ISE在Catalyst 3750 Series Switch的数据流重定向

Contents

Introduction

此条款描述用户数据流重定向如何工作和是必要为了由交换机重定向信息包的条件。

Prerequisites

Requirements

Cisco建议您有与这些题目思科身份服务引擎(ISE)配置和基础知识的经验：

- ISE配置和中央Web认证(CWA)流
- Cisco Catalyst交换机的CLI配置

Components Used

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个重要组件与ISE的配置。所有这些流由交换机介入数据流重定向使用方法：

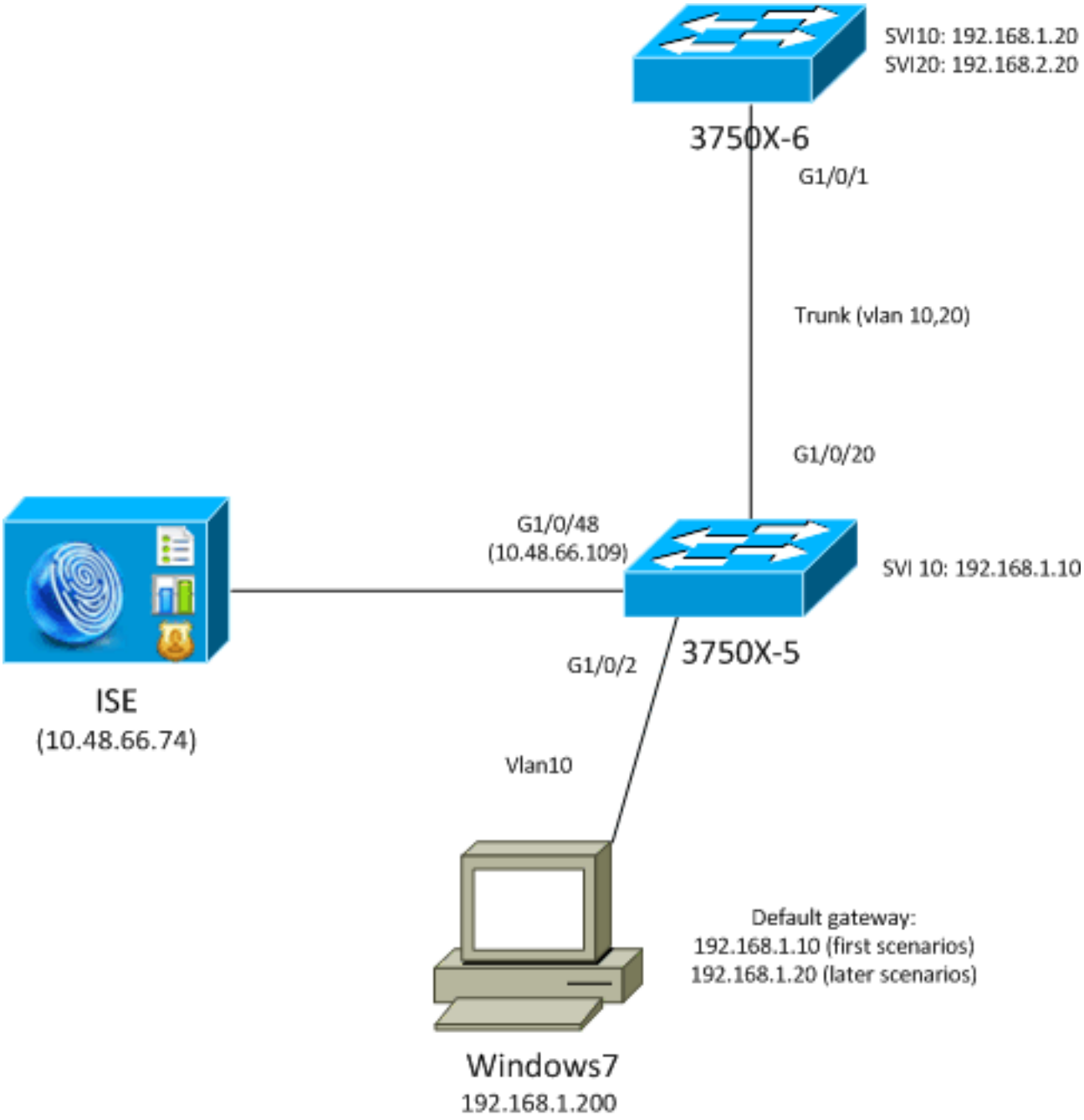
- CWA
- 客户端设置(CPP)
- 设备已注册(DRW)
- 本地请求方设置(NSP)
- 便携设备管理(MDM)

不正确地被配置的重定向是多个问题的原因配置的。典型的结果是不正确地冒出或显示客户门户的无法的网络准入控制(NAC)代理程序。

关于交换机没有Switch Virtual Interface (SVI)和客户端VLAN一样的方案，请参见前三个示例。

Troubleshoot

测试方案



测试在客户端被执行，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)名字(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)在此阶段允许所有数据流：

```
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允许此数据流，不用重定向：

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

应该重定向其他数据流：

```
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。

数据流不到达重定向ACL

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

```
debug epm redirect
```

对于客户端发送的每个ICMP信息包，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
```

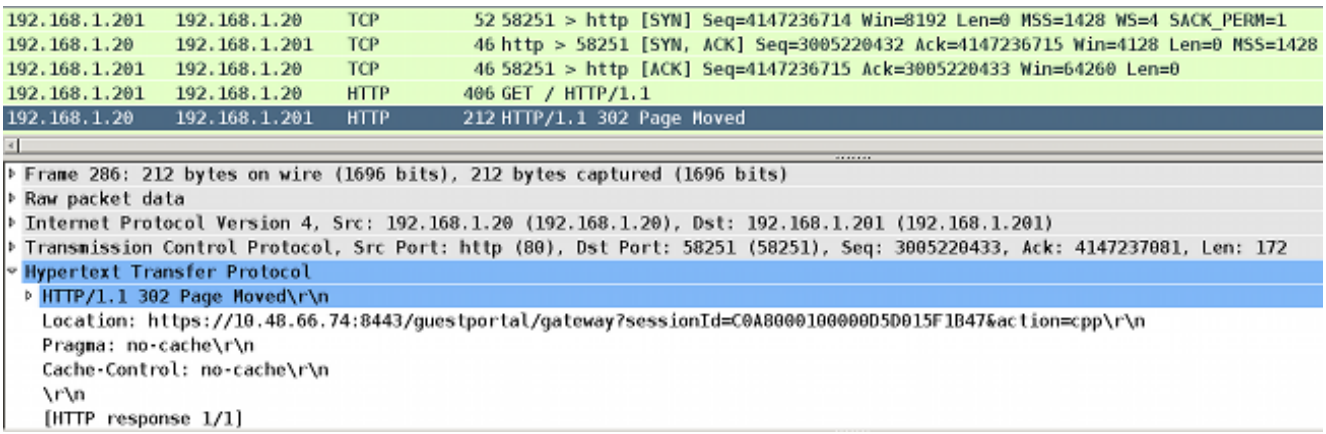
数据流到达重定向ACL

方案1 -目的地主机在同样VLAN，存在，并且是SVI 10

当您初始化数据流对直接地是第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. 客户端起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数据流从未重定向)。

2. 交换机截住会话，既使当目的地IP地址在该交换机没有被配置。在客户端和交换机之间的TCP握手完成。在此阶段，其他信息包没有被发送在交换机外面。在此方案中，客户端(192.168.1.201)起动了一次TCP会话用存在于该VLAN的另一台主机(192.168.1.20)，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，并且发送HTTP请求，交换机返回与重定向的HTTP回应到ISE (位置报头)。

   这些步骤由调试确认。有几ACL命中：

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

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

Note:交换机拦截会话，并且该数据流在有嵌入式信息包获取的(EPC)交换机可以因而被捕获。早先捕获用在交换机的EPC获得。

方案2 -目的地主机在同样VLAN，不存在，并且是SVI 10

如果目的地主机192.168.1.20发生故障(不回应)，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NAC代理程序使用默认网关发现。默认网关应该总是回应和触发重定向。

方案3 -目的地主机在另外VLAN，存在，并且是SVI 10

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 (已知的目的地MAC地址)。
4. 重定向在第一个示例相似地被触发正如。
5. 交换机截住会话和返回重定向对ISE服务器的HTTP回应。
6. 客户访问不出问题ISE服务器(该数据流没有重定向)。

Note:如果默认网关在同一台交换机或在一个上行设备，不重要。从该网关接受ARP响应为了

触发重定向进程只是必要的。另外，是必要的ISE可及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，特别是如果它是第2层(L2)防火墙和L2信息包横不同的链路(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，并且是SVI 10

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，只有当特定情况被匹配时。

交换机的问题是如何从一不同的SVI返回对客户端的回应。确定是难的应该使用哪源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)的主机与设置的目的地MAC地址对在上行交换机被定义的默认网关。该信息包到达重定向ACL，由调试显示。
2. 交换机验证是否有路由回到客户端。切记SVI 10是DOWN。
3. 如果有路由回到客户端的交换机没有另一SVI，没有截断该信息包也没有重定向，既使当企业策略管理器(EPM)日志表明ACL被到达。远端主机也许返回SYN ACK，但是交换机不回到客户端(VLAN10)有路由并且丢弃信息包。因为到达了重定向ACL，信息包不可能仅被转换(L2)。
4. 如果交换机有路由给客户端VLAN通过一不同的SVI，截断该信息包并且照常执行重定向。与Url重新定向的回应不去直接地客户端，然而通过根据路由决策/路由器的一个不同的交换机。

注意非对称这里：

- 交换机拦截从客户端收到的数据流本地。
- 那的回应，包括HTTP重定向，通过根据路由的上行交换机被发送。
- 这是，当防火墙的典型的问题也许发生，并且需要TCP旁路。
- 对ISE的数据流，没有重定向，是对称的。仅重定向是不对称的。

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。不重要远端主机存在。正确的路由是什么是重要的。

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服务是失效的， EPM表示，信息包到达重定向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服务没有对于HTTP重定向是必需的，但是对于HTTPS重定向是必需的。NAC代理程序能使用两个ISE发现。所以，建议对enable (event)两个。

重定向ACL -不正确协议和端口，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服务器监听。

Related Information

- **与交换机和身份服务引擎配置示例的中央Web认证**
- **思科身份服务引擎用户指南，版本 1.2**
- Technical Support & Documentation - Cisco Systems