ISE Traffic Redirection on the Catalyst 3750 Series Switch

Document ID: 117278

Contributed by Michal Garcarz, Cisco TAC Engineer.
Jan 30, 2014

Contents

Introduction

This article describes how user traffic redirection works and the conditions that are necessary in order to redirect the packet by the switch.

Prerequisites

Requirements

Cisco recommends that you have experience with the Cisco Identity Services Engine (ISE) configuration and basic knowledge of these topics:

- ISE deployments and Central Web Authentication (CWA) flows
- CLI configuration of Cisco Catalyst switches

Components Used

The information in this document is based on these software and hardware versions:

- Microsoft Windows 7
- Cisco Catalyst 3750X Series Switch Software, Versions 15.0 and Later

- ISE Software, Versions 1.1.4 and Later

Background Information

User traffic redirection on the switch is a critical component for most of the deployments with the ISE. All of these flows involve usage of traffic redirection by the switch:

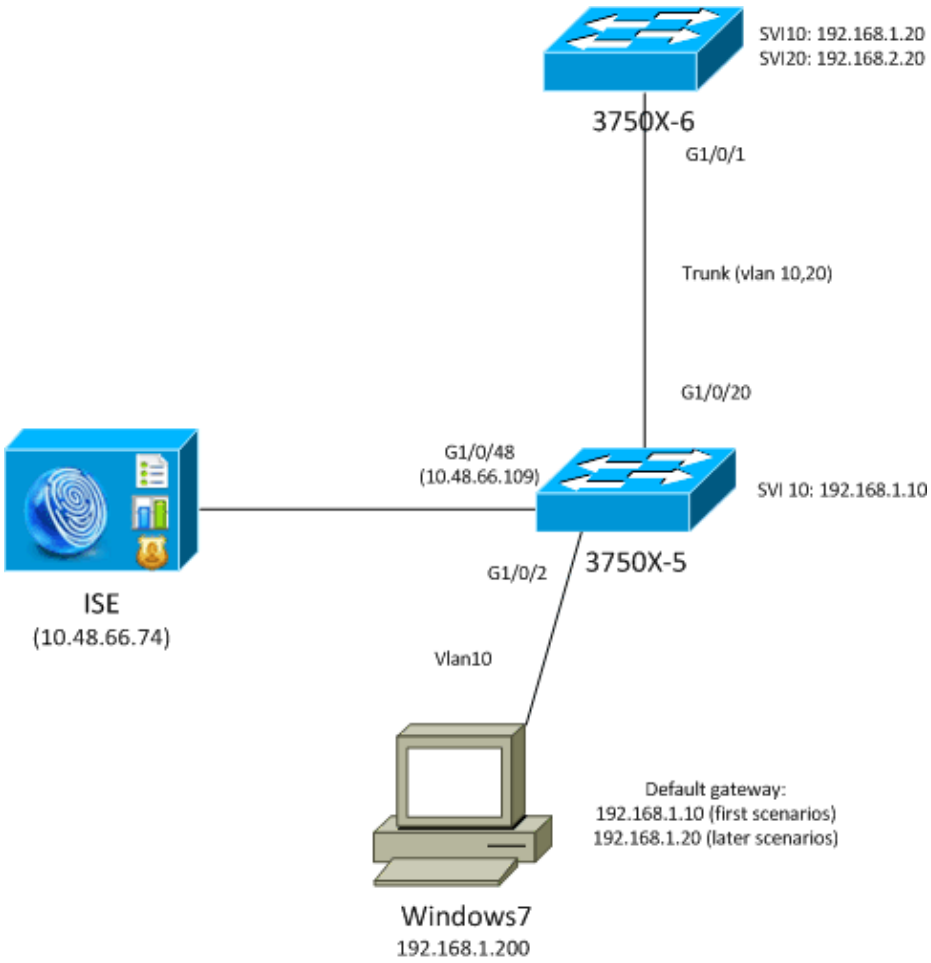
- CWA
- Client Provisioning (CPP)
- Device Registration (DRW)
- Native Supplicant Provisioning (NSP)
- Mobile Device Management (MDM)

Incorrectly configured redirection is the cause of multiple problems with the deployment. The typical result is a Network Admission Control (NAC) Agent that does not pop up correctly or an inability to display the Guest Portal.

For scenarios in which the switch does not have the same Switch Virtual Interface (SVI) as the client VLAN, refer to the last three examples.

Troubleshoot

Test Scenario



Tests are performed on the client, which should be redirected to ISE for provisioning (CPP). The user is authenticated via MAC Authentication Bypass (MAB) or 802.1x. ISE returns the authorization profile with the redirect Access Control List (ACL) name (REDIRECT_POSTURE) and redirect URL (redirects 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
```

The Downloadable ACL (DACL) permits all traffic at this stage:

```
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
```

The redirect ACL allows this traffic without redirection:

- All traffic to the ISE (10.48.66.74)
- Domain Name System (DNS) and Internet Control Message Protocol (ICMP) traffic

All other traffic should be redirected:

```
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
```

The switch has a SVI in the same VLAN as the user:

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

In the next sections, this is modified in order to present the potential impact.

Traffic Does Not Reach the Redirect ACL

When you try to ping any host, you should receive a response because that traffic is not redirected. In order to confirm, run this debug:

debug epm redirect

For each ICMP packet sent by the client, the debugs should present:

```
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]
```

In order to confirm, examine the 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
```

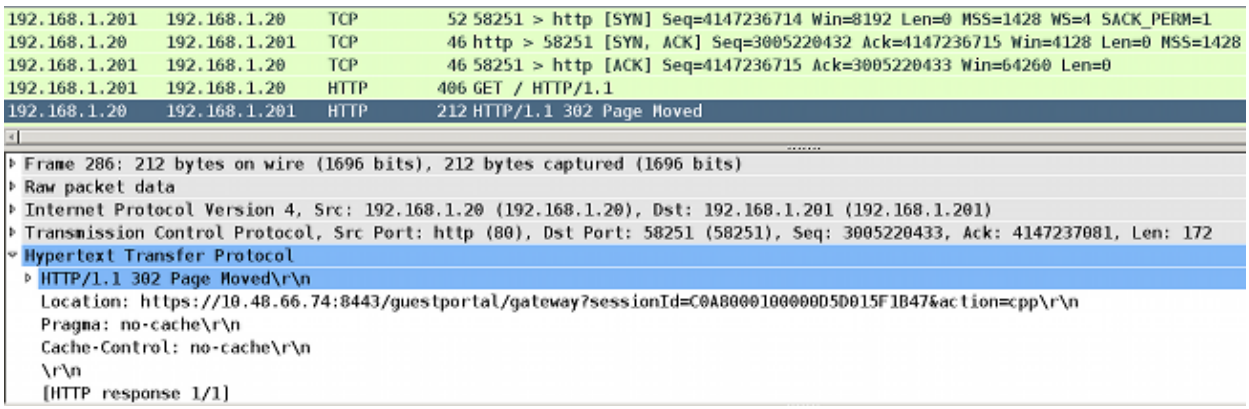
Traffic Reaches the Redirect ACL

Scenario 1 − Destination Host is in Same VLAN, Exists, and is SVI 10 UP

When you initiate the traffic to the IP address that is directly Layer 3 (L3) reachable by the switch (the network for the switch has an SVI interface), here is what happens:

1. The client initiates an Address Resolution Protocol (ARP) resolution request for the destination host (192.168.1.20) in the same VLAN and receives a response (ARP traffic is never redirected).

2. The switch intercepts that session, even when the destination IP address is not configured on that switch. TCP handshaking between the client and the switch is finished. At this stage, no other packets are sent outside of the switch. In this scenario, the client (192.168.1.201) has initiated a TCP session with the other host that exists in that VLAN (192.168.1.20) and for which the switch has an SVI interface UP (with the IP address of 192.168.1.10):



3. After the TCP session is established and the HTTP request is sent, the switch returns the HTTP response with the redirection to ISE (Location header).

   These steps are confirmed by debugs. There are several 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
```

   This can also be confirmed by more detailed debugs:

```
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. The client connects to the ISE directly (Secure Sockets Layer (SSL) session to 10.48.66.74:8443). This packet does not trigger redirection:

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

   Note: The session is intercepted by the switch, and thus that traffic can be captured on the switch with Embedded Packet Capture (EPC). The previous capture was taken with EPC on the switch.

Scenario 2 − Destination Host is in Same VLAN, Does Not Exist, and is SVI 10 UP

If the destination host 192.168.1.20 is down (does not respond), the client does not receive an ARP reply (the switch does not intercept ARP), and the client does not send a TCP SYN. Redirection never occurs.

This is why the NAC Agent uses a default gateway for a discovery. A default gateway should always respond and trigger redirects.

Scenario 3 − Destination Host is in Different VLAN, Exists, and is SVI 10 UP

Here is what happens in this scenario:

1. The client tries to access HTTP://8.8.8.8.

2. That network is not on any SVI on the switch.
3. The client sends a TCP SYN for that session to the default gateway 192.168.1.10 (destination MAC address known).

4. The redirection is triggered in exactly the same way as in the first example.

5. The switch intercepts that session and returns an HTTP response that redirects to the ISE server.

6. The client accesses the ISE server without problems (that traffic is not redirected).

Note: It does not matter if the default gateway is on the same switch or on an upstream device. It is only necessary to receive an ARP response from that gateway in order to trigger the redirect process. Additionally, it is necessary that ISE accessibility via the default gateway is permitted. Pay special attention if a firewall is on the patch, especially if it is a Layer 2 (L2) firewall and L2 packets traverse different links (then a TCP state bypass might be necessary on the firewall).

Scenario 4 − Destination Host is in Different VLAN, Does Not Exist, and is SVI 10 UP

This scenario is exactly the same as Scenario 3. It does not matter if the destination host in a remote VLAN exists or not.

Scenario 5 − Destination Host is in Different VLAN, Exists, and is SVI 10 DOWN

If the switch does not have SVI UP in the same VLAN as the client, it can still perform redirection but only when specific conditions are matched.

The problem for the switch is how to return the response to the client from a different SVI. It is difficult to determine which source MAC address should be used.

The flow is different from when SVI is UP:

1. The client sends a TCP SYN to the host in a different VLAN (192.168.2.20) with a destination MAC address set to a default gateway which is defined on the upstream switch. That packet reaches the redirect ACL, which is shown by debugs.
2. The switch verifies if it has a routing back to the client. Remember that SVI 10 is DOWN.
3. If the switch does not have another SVI that has a routing back to the client, that packet is not intercepted or redirected, even when Enterprise Policy Manager (EPM) logs indicate that ACL is reached. The remote host might return a SYN ACK, but the switch does not have a routing back to the client (VLAN10) and drops the packet. The packet cannot just be switched back (L2), because it reached the redirect ACL.
4. If the switch does have a routing to the client VLAN via a different SVI, it intercepts that packet and performs the redirect as usual. The response with URL−redirect does not go directly to the client, but via a different switch/router based on the routing decision.

Notice the asymmetry here:

- Traffic received from the client is intercepted locally by the switch.

- The response for that, which includes the HTTP redirect, is sent via the upstream switch based on the routing.

- This is when typical problems with the firewall might occur, and a TCP bypass is required.

- Traffic to the ISE, which is not redirected, is symmetrical. Only the redirection itself is asymmetric.

Scenario 6 − Destination Host is in Different VLAN, Does Not Exist, and is SVI 10 DOWN

This scenario is exactly the same as Scenario 5. It does not matter that the remote host exists. The correct routing is what is important.

Scenario 7 − HTTP Service is Down

As presented in Scenario 6, the HTTP process on the switch plays an important role. If the HTTP service is disabled, EPM shows that the packet reaches the redirect ACL:

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

However, the redirection never occurs.

The HTTPS service on the switch is not required for a HTTP redirect, but it is required for HTTPS redirect. The NAC Agent can use both for ISE discovery. Therefore, it is advised to enable both.

Redirect ACL − Incorrect Protocols and Port, No Redirection

Notice that the switch can only intercept HTTP or HTTPS traffic that works on standard ports (TCP/80 and TCP/443). If HTTP/HTTPS works on a nonstandard port, it can be configured with the ***ip port−map http*** command. Also, the switch must have its HTTP server listen on that port (***ip http port***).

Related Information

- ***Central Web Authentication with a Switch and Identity Services Engine Configuration Example***
- ***Cisco Identity Services Engine User Guide, Release 1.2***
- ***Technical Support & Documentation − Cisco Systems***

Updated: Jan 30, 2014 Document ID: 117278