ISE Traffic Redirectie op Catalyst 3750 Series-switch

Inhoud

Inleiding

Dit artikel beschrijft hoe de omleiding van het gebruikersverkeer werkt en de voorwaarden die nodig zijn om het pakket met de schakelaar te kunnen omleiden.

Voorwaarden

Vereisten

Cisco raadt u aan ervaring te hebben met de configuratie van Cisco Identity Services Engine (ISE) en basiskennis van deze onderwerpen:

- ISE-implementaties en Central Web Verificatie (CWA)-stromen
- CLI-configuratie van Cisco Catalyst-switches

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Microsoft Windows 7
- Software voor Cisco Catalyst 3750X Series-switch, versies 15.0 en hoger
- ISE-software, versie 1.1.4 en hoger

Achtergrondinformatie

De omleiding van het gebruikersverkeer op de schakelaar is een kritieke component voor het grootste gedeelte van de implementaties met ISE. Al deze stromen omvatten het gebruik van omleiding door de switch:

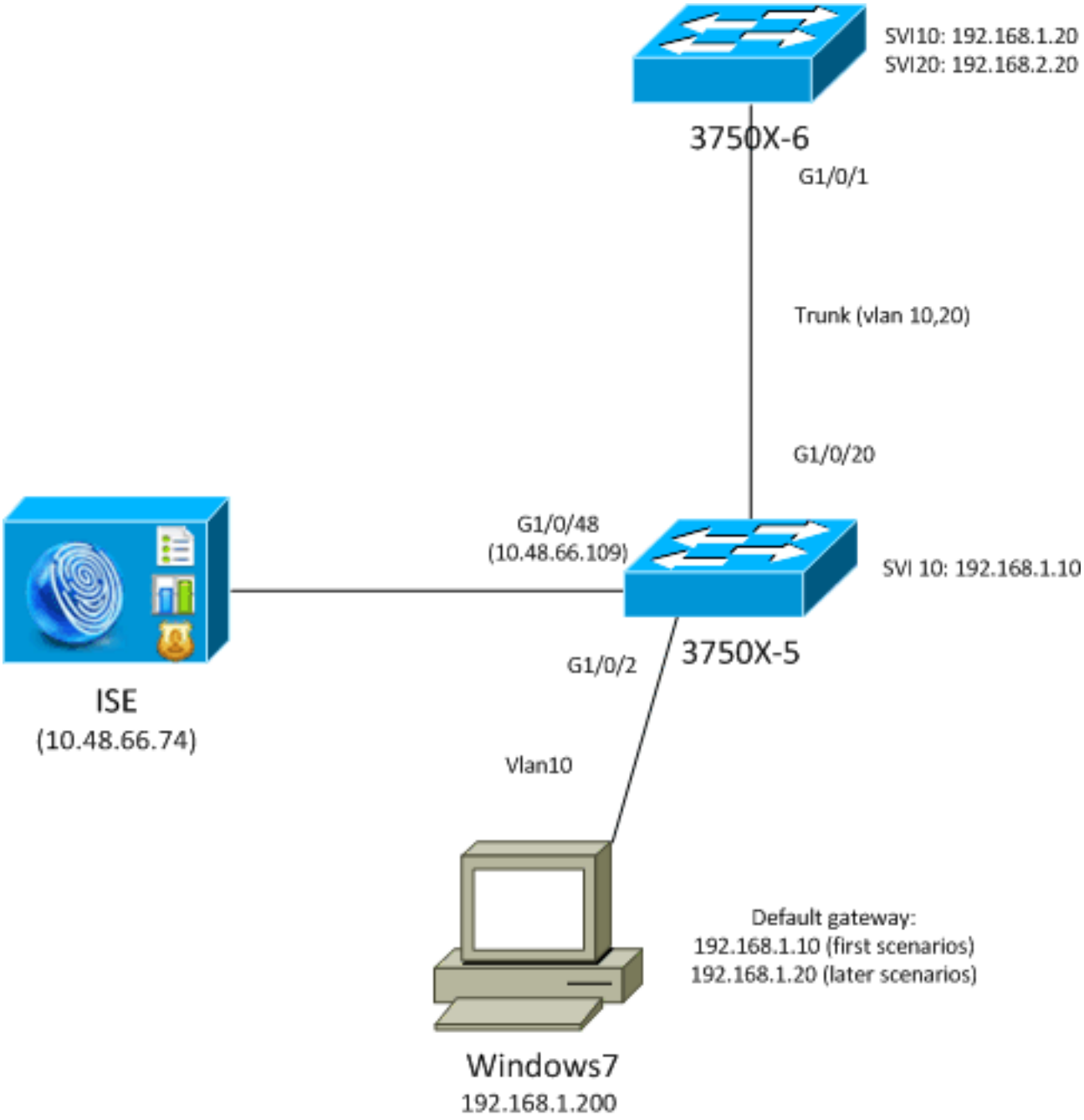
- CWA
- Clientprovisioning (CPP)
- Apparaatregistratie (DRW)
- Native Supply Provisioning (NSP)
- Mobiel apparaatbeheer (MDM)

Onjuist geconfigureerd omleiding is de oorzaak van meerdere problemen met de implementatie. Het typische resultaat is een Agent Network Admission Control (NAC) die niet correct verschijnt of een onvermogen om het Guest Portal weer te geven.

Voor scenario's waarin de switch niet dezelfde Switch Virtual Interface (SVI) heeft als de client-VLAN, raadpleeg de laatste drie voorbeelden.

Problemen oplossen

Testscenario



Er worden tests uitgevoerd op de client, die naar ISE moet worden omgeleid voor provisioning (CPP). De gebruiker is gecertificeerd via de MAC-verificatie-omzeilingstaak (MAB) of 802.1x. ISE geeft het autorisatieprofiel terug met de naam van de toegangscontrolelijst (ACL) (REDIRECT_POSTURE) en stuur URL (omleiding naar 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
```

DACL (Downloadbaar) maakt al verkeer in deze fase mogelijk:

```
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
```

Hiermee kan ACL-richting worden omgeleid:

- Alle verkeer naar de ISE (10.48.66.74)
- Domain Name System (DNS) en Internet Control Message Protocol (ICMP)-verkeer

Al het andere verkeer moet worden omgeleid:

```
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
```

De switch heeft een SVI in hetzelfde VLAN als de gebruiker:

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

In de volgende rubrieken wordt dit gewijzigd om het mogelijke effect te presenteren.

Verkeer bereikt geen bereik van ACL-richting

Wanneer u probeert een host te pingelen, dient u een reactie te ontvangen omdat dat verkeer niet opnieuw is gericht. Voer dit debug in om te bevestigen:

```
debug epm redirect
```

Voor elk ICMP-pakket dat door de client wordt verzonden, dienen de distributeurs:

```
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]
```

Controleer de ACL-code (Coördinator:

```
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
```

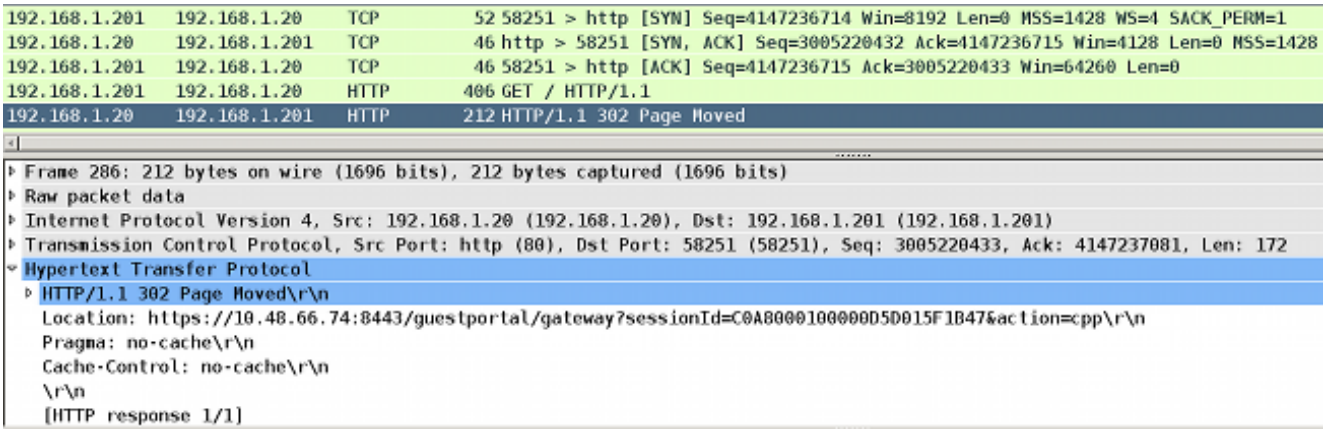
Verkeer bereikt omleiding ACL

Scenario 1 - De doelhost is in hetzelfde VLAN aanwezig, bestaat en is SVI 10 UP

Wanneer u het verkeer naar het IP-adres start dat direct Layer 3 (L3) bereikbaar is door de schakelaar (het netwerk voor de schakelaar heeft een SVI-interface), is dit wat er gebeurt:

1. De client initieert een adresresolutie Protocol (ARP) voor de doelhost (192.168.1.20) in hetzelfde VLAN en ontvangt een respons (ARP-verkeer wordt nooit hergericht).

2. De switch onderschept die sessie, zelfs wanneer het IP-adres van de bestemming niet op die switch is ingesteld. TCP handshaking tussen de client en de switch is voltooid. In dit stadium worden er geen andere pakketten buiten de schakelaar verzonden. In dit scenario heeft de client (192.168.1.201) een TCP-sessie gestart met de andere host die in dat VLAN bestaat (192.168.1.20) en waarvoor de switch een SVI-interface-UP heeft (met het IP-adres van 192.168.1.10):



3. Nadat de TCP sessie is ingesteld en het HTTP verzoek wordt verzonden, geeft de switch de HTTP respons terug met de omleiding naar ISE (Location header).

   Deze stappen worden bevestigd door insecten. Er zijn verschillende ACL-hits:

```
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
```

Dit kan ook worden bevestigd door meer gedetailleerde analyses:

```
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. De client sluit aan op de ISE direct (Secure Socket Layer (SSL) sessie aan 10.48.66.74:8443). Dit pakje geeft geen omleiding:

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

Opmerking: De sessie wordt onderschept door de schakelaar, en dus kan dat verkeer op de switch worden opgenomen met Ingesloten Packet Capture (EPC). De vorige opname werd genomen met EPC op de schakelaar.

Scenario 2 - De plaats van de bestemming is in hetzelfde VLAN, bestaat niet, en is SVI 10 UP

Als de doelhost 192.168.1.20 is neergedaald (reageert niet), ontvangt de client geen ARP-antwoord (de switch onderschept geen ARP) en de client stuurt geen TCP SYN. Er gebeurt nooit omleiding.

Dit is waarom de NAC Agent een standaardgateway gebruikt voor een ontdekking. Een standaardgateway zou altijd moeten reageren en redirecties veroorzaken.

Scenario 3 - De doelhost is in verschillende VLAN's aanwezig, bestaat en is SVI 10 UP

Dit is wat er bij dit scenario gebeurt:

1. De client probeert toegang te krijgen tot HTTP://8.8.8.8.

2. Dat netwerk staat niet op een SVI aan de schakelaar.
3. De client stuurt een TCP SYN voor die sessie naar de standaard gateway 192.168.1.10 (bestemmings-MAC-adres bekend).

4. De omleiding wordt op precies dezelfde manier geactiveerd als in het eerste voorbeeld.

5. De switch onderscheppt die sessie en retourneert een HTTP respons die wordt teruggeleid naar de ISE server.

6. De client heeft zonder problemen toegang tot de ISE-server (dat verkeer niet opnieuw is gericht).

   Opmerking: Het maakt niet uit of de standaardgateway op dezelfde schakelaar of op een stroomopwaarts apparaat is. Het is alleen nodig om een ARP-respons van die gateway te ontvangen om het omleidingsproces te starten. Daarnaast is het nodig dat ISE-toegankelijkheid via de standaardgateway wordt toegestaan. Let goed op als er een firewall op het stopcontact staat, vooral als het een Layer 2 (L2) firewall is en L2-pakketten verschillende links oversteken (dan kan een TCP-statustbypass nodig zijn op de firewall).

Scenario 4 - De plaats van de bestemming is in verschillend VLAN, bestaat niet, en is SVI 10 UP

Dit scenario is precies het zelfde als Scenario 3. Het maakt niet uit of de bestemmingsgastheer in een ver VLAN al dan niet bestaat.

Scenario 5 - De plaats van de bestemming is in verschillend VLAN, bestaat, en is SVI 10 DOWN

Als de switch geen SVI UP in hetzelfde VLAN heeft als de client, kan deze nog steeds omleiding uitvoeren, maar alleen wanneer de specifieke omstandigheden worden aangepast.

Het probleem voor de switch is hoe je de reactie op de client van een andere SVI teruggeeft. Het is moeilijk te bepalen welk bron-MAC-adres moet worden gebruikt.

De stroom is anders dan wanneer SVI omhoog is:

1. De client stuurt een TCP SYN naar de host in een ander VLAN (192.168.2.20) met een bestemmings-MAC-adres dat op een standaardgateway is ingesteld die op de upstream-switch is gedefinieerd. Dat pakje bereikt de om te zetten ACL, dat door middel van debugs wordt weergegeven.
2. De switch verifieert of het een routing terug naar de client heeft. Onthoud dat SVI 10 is neergehaald.
3. Als de switch geen andere SVI heeft die een routing terug naar de client heeft, wordt dat pakket niet onderschept of opnieuw gericht, zelfs wanneer de logboeken van Enterprise Policy Manager (EPM) aangeven dat ACL wordt bereikt. De afstandsbediening kan een SYN ACK teruggeven, maar de switch heeft geen routing naar de client (VLAN10) en brengt het pakket weg. Het pakket kan niet zomaar worden teruggezet (L2), omdat het ACL-richting heeft bereikt.
4. Als de switch wel een routing naar de client-VLAN via een andere SVI heeft, onderschept hij die pakketjes en voert hij zoals gewoonlijk de herleiding uit. De reactie met URL-redirect gaat niet rechtstreeks naar de client, maar via een andere switch/router gebaseerd op het routingbesluit.

Let hier op de asymmetrie:

- Het verkeer dat van de client wordt ontvangen, wordt lokaal door de switch onderschept.
- De reactie daarvoor, die HTTP redirect omvat, wordt verzonden via de upstream switch

gebaseerd op de routing.

- Dit is wanneer er typische problemen met de firewall kunnen voorkomen, en er is een TCP-bypass vereist.
- Verkeer naar ISE, dat niet wordt omgeleid, is symmetrisch. Alleen de omleiding zelf is asymmetrisch.

Scenario 6 - De plaats van de bestemming is in verschillend VLAN, bestaat niet, en is SVI 10 DOWN

Dit scenario is precies het zelfde als Scenario 5. Het maakt niet uit dat de afstandsbediening bestaat. De juiste routing is belangrijk.

Scenario 7 - HTTP-service is afgebroken

Zoals wordt getoond in scenario 6, speelt het HTTP-proces op de switch een belangrijke rol. Als de HTTP-service is uitgeschakeld, toont EPM aan dat het pakket de doorlopende ACL bereikt:

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

Maar die omleiding gebeurt nooit.

De HTTPS-service op de schakelaar is niet vereist voor een HTTP-omleiding, maar is vereist voor HTTPS-omleiding. De NAC Agent kan beide gebruiken voor ISE-ontdekking. Daarom wordt aanbevolen beide in te schakelen.

ACL omleiden - onjuist protocollen en poort zonder omleiding

Merk op dat de switch alleen HTTP- of HTTPS-verkeer kan onderscheppen dat op standaardpoorten (TCP/80 en TCP/443) werkt. Als HTTP/HTTPS op een niet standaardpoort werkt, kan het worden geconfigureerd met de **ip port-map http** opdracht. Ook, moet de schakelaar zijn HTTP server hebben om op die haven te luisteren (**ip http poort**).

Gerelateerde informatie

- Central-webverificatie met een Configuratievoorbeeld van Switch- en Identity Services Engine
- Gebruikershandleiding voor Cisco Identity Services Engine, release 1.2
- Technische ondersteuning en documentatie – Cisco Systems