FWSM替换透明防火墙的故障排查

目录

技术领域

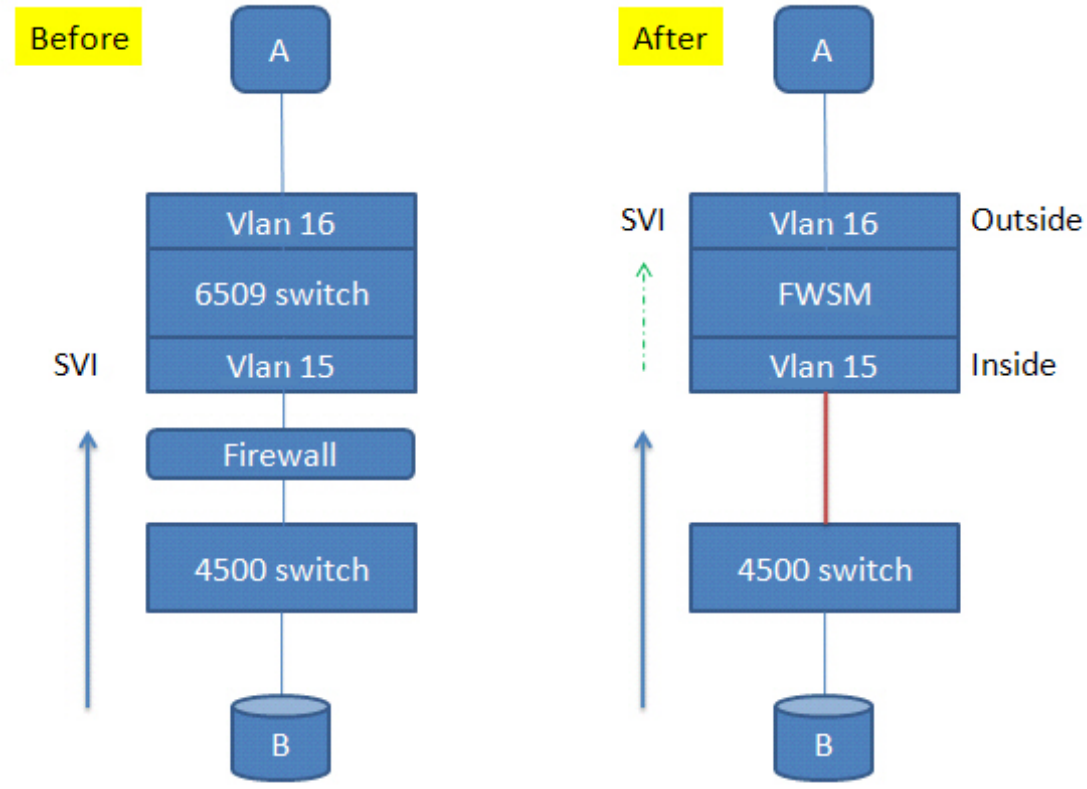
FWSM LAN-Switch

问题描述

用户尝试使用FWSM 模块替换一个第三方的透明防火墙设备，在替换后发现网络中断。

逻辑拓扑结构

在用FWSM替换第三方防火墙前/后的拓扑结构：



' Third-party firewall working in transparent Mode

配置说明

数据流量从B到A流经防火墙的控制。

在用FWSM替换前，VLAN 15 的SVI 起在6509交换机的MSFC上，第三方防火墙工作于透明模式，从主机B的默认网关指向interface vlan 15的IP 地址。

在用FWSM替换后，用户先no掉VLAN 15的SVI的地址，将相同地址配置到Interface Vlan 16上。

主机B的默认网关不变。

vlan15 为inside vlan，vlan 16为 outside vlan。

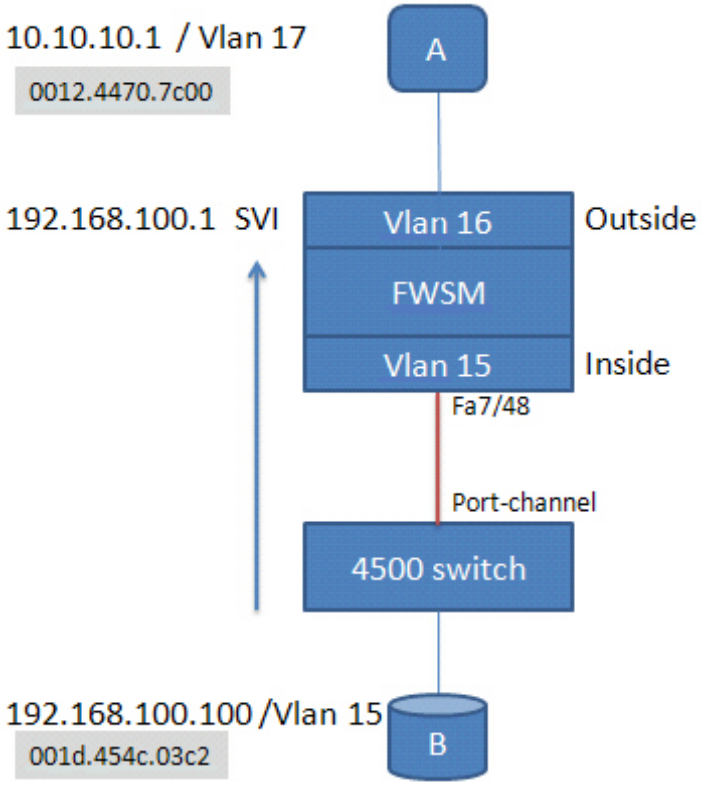
工作在透明模式下的配置如下：

```
interface Vlan15
 nameif inside
 bridge-group 1
 security-level 100
!
interface Vlan16
 nameif outside
 bridge-group 1
 security-level 0
!
interface BVI1
 ip address 192.168.100.254 255.255.255.0
route outside 0.0.0.0 0.0.0.0 192.168.100.1 1
```

防火墙的策略配置允许IP，及二层BPDU报文全部通过。

```
access-list permitany extended permit ip any any
access-list BPDU ethertype permit bpdu
access-group BPDU in interface inside
access-group BPDU in interface outside
access-group permitany in interface outside
access-group permitany in interface inside
```

替换后的拓扑结构



6509交换机和4506交换机间有port channel，Trunk 放行来自4506下层的VLAN。

10.10.10.1 是6509交换机上interface vlan 17 的IP 地址，在交换机上，所有的VLAN三层接口的MAC地址都是一样的，在本环境下为 0012:4470:7c00。

192.168.100.100是6509下联的4506交换机下vlan 15的一个主机，其MAC地址为001d.454c.03c2.

诊断步骤

1. 由于从B到A的流量被阻断，先检查交换机上的Mac 地址的学习状态。 从B去向A的流量，必须经过防火墙模块，对于交换机而言，必须知道去往Mac 地址为0012:4470:7c00该向交换机上哪个接口发送。

```
65-2#show mac-address-table | include 03c2192.168.100.100MAC
*   15  001d.454c.03c2 dynamic Yes 100 Po15
```

当从192.168.100.100 ping 10.10.10.1的时候，192.168.100.100的mac 地址会被交换机从4506和6509之间的trunk接口动态地学到，此为正常情况。

```
65-2#show mac-address-table | include 7c00   int VLAN 17 MAC
*   16  0012.4470.7c00    static  No           -   Router
*   17  0012.4470.7c00    static  No           -   Router
*   15  0012.4470.7c00    static  No           -   Router
```

对于交换机而言，所有的interface vlan 的接口都是继承相同的MAC 地址，在VLAN 15收到去往特定MAC地址存在多条路径的时候，会首先向其所在的vlan的默认网关发送，现在数据包被阻断

，所以怀疑 两点， vlan 15不知道如何转发数据包，或将该包发送到了一个黑洞中，或者在FWSM上的vlan retag没有正常执行。需要进一步从interface vlan 接口状态，及在防火墙模块上抓包去分析从trunk口下来的具有vlan tag 15的数据包去往何处。

2. 防火墙模块（FWSM）工作在透明模式下的时候，FWSM与交换机背板间存在一个内置的port-channel，所有VLAN间的流量转发，需要FWSM做vlan 流量的retag。所以在正常设计模式下，划归到防火墙中的所有VLAN中，只能有一个VLAN在MSFC上具有SVI接口，否则会导致流量bypass防火墙接口检查。据此，在用户环境中VLAN15的数据包的流量应该在二层被retag成VLAN16的数据包，再被发送到vlan16的三层接口路由到其他网段。
3. 在交换机上检查interface vlan 15 发现如下输出：

```
Vlan15 is up, line protocol is up
  Hardware is EtherSVI, address is 0012.4470.7c00   (bia 0012.4470.7c00)
```

这说明，尽管用户在将interface vlan 15的接口IP移植给vlan16 后，但是并没有在本地将该接口shutdown，或no掉，导致来自VLAN 15的数据包，发现从本地interface vlan 15也可以学到目的Mac，就不会讲流量转发进FWSM到交换机间的内置port-channel。而int vlan 15 没有配IP，所以自然也不会将该流量路由转发出去，形成本地的一个黑洞。

4. 执行修复措施，no掉interface vlan 15，发现流量可以正常通过。重新show mac-address-table，发现了如下变化：

```
65-2#show mac-address-table | include 03c2
* 16 001d.454c.03c2 dynamic Yes   315 Po271
* 15 001d.454c.03c2 dynamic Yes   315 po15

65-2#show mac-address-table | include 7c00
* 16 0012.4470.7c00 static No   - Router
* 17 0012.4470.7c00 static No   - Router
* 13 0012.4470.7c00 static No   - Router
* 15 0012.4470.7c00 dynamic Yes   380 Po271
```

- 补充，另外还可以利用在防火墙模块上进行双向抓包来判断实际流量是否流经FWSM。

1. 对应于interface vlan 17的在MSFC上的SVI 地址，可以从两个地方学到，其中发生改变的一个就是，PO271（fwsm和chassis间的port-channel），这样当6509的VLAN 15再收到去往别的vlan 的包，就知道该将此包经由po271送交给FWSM进行retag处理。
2. 对应于vlan 15主机的MAC 地址同样可以从两个地方学到，多了一项从po271可以学到下层vlan15主机的IP地址，这样当从A 去往 B的流量，在包先抵达了vlan 16后，会从与本地vlan 相连的po271接口将其发送给FWSM进行vlan 的retag处理。

总结

1. 对于FWSM工作在透明模式下的MAC地址学习，建立一个正常模型，将有助于我们快速锁定问题的可能原因。
2. FWSM工作在透明模式下，对于嵌入用户当前网络具有很大的便利性，可减少网络拓扑的更改，但是必须深入理解VLAN SVI和FWSM 的关系，对调整后的SVI接口作出必要的调整。

最佳实践就是，划入FWSM的VLAN中只能有一个VLAN具有SVI。其他vlan 如果起了SVI，但是没有配IP地址，最好将该SVI删除。