정책 기반 VPN 터널 내 암호화 ACL 카운터 이해

목차

소개

이 문서에서는 정책 기반 VPN 터널 내의 암호화 ACL(Access Control List) 카운터의 동작을 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- Cisco IOS® /Cisco IOS® XE 플랫폼의 정책 기반 사이트 대 사이트 VPN
- Cisco IOS/Cisco IOS XE Platform의 액세스 제어 목록

사용되는 구성 요소

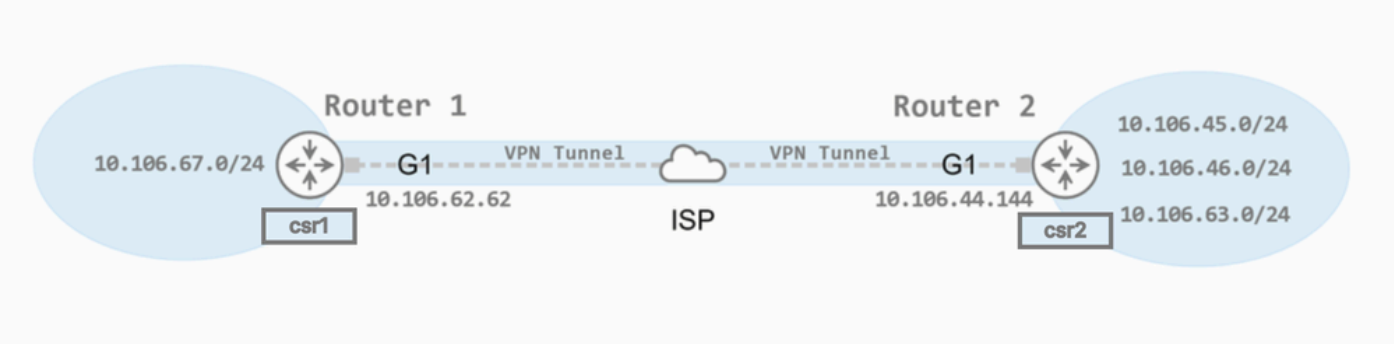
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco C8kv, 버전 17.12.04(MD)

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.

토폴로지



토폴로지

시나리오

서로 다른 두 가지 시나리오를 검토함으로써 서로 다른 피어에서 트래픽이 시작되고 터널이 재설정될 때 ACL 적중 횟수가 어떻게 영향을 받는지 파악하는 데 목적이 있습니다.

1. 시나리오 1: VPN 터널이 비활성 상태일 때 라우터 1에서 시작된 트래픽

   이 시나리오에서는 VPN 터널이 초기에 중단되고 트래픽이 Router1에서 시작될 때 ACL 적중 횟수의 변경 사항을 분석합니다. 이 분석을 통해 초기 설정 및 암호화 ACL 카운터가 첫 번째 트래픽 흐름 시도에 어떻게 반응하는지 알 수 있습니다.

2. 시나리오 2: VPN 터널이 활성 상태일 때 라우터 2에서 시작된 트래픽

   이 시나리오에서는 VPN 터널이 이미 설정되어 있고 Router2에서 시작된 트래픽에 대해 살펴봅니다. 이 시나리오에서는 터널이 활성 상태이고 다른 피어에서 트래픽이 유입될 때 ACL 카운터가 어떻게 동작하는지 알아봅니다.

이러한 시나리오를 비교하여 다양한 조건에서 VPN 터널의 ACL 카운터 역학을 포괄적으로 이해할 수 있습니다.

설정

피어로 지정된 2개의 Cisco C8kv 라우터 간에 정책 기반 Site-to-Site VPN 터널을 구성했습니다. 라우터1의 이름은 "csr1"이고 라우터2의 이름은 "csr2"입니다.

Router1의 암호화 컨피그레이션

```
csr1#sh ip int br
Interface              IP-Address      OK?   Method   Status   Protocol
```

```
GigabitEthernet1     10.106.62.62     YES   NVRAM    up       up
GigabitEthernet2     10.106.67.27     YES   NVRAM    up       up
```

```
csr1#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
   set peer 10.106.44.144
   set transform-set new_ts
   set ikev2-profile new_profile
   match address new_acl
```

```
csr1#sh ip access-lists new_acl
Extended IP access list new_acl
   10 permit ip 10.106.67.0 0.0.0.255 10.106.45.0 0.0.0.255 log
   20 permit ip 10.106.67.0 0.0.0.255 10.106.46.0 0.0.0.255
   30 permit ip 10.106.67.0 0.0.0.255 10.106.63.0 0.0.0.255 log
```

```
csr1#sh run int GigabitEthernet1
Building configuration...

Current configuration : 162 bytes
!
interface GigabitEthernet1
ip address 10.106.62.62 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

라우터2의 암호화 컨피그레이션

```
csr2#sh ip int br
Interface              IP-Address        OK?     Method       Status     Protocol
GigabitEthernet1       10.106.44.144     YES     NVRAM        up         up
GigabitEthernet2       10.106.45.145     YES     NVRAM        up         up
GigabitEthernet3       10.106.46.146     YES     NVRAM        up         up
GigabitEthernet4       10.106.63.13      YES     NVRAM        up         up
```

```
csr2#sh run | sec crypto map
crypto map nigarapa_map 100 ipsec-isakmp
   set peer 10.106.62.62
   set transform-set new_ts
   set ikev2-profile new_profile
   match address new_acl
```

```
csr2#sh ip access-lists new_acl
Extended IP access list new_acl
   10 permit ip 10.106.45.0 0.0.0.255 10.106.67.0 0.0.0.255
   20 permit ip 10.106.46.0 0.0.0.255 10.106.67.0 0.0.0.255
   30 permit ip 10.106.63.0 0.0.0.255 10.106.67.0 0.0.0.255
```

```
csr2#sh run int GigabitEthernet1
Building configuration...

Current configuration : 163 bytes
!
interface GigabitEthernet1
ip address 10.106.44.144 255.255.255.0
ip nat outside
negotiation auto
no mop enabled
no mop sysid
crypto map nigarapa_map
end
```

VPN 터널 내 Crypto Access Control List 카운터의 동작 분석

처음에는 두 디바이스 모두 각각의 암호화 액세스 목록에서 ACL 적중 횟수가 0입니다.

두 피어 디바이스의 각 암호화 액세스 목록에서 Access Control List 적중 횟수가 0입니다.

시나리오 1: VPN 터널이 비활성 상태일 때 라우터 1에서 시작된 트래픽

초기 상태:

Router1(IP: 10.106.67.27) 및 라우터2(IP: 10.106.45.145는 현재 비활성 상태입니다.

수행한 작업:

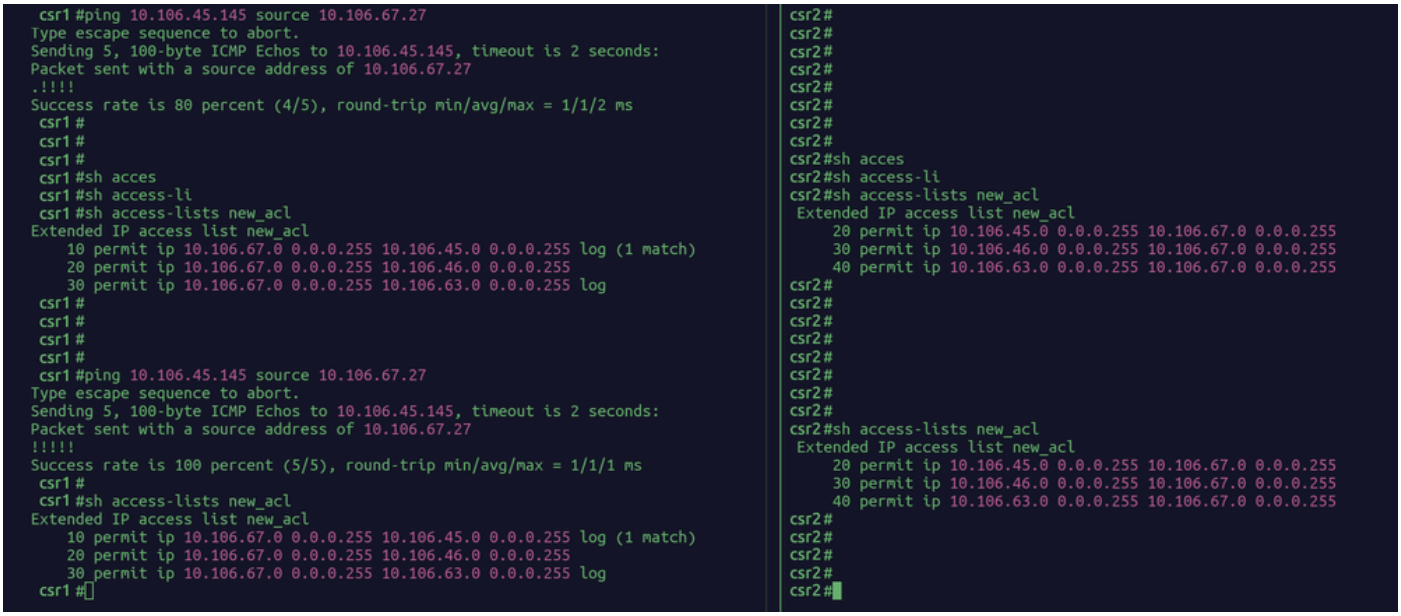
트래픽은 Router2와의 통신을 설정하기 위해 Router1에서 시작됩니다.

관찰:

1. ACL 카운터 동작:
   a. Router1에서 트래픽을 시작하면 Router1의 ACL(Access Control List) 카운터가 눈에 띄게 증가합니다. 이 증가는 터널이 설정하려고 시도하는 순간에 한 번만 발생합니다.
   b. ACL 카운터의 증가는 이 시나리오의 Router1인 시작 라우터에서만 관찰됩니다. 이 단계에서 라우터2는 ACL 카운터의 변경 사항을 반영하지 않습니다.

2. 터널 설정:
   a. 트래픽 시작에 해당하는 초기 증가 후 첫 번째와 라우터 2 간의 터널이 성공적으로 설정됩니다.
   b. 터널 설정 후, Router1의 ACL 카운터가 안정화되며 더 이상 증가하지 않습니다. 이는 ACL 규칙이 일치했으며 현재 설정된 터널을 통해 트래픽을 지속적으로 허용하고 있음을 나타냅니다.
3. 터널 재시작:
   Router1의 ACL 카운터는 터널이 삭제되어 다시 설정해야 하는 경우에만 또 다른 증가를 경험합니다. 이는 ACL 규칙이 터널이 활성화된 후 지속적인 데이터 전송이 아니라 터널 설정을 시도하는 초기 트래픽 시작에 의해 트리거된다는 것을 의미합니다.

요약하면, 이 시나리오에서는 Router1의 ACL 카운터가 터널 생성을 위한 초기 트래픽 시도에 민감하지만 VPN 터널이 가동되고 작동하면 고정 상태로 유지된다는 것을 보여줍니다.



시나리오 1

시나리오 2: VPN 터널이 활성 상태일 때 라우터2에서 시작된 트래픽

초기 상태:

Router1(IP: 10.106.67.27) 및 라우터2(IP: 10.106.45.145)이 현재 활성 상태이며 작동 중입니다.

수행한 작업:

1. 터널이 가동되는 동안 Router2에서 Router1으로 트래픽이 시작됩니다.
2. 그런 다음 터널이 의도적으로 지워지거나 재설정됩니다.
3. 터널이 지워지면 Router2가 트래픽을 다시 시작하여 연결을 다시 설정합니다.

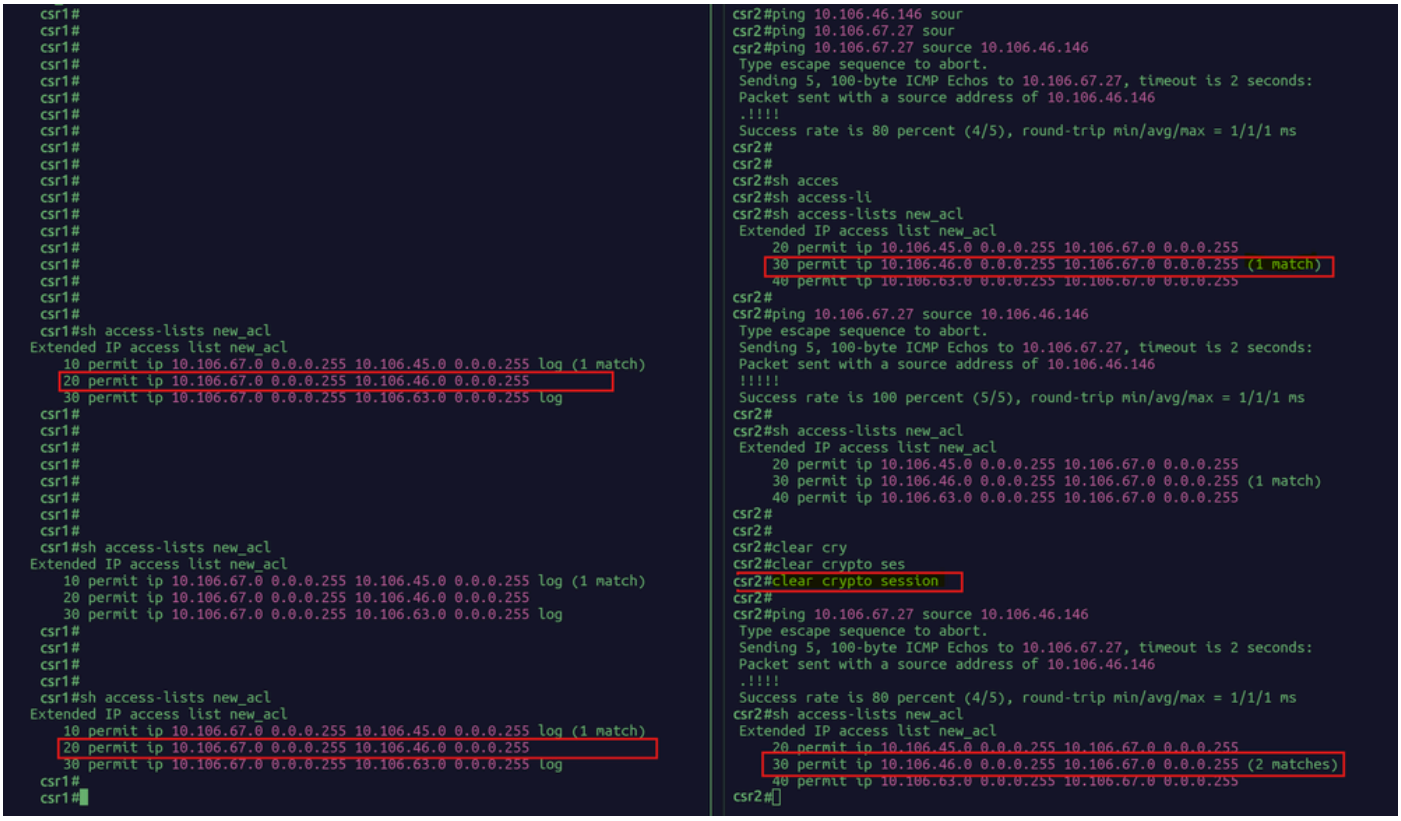
관찰:

1. 초기 트래픽 시작:
   a. 터널이 이미 설정된 상태에서 라우터2에서 처음으로 트래픽이 시작되면 ACL(Access Control List) 카운터가 즉시 변경되지 않습니다.

b. 이는 이미 설정된 터널 내에서 진행 중인 트래픽이 ACL 카운터 증분을 트리거하지 않음을 나타냅니다.

2. 터널 지우기 및 다시 시작:
   a. 터널을 지우면 첫 번째 라우터와 라우터 2 간의 설정된 연결이 일시적으로 중단됩니다. 따라서 후속 트래픽에 대한 재설정 프로세스가 필요합니다.
   b. 터널이 지워진 후 Router2에서 트래픽이 다시 시작되면 Router2의 ACL 카운터에서 관찰할 수 있는 증가분이 있습니다. 이 증가분은 터널 생성을 용이하게 하기 위해 ACL 규칙이 한 번 더 관련되어 있음을 나타냅니다.
3. ACL 카운터 특이성:
   ACL 카운터의 증분은 트래픽을 시작하는 쪽에서만 발생하며, 이 경우 Router2입니다. 이 동작은 시작 쪽에서 트래픽 시작 프로세스를 모니터링하고 제어하는 ACL의 역할을 강조하는 반면, 이 단계에서 Router1의 ACL 카운터는 영향을 받지 않습니다.

요약하면, 이 시나리오에서는 VPN 터널을 다시 설정할 때 Router2의 ACL 카운터가 트래픽 시작에 응답함을 보여줍니다. 활성 터널 내에서 정기적인 트래픽 흐름에 따라 카운터가 증가하지는 않지만, 터널 재설정이 필요한 경우에는 그에 대응하여 터널 시작 이벤트를 정밀하게 추적할 수 있습니다.



시나리오 2

결론:

암호화 ACL 카운터의 동작은 VPN 터널의 시작 단계 동안에만 히트 수를 등록한다는 것을 나타냅니다.

개시자별 증가: 터널이 Router1에서 시작되면 히트 수가 Router1에서만 증가합니다. 마찬가지로, 시작이 Router2에서 발생하면 히트 수는 Router2에서만 증가합니다. 이렇게 하면 소스에서 트래픽 시작 프로세스를 모니터링하는 데 ACL의 역할이 강조됩니다.

안정성 구축 후: 터널이 성공적으로 설정되면 두 피어의 ACL 카운터는 변경되지 않았으므로 더 이상 적중이 발생하지 않음을 나타냅니다. 이러한 안정성은 터널이 지워지거나 재설정될 때까지 지속되며 트래픽 초기화가 다시 시도됩니다.
이 동작은 터널 생성의 초기 단계를 추적 및 제어하는 액세스 제어 목록의 기능을 강조하여 설정된 터널 내의 후속 데이터 흐름이 적중 횟수에 영향을 미치지 않도록 합니다.

핵심 요점:

ACL 카운터 동작: ACL 카운터는 터널 시작 프로세스 중에 개시자 측에서만 등록합니다. 이는 카운터가 터널 설정을 트리거하는 초기 트래픽을 모니터링하도록 설계되었음을 나타냅니다.

설정 후 정적 카운터: 터널이 활성화되고 설정되면 ACL 카운터는 변경되지 않습니다. 터널이 재설정되고 다시 시작해야 하는 경우가 아니면 추가 작업을 반영하지 않으므로 초기 트래픽 이벤트에 중점을 둡니다.

트래픽 시작 특이성: ACL 적중 횟수는 터널을 시작하는 피어에 따라 다릅니다. 이러한 특이성으로 VPN 연결을 시작하는 측에 대한 정확한 추적을 보장하므로 정확한 모니터링 및 제어가 가능합니다
.

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.