Catalyst 3750 Series 스위치의 ISE 트래픽 리디렉션

목차

소개
사전 요구 사항
요구 사항
사용되는 구성 요소
배경 정보
문제 해결
테스트 시나리오
트래픽이 리디렉션 ACL에 도달하지 않음
트래픽이 리디렉션 ACL에 도달함
시나리오 1 - 대상 호스트가 동일한 VLAN에 있고 존재하며 SVI 10 UP입니다.
시나리오 2 - 대상 호스트가 동일한 VLAN에 있고 존재하지 않으며 SVI 10 UP입니다.
시나리오 3 - 대상 호스트가 다른 VLAN에 있고, 존재하며, SVI 10 UP입니다.
시나리오 4 - 대상 호스트가 다른 VLAN에 있고 존재하지 않으며 SVI 10 UP입
시나리오 5 - 대상 호스트가 다른 VLAN에 있고, 존재하며, SVI 10 DOWN입니다.
시나리오 6 - 대상 호스트가 다른 VLAN에 있고 존재하지 않으며 SVI 10 DOWN입
시나리오 7 - HTTP 서비스가 다운되었습니다.
리디렉션 ACL - 잘못된 프로토콜 및 포트, 리디렉션 없음
관련 정보

소개

이 문서에서는 사용자 트래픽 리디렉션의 작동 방식 및 스위치에서 패킷을 리디렉션하는 데 필요한 조건에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco는 Cisco ISE(Identity Services Engine) 컨피그레이션 및 이러한 주제에 대한 기본적인 지식을 보유하고 있는 것을 권장합니다.

- ISE 구축 및 CWA(Central Web Authentication) 흐름
- Cisco Catalyst 스위치의 CLI 구성

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft Windows 7
- Cisco Catalyst 3750X Series Switch Software, 버전 15.0 이상
- ISE 소프트웨어, 버전 1.1.4 이상

배경 정보

스위치에서 사용자 트래픽 리디렉션은 ISE를 사용하는 대부분의 구축에서 중요한 구성 요소입니다 .이러한 모든 흐름에는 스위치에 의한 트래픽 리디렉션 사용이 포함됩니다.

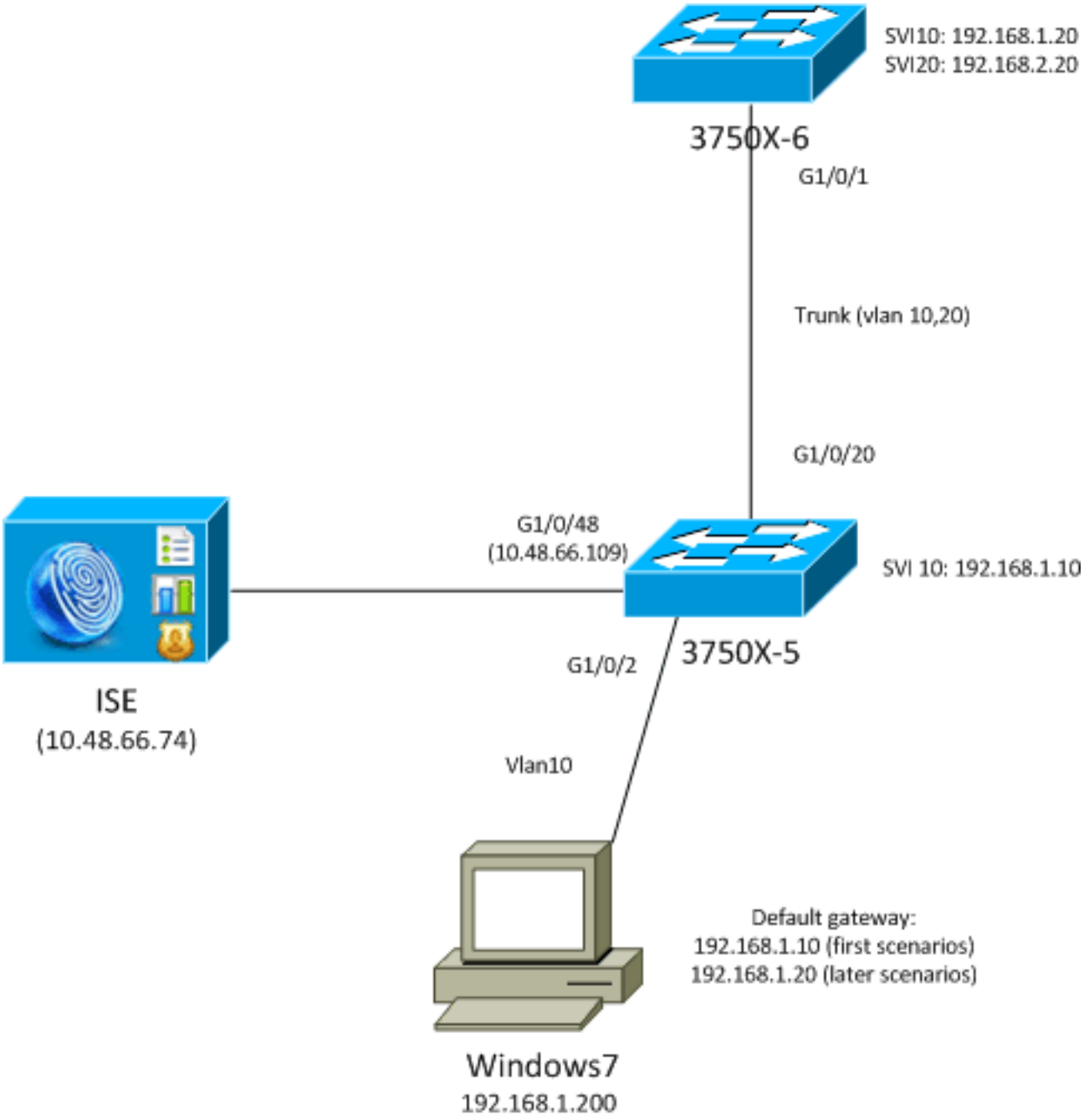
- CWA
- 클라이언트 프로비저닝(CPP)
- 장치 등록(DRW)
- 네이티브 서 플리 컨 트 프로비저닝 (NSP)
- 모바일 장치 관리(MDM)

잘못 구성된 리디렉션은 구축 시 여러 문제의 원인입니다.일반적인 결과는 NAC(Network Admission Control) 에이전트가 올바르게 팝업되지 않거나 게스트 포털을 표시할 수 없다는 것입니다.

스위치에 클라이언트 VLAN과 동일한 SVI(Switch Virtual Interface)가 없는 시나리오는 마지막 세 가지 예를 참조하십시오.

문제 해결

테스트 시나리오



테스트는 클라이언트에 대해 수행되며, CPP(프로비저닝)를 위해 ISE로 리디렉션되어야 합니다. 사용자는 MAB(MAC Authentication Bypass) 또는 802.1x를 통해 인증됩니다.ISE는 리디렉션 ACL(Access Control List) 이름(REDIRECT_POSTURE)과 리디렉션 URL(ISE로 리디렉션)을 사용하여 권한 부여 프로파일을 반환합니다.

```
bsns-3750-5#show authentication sessions interface g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.36ce
          IP Address:  192.168.1.201
           User-Name:  cisco
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  10
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_TRAFFIC-51ef7db1
```

```
    URL Redirect ACL:  REDIRECT_POSTURE
        URL Redirect:  https://10.48.66.74:8443/guestportal/gateway?sessionId=
C0A8000100000D5D015F1B47&action=cpp
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A8000100000D5D015F1B47
     Acct Session ID:  0x00011D90
              Handle:  0xBB000D5E

Runnable methods list:
      Method   State
      dot1x    Authc Success
```

DACL(Downloadable ACL)은 이 단계에서 모든 트래픽을 허용합니다.

```
bsns-3750-5#show ip access-lists xACSACLx-IP-PERMIT_ALL_TRAFFIC-51ef7db1
Extended IP access list xACSACLx-IP-PERMIT_ALL_TRAFFIC-51ef7db1 (per-user)
   10 permit ip any any
```

리디렉션 ACL은 리디렉션 없이 이 트래픽을 허용합니다.

- ISE에 대한 모든 트래픽(10.48.66.74)
- DNS(Domain Name System) 및 ICMP(Internet Control Message Protocol) 트래픽

다른 모든 트래픽은 리디렉션되어야 합니다.

```
bsns-3750-5#show ip access-lists REDIRECT_POSTURE
Extended IP access list REDIRECT_POSTURE
   10 deny ip any host 10.48.66.74 (153 matches)
   20 deny udp any any eq domain
   30 deny icmp any any (10 matches)
   40 permit tcp any any eq www (78 matches)
   50 permit tcp any any eq 443
```

이 스위치는 사용자와 동일한 VLAN에 SVI가 있습니다.

```
interface Vlan10
 ip address 192.168.1.10 255.255.255.0
```

다음 섹션에서는 잠재적인 영향을 나타내기 위해 이 내용이 수정됩니다.

트래픽이 리디렉션 ACL에 도달하지 않음

호스트를 ping할 때 해당 트래픽이 리디렉션되지 않으므로 응답을 받아야 합니다.확인하려면 다음 디버그를 실행합니다.

```
debug epm redirect
```

클라이언트가 전송하는 각 ICMP 패킷에 대해 디버그가 있어야 합니다.

```
Jan 9 09:13:07.861: epm-redirect:IDB=GigabitEthernet1/0/2: In
epm_host_ingress_traffic_qualify ...
Jan 9 09:13:07.861: epm-redirect:epm_redirect_cache_gen_hash:
IP=192.168.1.201 Hash=562
Jan 9 09:13:07.861: epm-redirect:IP=192.168.1.201: CacheEntryGet Success
Jan 9 09:13:07.861: epm-redirect:IP=192.168.1.201: Ingress packet on
[idb= GigabitEthernet1/0/2] didn't match with [acl=REDIRECT_POSTURE]
```

확인하려면 ACL을 확인합니다.

```
bsns-3750-5#show ip access-lists REDIRECT_POSTURE
Extended IP access list REDIRECT_POSTURE
   10 deny ip any host 10.48.66.74 (153 matches)
   20 deny udp any any eq domain
    30 deny icmp any any (4 matches)
   40 permit tcp any any eq www (78 matches)
   50 permit tcp any any eq 443
```

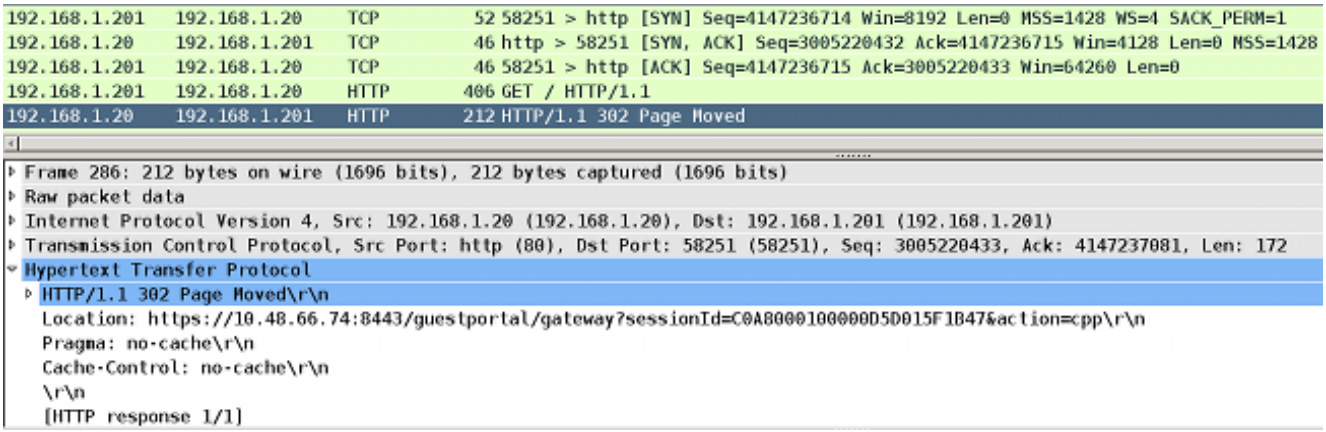
트래픽이 리디렉션 ACL에 도달함

시나리오 1 - 대상 호스트가 동일한 VLAN에 있고 존재하며 SVI 10 UP입니다.

스위치에서 직접 연결할 수 있는 L3(Layer 3)의 IP 주소에 대한 트래픽을 시작할 때(스위치의 네트워크에 SVI 인터페이스가 있음) 다음과 같은 상황이 발생합니다.

1. 클라이언트는 동일한 VLAN에서 대상 호스트(192.168.1.20)에 대한 ARP(Address Resolution Protocol) 확인 요청을 시작하고 응답을 수신합니다(ARP 트래픽은 리디렉션되지 않음).

2. 스위치는 대상 IP 주소가 해당 스위치에 구성되지 않은 경우에도 해당 세션을 차단합니다.클라이언트와 스위치 간의 TCP 핸드셰이킹이 완료되었습니다.이 단계에서는 스위치 외부로 다른 패킷이 전송되지 않습니다.이 시나리오에서는 클라이언트(192.168.1.201)이 해당 VLAN(192.168.1.20)에 있고 스위치에 SVI 인터페이스 UP(IP 주소 192.168.1.10)이 있는 다른 호스트와의 TCP 세션을 시작했습니다.



3. TCP 세션이 설정되고 HTTP 요청이 전송되면 스위치는 ISE로의 리디렉션과 함께 HTTP 응답을 반환합니다(위치 헤더).

   이러한 단계는 디버그에 의해 확인됩니다.여러 ACL 적중 수가 있습니다.

```
epm-redirect:IP=192.168.1.201: Ingress packet on [idb= GigabitEthernet1/0/2]
matched with [acl=REDIRECT_POSTURE]
epm-redirect:Fill in URL=https://10.48.66.74:8443/guestportal/gateway?sessionId=
C0A8000100000D5D015F1B47&action=cpp for redirection
epm-redirect:IP=192.168.1.201: Redirect http request to https:
//10.48.66.74:8443/guestportal/gateway?sessionId=C0A8000100000D5D015F1B47&action=cpp
```

```
epm-redirect:EPM HTTP Redirect Daemon successfully created
```

자세한 디버깅:

```
debug ip http all

http_epm_http_redirect_daemon: got redirect request
HTTP: token len 3: 'GET'
http_proxy_send_page: Sending http proxy page
http_epm_send_redirect_page: Sending the Redirect page to ...
```

4. 클라이언트는 ISE에 직접(SSL(Secure Sockets Layer) 세션 10.48.66.74:8443에 연결) 이 패킷은 리디렉션을 트리거하지 않습니다.

```
epm-redirect:IP=192.168.1.201: Ingress packet on [idb= GigabitEthernet1/0/2] didn't
match with [acl=REDIRECT_POSTURE]
```

참고:세션이 스위치에 의해 가로채기 때문에 EPC(Embedded Packet Capture)를 사용하여 스위치에서 트래픽을 캡처할 수 있습니다. 이전 캡처는 스위치에 EPC를 사용하여 가져왔습니다.

시나리오 2 - 대상 호스트가 동일한 VLAN에 있고 존재하지 않으며 SVI 10 UP입니다.

목적지 호스트 192.168.1.20이 다운되어(응답하지 않음), 클라이언트는 ARP 응답을 수신하지 않으며(스위치는 ARP를 차단하지 않음), 클라이언트는 TCP SYN을 전송하지 않습니다.리디렉션이 발생하지 않습니다.

이것이 NAC Agent가 검색에 기본 게이트웨이를 사용하는 이유입니다.기본 게이트웨이는 항상 응답하고 리디렉션을 트리거해야 합니다.

시나리오 3 - 대상 호스트가 다른 VLAN에 있고, 존재하며, SVI 10 UP입니다.

이 시나리오에서는 다음과 같은 상황이 발생합니다.

1. 클라이언트가 HTTP://8.8.8.8에 액세스하려고 시도합니다.
2. 해당 네트워크는 스위치의 SVI에 없습니다.
3. 클라이언트는 해당 세션에 대한 TCP SYN을 기본 게이트웨이 192.168.1.10(대상 MAC 주소 알 수 있음)으로 전송합니다.
4. 리디렉션은 첫 번째 예와 동일한 방식으로 트리거됩니다.
5. 스위치는 해당 세션을 인터셉트하고 ISE 서버로 리디렉션하는 HTTP 응답을 반환합니다.

6. 클라이언트는 문제 없이 ISE 서버에 액세스합니다(트래픽이 리디렉션되지 않음).

참고:기본 게이트웨이가 동일한 스위치에 있는지 또는 업스트림 디바이스에 있는지 여부는 중요하지 않습니다.리디렉션 프로세스를 트리거하려면 해당 게이트웨이로부터 ARP 응답을 받아야 합니다.또한 기본 게이트웨이를 통한 ISE 액세스 가능이 허용되어야 합니다.방화벽이 패치에 있는 경우 특히 L2(Layer 2) 방화벽이고 L2 패킷이 다른 링크를 통과하는 경우(방화벽에서 TCP 상태 우회가 필요할 수 있음) 특별히 주의해야 합니다.

시나리오 4 - 대상 호스트가 다른 VLAN에 있고 존재하지 않으며 SVI 10 UP임

이 시나리오는 시나리오 3과 정확히 동일합니다. 원격 VLAN의 대상 호스트가 존재하는지 여부는 중요하지 않습니다.

시나리오 5 - 대상 호스트가 다른 VLAN에 있고, 존재하며, SVI 10 DOWN입니다.

스위치에서 클라이언트와 동일한 VLAN에 SVI UP가 없는 경우 리디렉션을 계속 수행할 수 있지만 특정 조건이 일치하는 경우에만 가능합니다.

스위치의 문제는 다른 SVI에서 클라이언트에 응답을 반환하는 방법입니다.어떤 소스 MAC 주소를 사용해야 할지 결정하기가 어렵습니다.

플로우는 SVI가 UP인 경우와 다릅니다.

1. 클라이언트는 대상 MAC 주소가 업스트림 스위치에 정의된 기본 게이트웨이로 설정된 다른 VLAN(192.168.2.20)의 호스트에 TCP SYN을 전송합니다.해당 패킷은 디버그에 의해 표시되는 리디렉션 ACL에 도달합니다.
2. 스위치에서 클라이언트로 다시 라우팅이 있는지 확인합니다.SVI 10이 다운되었습니다.
3. 스위치에 클라이언트로 다시 라우팅되는 다른 SVI가 없는 경우, EPM(Enterprise Policy Manager) 로그가 ACL에 도달했음을 나타내는 경우에도 해당 패킷이 가로채거나 리디렉션되지 않습니다.원격 호스트가 SYN ACK를 반환할 수 있지만 스위치에 클라이언트(VLAN10)로 라우팅이 없어 패킷을 삭제합니다.패킷이 리디렉션 ACL에 도달했기 때문에 다시(L2)으로 전환할 수 없습니다.
4. 스위치에 다른 SVI를 통해 클라이언트 VLAN에 대한 라우팅이 있는 경우 해당 패킷을 인터셉트하고 평소와 같이 리디렉션을 수행합니다.URL 리디렉션을 사용하는 응답은 클라이언트로 직접 이동되지 않고 라우팅 결정에 따라 다른 스위치/라우터를 통해 전송됩니다.

비대칭성은 다음과 같습니다.

- 클라이언트에서 수신된 트래픽은 스위치에 의해 로컬로 차단됩니다.
- HTTP 리디렉션을 포함하는 그에 대한 응답은 라우팅을 기반으로 업스트림 스위치를 통해 전송됩니다.
- 이는 방화벽에 일반적인 문제가 발생할 수 있으며 TCP 우회가 필요한 경우입니다.
- 리디렉션되지 않은 ISE로의 트래픽은 대칭적입니다.리디렉션 자체만 비대칭입니다.

시나리오 6 - 대상 호스트가 다른 VLAN에 있고 존재하지 않으며 SVI 10 DOWN임

이 시나리오는 시나리오 5와 정확히 동일합니다. 원격 호스트가 존재해도 상관없습니다.중요한 것은 올바른 라우팅입니다.

시나리오 7 - HTTP 서비스가 다운되었습니다.

시나리오 6에서 설명한 것처럼 스위치의 HTTP 프로세스는 중요한 역할을 합니다.HTTP 서비스가 비활성화된 경우 EPM은 패킷이 리디렉션 ACL에 도달함을 표시합니다.

```
epm-redirect:IP=192.168.1.201: Ingress packet on [idb= GigabitEthernet1/0/2] matched
with [acl=REDIRECT_POSTURE]
```

그러나 리디렉션은 발생하지 않습니다.

스위치의 HTTPS 서비스는 HTTP 리디렉션에 필요하지 않지만 HTTPS 리디렉션에 필요합니다 .NAC Agent는 ISE 검색에 둘 다 사용할 수 있습니다.따라서 둘 다 활성화하는 것이 좋습니다.

리디렉션 ACL - 잘못된 프로토콜 및 포트, 리디렉션 없음

스위치는 표준 포트(TCP/80 및 TCP/443)에서 작동하는 HTTP 또는 HTTPS 트래픽만 가로채는 것을 확인할 수 있습니다. HTTP/HTTPS가 비표준 포트에서 작동하는 경우 **ip port-map http** 명령으로 구성할 수 있습니다.또한 스위치에는 해당 포트(**ip http 포트**)에서 HTTP 서버가 수신 대기해야 합니다.

관련 정보

- 스위치 및 ISE(Identity Services Engine)를 사용한 중앙 웹 인증 구성 예
- Cisco Identity Services Engine 사용 설명서, 릴리스 1.2
- 기술 지원 및 문서 – Cisco Systems