Cisco Catalyst 6000/6500 Running CatOS Software로 세분화된 트래픽 분석을 위한 VACL 캡처

목차

소개

이 문서에서는 네트워크 트래픽 분석에 VACL(VLAN Access Control List)(ACL) 캡처 포트 기능을 사용하기 위한 샘플 컨피그레이션을 보다 세분화하여 제공합니다. 또한 이 문서에서는 VLAN 기반 SPAN(Switched Port Analyzer)(VSPAN) 사용과 달리 VACL 캡처 포트 사용의 이점을 설명합니다.

Cisco IOS® 소프트웨어를 실행하는 Cisco Catalyst 6000/6500에서 VACL 캡처 포트 기능을 구성하려면 Cisco Catalyst 6000/6500 Running Cisco IOS Software를 사용하여 세분화된 트래픽 분석을 위한 VACL 캡처를 참조하십시오.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- 가상 LAN - 자세한 내용은 가상 LAN/VLAN 트렁킹 프로토콜(VLAN/VTP) - 소개를 참조하십시

오.
- 액세스 목록 - 자세한 내용은 액세스 제어 구성을 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 Catalyst OS 릴리스 8.1(2)을 실행하는 Cisco Catalyst 6506 Series 스위치를 기반으로 합니다.

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.

관련 제품

이 구성은 Catalyst OS 릴리스 6.3 이상을 실행하는 Cisco Catalyst 6000/6500 Series 스위치에서도 사용할 수 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

VLAN 기반 SPAN

SPAN은 분석을 위해 VLAN에 있는 하나 이상의 소스 포트 또는 하나 이상의 VLAN에서 대상 포트로 트래픽을 복사합니다. 로컬 SPAN은 동일한 Catalyst 6500 Series 스위치에서 소스 포트, 소스 VLAN 및 목적지 포트를 지원합니다.

소스 포트는 네트워크 트래픽 분석을 위해 모니터링되는 포트입니다. 소스 VLAN은 네트워크 트래픽 분석을 위해 모니터링되는 VLAN입니다. VSPAN(VLAN-based SPAN)은 하나 이상의 VLAN에서 네트워크 트래픽을 분석합니다. VSPAN을 인그레스 SPAN, 이그레스 SPAN 또는 둘 다로 구성할 수 있습니다. 소스 VLAN의 모든 포트가 VSPAN 세션의 운영 소스 포트가 됩니다. 관리 소스 VLAN에 속한 대상 포트는 운영 소스에서 제외됩니다. 관리 소스 VLAN에서 포트를 추가 또는 제거하면 그에 따라 운영 소스가 수정됩니다.

VSPAN 세션에 대한 지침:

- 트렁크 포트는 VSPAN 세션의 소스 포트로 포함되지만, 이러한 VLAN이 트렁크에 대해 활성 상태인 경우 관리 소스 목록에 있는 VLAN만 모니터링됩니다.
- 인그레스(ingress) 및 이그레스(egress) SPAN이 구성된 VSPAN 세션의 경우, 시스템은 다음과 같은 수퍼바이저 엔진 유형에 따라 작동합니다.WS-X6K-SUP1A-PFC, WS-X6K-SUP1A-MSFC, WS-X6K-S1A-MSFC2, WS-X6K-S2-PFC2, WS-X6K-S1A-MSFC2, WS-SUP72-WS sup32-GE-3B - 패킷이 동일한 VLAN에서 스위칭되는 경우 SPAN 목적지 포트에 의해 2개의 패킷이 전달됩니다.WS-X6K-SUP1-2GE, WS-X6K-SUP1A-2GE - SPAN 목적지 포트에 의해 패킷이 하나만 전달됩니다.
- 인밴드 포트는 VSPAN 세션의 운영 소스로 포함되지 않습니다.
- VLAN이 지워지면 VSPAN 세션의 소스 목록에서 제거됩니다.
- 관리 소스 VLAN 목록이 비어 있으면 VSPAN 세션이 비활성화됩니다.

- VSPAN 컨피그레이션에는 비활성 VLAN이 허용되지 않습니다.
- 소스 VLAN 중 하나가 RSPAN VLAN이 되는 경우 VSPAN 세션이 비활성화됩니다.

소스 VLAN에 대한 자세한 내용은 소스 VLAN의 특성을 참조하십시오.

VLAN ACL

VACL은 모든 트래픽을 제어할 수 있습니다. 스위치에서 VACL을 구성하여 VLAN으로 라우팅되거나 VLAN 내에서 브리지된 모든 패킷에 적용할 수 있습니다. VACL은 보안 패킷 필터링 및 트래픽을 특정 물리적 스위치 포트로 리디렉션하는 데 엄격하게 사용됩니다. Cisco IOS ACL과 달리 VACL은 방향(입력 또는 출력)으로 정의되지 않습니다.

IP 및 IPX에 대한 레이어 3 주소의 VACL을 구성할 수 있습니다. 다른 모든 프로토콜은 MAC 주소 및 EtherType을 통해 MAC VACL을 사용하여 액세스를 제어합니다. IP 트래픽 및 IPX 트래픽은 MAC VACL에 의해 제어되지 않습니다. 기타 모든 트래픽 유형(AppleTalk, DECnet 등)은 MAC 트래픽으로 분류됩니다. MAC VACL은 이 트래픽을 제어하는 데 사용됩니다.

VACL에서 지원되는 ACE

VACL에는 순서가 지정된 ACE(액세스 제어 항목) 목록이 포함되어 있습니다. 각 VACL에는 한 가지 유형의 ACE만 포함될 수 있습니다. 각 ACE에는 패킷의 내용과 일치하는 여러 필드가 포함되어 있습니다. 각 필드에는 관련 비트를 나타내는 관련 비트 마스크가 있을 수 있습니다. 일치 발생 시 시스템이 패킷으로 무엇을 해야 하는지 설명하는 작업이 각 ACE와 연결됩니다. 작업은 기능에 따라 다릅니다. Catalyst 6500 Series 스위치는 하드웨어에서 세 가지 유형의 ACE를 지원합니다.

- IP ACE
- IPX ACE
- 이더넷 ACE

이 표에는 각 ACE 유형과 연관된 매개변수가 나열되어 있습니다.

ACE 유형	TCP 또는 UDP	ICMP	기타 IP	IPX	이더넷
레이어 4 매개변수	소스 포트	-	-	-	-
	소스 포트 운영자	-	-	-	-
	대상 포트	-	-	-	-
	대상 포트 운영자	ICMP 코드	-	-	-
	해당 없음	ICMP 유형	해당 없음	-	-
레이어 3 매개변수	IP ToS 바이트	IP ToS 바이트	IP ToS 바이트	-	-

	IP 소스 주소	IP 소스 주소	IP 소스 주소	IPX 소스 네트워크	-
	IP 대상 주소	IP 대상 주소	IP 대상 주소	IP 대상 네트워크	-
	-	-	-	IP 대상 노드	-
	TCP 또는 UDP	ICMP	기타 프로토콜	IPX 패킷 유형	-
레이어 2 매개변수	-	-	-	-	이더 타입
	-	-	-	-	이더넷 소스 주소
	-	-	-	-	이더넷 대상 주소

VSPAN 사용량에 대한 VACL 사용의 장점

트래픽 분석을 위한 VSPAN 사용에는 몇 가지 제한이 있습니다.

- VLAN에서 흐르는 모든 레이어 2 트래픽이 캡처됩니다. 이렇게 하면 분석할 데이터의 양이 늘어납니다.
- Catalyst 6500 Series 스위치에서 구성할 수 있는 SPAN 세션 수는 제한됩니다. 자세한 내용은 기능 요약 및 제한 사항을 참조하십시오.
- 목적지 포트는 모니터링되는 모든 소스 포트에 대해 송수신된 트래픽의 복사본을 수신합니다. 목적지 포트가 오버서브스크립션되는 경우 혼잡이 발생할 수 있습니다. 이러한 혼잡은 하나 이상의 소스 포트에서 트래픽 포워딩에 영향을 줄 수 있습니다.

VACL 캡처 포트 기능은 이러한 제한 사항을 극복하는 데 도움이 됩니다. VACL은 주로 트래픽을 모니터링하도록 설계되지 않았습니다. 그러나 트래픽을 분류하는 다양한 기능을 통해 네트워크 트래픽 분석이 훨씬 더 간소화될 수 있도록 캡처 포트 기능이 도입되었습니다. 다음은 VSPAN을 통한 VACL 캡처 포트 사용의 장점입니다.

- 세분화된 트래픽 분석VACL은 소스 IP 주소, 대상 IP 주소, 레이어 4 프로토콜 유형, 소스 및 목적지 레이어 4 포트 및 기타 정보를 기준으로 매칭할 수 있습니다. 이 기능을 통해 VACL은 세분화된 트래픽 식별 및 필터링에 매우 유용합니다.
- 세션 수VACL은 하드웨어에서 시행됩니다. 생성할 수 있는 ACE의 수는 스위치에서 사용 가능한 TCAM에 따라 다릅니다.
- 대상 포트 오버서브스크립션세분화된 트래픽 식별은 대상 포트로 전달할 프레임 수를 줄여 초과 서브스크립션의 가능성을 최소화합니다.
- 성능VACL은 하드웨어에서 시행됩니다. Cisco Catalyst 6500 Series 스위치의 VLAN에 VACL을 적용할 경우 성능 저하가 발생하지 않습니다.

구성

이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

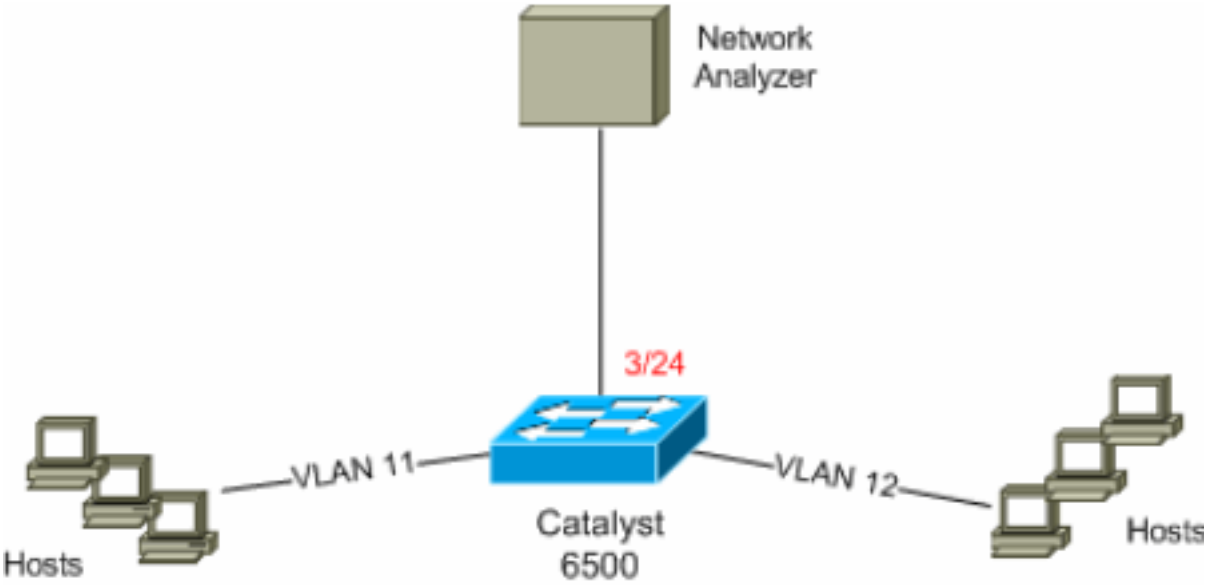
이 문서에서는 다음 구성을 사용합니다.

- VLAN 기반 SPAN을 사용한 컨피그레이션
- VACL을 사용한 구성

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 섹션에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



VLAN 기반 SPAN을 사용한 컨피그레이션

이 컨피그레이션 예에서는 VLAN 11과 VLAN 12에서 흐르는 모든 레이어 2 트래픽을 캡처하고 Network Analyzer 디바이스로 전송하는 데 필요한 단계를 나열합니다.

1. 관심 있는 트래픽을 지정합니다.이 예에서는 VLAN 100 및 VLAN 200에서 이동하는 트래픽입니다.

```
6K-CatOS> (enable) set span 11-12 3/24
!--- where 11-12 specifies the range of source VLANs and 3/24 specify the destination port.

2007 Jul 12 21:45:43 %SYS-5-SPAN_CFGSTATECHG:local span session inactive for des
tination port 3/24

Destination     : Port 3/24
Admin Source    : VLAN 11-12
Oper Source     : Port 3/11-12,16/1
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Status          : active

6K-CatOS> (enable) 2007 Jul 12 21:45:43 %SYS-5-SPAN_CFGSTATECHG:local span sessi
on active for destination port 3/24
```

이를 통해 VLAN 11 및 VLAN 12에 속하는 모든 레이어 2 트래픽이 복사되어 포트 3/24로 전송됩니다.

2. **show span all** 명령을 사용하여 SPAN 컨피그레이션을 확인합니다.

```
6K-CatOS> (enable) show span all

Destination     : Port 3/24
Admin Source    : VLAN 11-12
Oper Source     : Port 3/11-12,16/1
Direction       : transmit/receive
Incoming Packets: disabled
Learning        : enabled
Multicast       : enabled
Filter          : -
Status          : active


Total local span sessions:  1

No remote span session configured
6K-CatOS> (enable)
```

VACL을 사용한 구성

이 컨피그레이션 예에서는 네트워크 관리자의 여러 요구 사항이 있습니다.

- VLAN 12의 호스트 범위(10.12.12.128/25)에서 VLAN 11의 특정 서버(10.11.11.100)로의 HTTP 트래픽을 캡처해야 합니다.
- 그룹 주소 239.0.0.100으로 향하는 전송 방향의 UDP(Multicast User Datagram Protocol) 트래픽을 VLAN 11에서 캡처해야 합니다.

1. 보안 ACL을 사용하여 흥미로운 트래픽을 정의합니다. 정의된 모든 ACE에 대해 키워드 **캡처**를 언급해야 합니다.

```
6K-CatOS> (enable) set security acl ip HttpUdp_Acl permit tcp 10.12.12.128 0.0.0.127 host
10.11.11.100 eq www capture
!--- Command wrapped to the second line. HttpUdp_Acl editbuffer modified. Use 'commit'
command to apply changes. 6K-CatOS> (enable) set security acl ip HttpUdp_Acl permit udp any
host 239.0.0.100 capture
HttpUdp_Acl editbuffer modified. Use 'commit' command to apply changes.
```

2. ACE 컨피그레이션이 올바르고 올바른 순서로 되어 있는지 확인합니다.

```
6K-CatOS> (enable) show security acl info HttpUdp_Acl editbuffer
set security acl ip HttpUdp_Acl
-------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
ACL HttpUdp_Acl Status: Not Committed
6K-CatOS> (enable)
```

3. 하드웨어에 ACL을 커밋합니다.

```
6K-CatOS> (enable) commit security acl HttpUdp_Acl
ACL commit in progress.

ACL 'HttpUdp_Acl' successfully committed.
6K-CatOS> (enable)
```

4. ACL의 상태를 확인합니다.

```
6K-CatOS> (enable) show security acl info HttpUdp_Acl editbuffer
set security acl ip HttpUdp_Acl
-------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
```

```
ACL HttpUdp_Acl Status: Committed
6K-CatOS> (enable)
```

5. 적절한 VLAN에 VLAN 액세스 맵을 적용합니다.

```
6K-CatOS> (enable) set security acl map HttpUdp_Acl ?
  <vlans>                    Vlan(s) to be mapped to ACL
6K-CatOS> (enable) set security acl map HttpUdp_Acl 11
Mapping in progress.

ACL HttpUdp_Acl successfully mapped to VLAN 11.
6K-CatOS> (enable)
```

6. ACL과 VLAN 간의 매핑을 확인합니다.

```
6K-CatOS> (enable) show security acl map HttpUdp_Acl
ACL HttpUdp_Acl is mapped to VLANs:
11
6K-CatOS> (enable)
```

7. 캡처 포트를 구성합니다.

```
6K-CatOS> (enable) set vlan 11 3/24
VLAN  Mod/Ports
---- ----------------------
11    3/11,3/24
6K-CatOS> (enable)


6K-CatOS> (enable) set security acl capture-ports 3/24
Successfully set 3/24 to capture ACL traffic.
6K-CatOS> (enable)
```

참고: ACL이 여러 VLAN에 매핑된 경우 캡처 포트를 모든 VLAN에 구성해야 합니다. 캡처 포트에서 여러 VLAN을 허용하려면 포트를 트렁크로 구성하고 ACL에 매핑된 VLAN만 허용합니다. 예를 들어, ACL이 VLAN 11과 12에 매핑된 경우 컨피그레이션을 완료합니다.

```
6K-CatOS> (enable) clear trunk 3/24 1-10,13-1005,1025-4094
6K-CatOS> (enable) set trunk 3/24 on dot1q 11-12
6K-CatOS> (enable) set security acl capture-ports 3/24
```

8. 캡처 포트 컨피그레이션을 확인합니다.

```
6K-CatOS> (enable) show security acl capture-ports
ACL Capture Ports: 3/24
6K-CatOS> (enable)
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다. OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show security acl info(보안 acl 정보 표시)** - 현재 구성되었거나 NVRAM 및 하드웨어에 마지막으로 커밋된 VACL의 내용을 표시합니다.

```
6K-CatOS> (enable) show security acl info HttpUdp_Acl
set security acl ip HttpUdp_Acl
---------------------------------------------------
1. permit tcp 10.12.12.128 0.0.0.127 host 10.11.11.100 eq 80 capture
2. permit udp any host 239.0.0.100 capture
6K-CatOS> (enable)
```

- **show security acl map** - 특정 ACL, 포트 또는 VLAN에 대한 ACL-to-VLAN 또는 ACL-to-port 매핑을 표시합니다.

```
6K-CatOS> (enable) show security acl map all
ACL Name                         Type Vlans
```

```
-------------------------------- ---- -----
HttpUdp_Acl                        IP   11
6K-CatOS> (enable)
```

- **show security acl capture-ports** - 캡처 포트의 목록을 표시합니다.

```
6K-CatOS> (enable) show security acl capture-ports
ACL Capture Ports: 3/24
6K-CatOS> (enable)
```

문제 해결

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

관련 정보

- Cisco IOS Software를 실행하는 Cisco Catalyst 6000/6500을 통한 세분화된 트래픽 분석을 위한 VACL 캡처
- 액세스 제어 구성 - Catalyst 6500 Series 소프트웨어 구성 가이드, 8.6
- LAN 제품 지원 페이지
- LAN 스위칭 지원 페이지
- 기술 지원 및 문서 – Cisco Systems