ISE Traffic Redirection sugli switch Catalyst serie 3750

Sommario

Introduzione

In questo documento viene descritto il funzionamento del reindirizzamento del traffico degli utenti e le condizioni necessarie per reindirizzare il pacchetto dallo switch.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza della configurazione di Cisco Identity Services Engine (ISE) e delle conoscenze base sugli argomenti seguenti:

- Implementazioni ISE e flussi CWA (Central Web Authentication)
- Configurazione CLI degli switch Cisco Catalyst

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Microsoft Windows 7
- Software Cisco Catalyst serie 3750X Switch, versioni 15.0 e successive
- Software ISE, versioni 1.1.4 e successive

Premesse

Il reindirizzamento del traffico utente sullo switch è un componente critico per la maggior parte delle implementazioni con ISE. Tutti questi flussi implicano l'uso del reindirizzamento del traffico da parte dello switch:

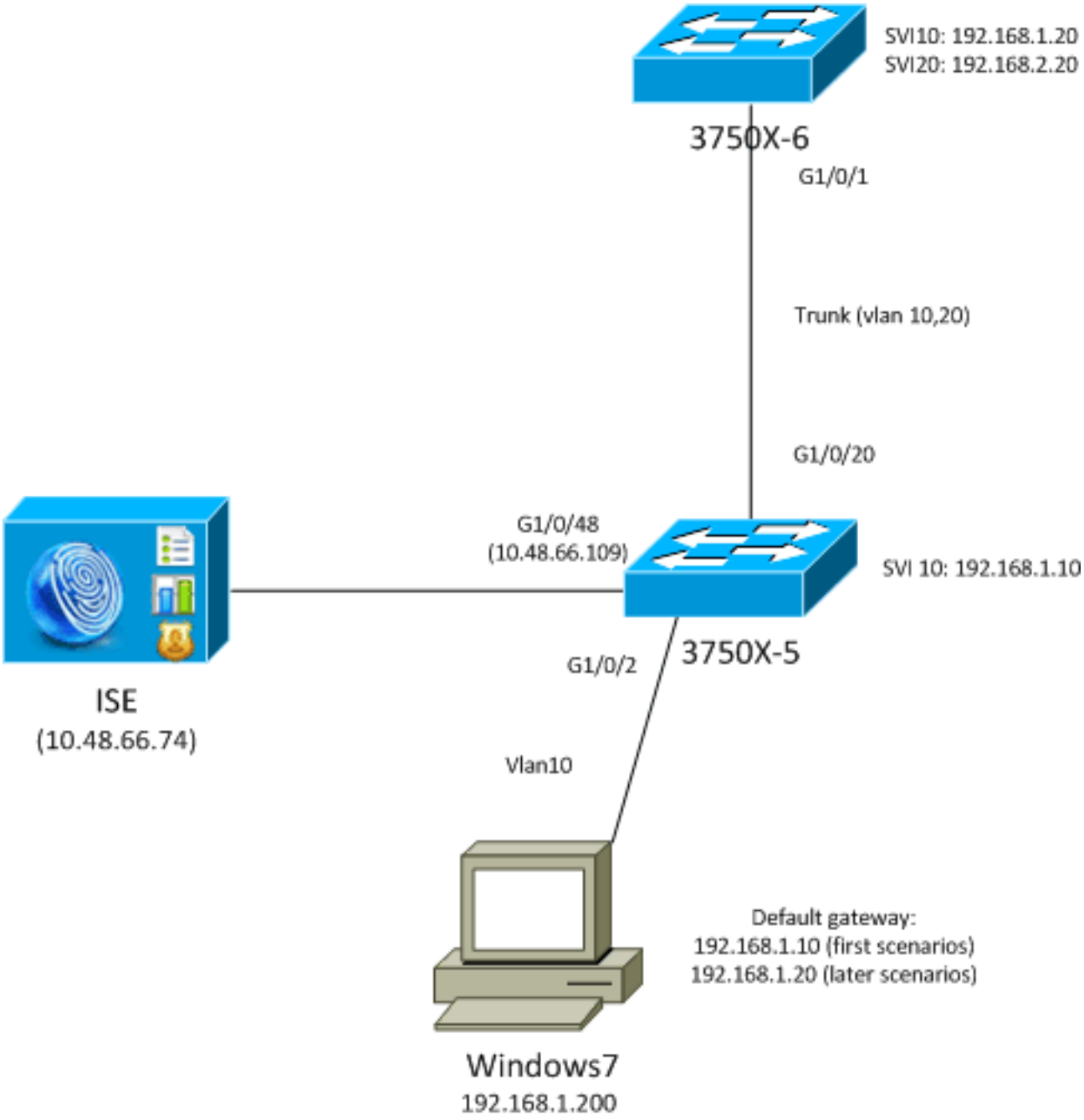
- CWA
- CPP (Client Provisioning)
- DRW (Device Registration)
- NSP (Native Supplicant Provisioning)
- MDM (Mobile Device Management)

Il reindirizzamento non configurato correttamente è la causa di più problemi nella distribuzione. Il risultato tipico è un agente NAC (Network Admission Control) che non viene visualizzato correttamente o che non è in grado di visualizzare il portale guest.

Per gli scenari in cui lo switch non ha la stessa interfaccia virtuale dello switch (SVI) della VLAN client, fare riferimento agli ultimi tre esempi.

Risoluzione dei problemi

Scenario di test



I test vengono eseguiti sul client, che deve essere reindirizzato ad ISE for provisioning (CPP). L'utente viene autenticato tramite MAC Authentication Bypass (MAB) o 802.1x. ISE restituisce il profilo di autorizzazione con il nome ACL (Access Control List) di reindirizzamento (REDIRECT_POSTURE) e l'URL di reindirizzamento (reindirizzamento 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
```

L'ACL scaricabile (DACL) consente tutto il traffico in questa 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
```

L'ACL di reindirizzamento consente il traffico seguente senza reindirizzamento:

- Tutto il traffico diretto all'ISE (10.48.66.74)
- Traffico DNS (Domain Name System) e ICMP (Internet Control Message Protocol)

Tutto il resto del traffico deve essere reindirizzato:

```
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
```

Lo switch ha una SVI nella stessa VLAN dell'utente:

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

Nelle sezioni seguenti, questa opzione viene modificata per presentare l'impatto potenziale.

Il traffico non raggiunge l'ACL di reindirizzamento

Quando si tenta di eseguire il ping su un host, è consigliabile ricevere una risposta in quanto il traffico non viene reindirizzato. Per confermare, eseguire il debug:

```
debug epm redirect
```

Per ciascun pacchetto ICMP inviato dal client, i debug devono presentare:

```
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]
```

Per conferma, esaminare 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
```

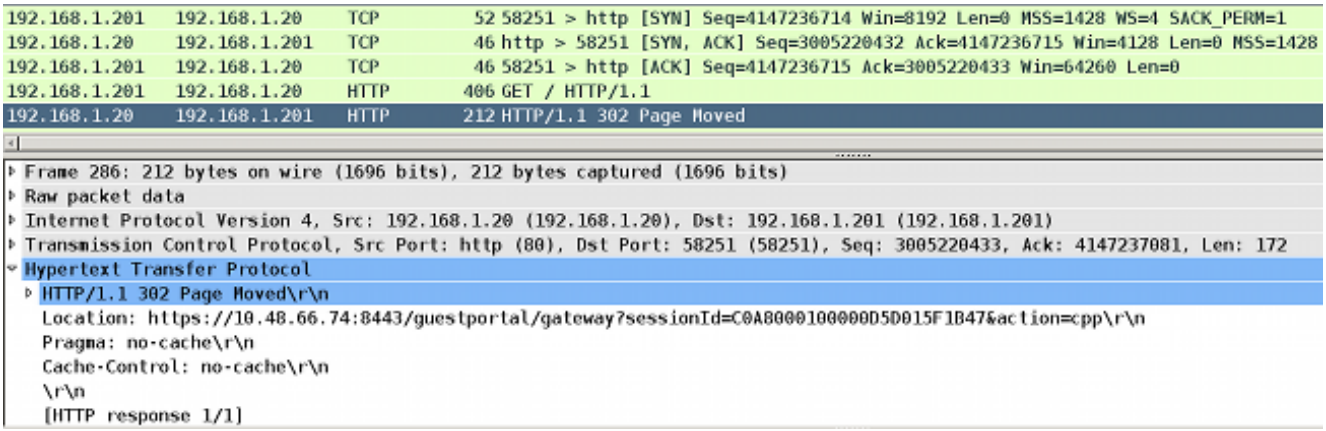
Il traffico raggiunge l'ACL di reindirizzamento

Scenario 1 - L'host di destinazione è sulla stessa VLAN, esiste ed è SVI 10 UP

Quando si avvia il traffico verso l'indirizzo IP direttamente sul layer 3 (L3) raggiungibile dallo switch (la rete dello switch è dotata di interfaccia SVI), si verifica quanto segue:

1. Il client avvia una richiesta di risoluzione Address Resolution Protocol (ARP) per l'host di destinazione (192.168.1.20) nella stessa VLAN e riceve una risposta (il traffico ARP non viene mai reindirizzato).

2. Lo switch intercetta tale sessione, anche quando l'indirizzo IP di destinazione non è configurato su tale switch. Handshake TCP tra il client e lo switch terminato. In questa fase, non è possibile inviare altri pacchetti all'esterno dello switch. In questo scenario, il client (192.168.1.201) ha avviato una sessione TCP con l'altro host presente nella VLAN (192.168.1.20) e per cui lo switch ha un'interfaccia SVI attiva (con indirizzo IP 192.168.1.10):



3. Dopo aver stabilito la sessione TCP e aver inviato la richiesta HTTP, lo switch restituisce la risposta HTTP con il reindirizzamento a ISE (Location header).

   Queste operazioni sono confermate dai debug. Sono disponibili diversi riscontri 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
```

Questa condizione può essere confermata anche da debug più dettagliati:

```
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. Il client si connette direttamente all'ISE (sessione SSL (Secure Sockets Layer) a 10.48.66.74:8443). Questo pacchetto non attiva il reindirizzamento:

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

Nota: La sessione viene intercettata dallo switch e quindi il traffico può essere acquisito sullo switch con l'EPC (Embedded Packet Capture). La precedente acquisizione è stata effettuata con EPC sullo switch.

Scenario 2 - L'host di destinazione si trova nella stessa VLAN, non esiste e si trova nella SVI 10 UP

Se l'host di destinazione 192.168.1.20 non è attivo (non risponde), il client non riceve una risposta ARP (lo switch non intercetta ARP) e non invia un messaggio TCP SYN. Il reindirizzamento non viene mai eseguito.

Ecco perché l'agente NAC utilizza un gateway predefinito per un rilevamento. Un gateway predefinito deve sempre rispondere e attivare reindirizzamenti.

Scenario 3 - L'host di destinazione si trova in una VLAN diversa, esiste ed è SVI 10 UP

Di seguito è riportato ciò che accade in questo scenario:

1. Il client tenta di accedere a HTTP://8.8.8.8.

2. La rete non è su alcuna SVI dello switch.
3. Il client invia un TCP SYN per quella sessione al gateway predefinito 192.168.1.10 (indirizzo MAC di destinazione noto).

4. Il reindirizzamento viene attivato esattamente come nel primo esempio.

5. Lo switch intercetta tale sessione e restituisce una risposta HTTP che reindirizza al server

ISE.

6. Il client accede al server ISE senza problemi (il traffico non viene reindirizzato).

   Nota: Non importa se il gateway predefinito si trova sullo stesso switch o su un dispositivo upstream. È necessario solo ricevere una risposta ARP da tale gateway per avviare il processo di reindirizzamento. Inoltre, è necessario che sia consentita l'accessibilità ISE tramite il gateway predefinito. Prestare particolare attenzione se sulla patch è presente un firewall, soprattutto se si tratta di un firewall di layer 2 (L2) e i pacchetti L2 attraversano collegamenti diversi (potrebbe essere necessario un bypass dello stato TCP sul firewall).

Scenario 4 - L'host di destinazione si trova su una VLAN diversa, non esiste e corrisponde a SVI 10 UP

Questo scenario è esattamente uguale allo scenario 3. Non importa se l'host di destinazione in una VLAN remota esiste o meno.

Scenario 5 - L'host di destinazione si trova in una VLAN diversa, esiste ed è SVI 10 DOWN

Se lo switch non dispone di SVI UP nella stessa VLAN del client, può comunque eseguire il reindirizzamento, ma solo quando vengono soddisfatte condizioni specifiche.

Il problema dello switch è come restituire la risposta al client da una SVI diversa. È difficile determinare quale indirizzo MAC di origine utilizzare.

Il flusso è diverso da quando SVI è attivo:

1. Il client invia un TCP SYN all'host in una VLAN diversa (192.168.2.20) con un indirizzo MAC di destinazione impostato su un gateway predefinito definito sullo switch a monte. Il pacchetto raggiunge l'ACL di reindirizzamento, mostrato dai debug.
2. Lo switch verifica se dispone di un routing di ritorno al client. Tenere presente che la SVI 10 non è attiva.
3. Se lo switch non dispone di un'altra SVI con routing al client, il pacchetto non viene intercettato o reindirizzato, anche quando i log di Enterprise Policy Manager (EPM) indicano che è stato raggiunto l'ACL. L'host remoto potrebbe restituire un SYN ACK, ma lo switch non ha un routing verso il client (VLAN10) e scarta il pacchetto. Il pacchetto non può essere semplicemente reindirizzato (L2), perché ha raggiunto l'ACL di reindirizzamento.
4. Se lo switch ha un routing alla VLAN client tramite una SVI diversa, intercetta il pacchetto ed esegue il reindirizzamento come di consueto. La risposta con reindirizzamento URL non viene inviata direttamente al client, ma tramite uno switch/router diverso in base alla decisione di routing.

Notate l'asimmetria qui:

- Il traffico ricevuto dal client viene intercettato localmente dallo switch.
- La risposta, che include il reindirizzamento HTTP, viene inviata tramite lo switch a monte in base al routing.

- In questo caso, potrebbero verificarsi problemi tipici con il firewall ed è necessario un bypass TCP.

- Il traffico diretto all'ISE, che non è reindirizzato, è simmetrico. Solo il reindirizzamento è asimmetrico.

Scenario 6 - L'host di destinazione si trova in una VLAN diversa, non esiste e la VLAN è SVI 10 DOWN

Questo scenario è esattamente uguale allo scenario 5. L'esistenza dell'host remoto è irrilevante. Ciò che è importante è che il routing sia corretto.

Scenario 7 - Servizio HTTP non attivo

Come illustrato nello scenario 6, il processo HTTP sullo switch svolge un ruolo importante. Se il servizio HTTP è disabilitato, EPM mostra che il pacchetto raggiunge l'ACL di reindirizzamento:

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

Tuttavia, il reindirizzamento non viene mai eseguito.

Il servizio HTTPS sullo switch non è necessario per un reindirizzamento HTTP, ma è necessario per il reindirizzamento HTTPS. L'agente NAC può utilizzare entrambi per il rilevamento ISE. Si consiglia pertanto di abilitare entrambi.

ACL di reindirizzamento - Protocolli e porte non corretti, nessun reindirizzamento

Lo switch può intercettare solo il traffico HTTP o HTTPS che funziona sulle porte standard (TCP/80 e TCP/443). Se il protocollo HTTP/HTTPS funziona su una porta non standard, è possibile configurarlo con il comando **ip port-map http**. Inoltre, lo switch deve avere il proprio server HTTP in ascolto su quella porta (**porta ip http**).

Informazioni correlate

- Esempio di autenticazione Web centrale con uno switch e configurazione di Identity Services Engine
- Guida dell'utente di Cisco Identity Services Engine, versione 1.2
- Documentazione e supporto tecnico – Cisco Systems