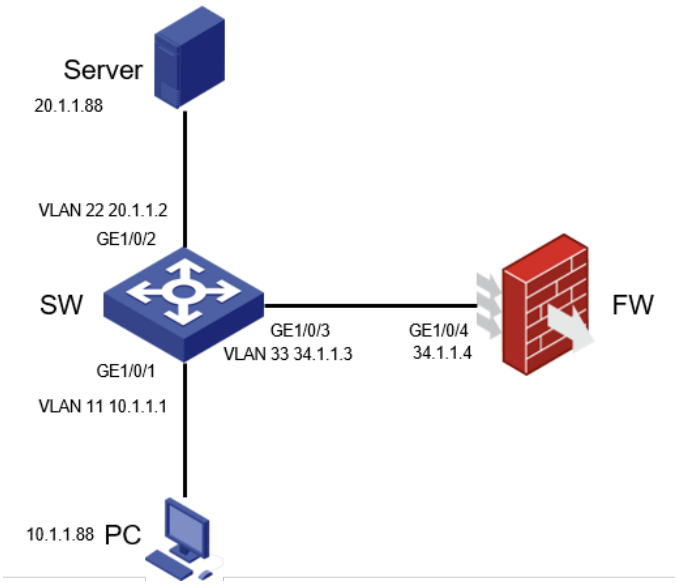
防火墙旁挂 Comware V7 平台交换机PBR部署流量三层转发环路故障经验案例

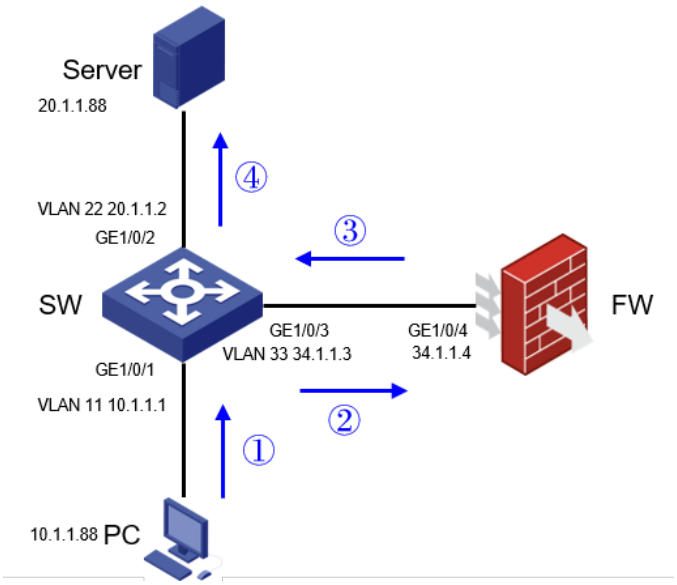
策略路由 IP转发 IP性能优化 产品特性 丁犁 2021-07-27 发表

组网及说明

组网简化拓扑如下图所示，PC 将上传数据给 Server，要求该上传数据流量，经过 FW 过滤转发。SW 作为 PC 和 Server 的网关，承担三层转发。



根据需求，其业务流量转发，如下图所示，按照 ① -> ② -> ③ -> ④ 路径转发。



具体部署思路为：

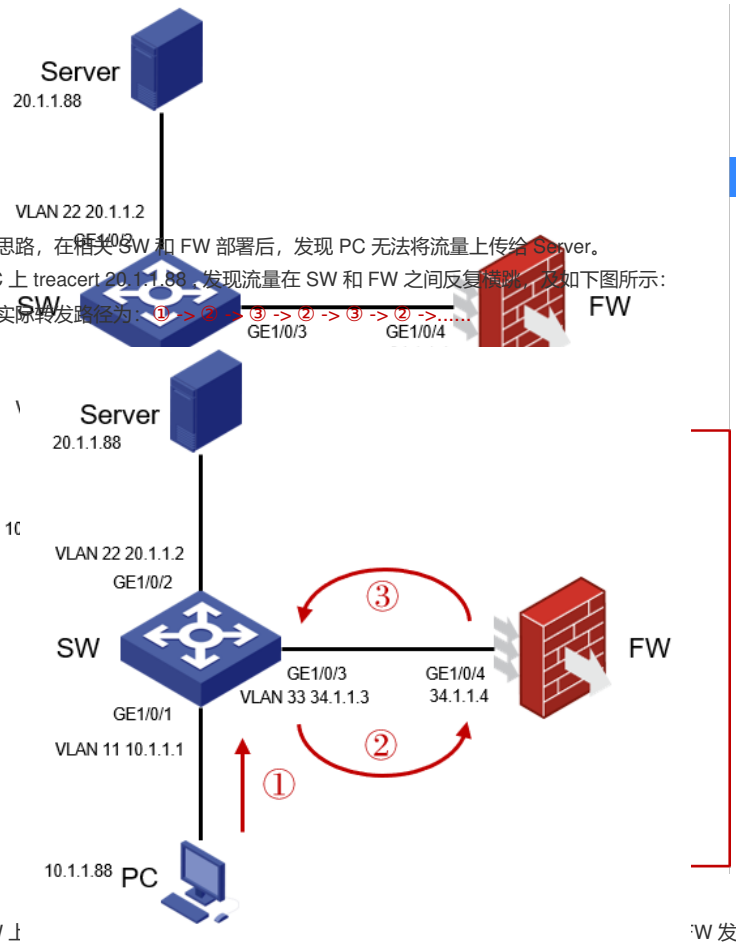
1、在 SW 的 PC 网关 Vlan-interface 11 上部署 PBR，将流量重定向给FW，及实现 ① -> ② 转发。

问题描述

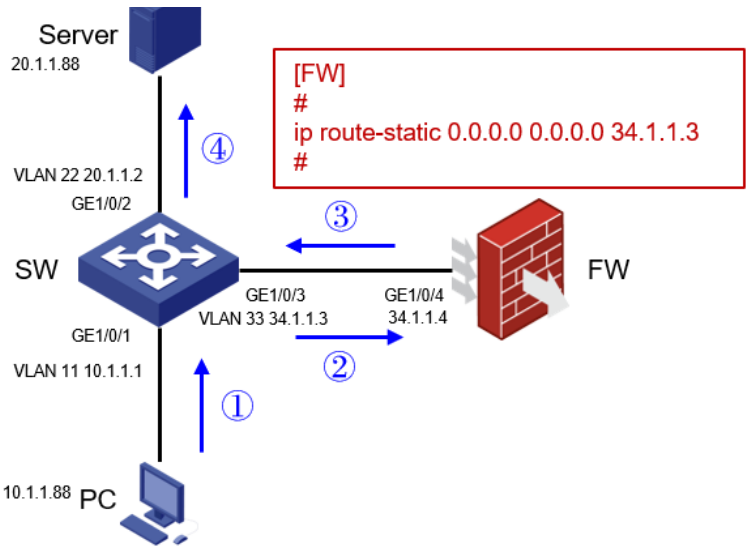
根据部署思路，在楷天 SW 和 FW 部署后，发现 PC 无法将流量上传给 Server。

通过在PC 上 treacert 20.1.1.88，发现流量在 SW 和 FW 之间反复横跳，如下图所示：

上传流量实际转发路径为：① -> ② -> ③ -> ② -> ③ -> ② ->.....

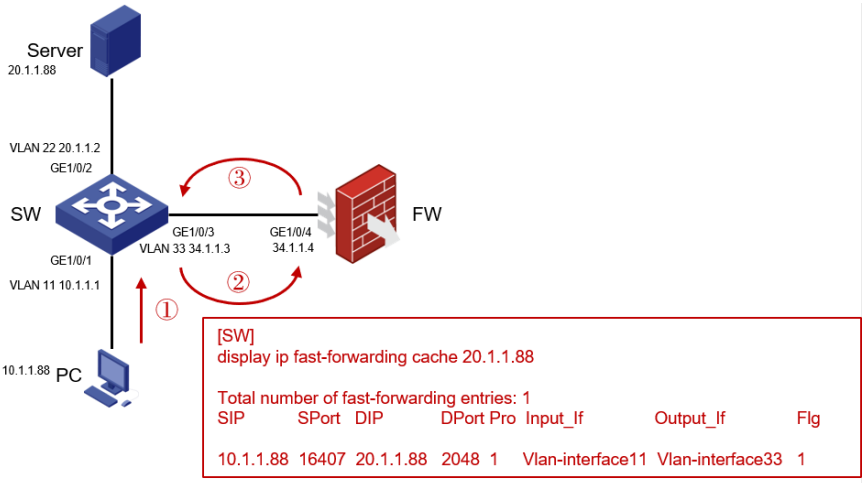


2、在 FW 上 W 发来的流量后，查找



过程分析

通过检查 SW 上的 快速转发表 ip fast-forwarding cache ， 发现 “源IP=10.1.1.88，目前IP=20.1.1.88”的流量，在 SW 的快转表中，始终指向 FW 作为下一跳。




```
[SW]
display ip fast-forwarding cache 20.1.1.88

Total number of fast-forwarding entries: 1
SIP          SPort  DIP          DPort Pro  Input_If          Output_If         Flg

10.1.1.88  16407  20.1.1.88  2048  1    Vlan-interface11  Vlan-interface33  1
```

因此当流量首次经过 ① -> ② -> ③ ，SW 收到了 FW 转发回来的流量后，仍然按照前期（① -> ② ）形成的快速转发表，将流量又再次扔给 FW，因此导致流量转发路径始终为 ① -> ② -> ③ -> ② -> ③ -> ② ->.....

解决方法

目前 Comware V7 平台交换机设备缺省均使能了 “快速转发功能”和“ 快速转发负载分担功能”，表项老化时间缺省为30秒。

开启快速转发负载分担功能后，当一条数据流从不同入接口上来进行转发时，不再根据入接口不同区分数据流，根据报文中的信息标识一条数据流。
因此按照上述故障案例，PC to Server 的流量，对于 SW 而言 无论是从 Vlan-interface 11 收到，还是从 Vlan-interface 33收到，缺省 SW 认为是同一个流量，及按照 display ip fast-forwarding cache 快速转发表转发。

要解决上述旁路转发的问题，需要在 SW 上关闭快速转发负载分担功能，及 增加 [SW] undo ip fast-forwarding load-sharing
关闭快速转发负载分担功能后，将会根据入接口的不同对已标识的数据流再次做出区分，即将入接口作为区分数据流的另一特征标识。及从 FW 发回给 SW 的流量将不再直接匹配 display ip fast-forwarding cache 快速转发表转发，而是 SW 重新进行转发计算，将流量从 Server 网关接口发送给 Server。