Reorientação do tráfego ISE no Catalyst 3750 Series Switch

Índice

Introdução

Este artigo descreve como a reorientação do tráfego de usuário trabalha e as circunstâncias que são necessárias a fim reorientar o pacote pelo interruptor.

Pré-requisitos

Requisitos

Cisco recomenda que você tem a experiência com a configuração do Cisco Identity Services Engine (ISE) e o conhecimento básico destes assuntos:

- Disposições ISE e fluxos centrais da autenticação da Web (CWA)
- Configuração de CLI do Switches do Cisco catalyst

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Microsoft Windows 7
- Software do Cisco Catalyst 3750X Series Switch, versões 15.0 e mais recente
- Software ISE, versões 1.1.4 e mais recente

Informações de Apoio

A reorientação do tráfego de usuário no interruptor é um componente crítico para a maioria das disposições com o ISE. Todos estes fluxos envolvem o uso da reorientação do tráfego pelo interruptor:

- CWA
- Abastecimento do cliente (CPP)
- Registro do dispositivo (DRW)
- Abastecimento nativo do suplicante (NSP)
- Gerenciamento de dispositivo móvel (MDM)

A reorientação incorretamente configurada é a causa dos problemas múltiplos com o desenvolvimento. O resultado típico é um agente do Network Admission Control (NAC) que não estale acima corretamente ou uma incapacidade indicar o portal do convidado.

Para as encenações em que o interruptor não tem a mesma interface virtual do interruptor (SVI) que o cliente VLAN, refira os últimos três exemplos.

Troubleshooting

Cenário de teste

Os testes são executados no cliente, que deve ser reorientado ao ISE para o abastecimento (CPP). O usuário é autenticado através do desvio da autenticação de MAC (MAB) ou do 802.1x. O ISE retorna o perfil da autorização com o nome do Access Control List da reorientação (ACL) (REDIRECT_POSTURE) e reorienta a URL (reorienta ao 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
```

O ACL baixável (DACL) permite todo o tráfego nesta fase:

```
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
```

A reorientação ACL permite este tráfego sem reorientação:

- Todo o tráfego ao ISE (10.48.66.74)
- Tráfego do Domain Name System (DNS) e do Internet Control Message Protocol (ICMP)

Todo tráfego restante deve 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
```

O interruptor tem um SVI no mesmo VLAN que o usuário:

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

Nas próximas seções, isto é alterado a fim apresentar o impacto potencial.

O tráfego não alcança a reorientação ACL

Quando você tenta sibilar todo o host, você deve receber uma resposta porque esse tráfego não é reorientado. A fim confirmar, execute isto debugam:

```
debug epm redirect
```

Para cada pacote ICMP enviado pelo cliente, debuga deve apresentar:

```
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]
```

A fim confirmar, examine o 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
```

O tráfego alcança a reorientação ACL

Encenação 1 - O host de destino está no mesmo VLAN, existe, e é SVI 10 ACIMA

Quando você inicia o tráfego ao endereço IP de Um ou Mais Servidores Cisco ICM NT que é diretamente a camada 3 (L3) alcançável pelo interruptor (a rede para o interruptor tem uma relação SVI), é aqui o que acontece:

1. O cliente inicia um pedido da definição do Address Resolution Protocol (ARP) para o host de destino (192.168.1.20) no mesmo VLAN e recebe uma resposta (o tráfego ARP é reorientado nunca).

2. As intercepções do interruptor que sessão, mesmo quando o endereço IP de destino não é configurado nesse interruptor. O aperto de mão TCP entre o cliente e o interruptor é terminado. Nesta fase, nenhum outro pacote é enviado fora do interruptor. Nesta encenação, o cliente (192.168.1.201) iniciou uma sessão de TCP com o outro host que existem nesse VLAN (192.168.1.20) e para qual o interruptor tem uma relação SVI ACIMA (com o endereço IP de Um ou Mais Servidores Cisco ICM NT de 192.168.1.10):

3. Depois que a sessão de TCP é estabelecida e o pedido do HTTP está enviado, o interruptor retorna a resposta HTTP com a reorientação a ISE (encabeçamento do lugar).

   Estas etapas são confirmadas por debugam. Há diversas batidas 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
   ```

   Isto pode igualmente ser confirmado por mais detalhado debuga:

   ```
   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. O cliente conecta ao ISE diretamente (sessão do secure sockets layer (SSL) a 10.48.66.74:8443). Este pacote não provoca a reorientação:

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

Nota: A sessão é interceptada pelo interruptor, e assim esse tráfego pode ser capturado no interruptor com captura de pacote de informação encaixada (EPC). A captação precedente foi tomada com o EPC no interruptor.

Encenação 2 - O host de destino está no mesmo VLAN, não existe, e é SVI 10 ACIMA

Se o host de destino 192.168.1.20 está para baixo (não responde), o cliente não recebe uma resposta ARP (o interruptor não intercepta o ARP), e o cliente não envia um TCP SYN. A reorientação nunca ocorre.

Eis porque o agente NAC usa um gateway padrão para uma descoberta. Um gateway padrão deve sempre responder e o disparador reorienta.

Encenação 3 - O host de destino está no VLAN diferente, existe, e é SVI 10 ACIMA

Éaqui o que acontece nesta encenação:

1. As tentativas do cliente para alcançar HTTP://8.8.8.8.

2. Essa rede não está em nenhum SVI no interruptor.
3. O cliente envia um TCP SYN para essa sessão ao gateway padrão 192.168.1.10 (endereço MAC de destino conhecido).

4. A reorientação é provocada exatamente da mesma forma como no primeiro exemplo.

5. As intercepções do interruptor que sessão e retornam uma resposta HTTP que reoriente ao server ISE.

6. Os acessos do cliente o server ISE sem problemas (esse tráfego não é reorientado).

Nota: Não importa se o gateway padrão está no mesmo interruptor ou em um dispositivo ascendente. É somente necessário receber uma reação ARP desse gateway a fim provocar o processo da reorientação. Adicionalmente, é necessário que a acessibilidade ISE através do gateway padrão está permitida. Pague a atenção especial se um Firewall está na correção de programa, especialmente se é um Firewall da camada 2 (L2) e uns links diferentes transversais dos pacotes L2 (então um desvio do estado TCP pôde ser necessário no Firewall).

Encenação 4 - O host de destino está no VLAN diferente, não existe, e é SVI 10 ACIMA

Esta encenação é exatamente a mesma que a encenação 3. Não importa se o host de destino em um VLAN remoto existe ou não.

Encenação 5 - O host de destino está no VLAN diferente, existe, e é SVI 10 PARA BAIXO

Se o interruptor não tem o SVI ACIMA no mesmo VLAN que o cliente, pode ainda executar a reorientação mas somente quando as circunstâncias específicas são combinadas.

O problema para o interruptor é como retornar a resposta ao cliente de um SVI diferente. É difícil determinar que endereço MAC de origem deve ser usado.

O fluxo é diferente de quando o SVI está ACIMA:

1. O cliente envia um TCP SYN ao host em um VLAN diferente (192.168.2.20) com um endereço MAC de destino ajustado a um gateway padrão que seja definido no interruptor ascendente. Esse pacote alcança a reorientação ACL, por que é mostrado debuga.
2. O interruptor verifica se tem um roteamento de volta ao cliente. Recorde que o SVI 10 está PARA BAIXO.
3. Se o interruptor não tem um outro SVI que tenha um roteamento de volta ao cliente, esse pacote não está interceptado nem está reorientado, mesmo quando os logs do gerente da política da empresa (EPM) indicam que o ACL está alcançado. O host remoto pôde retornar um SYN ACK, mas o interruptor não tem um roteamento de volta ao cliente (VLAN10) e deixa cair o pacote. O pacote não pode apenas ser comutado para trás (L2), porque alcançou a reorientação ACL.
4. Se o interruptor tem um roteamento ao cliente VLAN através de um SVI diferente, intercepta esse pacote e executa a reorientação como de costume. A resposta com URL-reorienta não vai diretamente ao cliente, mas através de um interruptor/roteador diferentes baseados na decisão de roteamento.

Observe a assimetria aqui:

- O tráfego recebido do cliente é interceptado localmente pelo interruptor.
- A resposta para aquela, que inclui o HTTP reorienta, é enviada através do interruptor ascendente baseado no roteamento.
- Isto é quando os problemas típicos com o Firewall puderam ocorrer, e um desvio TCP é exigido.
- Trafique ao ISE, que não é reorientado, é simétrico. Somente a reorientação própria é assimétrica.

Encenação 6 - O host de destino está no VLAN diferente, não existe, e é SVI 10 PARA BAIXO

Esta encenação é exatamente a mesma que a encenação 5. Não importa que o host remoto exista. O roteamento correto é o que é importante.

Encenação 7 - O serviço HTTP está para baixo

Como apresentado na encenação 6, o processo HTTP no interruptor joga um papel importante. Se o serviço HTTP é desabilitado, o EPM mostra que o pacote alcança a reorientação ACL:

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

Contudo, a reorientação nunca ocorre.

O serviço HTTPS no interruptor não é exigido para um HTTP reorienta, mas exige-se para o HTTPS reorienta. O agente NAC pode usar ambos para a descoberta ISE. Consequentemente, recomenda-se para permitir ambos.

Reoriente o ACL - Protocolos incorretos e porta, nenhuma reorientação

Observe que o interruptor pode somente interceptar o tráfego HTTP ou HTTPS que trabalha em portas padrão (TCP/80 e TCP/443). Se o HTTP/HTTPS trabalha em uma porta não padronizada, pode ser configurado com o comando **HTTP do mapa de porta IP**. Também, o interruptor deve mandar seu Server do HTTP escutar nessa porta (**porta do HTTP de IP**).

Informações Relacionadas

- Autenticação da Web central com um exemplo de configuração do interruptor e do Identity Services Engine
- Guia do Usuário do Cisco Identity Services Engine, liberação 1.2
- Suporte Técnico e Documentação - Cisco Systems