETVPN은 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 시작하는 것이 좋습니다. 따라서 생산 환경이 부정적인 영향을 받지 않도록 해야 합니다.이 섹션에서는 이러한 프로세스를 지원하기 위해 일반적으로 사용되는 몇 가지 도구에 대해 설명합니다.

컨트롤 플레인 디버깅 도구

명령 표시

show 명령은 GETVPN 환경에서 런타임 작업을 표시하기 위해 일반적으로 사용됩니다.

Syslog

GETVPN에는 중요한 프로토콜 이벤트 및 오류 조건을 위한 향상된 syslog 메시지 집합이 있습니다 .디버그를 실행하기 전에 항상 맨 먼저 확인해야 합니다.

GDOI(Group Domain of 해석) 이벤트 추적

이 기능은 버전 15.1(3)T에 추가되었습니다.이벤트 추적 기능을 사용하면 GDOI 이벤트 및 오류가 발생할 경우 항상 사용 가능한 경량 추적을 제공합니다.또한 예외 조건에 대해 traceback이 활성화된 exit-path 추적도 있습니다.

GDOI 조건부 디버깅

이 기능은 버전 15.1(3)T에 추가되었습니다.피어 주소를 기반으로 지정된 디바이스에 대해 필터링된 디버그를 허용하며 가능한 경우 항상, 특히 키 서버에서 사용해야 합니다.

전역 암호화 및 GDOI 디버그

이는 다양한 GETVPM 디버그입니다.관리자는 대규모 환경에서 디버깅할 때 주의해야 합니다 .GDOI 디버그를 사용하면 디버깅 세분화를 위해 5개의 디버그 수준이 제공됩니다.

```
GM1#debug crypto gdoi gm rekey ?
all-levels All levels
detail Detail level
error Error level
event Event level
packet Packet level
terse Terse level
```

디버그 수준	혜택
오류	오류 조건
테르세	사용자 및 프로토콜 문제에 대한 중요 메시지
이벤트	상태 전환 및 키 보내기 및 받기 등의 이벤트
세부 정보	가장 자세한 디버그 메시지 정보
패킷	자세한 패킷 정보 덤프 포함
모두	위의 모든 항목

데이터 플레인 디버깅 도구

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)

문제 해결

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(Group Members) 및 KS(Key Servers)에서 **show tech** 명령을 입력하고 필요한 경우 **show ip route** 명령의 출력을 글로벌 및 각 관련 VRF(Virtual Routing and Forwarding)에서 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 항

상 동일한 출력의 여러 이터레이션을 수집합니다.

IKE 설정 문제 해결

등록 프로세스가 처음 시작되면 GM과 KS는 GDOI 트래픽을 보호하기 위해 IKE(Internet Key Exchange) 세션을 협상합니다.

- GM에서 IKE가 성공적으로 설정되었는지 확인합니다.

```
gm1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
172.16.1.9 172.16.1.1 GDOI_REKEY 1068 ACTIVE
172.16.1.1 172.16.1.9 GDOI_IDLE 1067 ACTIVE
```

참고:등록 기준인 GDOI_IDLE 상태는 초기 등록 이후 더 이상 필요하지 않으므로 빠르게 시간 초과되고 사라집니다.

- KS에서 다음을 확인해야 합니다.

```
ks1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
172.16.1.1 172.16.1.9 GDOI_IDLE 1001 ACTIVE
```

참고:키 재설정 세션은 KS에서 필요한 경우에만 나타납니다.

해당 상태에 도달하지 않은 경우 다음 단계를 완료합니다.

- 실패 원인에 대한 자세한 내용은 다음 명령의 출력을 확인하십시오.
  `router# show crypto isakmp statistics`
- 이전 단계가 도움이 되지 않는 경우 일반적인 IKE 디버그를 활성화하면 프로토콜 레벨 정보를 얻을 수 있습니다.
  `router# debug crypto isakmp`
  참고:
  * IKE가 사용되더라도 일반 UDP/500 포트에서 사용되지 않고 UDP/848에서 사용됩니다.
  * 이 수준에서 문제가 발생하면 KS 및 영향을 받는 GM 모두에 대한 디버그를 제공하십시오.

- 그룹 키 리키에 대한 RSA(Rivest-Shamir-Adleman) 서명에는 의존하기 때문에 KS는 RSA 키가 구성되어 **있어야** 하며 그룹 컨피그레이션에 지정된 키와 동일한 이름을 가져야 합니다.

  이를 확인하려면 다음 명령을 입력합니다.

```
ks1# show crypto key mypubkey rsa
```

초기 등록 문제 해결

GM에서 등록 상태를 확인하려면 다음 명령의 출력을 검토합니다.

```
gm1# show crypto gdoi | i Registration status
Registration status  : Registered
gm1#
```

출력에 **Registered** 이외의 명령이 표시되면 다음 명령을 입력합니다.

GM에서

- 암호화 지원 인터페이스를 종료합니다.
  주의:대역 외 관리가 활성화되어야 합니다.

- 다음 디버깅 사용:

```
gm1# debug crypto gdoi infra packet
gm1# debug crypto gdoi gm packet
```

- KS 측에서 디버깅을 활성화합니다(다음 섹션 참조).

- KS 디버그가 준비되면 암호화 지원 인터페이스를 종료하고 등록을 기다립니다(프로세스를 가속화하기 위해 GM에서 **clear crypto gdoi** 명령을 실행합니다).

KS에서 다음을 수행합니다.

- KS에 RSA 키가 있는지 확인합니다.

```
ks1# show crypto key mypubkey rsa
```

- 다음 디버깅 사용:

```
ks1# debug crypto gdoi infra packet
ks1# debug crypto gdoi ks packet
```

정책 관련 문제 해결

등록 전에 정책 문제 발생(실패 닫기 정책과 관련)

이 문제는 GM에만 영향을 미치므로 GM에서 다음 출력을 수집하십시오.

```
gm1# show crypto ruleset
```

참고: Cisco IOS-XE에서? 패킷 분류가 소프트웨어에서 수행되지 않으므로 이 출력은 항상 비어 있습니다.

영향을 받는 디바이스의 **show tech** 명령 출력은 필요한 나머지 정보를 제공합니다.

정책 문제는 POST 등록 후 발생하며 푸시되는 글로벌 정책과 관련이 있습니다.

이 문제가 발생하는 방법에는 일반적으로 두 가지가 있습니다.

- KS가 이런 정책을 GM에 강요할 수는 없다.
- GM들 사이에 정책의 부분적인 적용이 있다.

두 문제 중 하나를 해결하는 데 도움이 되도록 다음 단계를 완료하십시오.

1. 영향을 받는 GM에서 다음 출력을 수집합니다.

```
gm1# show crypto gdoi acl
gm1# show crypto ruleset
```

2. GM에서 다음 디버깅 사용:

```
gm1# debug crypto gdoi infra packet
gm1# debug crypto gdoi gm acls packet
```

3. 영향을 받는 GM이 등록하는 KS에서 다음 출력을 수집합니다.

```
ks1# show crypto gdoi ks members
ks1# show crypto gdoi ks policy
```

참고:GM이 어떤 KS에 연결하는지 확인하려면 show crypto gdoi group 명령**을** 입력합니다.

4. 동일한 KS에서 다음 디버그를 활성화합니다.

```
ks1# debug crypto gdoi infra packet
ks1# debug crypto gdoi ks acls packet
```

5. GM에서 다음 명령을 사용하여 GM을 강제로 등록합니다.

```
clear crypto gdoi
```

정책 문제가 POST 등록 후 발생하며 글로벌 정책 및 로컬 재정의 병합과 관련이 있습니다.

이 문제는 일반적으로 암호화된 패킷이 수신되었음을 나타내는 메시지 형태로 나타납니다. 이는 로컬 정책이 암호화 되지 않아야 함을 나타내고 그 반대의 경우도 마찬가지입니다.이 경우 이전 섹션에서 요청한 모든 데이터 및 **show tech** 명령 출력이 필요합니다.

키 재설정 문제 해결

GM에서

- 다음 디버깅 수집:

```
gm1# debug crypto gdoi infra packet
gm1# debug crypto gdoi gm packet
gm1# debug crypto gdoi gm rekey packet
```

- GM에 GDOI_REKEY 유형의 IKE SA(Security Association)가 여전히 있는지 확인하려면 다음 명령을 입력합니다.

```
gm1# show crypto isakmp sa
```

KS에서 다음을 수행합니다.

- EACH KS에서 **show crypto key mypubkey rsa** 명령 출력을 수집합니다.키는 **동일해야** 합니다.
- KS에서 발생하는 작업을 보려면 다음 디버그를 입력합니다.

```
ks1# debug crypto gdoi infra packet
ks1# debug crypto gdoi ks packet
ks1# debug crypto gdoi ks rekey packet
```

TBAR(Time-based Anti-replay) 문제 해결

TBAR 기능을 사용하려면 여러 그룹에 걸쳐 시간을 유지해야 하므로 GM 유사 시간 클럭이 지속적으로 재동기화되어야 합니다.이 작업은 키 재설정 동안 또는 두 시간 간격으로 수행되며, 둘 중 먼저 수행됩니다.

> **참고:**모든 출력과 디버그는 GM과 KS에서 동시에 수집하여 상호 연관성을 적절하게 파악해야 합니다.

이 수준에서 발생하는 문제를 조사하려면 이 출력을 수집하십시오.

- GM에서

```
gm1# show crypto gdoi
gm1# show crypto gdoi replay
```

- KS에서:

```
ks1# show crypto gdoi ks members
ks1# show crypto gdoi ks replay
```

TBAR 시간 유지를 보다 동적으로 조사하려면 다음 디버그를 활성화합니다.

- GM의 경우

```
gm1# debug crypto gdoi gm rekey packet
gm1# debug crypto gdoi replay packet (verbosity might need to be lowered)
```

- KS에서:

```
ks1# debug crypto gdoi ks rekey packet
ks1# debug crypto gdoi replay packet (verbosity might need to be lowered)
```

Cisco IOS Version 15.2(3)T부터 TBAR 오류를 기록할 수 있는 기능이 추가되어 이러한 오류를 더 쉽게 찾아낼 수 있습니다.GM에서 다음 명령을 사용하여 TBAR 오류가 있는지 확인합니다.

```
R103-GM#show crypto gdoi gm replay
Anti-replay Information For Group GETVPN:
 Timebased Replay:
   Replay Value             : 512.11 secs
   Input Packets            : 0        Output Packets           : 0
   Input Error Packets    : 0        Output Error Packets    : 0
   Time Sync Error         : 0        Max time delta            : 0.00secs

TBAR Error History (sampled at 10pak/min):
   No TBAR errors detected
```

TBAR 문제를 해결하는 방법에 대한 자세한 내용은 시간 기반 재전송 방지 실패 를 참조하십시오.

KS 이중화 문제 해결

COOP(Cooperative)는 IKE 간 통신을 보호하기 위해 IKE 세션을 설정하므로, 이전에 IKE 설정에 대해 설명한 트러블슈팅 기술도 여기에 적용됩니다.

COOP별 문제 해결은 관련된 모든 KS에서 이 명령의 출력 확인을 구성합니다.

```
ks# show crypto gdoi ks coop
```

> **참고:**COOP KS를 구축하는 경우 발생하는 가장 일반적인 실수는 모든 KS에서 그룹에 대해 동일한 RSA 키(개인 및 공용)를 가져오는 것을 잊어버리는 것입니다.이렇게 하면 키 재설정 중에 문제가 발생합니다.KS 간의 공개 키를 확인 및 비교하려면 각 KS에서 **show crypto key mypubkey rsa** 명령의 출력을 비교합니다.

프로토콜 수준 문제 해결이 필요한 경우 관련된 모든 KS에서 이 디버그를 활성화합니다.

```
ks# debug crypto gdoi ks coop packet
```

FAQ

"% Setting rekey authentication rejected" 오류 메시지가 표시되는 이유는 무엇입니까?

이 행이 추가된 후 KS를 구성할 때 다음 오류 메시지가 표시됩니다.

```
KS(gdoi-local-server)#rekey authentication mypubkey rsa GETVPN_KEYS
% Setting rekey authentication rejected.
```

이 오류 메시지의 이유는 일반적으로 GETVPN_KEYS라는 키가 존재하지 않기 때문입니다.이 문제를 해결하려면 다음 명령을 사용하여 올바른 레이블로 키를 만듭니다.

```
crypto key generate rsa mod <modulus> label <label_name>
```

> **참고:**COOP 구축인 경우 끝에 exportable 키워드를 추가한 다음 다른 KS에서 동일한 키를 가져옵니다.

하나의 GETVPN 그룹에 대해 KS로 구성된 라우터가 동일한 그룹에 대해 GM으로 작동할 수 있습니까?

아니요. 모든 GETVPN 구축에는 동일한 그룹에 대해 GM으로 참여할 수 없는 전용 KS가 필요합니다.암호화, 라우팅, QoS 등의 가능한 모든 상호 작용을 통해 GM 기능을 KS에 추가하는 것은 이 중요한 네트워크 장치의 상태에 적합하지 않기 때문에 이 기능은 지원되지 않습니다.전체 GETVPN 구축이 작동하려면 항상 사용 가능해야 합니다.

관련 정보

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