

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

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Troubleshooting](#)

[Escenario de prueba](#)

[El tráfico no alcanza la reorientación ACL](#)

[El tráfico alcanza la reorientación ACL](#)

[Escenario 1 - La computadora principal de destino está en el mismo VLA N, existe, y es SVI 10 PARA ARRIBA](#)

[Escenario 2 - La computadora principal de destino está en el mismo VLA N, no existe, y es SVI 10 PARA ARRIBA](#)

[Escenario 3 - La computadora principal de destino está en diverso VLA N, existe, y es SVI 10 PARA ARRIBA](#)

[Escenario 4 - La computadora principal de destino está en diverso VLA N, no existe, y es SVI 10 PARA ARRIBA](#)

[Escenario 5 - La computadora principal de destino está en diverso VLA N, existe, y es SVI 10 ABAJO](#)

[Escenario 6 - La computadora principal de destino está en diverso VLA N, no existe, y es SVI 10 ABAJO](#)

[Escenario 7 - El servicio HTTP está abajo](#)

[Reoriente el ACL - Protocolos incorrectos y puerto, ningún cambio de dirección](#)

[Información Relacionada](#)

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 Switch.

Prerequisites

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 posterior
- Software ISE, versiones 1.1.4 y posterior

Antecedentes

El cambio de dirección del tráfico de usuarios en el Switch 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 Switch:

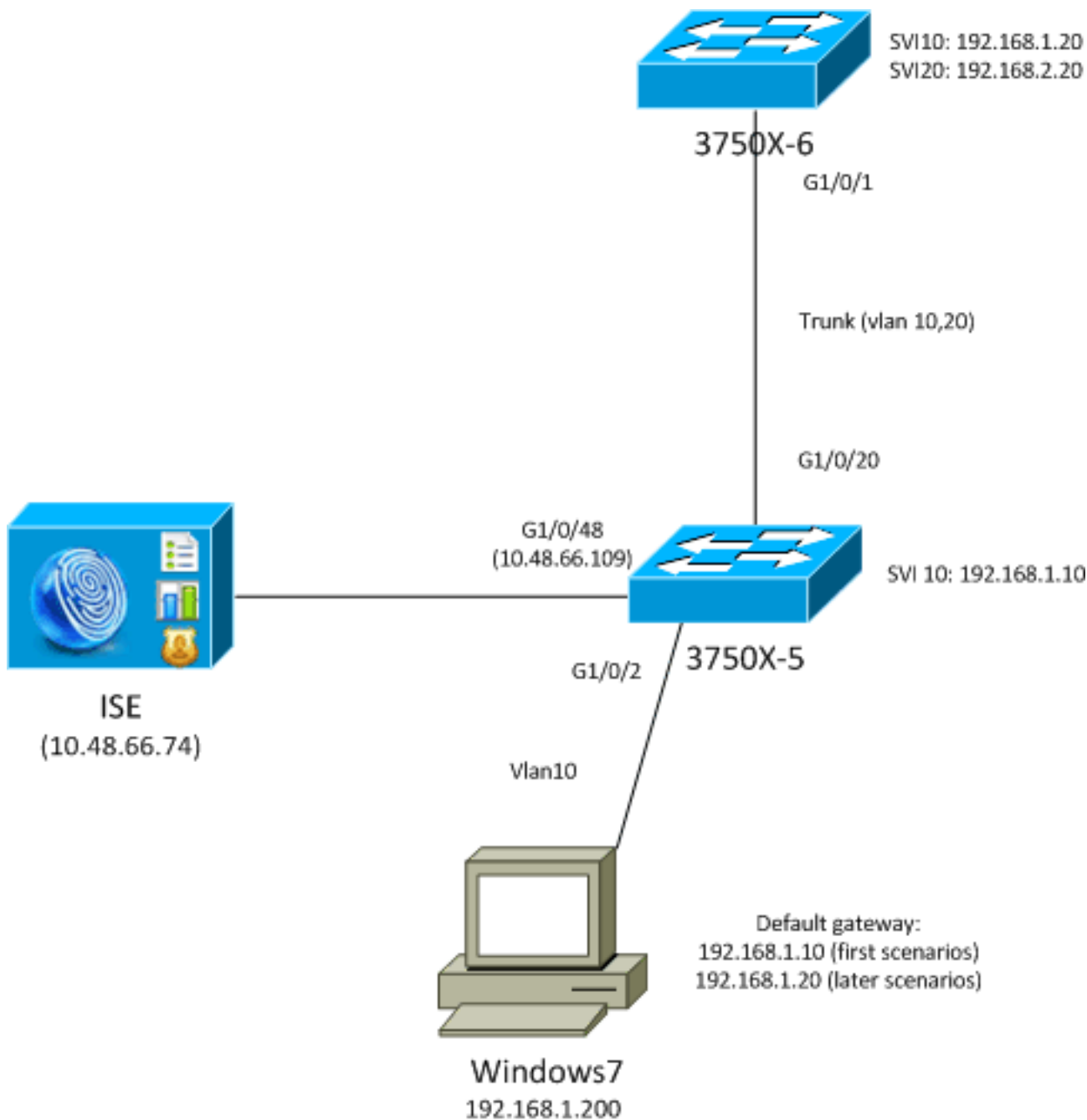
- CWA
- Aprovisionamiento del cliente (CPP)
- Registro del dispositivo (DRW)
- Disposición nativa del supplicant (NSP)
- Administración de dispositivo móvil (MDM)

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 escenarios en los cuales el Switch no tiene la misma interfaz virtual del Switch (SVI) que el VLA N del cliente, refiera a los tres ejemplos más recientes.

Troubleshooting

Escenario de prueba



Las pruebas se realizan en el cliente, que debe ser reorientado al ISE para disposición (CPP). Autentican al usuario vía puente de la autenticación de MAC (MAB) o el 802.1x. El 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 al 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=
COA8000100000D5D015F1B47&action=cpp
Session timeout: N/A
Idle timeout: N/A
Common Session ID: COA8000100000D5D015F1B47
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 Switch tiene un SVI en el mismo VLA N que el usuario:

```
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
```

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 este debug:

```
debug epm redirect
```

Para cada paquetes icmp enviados por el cliente, los debugs 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

Escenario 1 - La computadora principal de 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 Switch (la red para el Switch tiene una interfaz SVI), aquí es qué sucede:

1. El cliente inicia un pedido de la resolución del Address Resolution Protocol (ARP) la computadora principal de destino (192.168.1.20) en el mismo VLA N y recibe una respuesta (el tráfico ARP nunca se reorienta).
2. Las interceptaciones del Switch que sesión, incluso cuando el IP Address de destino no se configura en ese Switch. El apretón de manos TCP entre el cliente y el Switch se acaba. En esta etapa, no se envía ningunos otros paquetes fuera del Switch. En este escenario, 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 Switch una interfaz SVI PARA ARRIBA (con la dirección IP de 192.168.1.10):

192.168.1.201	192.168.1.20	TCP	52	58251 > http [SYN] Seq=4147236714 Win=8192 Len=0 MSS=1428 WS=4 SACK_PERM=1
192.168.1.20	192.168.1.201	TCP	46	http > 58251 [SYN, ACK] Seq=3005220432 Ack=4147236715 Win=4128 Len=0 MSS=1428
192.168.1.201	192.168.1.20	TCP	46	58251 > http [ACK] Seq=4147236715 Ack=3005220433 Win=64260 Len=0
192.168.1.201	192.168.1.20	HTTP	406	GET / HTTP/1.1
192.168.1.20	192.168.1.201	HTTP	212	HTTP/1.1 302 Page Moved

<p>Frame 286: 212 bytes on wire (1696 bits), 212 bytes captured (1696 bits)</p> <p>Raw packet data</p> <p>Internet Protocol Version 4, Src: 192.168.1.20 (192.168.1.20), Dst: 192.168.1.201 (192.168.1.201)</p> <p>Transmission Control Protocol, Src Port: http (80), Dst Port: 58251 (58251), Seq: 3005220433, Ack: 4147237081, Len: 172</p> <p>HyperText Transfer Protocol</p> <p>HTTP/1.1 302 Page Moved\r\n</p> <p>Location: https://10.48.66.74:8443/guestportal/gateway?sessionId=C0A800010000050015F1B47&action=cpp\r\n</p> <p>Pragma: no-cache\r\n</p> <p>Cache-Control: no-cache\r\n</p> <p>\r\n</p> <p>[HTTP response 1/1]</p>	
---	--

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

Estos pasos son confirmados por los debugs. 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 debugs más detallados:

```
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 Switch, y ese tráfico se puede capturar así en el Switch con la captura de paquetes integrada (EPC). La captura anterior fue tomada con el EPC en el Switch.

Escenario 2 - La computadora principal de destino está en el mismo VLA N, no existe, y es SVI 10 PARA ARRIBA

Si la computadora principal de destino 192.168.1.20 está abajo (no responde), el cliente no recibe una respuesta ARP (el Switch no intercepta el ARP), y el cliente no envía un TCP SYN. El cambio de dirección nunca ocurre.

Esta es la razón por la cual el agente del NAC utiliza un default gateway para una detección. Un default gateway debe responder siempre y el activador reorienta.

Escenario 3 - La computadora principal de destino está en diverso VLA N, existe, y es SVI 10 PARA ARRIBA

Aquí es qué sucede en este escenario:

1. Los intentos del cliente para acceder HTTP://8.8.8.8.

2. Esa red no está en ningún SVI en el Switch.
3. El cliente envía un TCP SYN para esa sesión al default gateway 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 Switch 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 default gateway está en el mismo Switch 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 default gateway 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).

Escenario 4 - La computadora principal de destino está en diverso VLA N, no existe, y es SVI 10 PARA ARRIBA

Este escenario es exactamente lo mismo que el escenario 3. No importa si existe la computadora principal de destino en un VLA N remoto o no.

Escenario 5 - La computadora principal de destino está en diverso VLA N, existe, y es SVI 10 ABAJO

Si el Switch 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 Switch es cómo volver la respuesta al cliente de un diverso SVI. Es difícil determinar qué MAC Address de origen debe ser utilizado.

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

1. El cliente envía un TCP SYN al host en un diverso VLA N (192.168.2.20) con una dirección MAC del destino fijada a un default gateway que se defina en el Switch por aguas arriba. Ese paquete alcanza la reorientación ACL, que es mostrada por los debugs.
2. El Switch verifica si tiene una encaminamiento de nuevo al cliente. Recuerde que el SVI 10 está ABAJO.
3. Si el Switch 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 Switch no tiene una encaminamiento de nuevo al cliente (VLAN10) y cae el paquete. El paquete no se puede apenas conmutar detrás (L2), porque alcanzó la reorientación ACL.
4. Si el Switch 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 Switch/router basados en la decisión de ruteo.

Note la asimetría aquí:

- El tráfico recibido del cliente es interceptado localmente por el Switch.
- La respuesta para la, que incluye el HTTP reorienta, se envía vía el Switch por aguas arriba basado en la encaminamiento.
- Esto es cuando los problemas comunes 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.

Escenario 6 - La computadora principal de destino está en diverso VLA N, no existe, y es SVI 10 ABAJO

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

Escenario 7 - El servicio HTTP está abajo

Según lo presentado en el escenario 6, el proceso HTTP en el Switch 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 Switch no se requiere para un HTTP reorienta, sino que se requiere para el HTTPS reorienta. El agente del NAC puede utilizar ambos para la detección ISE. Por lo tanto, se aconseja para habilitar ambos.

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

Note que el Switch puede interceptar solamente el tráfico HTTP o HTTPS que trabaja en los puertos estándares (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 del IP**. También, el Switch debe tener su servidor HTTP escuchar en ese puerto (**ip http puerto**).

Información Relacionada

- [Autenticación Web central con un ejemplo de configuración del Switch y del Identity Services Engine](#)
- [Guía del usuario del Cisco Identity Services Engine, versión 1.2](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)