Redirection du trafic ISE sur le commutateur de gamme Catalyst 3750

Contenu

Introduction

Cet article décrit comment les travaux de redirection du trafic d'utilisateur et les conditions qui sont nécessaires afin de réorienter le paquet par le commutateur.

Conditions préalables

Exigences

Cisco recommande que vous ayez l'expérience avec la configuration du Logiciel Cisco Identity Services Engine (ISE) et la connaissance de base de ces thèmes :

- Déploiements ISE et écoulements centraux de l'authentification Web (CWA)
- Configuration CLI des commutateurs Cisco Catalyst

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Microsoft Windows 7
- Logiciel de commutateur de gamme de Cisco Catalyst 3750X, versions 15.0 et ultérieures
- Logiciel ISE, versions 1.1.4 et ultérieures

Informations générales

La redirection du trafic d'utilisateur sur le commutateur est un élément essentiel pour la plupart des déploiements avec l'ISE. Tous ces écoulements comportent l'utilisation de la redirection du trafic par le commutateur :

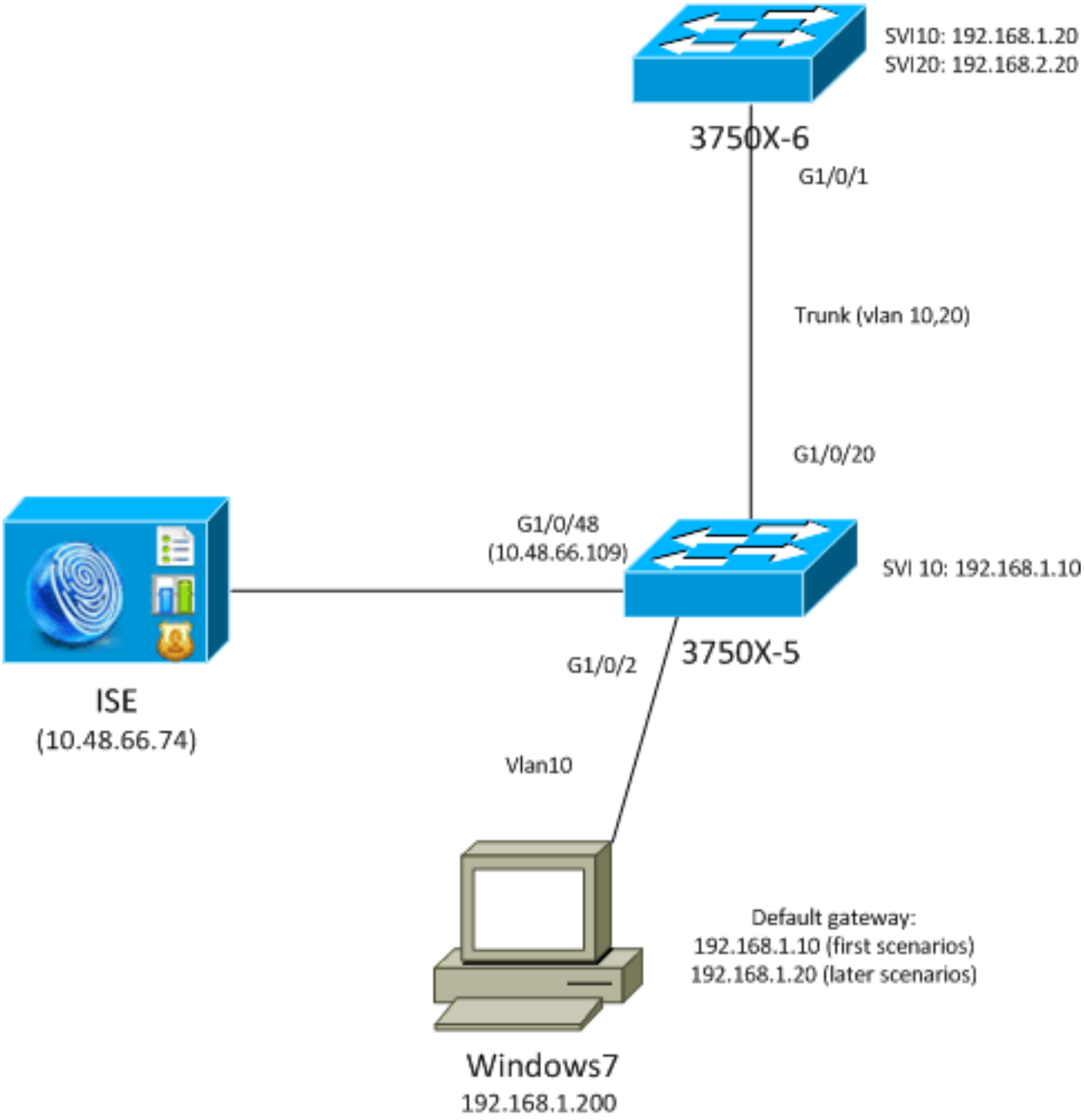
- CWA
- Ravitaillement de client (CPP)
- Enregistrement de périphérique (DRW)
- Ravitaillement indigène de suppliant (NSP)
- Gestion de périphérique mobile (MDM)

La redirection inexactement configurée est la cause de plusieurs problèmes avec le déploiement. Le résultat typique est un agent de Contrôle d'admission au réseau (NAC) qui ne s'affiche pas correctement ou une incapacité d'afficher le portail d'invité.

Pour les scénarios dans lesquels le commutateur n'a pas même Switch Virtual Interface (SVI) que le client VLAN, référez-vous aux trois derniers exemples.

Dépanner

Scénario de test



Des essais sont réalisés sur le client, qui devrait être réorienté à ISE pour le ravitaillement (CPP). L'utilisateur est authentifié par l'intermédiaire de la dérivation d'authentification MAC (MAB) ou du 802.1x. ISE renvoie le profil d'autorisation avec le nom de liste de contrôle d'accès de réorientation (ACL) (REDIRECT_POSTURE) et réoriente URL (redirect to 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
```

L'ACL téléchargeable (DACL) permet tout le trafic à ce stade :

```
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
```

L'ACL de réorientation permet ce trafic sans redirection :

- Tous trafiquent à l'ISE (10.48.66.74)
- Le trafic de Système de noms de domaine (DNS) et de Protocole ICMP (Internet Control Message Protocol)

Tout autre trafic devrait être réorienté :

```
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
```

Le commutateur a un SVI dans le même VLAN que l'utilisateur :

```
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
```

Dans les sections suivantes, ceci est modifié afin de présenter l'impact potentiel.

Le trafic n'atteint pas l'ACL de réorientation

Quand vous essayez de cingler n'importe quel hôte, vous devriez recevoir une réponse parce que ce trafic n'est pas réorienté. Afin de confirmer, exécutez ceci mettent au point :

```
debug epm redirect
```

Pour chaque paquet d'ICMP envoyé par le client, met au point devrait présenter :

```
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]
```

Afin de confirmer, examinez l'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
```

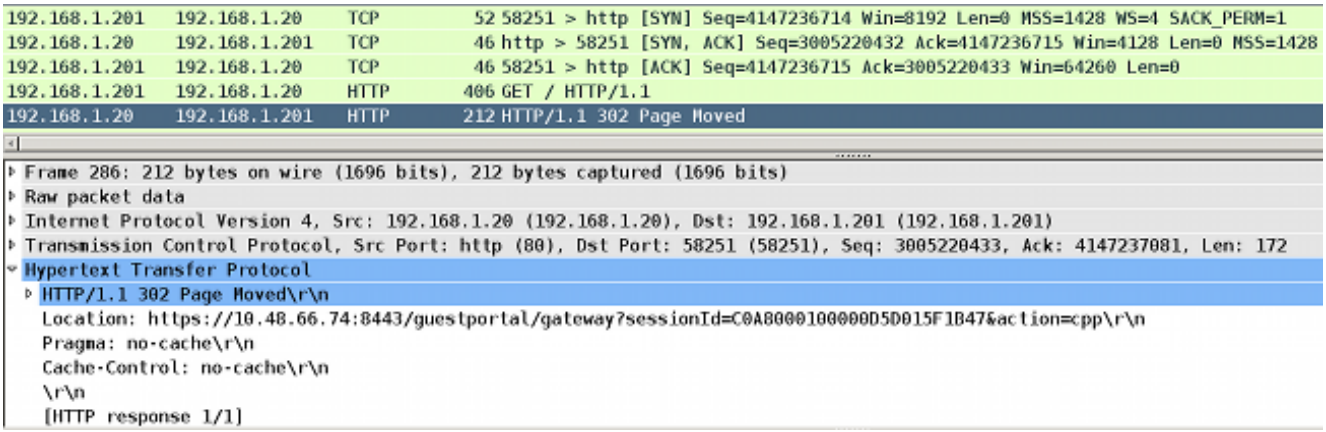
Le trafic atteint l'ACL de réorientation

Scénario 1 - La destination host est dans le même VLAN, existe, et est SVI 10 EN HAUSSE

Quand vous initiez le trafic à l'adresse IP qui est directement la couche 3 (L3) accessible par le commutateur (le réseau pour le commutateur a une interface SVI), voici ce qui se produit :

1. Le client initie une demande de résolution de Protocole ARP (Address Resolution Protocol) de la destination host (192.168.1.20) dans le même VLAN et reçoit une réponse (le trafic ARP n'est jamais réorienté).

2. Les interceptions de commutateur qui session, même lorsque l'adresse IP de destination n'est pas configurée sur ce commutateur. L'établissement de liaison de TCP entre le client et le commutateur est de finition. À ce stade, aucun autre paquet n'est envoyé en dehors de du commutateur. Dans ce scénario, le client (192.168.1.201) a initié une session TCP avec l'autre hôte qui existe dans ce VLAN (192.168.1.20) et pour ce qui le commutateur a une interface SVI (avec l'adresse IP de 192.168.1.10) :



3. Après que la session TCP soit établie et la demande de HTTP est envoyée, le commutateur renvoie la réponse de HTTP avec la redirection à ISE (en-tête d'emplacement).

   Ces étapes sont confirmées par met au point. Il y a plusieurs hit d'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
```

Ceci peut également être confirmé par plus détaillé met au point :

```
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. Le client se connecte à l'ISE directement session (de Secure Sockets Layer (SSL) à 10.48.66.74:8443). Ce paquet ne déclenche pas la redirection :

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

Note: La session est interceptée par le commutateur, et ce trafic peut être capturé ainsi sur le commutateur avec la capture incluse de paquet (CPE). La capture précédente a été prise avec la CPE sur le commutateur.

Scénario 2 - La destination host est dans le même VLAN, n'existe pas, et est SVI 10 EN HAUSSE

Si la destination host 192.168.1.20 est en baisse (ne répond pas), le client ne reçoit pas de réponse d'ARP (le commutateur n'intercepte pas l'ARP), et le client n'envoie pas une synchronisation de TCP. La redirection ne se produit jamais.

C'est pourquoi l'agent NAC utilise une passerelle par défaut pour une détection. Une passerelle par défaut devrait toujours répondre et le déclencheur réoriente.

Scénario 3 - La destination host est dans le VLAN différent, existe, et est SVI 10 EN HAUSSE

Voici ce qui se produit dans ce scénario :

1. Les essais de client pour accéder à HTTP://8.8.8.8.

2. Ce réseau n'est pas sur aucun SVI sur le commutateur.
3. Le client envoie une synchronisation de TCP pour cette session à la passerelle par défaut

192.168.1.10 (adresse MAC de destination connue).

4. La redirection est déclenchée de la même manière comme dans le premier exemple.

5. Les interceptions de commutateur qui session et renvoie une réponse de HTTP cette des redirect to le serveur ISE.

6. Les accès client le serveur ISE sans problèmes (ce trafic n'est pas réorienté).

Note: Il n'importe pas si la passerelle par défaut est sur le même commutateur ou sur un périphérique en amont. Il est seulement nécessaire de recevoir une réponse d'ARP de cette passerelle afin de déclencher le procédé de réorientation. Supplémentaire, il est nécessaire qu'on permette l'accessibilité ISE par l'intermédiaire de la passerelle par défaut. Prêtez la particulière attention si un Pare-feu est sur le correctif, particulièrement si c'est un Pare-feu de la couche 2 (L2) et liens transversaux des paquets L2 de différents (puis un contournement d'état de TCP pourrait être nécessaire sur le Pare-feu).

Scénario 4 - La destination host est dans le VLAN différent, n'existe pas, et est SVI 10 EN HAUSSE

Ce scénario est exactement identique que le scénario 3. Il n'importe pas si la destination host dans un distant VLAN existe ou pas.

Scénario 5 - La destination host est dans le VLAN différent, existe, et est SVI 10 EN BAISSE

Si le commutateur n'a pas le SVI dans le même VLAN que le client, il peut encore exécuter la redirection mais seulement quand des conditions spécifiques sont appariées.

Le problème pour le commutateur est comment renvoyer la réponse au client d'un SVI différent. Il est difficile de déterminer quelle adresse MAC source devrait être utilisée.

L'écoulement est différent de quand le SVI est :

1. Le client envoie une synchronisation de TCP à l'hôte dans un VLAN différent (192.168.2.20) avec une adresse MAC de destination réglée à une passerelle par défaut qui est définie sur le commutateur en amont. Ce paquet atteint l'ACL de réorientation, par lequel est affiché met au point.
2. Le commutateur vérifie s'il a un routage de nouveau au client. Souvenez-vous que SVI 10 est VERS LE BAS.
3. Si le commutateur n'a pas un autre SVI qui a un routage de nouveau au client, ce paquet n'est pas intercepté ou est réorienté, même lorsque les logs du Policy Manager d'entreprise (EPM) indiquent que l'ACL est atteint. Le serveur distant pourrait renvoyer une synchronisation ACK, mais le commutateur n'a pas un routage de nouveau au client (VLAN10) et relâche le paquet. Le paquet ne peut pas simplement être commuté de retour (L2), parce qu'il a atteint l'ACL de réorientation.
4. Si le commutateur a un routage au client VLAN par l'intermédiaire d'un SVI différent, il intercepte ce paquet et exécute la réorientation comme d'habitude. La réponse avec URL-

réorientent ne va pas directement au client, mais par l'intermédiaire d'un commutateur/de routeur différents basés sur la décision de routage.

Notez l'asymétrie ici :

- Le trafic reçu du client est intercepté localement par le commutateur.
- La réponse pour cela, qui inclut le HTTP réorientent, est envoyée par l'intermédiaire du commutateur en amont basé sur le routage.
- C'est quand les problèmes typiques avec le Pare-feu pourraient se poser, et un contournement de TCP est exigé.
- Trafiquez à l'ISE, qui n'est pas réorienté, est symétrique. Seulement la redirection elle-même est asymétrique.

Scénario 6 - La destination host est dans le VLAN différent, n'existe pas, et est SVI 10 EN BAISSE

Ce scénario est exactement identique que le scénario 5. Il n'importe pas que le serveur distant existe. Le routage correct est ce qui est important.

Scénario 7 - Le service HTTP est en baisse

Comme présenté dans le scénario 6, le processus de HTTP sur le commutateur joue un important rôle. Si le service HTTP est désactivé, EPM prouve que le paquet atteint l'ACL de réorientation :

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

Cependant, la redirection ne se produit jamais.

Le service HTTPS sur le commutateur n'est pas exigé pour un HTTP réorientent, mais on l'exige pour HTTPS réorientent. L'agent NAC peut utiliser chacun des deux pour la détection ISE. Par conséquent, on lui informe pour activer chacun des deux.

Réorientez l'ACL - Protocoles incorrects et port, aucune redirection

Notez que le commutateur peut seulement intercepter le trafic de HTTP ou HTTPS qui travaille aux ports standard (TCP/80 et TCP/443). Si HTTP/HTTPS travaille à un port non standard, il peut être configuré avec la commande de **HTTP d'ip port-map**. En outre, le commutateur doit faire écouter son serveur HTTP sur ce port (**ip http port**).

Informations connexes

- Authentification Web centrale avec un exemple de configuration de commutateur et de Cisco Identity Services Engine
- Guide de l'utilisateur de la plateforme de services d'identité de Cisco, version 1.2

- Support et documentation techniques - Cisco Systems