ISE在Catalyst 3750系列交换机的流量重定向

目录

简介

此条款如何描述用户数据流是必要为了由交换机重定向数据包的重定向工作和条件。

先决条件

要求

思科建议您有与这些主题思科身份服务引擎(ISE)配置和基础知识的体验：

- ISE部署和中央Web验证(CWA)流
- 思科Catalyst交换机的CLI配置

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Microsoft Windows 7
- Cisco Catalyst 3750X系列交换机软件，版本15.0和以上
- ISE软件，版本1.1.4和以上

背景信息

在交换机的用户数据流重定向是大多的一关键组件与ISE的部署。所有这些流由交换机介入流量重定向使用情况：

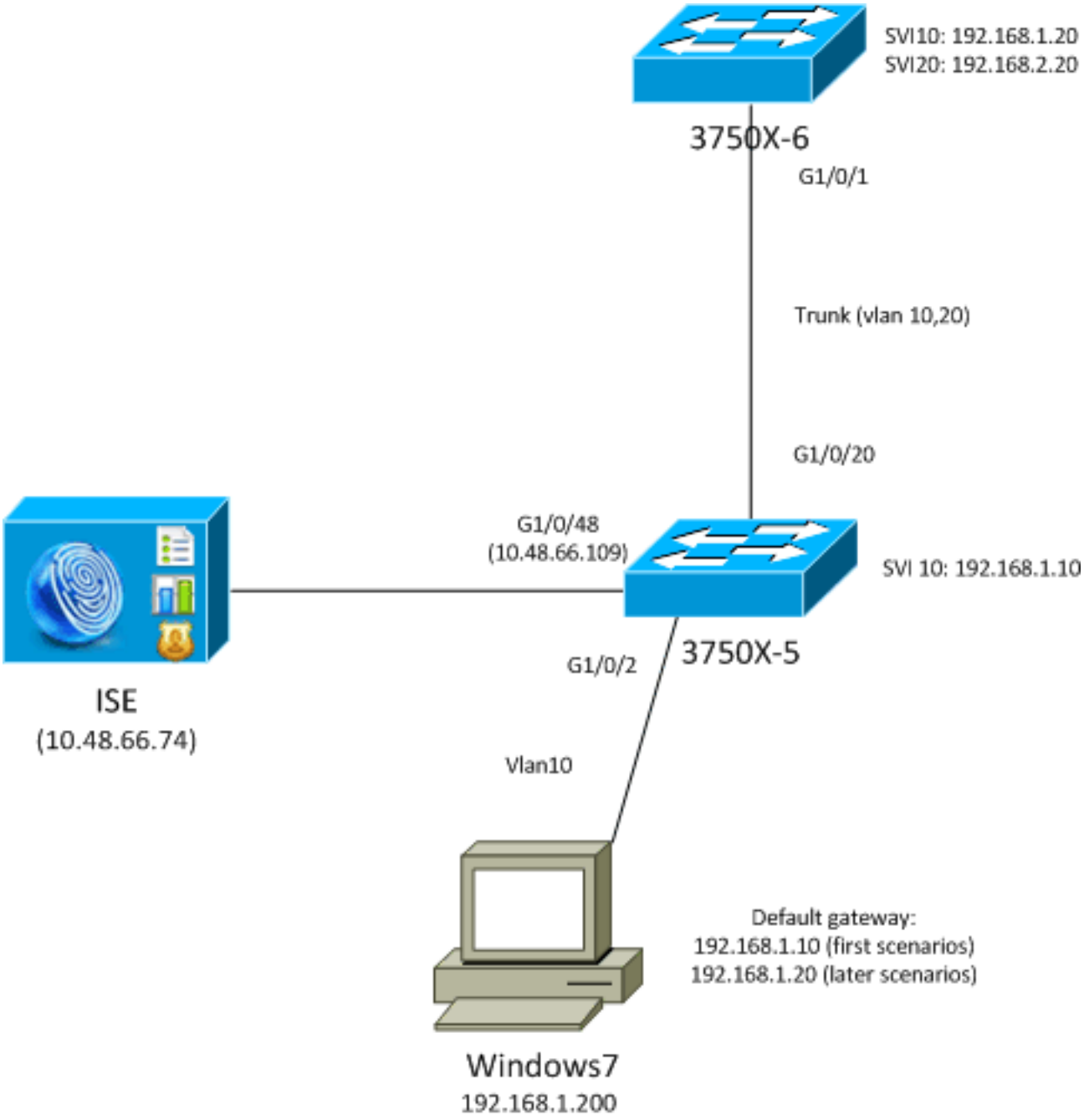
- CWA
- 客户端供应(CPP)
- 设备已注册(DRW)
- 本地请求方设置(NSP)
- 移动设备管理(MDM)

不正确地配置的重定向是多问题的原因与部署的。典型的结果是不正确地冒出或显示访客门户的无法的网络准入控制(NAC)代理程序。

对于交换机没有Switch Virtual Interface (SVI)和客户端VLAN一样的方案，参考最后三示例。

故障排除

测试方案



测验在客户端被执行，应该重定向到设置的ISE (CPP)。用户通过MAC验证旁路(MAB)或802.1x验证。ISE返回与重定向访问控制表(ACL)名称(REDIRECT_POSTURE)和重定向URL (对ISE的重定向的授权配置文件) ：

```
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
```

可下载的ACLs (DACL)在此阶段允许所有流量：

```
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
```

重定向ACL允许此流量，不用重定向：

- 对ISE (10.48.66.74)的所有流量
- 域名系统(DNS)和互联网控制消息协议(ICMP)流量

应该重定向其他流量：

```
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
```

交换机有一SVI在VLAN和用户一样：

```
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
```

在以下部分，修改这为了提交潜在影响。

流量不到达重定向ACL

当您设法ping所有主机时，您应该收到答复，因为该流量没有重定向。为了确认，请运行此调试：

```
debug epm redirect
```

对于客户端发送的每ICMP数据包，调试应该提交：

```
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]
```

为了确认，请检查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
```

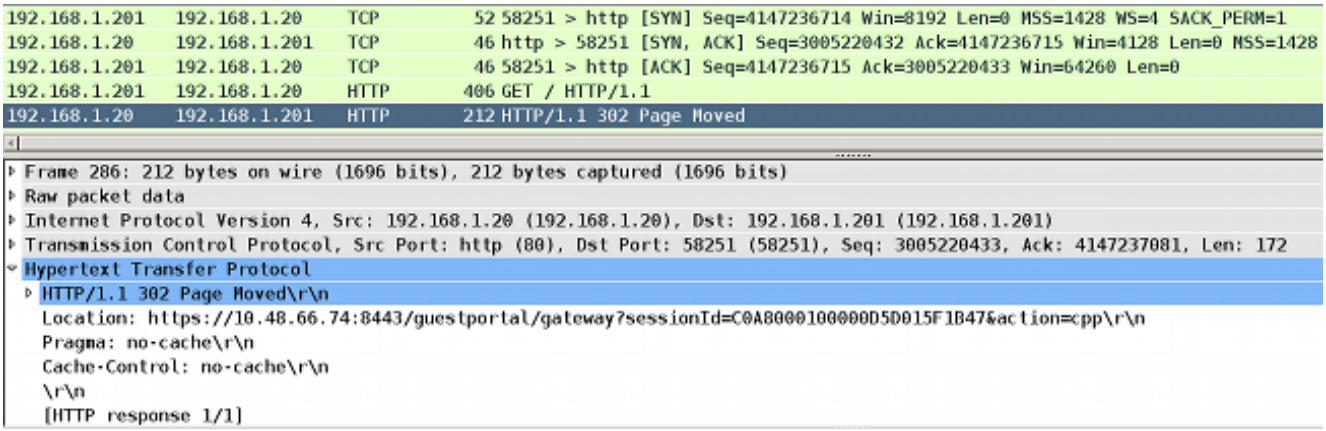
流量到达重定向ACL

方案1 -目的地主机在同样VLAN，存在，并且SVI 10上升

当您初始化流量对直接地是第3层的IP地址(L3)时可及的由交换机(有SVI接口)的交换机的网络，这是发生了什么：

1. 客户端启动一个地址解析服务(ARP)解决方法要求目的地主机(192.168.1.20)在同样VLAN并且收到答复(ARP流量从未重定向)。

2. 交换机截住会话，既使当目的IP地址在该交换机没有配置。在客户端和交换机之间的TCP握手完成。在此阶段，其他数据包没有被发送在交换机外面。在此方案中，客户端(192.168.1.201)启动一TCP会话用在该VLAN的另一台主机(192.168.1.20)存在，并且哪些交换机有一个SVI接口(用IP地址的192.168.1.10) ：



3. 在TCP会话建立后，并且HTTP请求发送，交换机返回与重定向的HTTP响应对ISE (位置报头)。

这些步骤由调试确认。有几ACL命中数：

```
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
```

这可能由更加详细的调试也确认：

```
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. 客户端直接地连接对ISE (安全套接字协议层(SSL)会话到10.48.66.74:8443)。此数据包不触发重定向：

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

注意：交换机拦截会话，并且该流量在有嵌入式数据包捕获的(EPC)交换机可以因而捕获。上一个捕获用在交换机的EPC获得。

方案2 -目的地主机在同样VLAN，不存在，并且SVI 10上升

如果目的地主机192.168.1.20发生故障(不响应)，客户端不收到ARP应答(交换机不拦截ARP)，并且客户端不发送TCP SYN。重定向从未发生。

这就是为什么美洲台代理程序使用默认网关发现。默认网关应该总是响应和触发重定向。

方案3 -目的地主机在另外VLAN，存在，并且SVI 10上升

这是什么在此方案发生：

1. 客户端设法访问HTTP://8.8.8.8。
2. 该网络不在交换机的任何SVI。
3. 客户端发送该会话的TCP SYN到默认网关192.168.1.10 (已知的目标MAC地址)。
4. 重定向在第一示例相似地被触发正如。
5. 交换机截住重定向对ISE服务器的会话和返回HTTP响应。
6. 访客接入不出问题ISE服务器(该流量没有重定向)。

注意：如果默认网关在同一交换机或在一个上行设备，不重要。收到从该网关的一ARP响应为了触发重定向进程只是必要的。另外，是必要的ISE可访问性通过默认网关允许。请给予特别注意，如果防火墙在补丁程序，特别是如果它是Layer2 (L2)防火墙和L2数据包横不同的链路(然后TCP状态旁路也许是必要的在防火墙)。

方案4 -目的地主机在另外VLAN，不存在，并且SVI 10上升

此方案正确地是相同的象方案3。如果在远程VLAN的目的地主机存在，不重要。

方案5 -目的地主机在另外VLAN，存在，并且是SVI 10 DOWN

如果交换机没有SVI在VLAN和客户端一样，可仍然执行重定向，但是，只有当特定情况匹配时。

交换机的问题是如何返回对客户端的答复从一不同的SVI。确定是很难的应该使用哪源MAC地址。

当SVI是UP时，流是与不同：

1. 客户端发送TCP SYN到在不同的VLAN (192.168.2.20)的主机与设置的一个目标MAC地址对在上行交换机定义的默认网关。该数据包到达重定向ACL，由调试显示。
2. 如果有一路由回到客户端，交换机验证。切记SVI 10是DOWN。
3. 如果有一路由回到客户端的交换机没有另一SVI，没有截断该数据包也没有重定向，既使当企业Policy Manager (EPM)日志表明ACL被到达。远程主机也许返回SYN ACK，但是交换机不回到客户端(VLAN10)有一路由并且丢弃数据包。因为到达了重定向ACL，数据包不可以仅是交换的上一步(L2)。
4. 如果交换机有一路由给客户端VLAN通过一不同的SVI，截断该数据包并且照常执行重定向。与Url重新定向的答复不去直接地客户端，然而通过根据路由决策/路由器的一个不同的交换机。

注意非对称此处：

- 交换机拦截从客户端接收的流量本地。
- 那的答复，包括HTTP重定向，通过根据路由的上行交换机被发送。
- 这是，当与防火墙的典型的问题也许发生，并且TCP旁路要求。
- 对ISE的流量，没有重定向，是对称的。仅重定向不对称。

方案6 -目的地主机在另外VLAN，不存在，并且是SVI 10 DOWN

此方案正确地是相同的象方案5。不重要远程主机存在。正确路由是什么是重要。

方案7 - HTTP服务发生故障

如被提交在方案6，在交换机的HTTP进程播放重要的角色。如果HTTP服务禁用， EPM显示数据包到达重定向ACL ：

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

然而，重定向从未发生。

在交换机的HTTPS服务没有为HTTP重定向要求，但是为HTTPS重定向要求。美洲台代理程序能使用两个ISE发现。所以，建议启用两个。

重定向ACL -不正确协议和波尔特，没有重定向

注意交换机能只拦截在标准端口作动的HTTP或HTTPS流量(TCP/80和TCP/443)。如果HTTP/HTTPS在一个非标准端口工作，可以用**ip port-map http**命令配置。并且，交换机在该端口(**IP HTTP端口**)必须安排其HTTP服务器侦听。

相关信息

- 与交换机和身份服务引擎配置示例的中央Web验证
- 思科身份服务引擎用户指南，版本1.2
- 技术支持和文档 - Cisco Systems