패킷 캡처와 관련된 IPsec 터널 및 일반적인 컨트롤 플레인 문제 해결

목차

소개

이 문서에서는 Cisco IOS® XE 라우터에서 사이트 간 VPN을 협상할 때 패킷 캡처, 기타 툴을 통해 컨트롤 플레인 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco IOS® CLI 구성에 대한 기본 지식
- IKEv2 및 IPsec에 대한 기본 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- CSR1000V - 버전 16.12.0을 실행하는 Cisco IOS XE Software.

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

배경 정보

패킷 캡처는 VPN 피어 디바이스 간에 패킷이 전송/수신되는지 여부를 확인하는 데 도움이 되는 강력한 도구입니다. 또한 IPsec 디버그와 함께 표시되는 동작이 캡처에 수집된 출력과 일치하는지 확인합니다. 디버그는 논리적 해석이며, 캡처는 피어 간의 물리적 상호 작용을 나타냅니다. 따라서 연결 문제를 확인하거나 취소할 수 있습니다.

유용한 툴

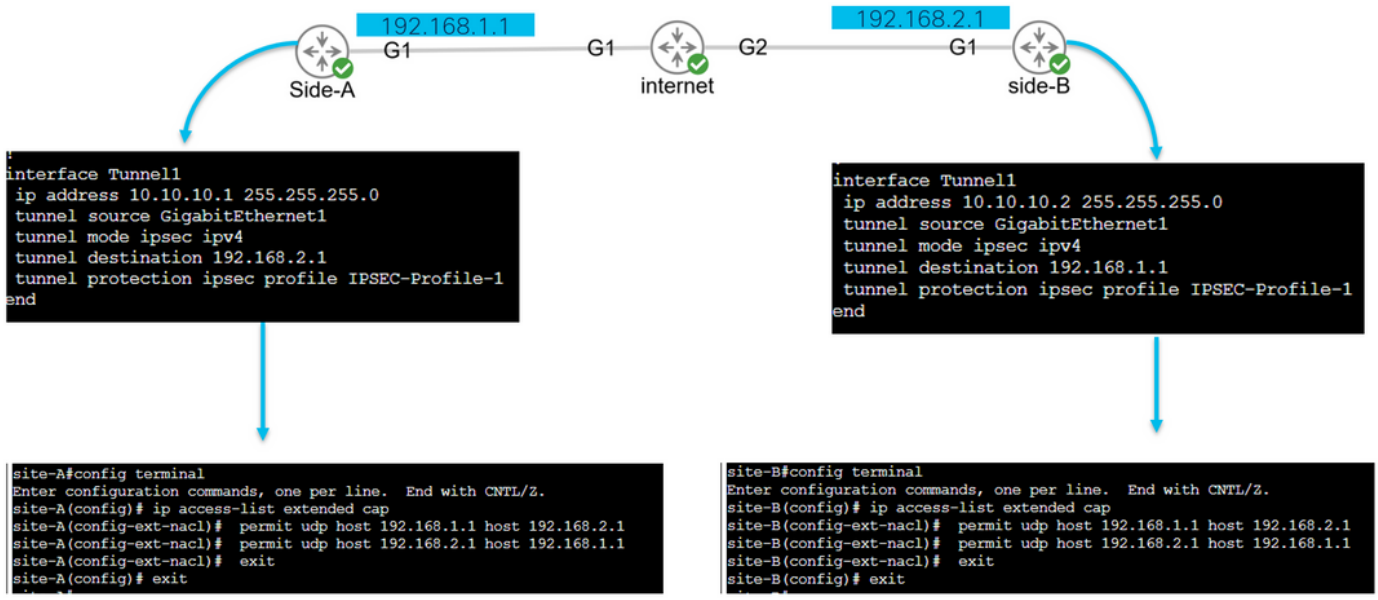
캡처를 구성하고, 출력을 추출하고, 더 자세히 분석하는 데 도움이 되는 유용한 툴이 있습니다. 그 중 일부는 다음과 같습니다.

- Wireshark: 잘 알려진 오픈 소스 패킷 분석기입니다.
- 모니터 캡처: 라우터의 Cisco IOS XE 기능은 캡처를 수집하고 트래픽 흐름의 모습, 수집된 프로토콜 및 타임스탬프를 간단하게 출력할 수 있도록 지원합니다.

IOS XE 라우터에서 캡처를 구성하는 방법

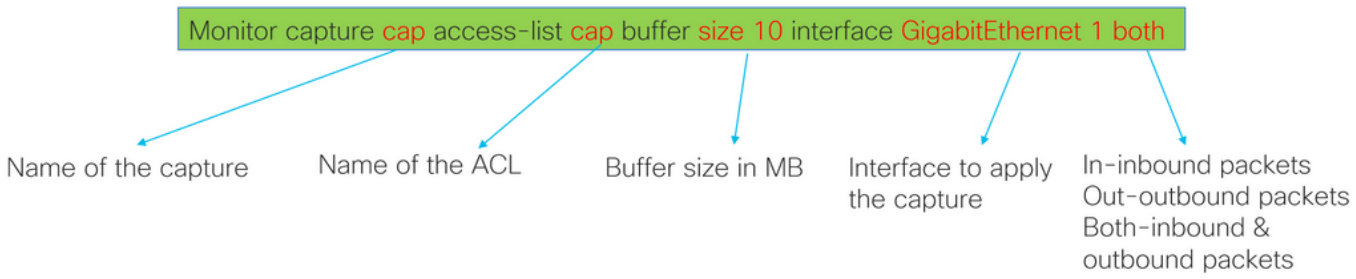
캡처는 수집할 트래픽의 유형, VPN 피어 또는 관련 트래픽의 세그먼트의 소스 및 목적지 주소를 정의하는 확장 ACL(access-list)을 사용합니다. 터널 협상은 NAT-T가 경로를 따라 활성화된 경우 UDP 포트 500 및 포트 4500을 사용합니다. 협상이 완료되고 터널이 설정되면 NAT-T가 활성화된 경우 관심 트래픽은 IP 프로토콜 50(ESP) 또는 UDP 4500을 사용합니다.

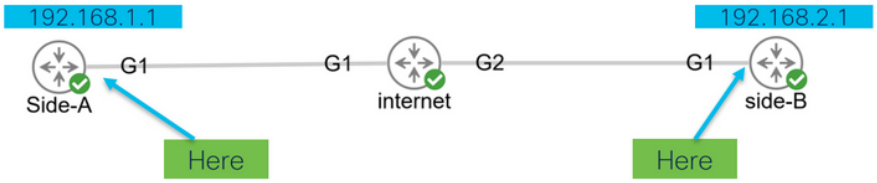
컨트롤 플레인 관련 문제를 해결하려면 VPN 피어 IP 주소를 사용하여 터널이 협상되는 방법을 캡처해야 합니다.




```
config terminal
ip access-list extended <ACL name>
permit udp host <local address> host <peer address>
permit udp host <peer address> host <source address>
exit
exit
```

구성된 ACL은 캡처된 트래픽의 범위를 좁히는 데 사용되며, 터널 협상에 사용되는 인터페이스에 배치됩니다.






```
monitor capture cap access-list cap buffer size 10 interface GigabitEthernet1 both
monitor capture  cap start
```

```
monitor capture cap access-list cap buffer size 10 interface GigabitEthernet1 both
monitor capture  cap start
```

```
Status Information for Capture cap
  Target Type:
 Interface: GigabitEthernet1, Direction: BOTH
   Status : Active
  Filter Details:
   Access-list: cap
  Buffer Details:
   Buffer Type: LINEAR (default)
   Buffer Size (in MB): 10
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
   Packet sampling rate: 0 (no sampling)
site-A#
```

```
Status Information for Capture cap
  Target Type:
 Interface: GigabitEthernet1, Direction: BOTH
   Status : Active
  Filter Details:
   Access-list: cap
  Buffer Details:
   Buffer Type: LINEAR (default)
   Buffer Size (in MB): 10
  Limit Details:
   Number of Packets to capture: 0 (no limit)
   Packet Capture duration: 0 (no limit)
   Packet Size to capture: 0 (no limit)
   Maximum number of packets to capture per second: 1000
   Packet sampling rate: 0 (no sampling)
site-B#
```

```
monitor capture <capture name> access-list <ACL name> buffer size <custom buffer size in MB> interface
```

캡처가 구성되면 이를 중지하거나 지우거나 다음 명령으로 수집된 트래픽을 추출하도록 조작할 수 있습니다.

- 일반 캡처 정보 확인: 모니터 캡처 표시
- 캡처 시작/중지: 캡처 상한 시작/중지 모니터링
- 캡처에서 패킷을 수집 중인지 확인: show monitor capture cap buffer
- 트래픽의 간략한 출력 보기: show monitor capture cap buffer brief
- 캡처 지우기: 캡처 캡 지우기 모니터링
- 캡처 출력을 추출합니다.
  - 모니터 캡 캡 버퍼 덤프
  - 모니터 캡처 캡 내보내기 bootflash:capture.pcap

패킷 캡처를 사용하여 터널 설정 분석

앞에서 설명한 것처럼 IPSec 터널을 협상하기 위해 NAT-T가 활성화된 경우 패킷이 포트 500 및 포트 4500을 사용하여 UDP를 통해 전송됩니다. 캡처를 사용하면 협상되는 단계(단계 1 또는 단계 2), 각 디바이스의 역할(개시자 또는 응답자), 방금 생성한 SPI 값 등의 패킷에서 추가 정보를 볼 수 있습니다.

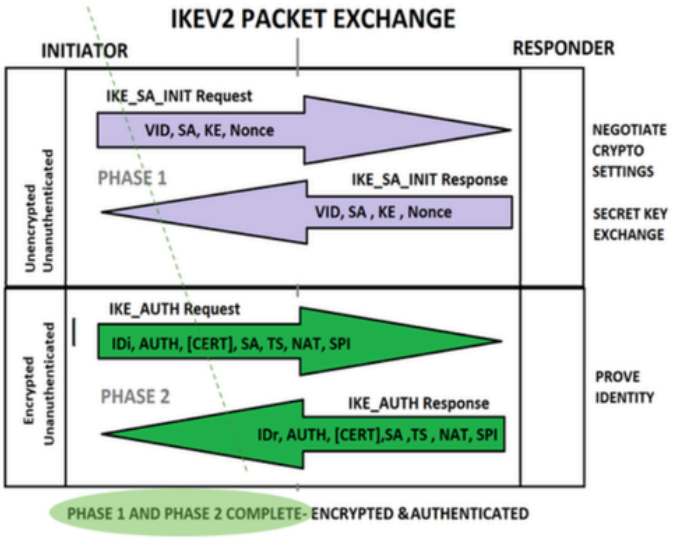
UDP 500/4500 packets seen.

Initiator and responder roles.

SPI values created.

Phase 1 in clear text.

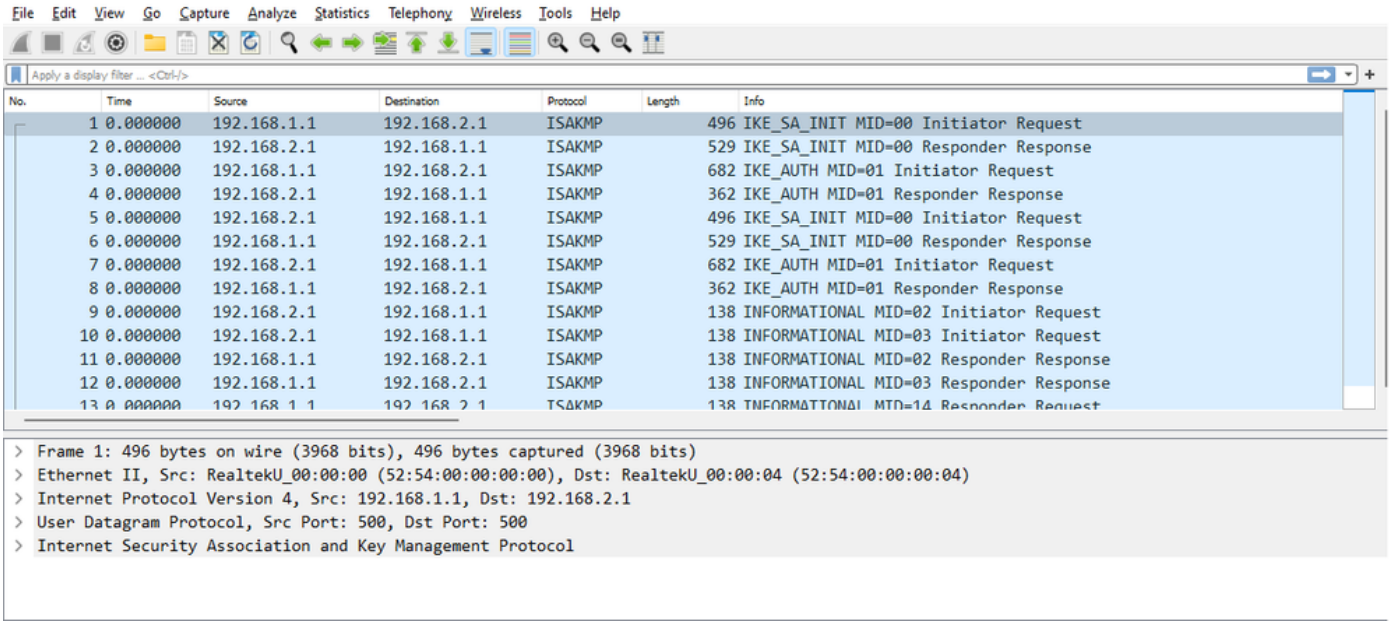
Phase 2 encrypted



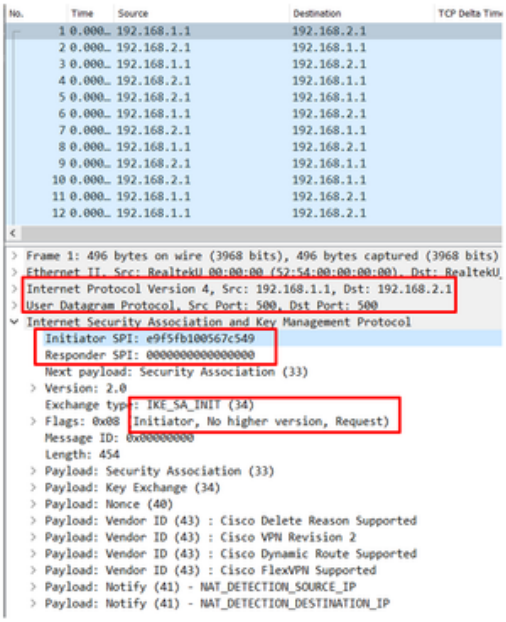
라우터에서 캡처의 간략한 출력을 표시하면 피어 간의 상호 작용이 확인되어 UDP 패킷을 전송합니다.

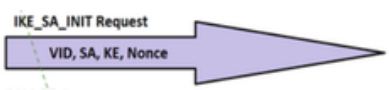
```
site-A#show monitor cap cap buffer brief
 ------------------------------------------------------------------------------
 #   size   timestamp     source               destination      dscp    protocol
 ------------------------------------------------------------------------------
   0  496    0.000000    192.168.1.1      ->  192.168.2.1      48 CS6  UDP
   1  529    0.011992    192.168.2.1      ->  192.168.1.1      48 CS6  UDP
   2  682    0.026991    192.168.1.1      ->  192.168.2.1      48 CS6  UDP
   3  362    0.035993    192.168.2.1      ->  192.168.1.1      48 CS6  UDP
   4  496    0.579016    192.168.2.1      ->  192.168.1.1      48 CS6  UDP
   5  529    0.593023    192.168.1.1      ->  192.168.2.1      48 CS6  UDP
   6  682    0.610020    192.168.2.1      ->  192.168.1.1      48 CS6  UDP
   7  362    0.616017    192.168.1.1      ->  192.168.2.1      48 CS6  UDP
   8  138    0.638019    192.168.2.1      ->  192.168.1.1      48 CS6  UDP
   9  138    0.638019    192.168.2.1      ->  192.168.1.1      48 CS6  UDP
  10  138    0.641009    192.168.1.1      ->  192.168.2.1      48 CS6  UDP
  11  138    0.655016    192.168.1.1      ->  192.168.2.1      48 CS6  UDP
```

덤프를 추출하고 라우터에서 pcap 파일을 내보내면 패킷에서 더 많은 정보가 wireshark를 사용하여 표시됩니다.



전송된 첫 번째 IKE_SA_INIT Exchange 패킷의 Internet Protocol 섹션에는 UDP 패킷의 소스 및 목적지 주소가 있습니다. User Datagram Protocol(사용자 데이터그램 프로토콜) 섹션에는 사용된 포트와 Internet Security Association and Key Management Protocol(인터넷 보안 연계 및 키 관리 프로토콜) 섹션에 프로토콜의 버전, 교환 중인 메시지 유형, 디바이스의 역할 및 생성된 SPI가 표시됩니다. IKEv2 디버그를 수집할 때 디버그 로그에 동일한 정보가 표시됩니다.





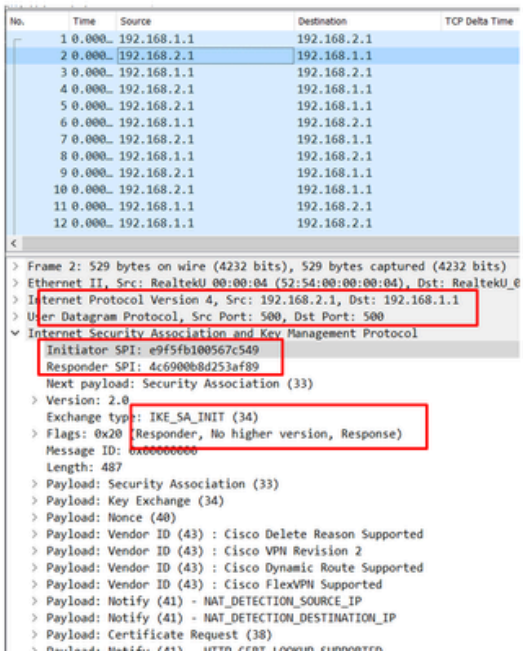
Unencrypted!

IKEv2:(SESSION ID = 18,SA ID = 2):Sending Packet [To 192.168.2.1:500/From 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 0000000000000000
Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
SA KE N VID VID VID VID NOTIFY(NAT_DETECTION_SOURCE_IP)
NOTIFY(NAT_DETECTION_DESTINATION_IP)

Debug crypto ikev2
Debug crypto ipsec

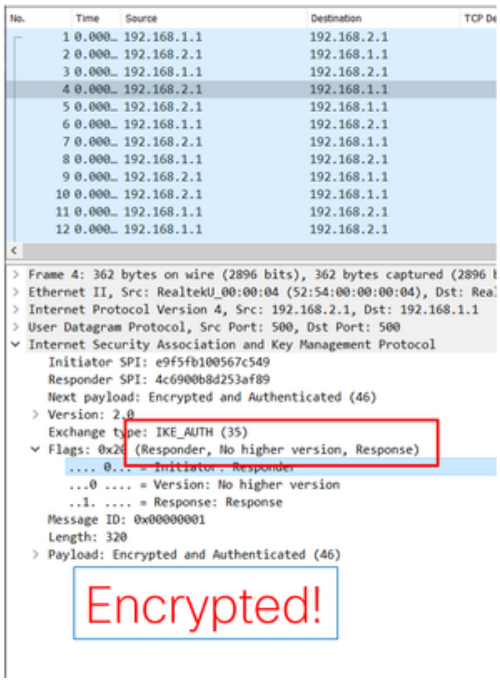
IKEv2:(SESSION ID = 18,SA ID = 2):Received Packet [From 192.168.2.1:500/To 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE
Payload contents:
SA KE N VID VID VID VID NOTIFY(NAT_DETECTION_SOURCE_IP) NOTIFY(NAT_DETECTION_DESTINATION_IP) CERTREQ NOTIFY(HTTP_CERT_LOOKUP_SUPPORTED)

Unencrypted!



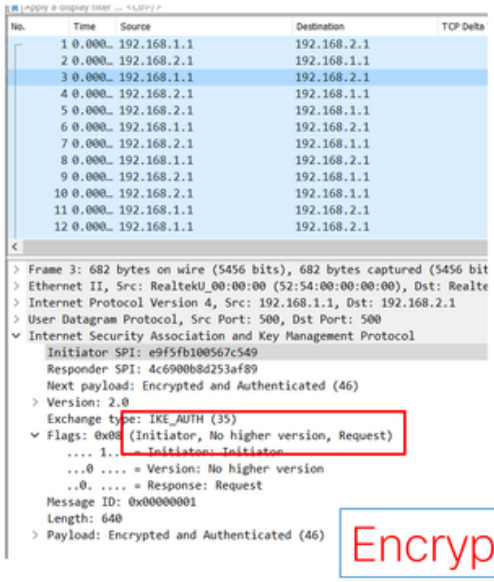
IKE_AUTH Exchange 협상이 발생하면 페이로드가 암호화되지만 이전에 생성된 SPI 및 생성되는 트랜잭션 유형과 같은 협상에 대한 일부 정보가 표시됩니다.

IKEv2:(SESSION ID = 18,SA ID = 2):Received Packet [From 192.168.2.1:500/To 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 1
IKEv2 IKE_AUTH Exchange RESPONSE



Encrypted!

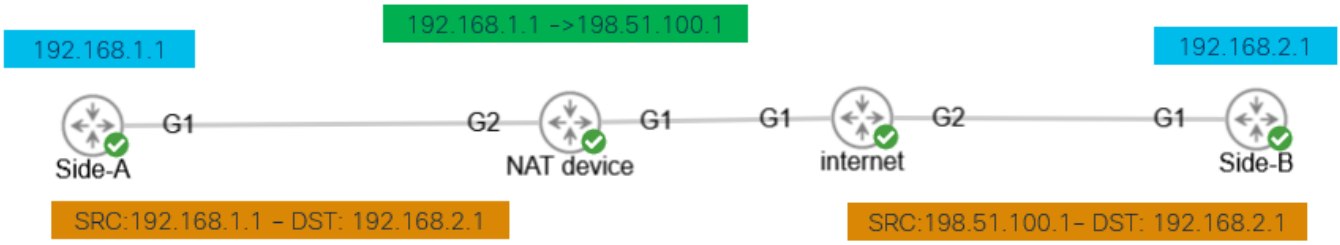
마지막 IKE_AUTH Exchange 패킷이 수신되면 터널 협상이 완료됩니다.



Encrypted!

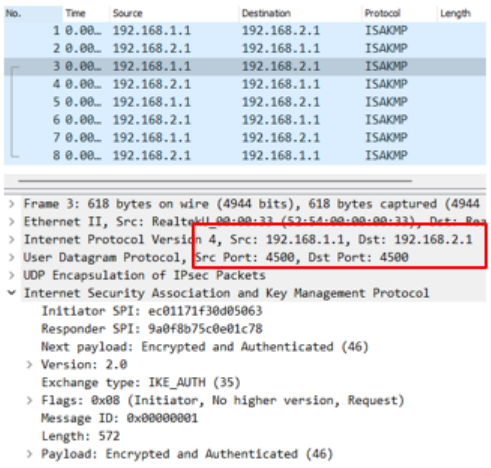
IKEv2:(SESSION ID = 18,SA ID = 2):Sending Packet [To 192.168.2.1:500/From 192.168.1.1:500/VRF i0:f0]
Initiator SPI : E9F5FB100567C549 - Responder SPI : 4C6900B8D253AF89
Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:
ENCR

Transaction When NAT is in Between(NAT가 다음 사이에 있는 경우 트랜잭션)



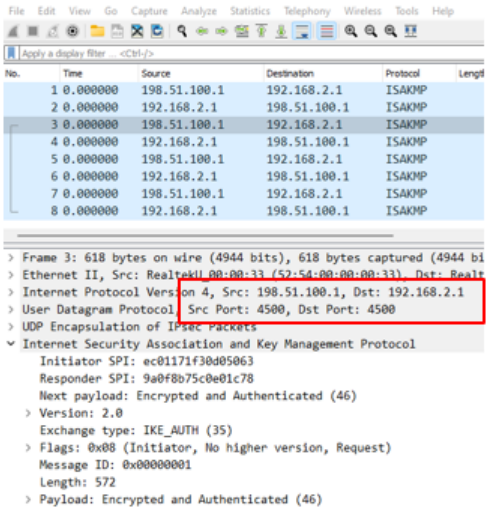
Nat-transversal은 터널 협상이 발생할 때 볼 수 있는 또 다른 기능입니다. 중간 디바이스에서 터널에 사용된 하나 또는 두 주소를 모두 시작하는 경우, 디바이스는 2단계(IKE_AUTH Exchange)가 협상될 때 UDP 포트를 500에서 4500으로 변경합니다.

A측에서 캡처한 내용:



IKEv2:(SESSION ID = 10,SA ID = 1):Received Packet [From 192.168.1.1:4500/To 192.168.2.1:4500/VRF i0:f0]
Initiator SPI : EC01171F30D05063 - Responder SPI : 9A0F8B75C0E01C78
Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
.....
IKEv2:(SESSION ID = 10,SA ID = 1):Stopping timer to wait for auth message
IKEv2:(SESSION ID = 10,SA ID = 1):Checking NAT discovery
IKEv2:(SESSION ID = 10,SA ID = 1):NAT INSIDE found
IKEv2:(SESSION ID = 10,SA ID = 1):NAT detected float to init port 4500, resp port 4500

B측에서 캡처한 내용:



IKEv2:(SESSION ID = 11,SA ID = 1):Sending Packet [To 192.168.2.1:4500/From 198.51.100.1:4500/VRF i0:f0]
Initiator SPI : EC01171F30D05063 - Responder SPI : 9A0F8B75C0E01C78
Message id: 1
IKEv2 IKE_AUTH Exchange REQUEST
Payload contents:

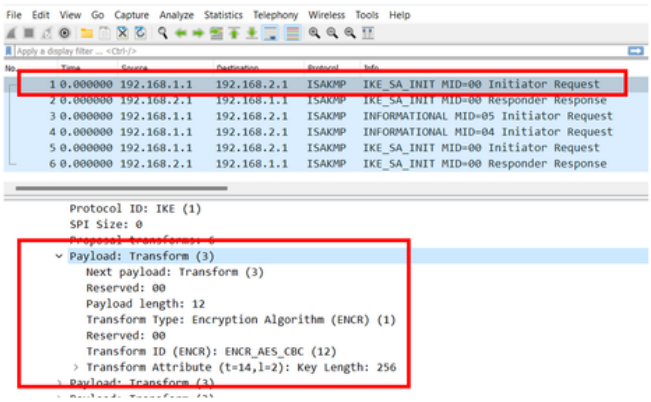
일반적인 컨트롤 플레인 문제

터널 협상에 영향을 미치는 로컬 또는 외부 요인이 있을 수 있으며, 캡처를 통해 식별할 수도 있습니다. 다음 시나리오가 가장 일반적입니다.

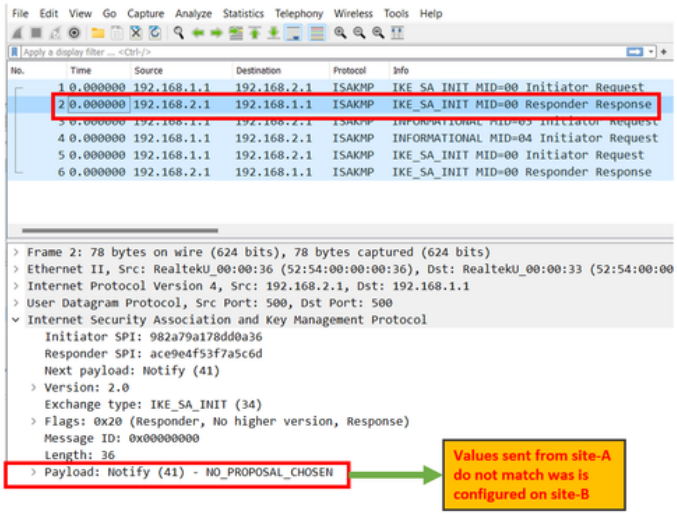
컨피그레이션 불일치

이 시나리오는 각 디바이스 1단계 및 2단계 컨피그레이션을 확인하여 해결할 수 있습니다. 그러나 원격 엔드에는 액세스할 수 없는 시나리오가 발생할 수 있습니다. 1단계 또는 2단계에서 패킷 내에서 NO_PROPOSAL_CHOSEN을 전송하는 디바이스를 식별하여 도움말을 캡처합니다. 이 응답은 컨피그레이션에 문제가 있을 수 있으며 어떤 단계를 조정해야 하는지를 나타냅니다.

Side-A



Side-B

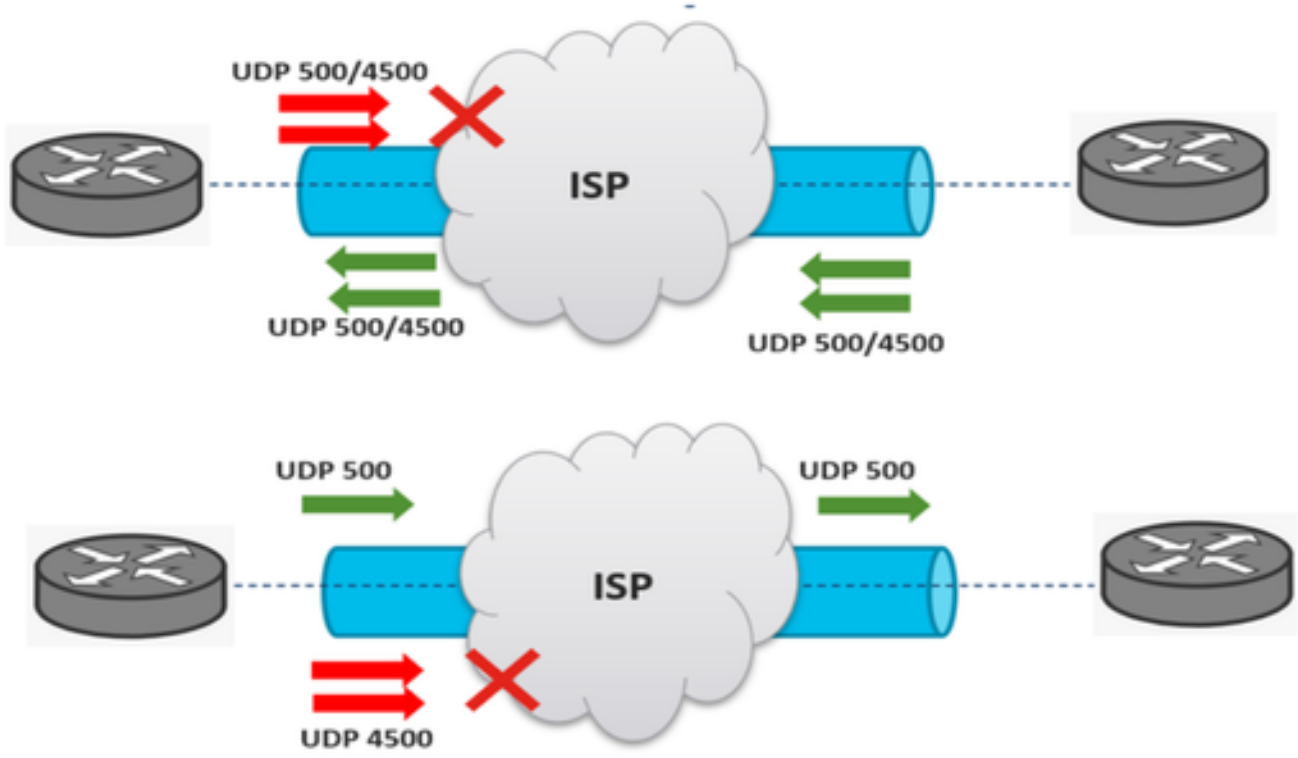


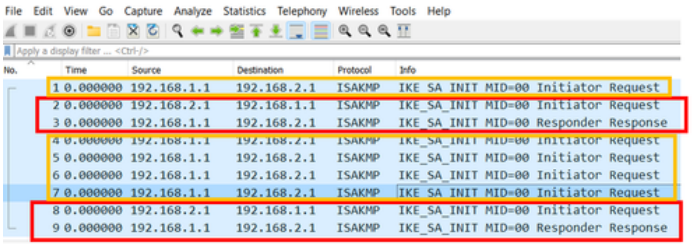
재전송

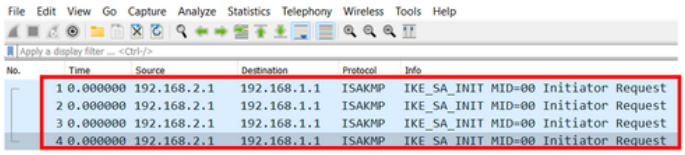
IPSec 터널 협상은 협상 패킷이 최종 디바이스 간의 경로를 따라 삭제되었기 때문에 실패할 수 있습

니다. 삭제된 패킷은 1단계 또는 2단계 패킷일 수 있습니다. 이 경우 응답 패킷이 예상되는 장치는 마지막 패킷을 재전송하고, 5회 시도 후 응답이 없으면 터널이 종료되어 처음부터 다시 시작됩니다.

터널의 양쪽에 있는 캡처를 통해 트래픽을 차단할 수 있는 항목과 트래픽이 영향을 받는 방향을 확인할 수 있습니다.







A device or service in between is blocking UDP packets that come from side-A

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.