Umleitung des ISE-Datenverkehrs auf dem Catalyst Switch der Serie 3750

Inhalt

Einführung

In diesem Artikel wird die Funktionsweise der Umleitung von Benutzerdatenverkehr und die Bedingungen beschrieben, die für die Umleitung des Pakets durch den Switch erforderlich sind.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Erfahrungen mit der Konfiguration der Cisco Identity Services Engine (ISE) zu verfügen und grundlegende Kenntnisse in folgenden Bereichen zu erwerben:

- ISE-Bereitstellungen und CWA-Flüsse (Central Web Authentication)

- CLI-Konfiguration von Cisco Catalyst Switches

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Microsoft Windows 7
- Cisco Catalyst Switches der Serie 3750X, Versionen 15.0 und höher
- ISE Software, Versionen 1.1.4 und höher

Hintergrundinformationen

Die Umleitung des Benutzerdatenverkehrs auf dem Switch ist für die meisten Bereitstellungen mit der ISE eine wichtige Komponente. All diese Datenflüsse beinhalten die Umleitung des Datenverkehrs durch den Switch:

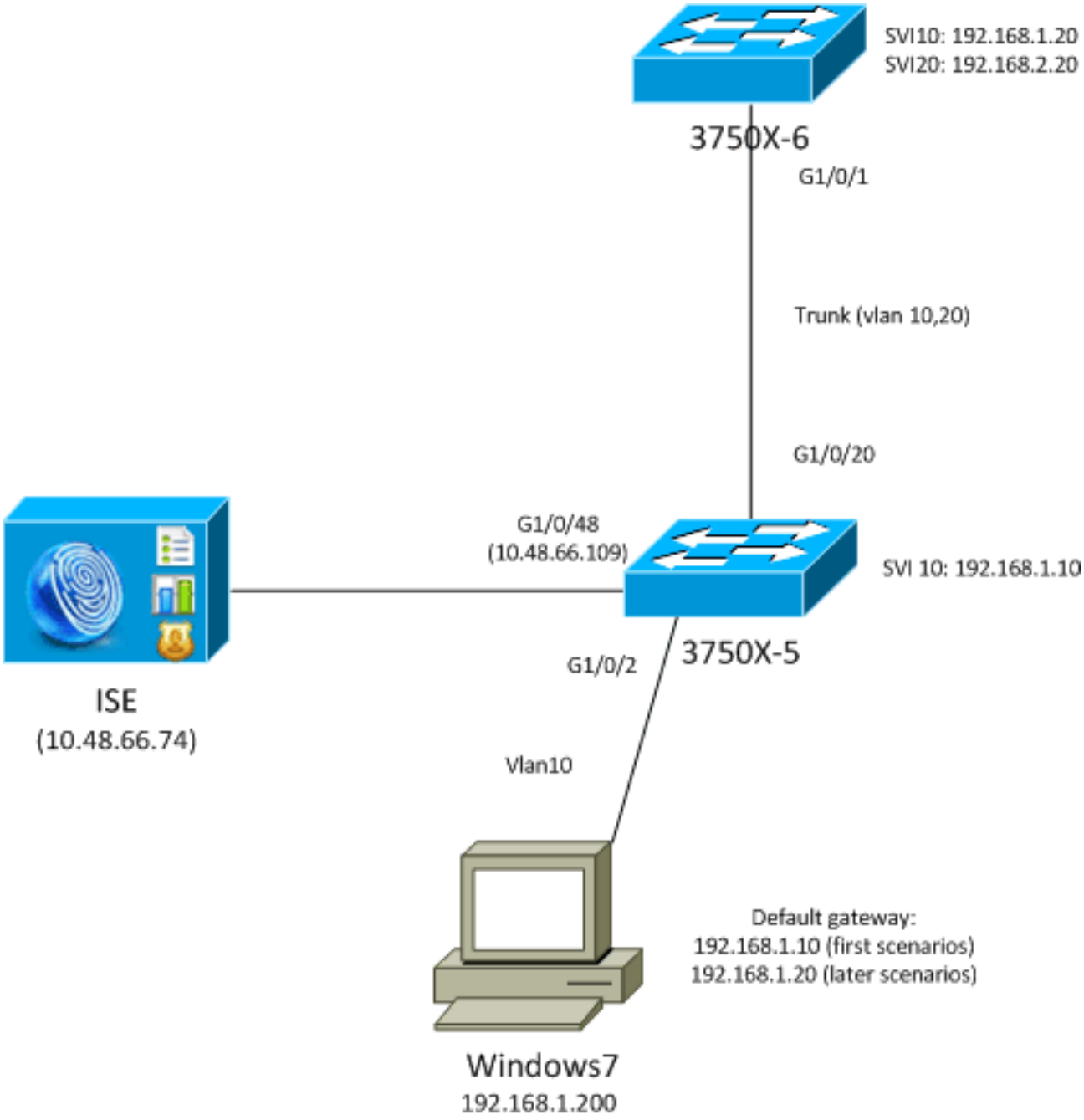
- CWA
- Client-Bereitstellung (CPP)
- Geräteregistrierung (DRW)
- Native Supplicant Provisioning (NSP)
- Mobile Device Management (MDM)

Die falsch konfigurierte Umleitung ist die Ursache für mehrere Probleme bei der Bereitstellung. Das typische Ergebnis ist ein NAC-Agent (Network Admission Control), der nicht korrekt angezeigt wird, oder eine Unmöglichkeit, das Gastportal anzuzeigen.

In Szenarien, in denen der Switch nicht über dieselbe Switch Virtual Interface (SVI) wie das Client-VLAN verfügt, finden Sie weitere Informationen in den letzten drei Beispielen.

Fehlerbehebung

Testszenario



Tests werden am Client durchgeführt, der zur Bereitstellung an die ISE (CPP) umgeleitet werden sollte. Der Benutzer wird über MAB (MAC Authentication Bypass) oder 802.1x authentifiziert. Die ISE gibt das Autorisierungsprofil mit dem Namen der ACL (Redirect Access Control List) (REDIRECT_POSTURE) zurück und leitet die URL (Redirect to ISE) um:

```
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
```

Die herunterladbare ACL (DACL) lässt den gesamten Datenverkehr in dieser Phase zu:

```
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
```

Die Umleitungs-ACL lässt diesen Datenverkehr ohne Umleitung zu:

- Gesamter Datenverkehr zur ISE (10.48.66.74)
- Domain Name System (DNS)- und Internet Control Message Protocol (ICMP)-Datenverkehr

Alle anderen Datenverkehrsarten sollten umgeleitet werden:

```
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
```

Der Switch verfügt über eine SVI im gleichen VLAN wie der Benutzer:

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

In den nächsten Abschnitten wird diese geändert, um die potenziellen Auswirkungen darzustellen.

Der Datenverkehr erreicht die Umleitungszugriffskontrollliste nicht.

Wenn Sie versuchen, einen Host zu pingen, sollten Sie eine Antwort erhalten, da dieser Datenverkehr nicht umgeleitet wird. Führen Sie zur Bestätigung dieses Debuggens aus:

```
debug epm redirect
```

Für jedes vom Client gesendete ICMP-Paket muss das Debuggen Folgendes enthalten:

```
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]
```

Überprüfen Sie zur Bestätigung die ACL:

```
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
```

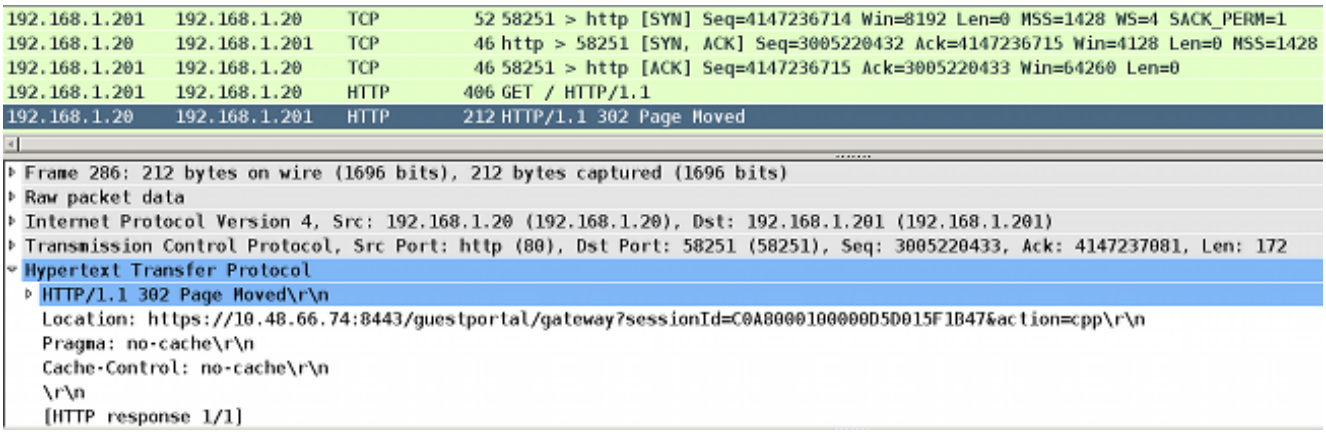
Datenverkehr erreicht die Umleitungs-ACL

Szenario 1: Der Ziel-Host befindet sich im selben VLAN, ist vorhanden und ist SVI 10 UP.

Wenn Sie den Datenverkehr an die IP-Adresse initiieren, die direkt über den Switch erreichbar ist (das Netzwerk für den Switch verfügt über eine SVI-Schnittstelle), geschieht Folgendes:

1. Der Client initiiert eine ARP-Auflösungsanfrage (Address Resolution Protocol) für den Zielhost (192.168.1.20) im gleichen VLAN und empfängt eine Antwort (ARP-Datenverkehr wird nie umgeleitet).

2. Der Switch fängt diese Sitzung an, selbst wenn die Ziel-IP-Adresse auf diesem Switch nicht konfiguriert ist. TCP-Handshaking zwischen Client und Switch ist abgeschlossen. In dieser Phase werden keine anderen Pakete außerhalb des Switches gesendet. In diesem Szenario hat der Client (192.168.1.201) eine TCP-Sitzung mit dem anderen Host initiiert, der in diesem VLAN (192.168.1.20) vorhanden ist und für den der Switch über eine SVI-Schnittstelle UP verfügt (mit der IP-Adresse 192.168.1.10):



3. Nachdem die TCP-Sitzung eingerichtet und die HTTP-Anfrage gesendet wurde, gibt der Switch die HTTP-Antwort mit der Umleitung an die ISE (Location-Header) zurück.

   Diese Schritte werden durch Debug bestätigt. Es gibt mehrere ACL-Treffer:

```
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
```

Dies kann auch durch detailliertere Debuggen bestätigt werden:

```
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. Der Client stellt eine direkte Verbindung zur ISE her (SSL-Sitzung (Secure Sockets Layer) mit 10.48.66.74:8443). Dieses Paket löst keine Umleitung aus:

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

Hinweis: Die Sitzung wird vom Switch abgefangen, sodass der Datenverkehr über Embedded Packet Capture (EPC) auf dem Switch erfasst werden kann. Die vorherige Erfassung wurde mit EPC auf dem Switch durchgeführt.

Szenario 2 - Der Ziel-Host ist im selben VLAN, nicht vorhanden und ist SVI 10 UP.

Wenn der Zielhost 192.168.1.20 ausgefallen ist (reagiert nicht), erhält der Client keine ARP-Antwort (der Switch fängt ARP nicht ab) und der Client sendet kein TCP-SYN. Eine Umleitung findet nie statt.

Aus diesem Grund verwendet der NAC Agent ein Standard-Gateway für eine Erkennung. Ein Standard-Gateway sollte immer reagieren und Umleitungen auslösen.

Szenario 3: Der Ziel-Host befindet sich in einem anderen VLAN, ist vorhanden und ist SVI 10 UP.

Folgendes geschieht in diesem Szenario:

1. Der Client versucht, auf HTTP://8.8.8.8 zuzugreifen.

2. Das Netzwerk befindet sich auf keiner SVI des Switches.
3. Der Client sendet eine TCP-SYN für diese Sitzung an das Standard-Gateway 192.168.1.10 (Ziel-MAC-Adresse bekannt).

4. Die Umleitung wird genau wie im ersten Beispiel ausgelöst.

5. Der Switch fängt diese Sitzung ab und gibt eine HTTP-Antwort zurück, die zum ISE-Server

umgeleitet wird.

6. Der Client greift problemlos auf den ISE-Server zu (dieser Datenverkehr wird nicht umgeleitet).

   Hinweis: Es spielt keine Rolle, ob sich das Standard-Gateway auf demselben Switch oder auf einem Upstream-Gerät befindet. Es ist nur erforderlich, eine ARP-Antwort von diesem Gateway zu erhalten, um den Umleitungsprozess auszulösen. Darüber hinaus ist es erforderlich, dass die ISE-Zugänglichkeit über das Standard-Gateway zugelassen wird. Achten Sie besonders darauf, wenn eine Firewall auf dem Patch installiert ist, insbesondere wenn es sich um eine Layer-2-Firewall (L2) und L2-Pakete handelt, die verschiedene Links durchlaufen (dann ist in der Firewall möglicherweise eine Umgehung des TCP-Zustands erforderlich).

Szenario 4 - Zielhost befindet sich in einem anderen VLAN, ist nicht vorhanden und ist SVI 10 UP

Dieses Szenario entspricht dem Szenario 3. Ob der Ziel-Host in einem Remote-VLAN vorhanden ist oder nicht, spielt keine Rolle.

Szenario 5: Der Ziel-Host befindet sich in einem anderen VLAN, ist vorhanden und ist SVI 10 DOWN.

Wenn der Switch nicht über SVI UP im selben VLAN wie der Client verfügt, kann er dennoch eine Umleitung durchführen, jedoch nur, wenn bestimmte Bedingungen erfüllt sind.

Das Problem für den Switch besteht darin, wie die Antwort von einer anderen SVI an den Client zurückgegeben wird. Es ist schwierig zu bestimmen, welche Quell-MAC-Adresse verwendet werden soll.

Der Fluss unterscheidet sich von dem, wenn SVI UP ist:

1. Der Client sendet eine TCP-SYN an den Host in einem anderen VLAN (192.168.2.20), wobei eine MAC-Zieladresse auf ein Standard-Gateway festgelegt ist, das auf dem Upstream-Switch definiert ist. Dieses Paket erreicht die Umleitungs-ACL, die von Debuggen angezeigt wird.
2. Der Switch prüft, ob ein Routing zurück zum Client vorhanden ist. Beachten Sie, dass SVI 10 ausgefallen ist.
3. Verfügt der Switch nicht über eine andere SVI, über die ein Routing zurück zum Client erfolgt, wird dieses Paket nicht abgefangen oder umgeleitet, selbst wenn die Protokolle des Enterprise Policy Manager (EPM) darauf hindeuten, dass die ACL erreicht ist. Der Remote-Host kann möglicherweise ein SYN ACK zurückgeben, aber der Switch verfügt nicht über ein Routing zurück zum Client (VLAN10) und verwirft das Paket. Das Paket kann nicht einfach zurückgeschaltet werden (L2), da es die ACL für die Umleitung erreicht hat.
4. Wenn der Switch über eine andere SVI zum Client-VLAN weitergeleitet wird, wird dieses Paket abgefangen und wie gewohnt umgeleitet. Die Antwort mit URL-Umleitung erfolgt nicht direkt an den Client, sondern über einen anderen Switch/Router, der auf der Routing-Entscheidung basiert.

Beachten Sie hier die Asymmetrie:

- Der vom Client empfangene Datenverkehr wird vom Switch lokal abgefangen.
- Die Antwort darauf, einschließlich der HTTP-Umleitung, wird basierend auf dem Routing über den Upstream-Switch gesendet.
- Dies ist der Fall, wenn typische Probleme mit der Firewall auftreten können und eine TCP-Umgehung erforderlich ist.
- Der Datenverkehr zur ISE, der nicht umgeleitet wird, ist symmetrisch. Nur die Umleitung selbst ist asymmetrisch.

Szenario 6 - Zielhost befindet sich in einem anderen VLAN, ist nicht vorhanden und ist SVI 10 DOWN.

Dieses Szenario entspricht dem Szenario 5. Es spielt keine Rolle, ob der Remotehost vorhanden ist. Das richtige Routing ist wichtig.

Szenario 7 - HTTP-Service ist ausgefallen

Wie in Szenario 6 dargestellt, spielt der HTTP-Prozess auf dem Switch eine wichtige Rolle. Wenn der HTTP-Dienst deaktiviert ist, zeigt EPM, dass das Paket die umgeleitete ACL erreicht:

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

Die Umleitung findet jedoch nie statt.

Der HTTPS-Service auf dem Switch ist für eine HTTP-Umleitung nicht erforderlich, für HTTPS-Umleitung jedoch erforderlich. Der NAC Agent kann beide für die ISE-Erkennung verwenden. Daher wird empfohlen, beide Optionen zu aktivieren.

Umleiten der ACL - Falsche Protokolle und Ports, keine Umleitung

Beachten Sie, dass der Switch nur HTTP- oder HTTPS-Datenverkehr abfangen kann, der an Standard-Ports (TCP/80 und TCP/443) funktioniert. Wenn HTTP/HTTPS auf einem nicht standardmäßigen Port funktioniert, kann er mit dem Befehl **ip port-map http** konfiguriert werden. Außerdem muss der Switch seinen HTTP-Server-Überwachungs-Port (**ip http port**) haben.

Zugehörige Informationen

- Zentrale Webauthentifizierung mit einem Konfigurationsbeispiel für einen Switch und eine Identity Services Engine
- Cisco Identity Services Engine-Benutzerhandbuch, Version 1.2
- Technischer Support und Dokumentation - Cisco Systems