防火墙插卡二层部署在三层交换机上典型配置举例

二层转发 旁路部署 IRF **胡伟** 2021-04-01 发表

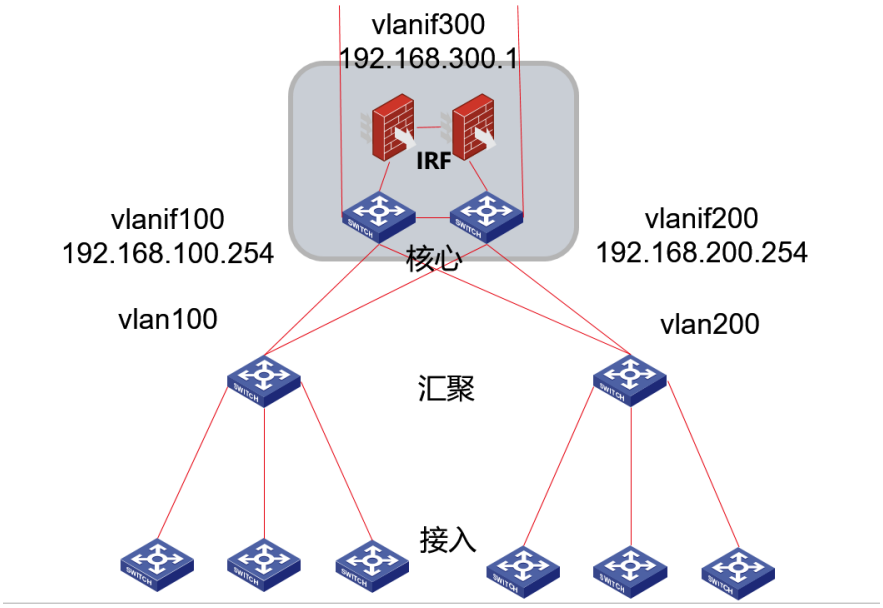
组网及说明

组网说明：

1，下联设备部署在不同的Vlan内，网关设置在交换机上，使用不同的Vlan-interface接口进行三层转发。

2，由于安全需要，在交换机上部署防火墙插卡，要求尽量不改变现网其他设备配置，使得流量能够经过防火墙转发。

3，交换机是堆叠环境，防火墙插卡也要求堆叠环境。



配置步骤

1，防火墙插卡堆叠要求。

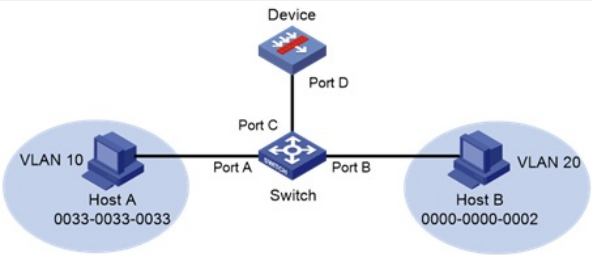
- 由于两台堆叠设备的心跳线不能跨二层设备，H3C SecBlade IV NGFW防火墙插卡仅支持前面板接口作为IRF物理端口。
- BFD MAD检测线可以用防火墙内联口，使用单独Vlan，跨交换机进行检测，注意交换机侧对应接口Vlan也要放通。
- 由于防火墙插卡强烈不建议双主部署，只建议主备部署即流量来回都在一台防火墙插卡上。二层模式下建议将所有业务内联口加入同一个二层聚合口，与交换机侧配置动态链路聚合，同时设置好聚合口成员接口链路优先级以及聚合口最大选中数，保证防火墙内联口一框的接口属于选中状态，另一框的接口属于非选中状态。同时配置冗余组，使得每一框的接口状态能够一起联动。

2，防火墙配置跨VLAN转发。

由于交换层部署在三层模式，流量上来时直接三层转发，不会经过防火墙。为了让流量经过防火墙处理，需要交换机首先将内网上送的流量经过二层透传到防火墙（即需要删除交换机对应原先内网vlan的三层虚接口），同时防火墙上配置跨Vlan转发，将交换机发过来的流量转换为另一个Vlan再送回到交换机，交换机再针对此Vlan设置三层虚接口（即内网网关），后面流程走正常三层转发即可。这样可以使得内网终端经过网关转发的流量能够经过防火墙进行处理一遍。

防火墙跨Vlan跨框原理如下：http://www.h3c.com/cn/d_202011/1353507_30005_0.htm#_Toc54611994

> **跨VLAN模式Bridge转发**
> 跨VLAN模式Bridge转发是在数据链路层完成不同VLAN间通信的一种技术。如1所示，目前这种技术主要应用在安全设备上。安全设备和交换机配合使用、经过交换机的二层网络流量由安全设备过滤后再进行转发的场景。
> 图1 Bridge转发工作机制



> 如1，交换机上配置的安全设备（Device）的Bridge转发实例（可以看作是实现一类Bridge转发模式的二层桥）为Bridge 1，Bridge 1中添加VLAN 10和VLAN 20。以ARP（Address Resolution Protocol，地址解析协议）实现为例，Bridge转发过程如下：
> (1) VLAN 10的Host A想要访问VLAN 20的Host B，Host A发送一个ARP请求报文。
> a. 交换机收到请求报文的处理过程：
> ¡ 交换机从接口Port A收到目的MAC未知的报文，交换机学习到该报文的源MAC地址0033-0033-0033，并记录该MAC地址所对应的VLAN 10和接口Port A。
> ¡ 交换机将该报文在VLAN 10内进行广播，同时该报文会通过交换机侧内联口Port C（即用于连接交换机与安全设备的接口）发送给安全设备。
> b. 安全设备收到请求报文的处理过程：
> ¡ 安全设备收到该报文，将报文源MAC地址学习到用户配置的Bridge转发实例Bridge 1内，并且学习到该MAC地址对应的VLAN 10及安全设备侧内联口Port D。
> ¡ 同时根据Bridge 1内用户配置的VLAN列表，将该报文在Bridge 1内配置的除报文所在VLAN 10以外的所有VLAN内进行发送，即在VLAN 20内发送该报文。在VLAN 20内发送的报文的VLAN ID将被替换为VLAN 20，生成新的报文，然后发送到VLAN 20。
> ¡ 安全设备通过安全设备侧内联口Port D将新报文发送给交换机。
> c. 交换机收到新报文的处理过程：
> ¡ 交换机从交换机侧内联口Port C收到新的报文，学习该报文的源MAC地址并记录该MAC地址所对应的VLAN 20和交换机侧内联口Port C。
> ¡ 同时交换机将报文在VLAN 20内广播。
> (2) VLAN 20的Host B收到新报文后，发现是要访问自己的报文，发送ARP应答报文。
> a. 交换机收到应答报文的处理过程：

¡ 交换机从接口Port B收到目的MAC地址0033-0033-0033的报文，交换机学习到该报文的源MAC地址0000-0000-0002并记录该MAC地址所对应的VLAN 20和接口Port B。

¡ 交换机收到目的MAC地址为0033-0033-0033的已知报文，根据目的MAC地址和VL

配置关键点

1，交换机上对应内网Vlan数目要增加一倍。

2，防火墙上也要创建对应的Vlan并且保证要全局下引用这些Vlan，同时放通对应安全策略。

安全设备

安全设备收到应答报文的处理过程

¡ 安全设备收到回复报文，将该报文源MAC地址学习到用户配置的Bridge转发实例Bridge 1内，并且学习到该MAC地址对应的VLAN 20及安全设备侧内联口Port D。