IPSec 터널 인터페이스를 통과하도록 AVC 트래픽을 활성화하는 해결 방법

목차

소개

이 문서에서는 IPSEC 터널을 통해 컬렉터에 AVC 트래픽을 전달하는 데 필요한 컨피그레이션에 대해 설명합니다.기본적으로 IPSEC 터널을 통해 컬렉터로 AVC 정보를 내보낼 수 없습니다

사전 요구 사항

Cisco에서는 이러한 주제에 대한 기본적인 지식을 얻을 것을 권장합니다.

- AVC(Application Visibility and Control)
- EzPM(Easy Performance Monitor)

배경 정보

Cisco AVC 기능은 여러 애플리케이션을 인식, 분석 및 제어하는 데 사용됩니다.AVC는 네트워크 인프라에 애플리케이션 인식 기능이 내장되어 있고 네트워크에서 실행되는 애플리케이션의 성능에 대한 가시성을 제공하므로 애플리케이션 대역폭 사용을 세부적으로 제어할 수 있는 애플리케이션별 정책을 구현하여 최종 사용자 환경을 개선할 수 있습니다.이 기술에 대한 자세한 내용은 여기를

참조하십시오.

EzPM은 기존의 성능 모니터링 컨피그레이션을 더 빠르고 쉽게 구성할 수 있는 방법입니다.현재 EzPM은 기존 성능 모니터 구성 모델의 완전한 유연성을 제공하지 않습니다.EzPM에 대한 자세한 내용은 여기를 참조하십시오.

제한 사항

현재 AVC는 통과 터널링 프로토콜 수를 지원하지 않습니다. 자세한 내용은 여기에서 확인할 수 있습니다.

IPSec(Internet Protocol Security)은 AVC에 대해 지원되지 않는 pass-through 터널링 프로토콜 중 하나이며 이 문서에서는 이 제한에 대한 가능한 해결 방법을 다룹니다.

구성

이 섹션에서는 지정된 제한을 시뮬레이션하는 데 사용되는 전체 컨피그레이션에 대해 설명합니다.

네트워크 다이어그램

이 네트워크 다이어그램에서 모든 라우터는 고정 경로를 사용하여 서로 연결할 수 있습니다.R1은 EzPM 컨피그레이션으로 구성되며 R2 라우터로 설정된 IPSec 터널 하나가 있습니다.R3는 Cisco Prime 또는 성능 데이터를 수집할 수 있는 다른 종류의 내보내기일 수 있는 수출자로 사용되고 있습니다.

AVC 트래픽은 R1에 의해 생성되고 R2를 통해 내보내기로 전송됩니다. R1은 IPSec 터널 인터페이스를 통해 AVC 트래픽을 R2로 전송합니다.

초기 컨피그레이션

이 섹션에서는 R1~R3의 초기 컨피그레이션에 대해 설명합니다.

R1

!
인터페이스 루프백0
ip 주소 1.1.1.1 255.255.255.255
!

인터페이스 GigabitEthernet0/1

ip 주소 172.16.1.1 255.255.255.0

이중 자동

속도 자동

!

ip 경로 0.0.0.0 0.0.0.0 172.16.1.2

!

R2

!

인터페이스 GigabitEthernet0/0/0

ip 주소 172.16.2.2 255.255.255.0

협상 자동

!

인터페이스 GigabitEthernet0/0/1

ip 주소 172.16.1.2 255.255.255.0

협상 자동

!

R3

!

인터페이스 GigabitEthernet0/0

ip 주소 172.16.2.1 255.255.255.0

이중 자동

속도 자동

!

ip 경로 0.0.0.0 0.0.0.0 172.16.2.2

!

IPSec 구성

이 섹션에서는 R1 및 R2 라우터의 IPSec 컨피그레이션에 대해 설명합니다.

R1

!

ip access-list 확장 IPSec_Match

```
 허용 ip any host 172.16.2.1
!
암호화 isakmp 정책 1
 encr aes 256
 해시 md5
 인증 사전 공유
 그룹 2
crypto isakmp key cisco123 address 172.16.1.2
!
!
crypto ipsec transform-set2 esp-aes 256 esp-sha-hmac
 모드 터널
!
!
암호화 맵 VPN 10 ipsec-isakmp
 피어 172.16.1.2 설정
 set transform-set2
 주소 IPSec_Match 일치
!
인터페이스 GigabitEthernet0/1
 ip 주소 172.16.1.1 255.255.255.0
 이중 자동
 속도 자동
 암호화 맵 VPN
!
```

R2

```
!
ip access-list 확장 IPSec_Match
 허용 ip 호스트 172.16.2.1 any
!
암호화 isakmp 정책 1
 encr aes 256
 해시 md5
 인증 사전 공유
 그룹 2
crypto isakmp key cisco123 address 172.16.1.1
!
!
crypto ipsec transform-set2 esp-aes 256 esp-sha-hmac
 모드 터널
!
!
암호화 맵 VPN 10 ipsec-isakmp
 피어 172.16.1.1 설정
 set transform-set2
 주소 IPSec_Match 일치
 역방향 경로
!
인터페이스 GigabitEthernet0/0/1
 ip 주소 172.16.1.2 255.255.255.0
 협상 자동
 cdp 활성화
 암호화 맵 VPN
```

!

IPSec 컨피그레이션이 예상대로 작동하는지 확인하려면 show crypto isakmp sa의 출력을 **확인합니다.**

```
R1#show crypto isakmp sa

IPv4  ISAKMP SA

dst src state conn id

IPv6  ISAKMP SA
```

보안 연결을 활성화하려면 R1에서 내보내기(R3, 172.16.2.1)을 ping합니다.

```
R1#ping 172.16.2.1

   .

5, 100 ICMP (172.16.2.1)     2.

!!!!!

 100%(5/5),  // = 1/1/4 ms

R1#
```

이제 라우터에는 활성 보안 연결이 설정되며, 이는 트래픽이 R1에서 시작되어 내보내기로 향하는 대상이 ESP가 캡슐화되었음을 확인합니다.

```
R1#show crypto isakmp sa

IPv4  ISAKMP SA

dst src state conn id

172.16.1.2 172.16.1.1 QM_IDLE 1002

IPv6  ISAKMP SA
```

EzPM 컨피그레이션

이 섹션에서는 R1 라우터의 EzPM 컨피그레이션에 대해 설명합니다.

R1

```
!

클래스 맵 match-all perf-mon-acl

 설명 PrimeAM 생성 엔티티 - 이 엔티티를 수정하거나 사용하지 마십시오.
```

프로토콜 ip 일치

!

성능 모니터 컨텍스트 성능 모니터 프로파일 애플리케이션 경험

내보내기 대상 172.16.2.1 소스 GigabitEthernet0/1 전송 udp 포트 9991

traffic-monitor application-traffic-stats

traffic monitor conversation-traffic-stats ipv4

traffic-monitor application-response-time ipv4

트래픽 모니터 미디어 ipv4 인그레스

트래픽 모니터 미디어 ipv4 이그레스

traffic monitor url ipv4 class-replace perf-mon-acl

!

모니터링해야 하는 인터페이스에 EzPM 프로필을 적용합니다.여기서는 루프백 0 인터페이스를 모니터링합니다.

R1

!

인터페이스 루프백0

ip 주소 1.1.1.1 255.255.255.255

성능 모니터 컨텍스트 성능 모니터

!

해결 방법

위의 컨피그레이션이 적용되면 **show performance monitor contextcontext**-*nameexporter*의 출력을 **가져옵니다**.

Output **Features** 옵션의 상태를 확인합니다. 기본적으로 **Not Used** 상태여야 합니다. 이는 예상되는 동작이며 AVC 트래픽이 여기서 캡슐화되거나 암호화되지 않는 이유입니다.

AVC 트래픽이 IPsec 터널 인터페이스를 통과하도록 하려면 **Output Features** 옵션이 사용됨 상태여야 합니다.이를 위해서는 흐름 내보내기 프로파일에서 명시적으로 활성화해야 합니다.아래는 이 옵션을 활성화하는 단계별 세부 절차입니다.

1단계

show performance monitor context -*name* **configuration** 명령의 전체 출력을 메모장에 저장합니다

.다음은 이 출력의 스냅샷입니다.

```
R1#show performance monitor context Performance-Monitor

!=============================================================================

!                 !

!=============================================================================

!

!========

!

flow exporter Performance-Monitor-1


  172.16.2.1

  GigabitEthernet0/1

 transport udp 9991

   ipfix

     300

 option interface-table timeout 300

  vrf-table timeout 300

  c3pl-class-table timeout 300

  c3pl-policy-table timeout 300

  sampler-table timeout 300

 option application-table timeout 300

 option application-attributes timeout 300

       300

—snip—
```

2단계

흐름 내보내기 프로필 아래에 **output-features** 옵션을 명시적으로 추가합니다.output-features 옵션을 추가한 후 흐름 내보내기 프로파일은 다음과 같습니다.

flow exporter Performance-Monitor-1

설명 성능 모니터 컨텍스트 성능 모니터 내보내기

대상 172.16.2.1

소스 GigabitEthernet0/1

transport udp 9991

내보내기 프로토콜 ipfix

템플릿 데이터 시간 초과 300

출력 기능

option interface-table timeout 300

옵션 vrf-table timeout 300

옵션 c3pl-class-table timeout 300

옵션 c3pl-policy-table timeout 300

옵션 sampler-table timeout 300

option application-table timeout 300

option application-attributes timeout 300

옵션 하위 애플리케이션 테이블 시간 초과 300

출력의 나머지 부분은 그대로 둡니다. 출력의 다른 부분은 변경하지 마십시오.

3단계

이제 인터페이스 및 라우터에서 EzPM 프로파일을 제거합니다.

!

인터페이스 루프백 0

성능 모니터 컨텍스트 성능 모니터 없음

종료

!

!

성능 모니터 없음 컨텍스트 성능 모니터 프로파일 애플리케이션 경험

!

4단계

R1 라우터에 수정된 컨피그레이션을 적용합니다.예기치 않은 동작이 발생할 수 있으므로 단일 명령이 누락되지 않도록 하십시오.

다음을 확인합니다.

이 섹션에서는 이 문서에서 확인하는 데 사용되는 확인 방법과 이 해결 방법을 통해 여기에 언급된 AVC 패킷의 제한을 극복하는 데 어떤 도움이 되었는지 설명합니다.

해결 방법을 적용하기 전에 IPSec 피어 라우터(R2)에서 받은 패킷이 삭제됩니다.다음 메시지도 생성됩니다.

```
%IPSEC-3-RECVD_PKT_NOT_IPSEC:Rec'd  IPSEC  . dest_addr= 172.16.2.1,
src_addr= 172.16.1.1, prot= 17
```

여기서 R2는 172.16.2.1으로 향하는 ESP 캡슐화된 패킷을 예상하지만 수신된 패킷은 일반 UDP 패킷(prot=17)이며 이러한 패킷을 삭제하는 것이 예상되는 동작입니다.아래 패킷 캡처는 R2에서 수신된 패킷이 ESP 캡슐화 대신 일반 UDP 패킷이며, 이는 AVC의 기본 동작입니다.

```
Internet Protocol Version 4, Src: 172.16.1.1 (172.16.1.1), Dst: 172.16.2.1 (172.16.2.1)
  Version: 4
  Header Length: 20 bytes
⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 1348
  Identification: 0x961a (38426)
⊞ Flags: 0x00
  Fragment offset: 0
  Time to live: 255
  Protocol: UDP (17)
⊞ Header checksum: 0xc56b [validation disabled]
  Source: 172.16.1.1 (172.16.1.1)
  Destination: 172.16.2.1 (172.16.2.1)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
User Datagram Protocol, Src Port: 50208 (50208), Dst Port: 9991 (9991)
  Source Port: 50208 (50208)
  Destination Port: 9991 (9991)
  Length: 1328
⊞ Checksum: 0xb7ec [validation disabled]
  [Stream index: 0]
Data (1320 bytes)
```

해결 방법을 적용한 후 아래 패킷 캡처에서 R2에서 수신된 AVC 패킷이 ESP로 캡슐화되었으며 R2에서 더 이상 오류 메시지가 나타나지 않음을 분명히 알 수 있습니다.

```
Internet Protocol Version 4, Src: 172.16.1.1 (172.16.1.1), Dst: 172.16.1.2 (172.16.1.2)
  Version: 4
  Header Length: 20 bytes
⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
  Total Length: 1448
  Identification: 0x0114 (276)
⊞ Flags: 0x00
  Fragment offset: 0
  Time to live: 255
  Protocol: Encap Security Payload (50)
⊞ Header checksum: 0x5aec [validation disabled]
  Source: 172.16.1.1 (172.16.1.1)
  Destination: 172.16.1.2 (172.16.1.2)
  [Source GeoIP: Unknown]
  [Destination GeoIP: Unknown]
Encapsulating Security Payload
  ESP SPI: 0x804c46a3 (2152482467)
  ESP Sequence: 203
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.