Cambio de dirección del tráfico ISE en el Catalyst 3750 Series Switch

Contenido

Introducción

Este artículo describe cómo el cambio de dirección del tráfico de usuarios trabaja y las condiciones que son necesarias para reorientar el paquete por el conmutador.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene experiencia con la configuración del Cisco Identity Services Engine (ISE) y el conocimiento básico de estos temas:

- Implementaciones ISE y flujos centrales de la autenticación Web (CWA)
- Configuración CLI del Switches del Cisco Catalyst

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Microsoft Windows 7
- Software del Cisco Catalyst 3750X Series Switch, versiones 15.0 y más adelante
- Software ISE, versiones 1.1.4 y más adelante

Antecedentes

El cambio de dirección del tráfico de usuarios en el conmutador es un componente crítico para la mayor parte de las implementaciones con el ISE. Todos estos flujos implican el uso del cambio de dirección del tráfico por el conmutador:

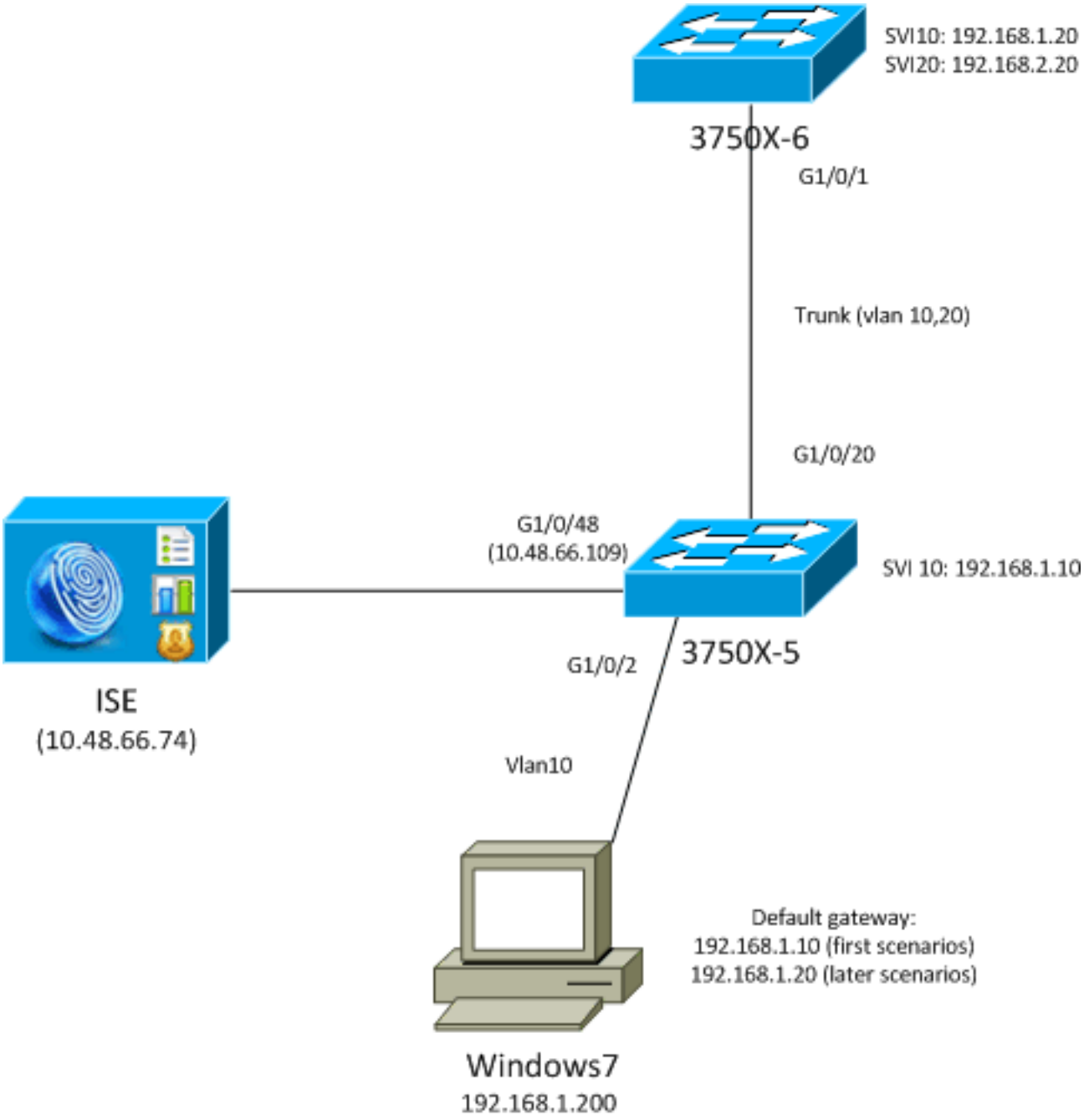
- CWA
- Aprovisionamiento del cliente (CPP)
- Registro del dispositivo (DRW)
- Aprovisionamiento nativo del suplicante (NSP)
- Administración de dispositivo móvil (MDM)

El cambio de dirección incorrectamente configurado es la causa de los varios problemas con el despliegue. El resultado típico es un agente del Network Admission Control (NAC) que no surge correctamente o una incapacidad para visualizar el portal del invitado.

Para los decorados en los cuales el conmutador no tiene la misma interfaz virtual del conmutador (SVI) que el VLA N del cliente, refiera a los tres ejemplos pasados.

Troubleshooting

Escenario de prueba



Las pruebas se realizan en el cliente, que debe ser reorientado a ISE para disposición (CPP). Autentican al usuario vía puente de la autenticación MAC (MAB) o el 802.1x. ISE vuelve el perfil de la autorización con el nombre de la lista de control de acceso (ACL) de la reorientación (REDIRECT_POSTURE) y reorienta el URL (reorienta a ISE):

```
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
```

ACL descargable (DACL) permite todo el tráfico en esta etapa:

```
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
```

La reorientación ACL permite este tráfico sin el cambio de dirección:

- Todo el tráfico al ISE (10.48.66.74)
- Tráfico del Domain Name System (DNS) y del Internet Control Message Protocol (ICMP)

El resto del tráfico debe ser reorientado:

```
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
```

El conmutador tiene un SVI en el mismo VLA N que el usuario:

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

En las siguientes secciones, esto se modifica para presentar el impacto potencial.

El tráfico no alcanza la reorientación ACL

Cuando usted intenta hacer ping cualquier host, usted debe recibir una respuesta porque ese tráfico no se reorienta. Para confirmar, ejecute esta depuración:

```
debug epm redirect
```

Para cada paquete ICMP enviado por el cliente, las depuraciones deben presentar:

```
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]
```

Para confirmar, examine el 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
```

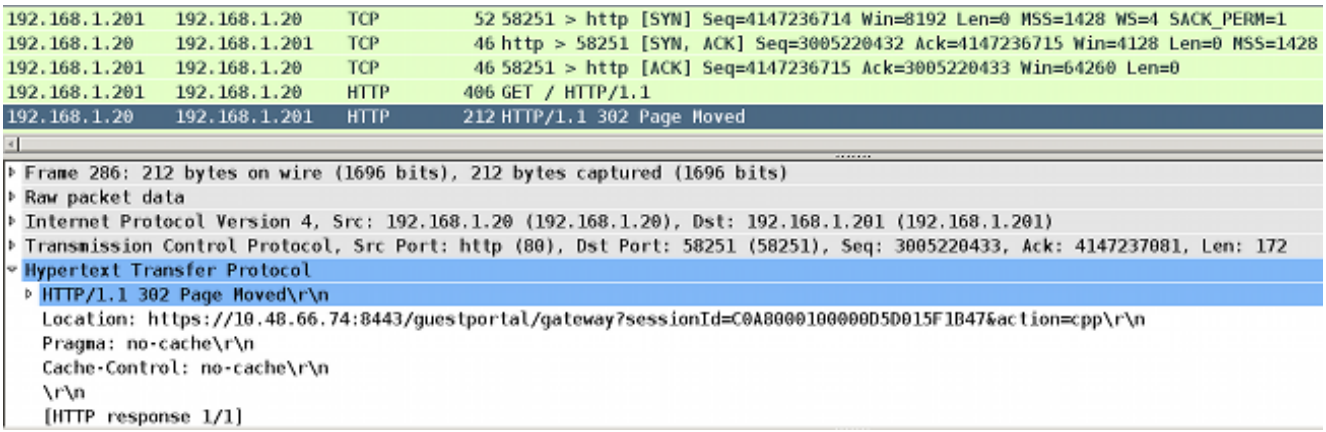
El tráfico alcanza la reorientación ACL

Decorado 1 - El host del destino está en el mismo VLA N, existe, y es SVI 10 PARA ARRIBA

Cuando usted inicia el tráfico a la dirección IP que es directamente la capa 3 (L3) accesible por el conmutador (la red para el conmutador tiene un interfaz SVI), aquí es qué sucede:

1. El cliente inicia un pedido de la resolución del Address Resolution Protocol (ARP) el host del destino (192.168.1.20) en el mismo VLA N y recibe una respuesta (el tráfico ARP nunca se reorienta).

2. Las interceptaciones del conmutador que sesión, incluso cuando la dirección IP del destino no se configura en ese conmutador. El apretón de manos TCP entre el cliente y el conmutador se acaba. En esta etapa, no se envía ningunos otros paquetes fuera del conmutador. En este decorado, el cliente (192.168.1.201) ha iniciado a una sesión TCP con el otro host que existe en ese VLA N (192.168.1.20) y para cuál tiene el conmutador un interfaz SVI PARA ARRIBA (con la dirección IP de 192.168.1.10):



3. Después de que establezcan a la sesión TCP y se envía la solicitud HTTP, el conmutador vuelve el HTTP de respuesta con el cambio de dirección a ISE (encabezado Location).

   Estos pasos son confirmados por las depuraciones. Hay varios golpes ACL:

```
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
```

Esto se puede también confirmar por depuraciones más detalladas:

```
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. El cliente conecta con el ISE directamente (sesión de Secure Sockets Layer (SSL) a 10.48.66.74:8443). Este paquete no acciona el cambio de dirección:

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

Note: La sesión es interceptada por el conmutador, y ese tráfico se puede capturar así en el conmutador con la captura de paquetes integrada (EPC). La captura anterior fue tomada con el EPC en el conmutador.

Decorado 2 - El host del destino está en el mismo VLA N, no existe, y es SVI 10 PARA ARRIBA

Si el host 192.168.1.20 del destino está abajo (no responde), el cliente no recibe una contestación ARP (el conmutador no intercepta el ARP), y el cliente no envía un SYN TCP. El cambio de dirección nunca ocurre.

Esta es la razón por la cual el agente NAC utiliza un gateway de valor por defecto para un descubrimiento. Un gateway de valor por defecto debe responder siempre y el activador reorienta.

Decorado 3 - El host del destino está en diverso VLA N, existe, y es SVI 10 PARA ARRIBA

Aquí es qué sucede en este decorado:

1. Los intentos del cliente para tener acceso a HTTP://8.8.8.8.

2. Esa red no está en ningún SVI en el conmutador.
3. El cliente envía un SYN TCP para esa sesión al gateway de valor por defecto 192.168.1.10 (dirección MAC del destino sabida).

4. El cambio de dirección se acciona de la misma manera como en el primer ejemplo.

5. Las interceptaciones del conmutador que la sesión y vuelven un HTTP de respuesta que

reorienta al servidor ISE.

6. Los accesos al cliente el servidor ISE sin los problemas (ese tráfico no se reorienta).

Note: No importa si el gateway de valor por defecto está en el mismo conmutador o en un dispositivo ascendente. Es solamente necesario recibir una respuesta ARP de ese gateway para accionar el proceso de la reorientación. Además, es necesario que la accesibilidad ISE vía el gateway de valor por defecto está permitida. Preste la especial atención si un Firewall está en la corrección, especialmente si es un Firewall de la capa 2 (L2) y links transversales de los paquetes L2 diversos (entonces puente del estado TCP pudo ser necesario en el Firewall).

Decorado 4 - El host del destino está en diverso VLA N, no existe, y es SVI 10 PARA ARRIBA

Este decorado es exactamente lo mismo que el decorado 3. No importa si existe el host del destino en un VLA N remoto o no.

Decorado 5 - El host del destino está en diverso VLA N, existe, y es SVI 10 ABAJO

Si el conmutador no tiene SVI PARA ARRIBA en el mismo VLA N que el cliente, puede todavía realizar el cambio de dirección pero solamente cuando se corresponden con las condiciones específicas.

El problema para el conmutador es cómo volver la respuesta al cliente de un diverso SVI. Es difícil determinar qué dirección MAC de la fuente debe ser utilizada.

El flujo es diferente de cuando el SVI está PARA ARRIBA:

1. El cliente envía un SYN TCP al host en un diverso VLA N (192.168.2.20) con una dirección MAC del destino fijada a un gateway de valor por defecto que se defina en el conmutador por aguas arriba. Ese paquete alcanza la reorientación ACL, que es mostrada por las depuraciones.
2. El conmutador verifica si tiene una encaminamiento de nuevo al cliente. Recuerde que el SVI 10 está ABAJO.
3. Si el conmutador no tiene otro SVI que tenga una encaminamiento de nuevo al cliente, ese paquete no se intercepta ni se reorienta, incluso cuando los registros del Administrador de directivas de la empresa (EPM) indican que el ACL está alcanzado. El host remoto pudo volver un SYN ACK, pero el conmutador no tiene una encaminamiento de nuevo al cliente (VLAN10) y cae el paquete. El paquete no se puede apenas cambiar detrás (L2), porque alcanzó la reorientación ACL.
4. Si el conmutador tiene una encaminamiento al VLA N del cliente vía un diverso SVI, intercepta ese paquete y realiza la reorientación como de costumbre. La respuesta con URL-reorienta no va directamente al cliente, pero vía un diversos conmutador/router basados en la decisión de la encaminamiento.

Note la asimetría aquí:

- El tráfico recibido del cliente es interceptado localmente por el conmutador.

- La respuesta para la, que incluye el HTTP reorienta, se envía vía el conmutador por aguas arriba basado en la encaminamiento.
- Esto es cuando los problemas típicos con el Firewall pudieron ocurrir, y se requiere puente TCP.
- Trafique al ISE, que no se reorienta, es simétrico. Solamente el cambio de dirección sí mismo es asimétrico.

Decorado 6 - El host del destino está en diverso VLA N, no existe, y es SVI 10 ABAJO

Este decorado es exactamente lo mismo que el decorado 5. No importa que exista el host remoto. La encaminamiento correcta es cuál es importante.

Decorado 7 - El servicio HTTP está abajo

Según lo presentado en el decorado 6, el proceso HTTP en el conmutador desempeña un papel importante. Si se inhabilita el servicio HTTP, el EPM muestra que el paquete alcanza la reorientación ACL:

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

Sin embargo, el cambio de dirección nunca ocurre.

El servicio HTTPS en el conmutador no se requiere para un HTTP reorienta, sino que se requiere para el HTTPS reorienta. El agente NAC puede utilizar ambos para el descubrimiento ISE. Por lo tanto, se aconseja para activar ambos.

Reoriente el ACL - Protocolos incorrectos y puerto, ningún cambio de dirección

Note que el conmutador puede interceptar solamente el tráfico HTTP o HTTPS que trabaja en los puertos estándars (TCP/80 y TCP/443). Si el HTTP/HTTPS trabaja en un puerto no estándar, puede ser configurado con el comando **HTTP del port-map IP**. También, el conmutador debe hacer que su servidor HTTP escuche en ese puerto (**ip http puerto**).

Información Relacionada

- Autenticación Web central con un ejemplo de la configuración del conmutador y del Identity Services Engine
- Guía de usuario de Cisco Identity Services Engine, versión 1.2
- Soporte Técnico y Documentación - Cisco Systems