防火墙静态路由实验

**目录**

[1 实验设想 2](#_Toc185714885)

[1.1 实验背景及目的 2](#_Toc185714886)

[1.2 流量路径 2](#_Toc185714887)

[1.3 实验要求图 3](#_Toc185714888)

[2 拓扑设计 3](#_Toc185714889)

[2.1 拓扑图设想 3](#_Toc185714891)

[2.2 拓扑图 3](#_Toc185714892)

[3 配置脚本 4](#_Toc185714893)

[3.1 完成对接口基础地址的配置和VLAN划分 4](#_Toc185714894)

[3.2安全策略 5](#_Toc185714895)

[3.3 PC1-PC3的流量路径控制 6](#_Toc185714896)

[3.4 PC2-PC4的流量路径控制 7](#_Toc185714897)

[3.5 PC1、PC2、PC3、PC4访问Server的流量路径控制 8](#_Toc185714898)

[4 结论 10](#_Toc185714899)

[4.1 遇到的问题 10](#_Toc185714900)

[4.2 心得体会 11](#_Toc185714901)

# 1 实验设想

# 1.1 实验背景及目的

互联网在全球范围内迅速普及，企业和个人计算机网络的互联互通成为常态。随着网络用户的增多，网络安全问题日益凸显，防火墙作为保护内部网络不受外部攻击的重要手段应运而生。

为了应对日益增长的网络攻击、互联网技术的快速发展和网络安全的迫切需求，防火墙发挥的作用是必不可少的。

基于此背景下面我们设想一个不同安全域之间互相访问的实验。

# 1.2 流量路径

从PC1到PC3的数据流需要经过V1-Vsys1-全局-Vsys2-V2这条路径。 从PC2到PC4的数据流需要经过V1-Vsys1-Vsys2-V2这条路径。 所有PC访问服务器需经过各自防火墙再到全局。

# 1.3 实验要求图

1实验要求图

# 拓扑设计



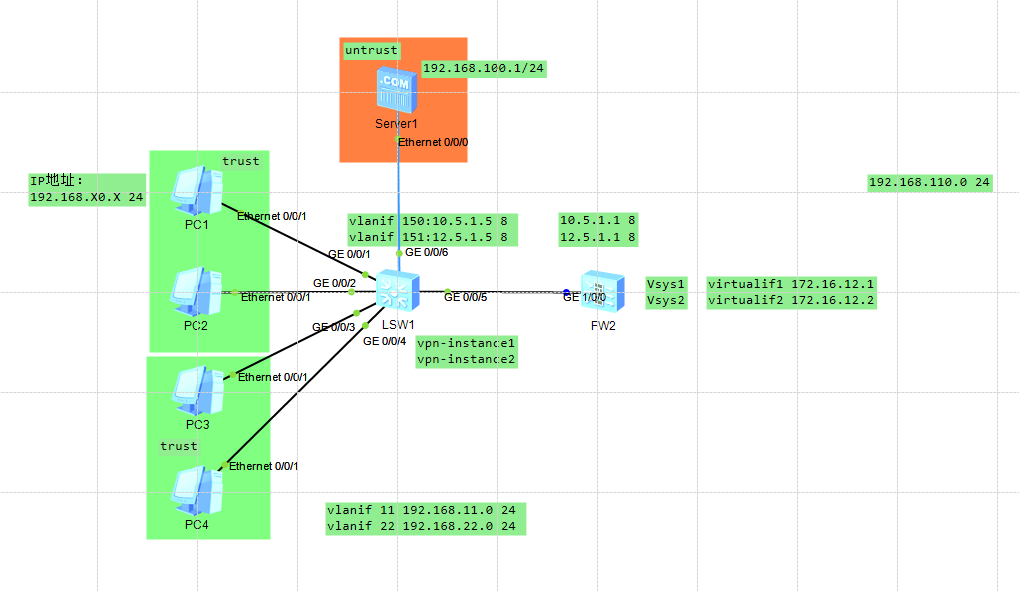
# 2.1 拓扑图设想

四个PC机（PC1到PC4），它们通过交换机（SW）连接到一个局域网内。

服务器也位于同一个局域网中，并与交换机全局相连。

局域网外有两个虚拟系统（VSYS1和VSYS2）。

# 2.2 拓扑图



2 拓扑图

# 配置脚本

# 3.1 完成对接口基础地址的配置和VLAN划分

在交换机SW1上创建对应VLAN以及对VLANIF进行三层地址配置。

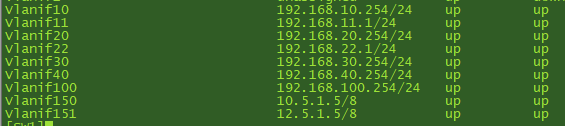


图3 - 1 交换机接口地址配置

对交换机SW1物理接口进行link-type配置以及放通对应的vlan。

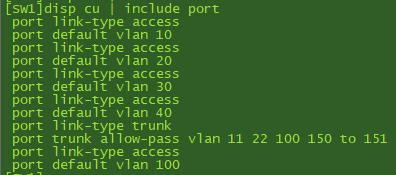


图3 - 2 交换机物理接口link-type配置

在防火墙FW1上创建对应VLAN以及对VLANIF进行三层地址配置。

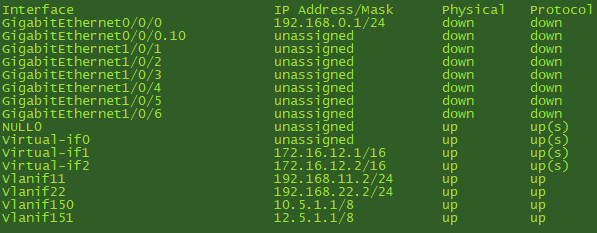


图3 - 3 防火墙vlan划分以及地址配置

对防火墙FW1物理接口切换为二层接口并进行link-type配置以及放通对应的vlan。

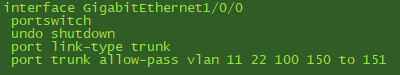


图3 - 4 防火墙接口link-type配置

# 3.2安全策略

在防火墙FW1根墙、vsys1、vsys2上放通安全策略并放通icmp协议报文。

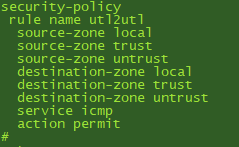


图3 - 5 安全策略

三者都是一样的安全策略，为了对流量进行静态配置，暂不配置源目地址。

# 3.3 PC1-PC3的流量路径控制

SW1上配置如下静态路由，从实例1内目的地址为30.0网段的路由转发给11.2，从防火墙发送过来的在全局，全局收到路由后转发给22.2，再由防火墙发回交换机实例2，实例2内直连路由所以不用配置静态。

回程路径中实例2内会收到一个目的地址为10.0网段的路由，转发给22.2，随后从防火墙发回交换机全局，全局再转发给11.2，再由防火墙发回交换机实例1，实例1内直连路由所以不用配置静态。

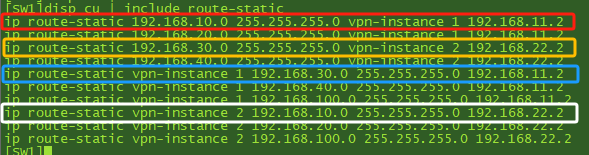


图3 - 6 PC1-PC3交换机静态路由

防火墙上配置如下静态路由，从交换机发到vsys1内目的地址为30.0网段的路由，转发给10.5.1.5全局，随后vsys2会收到路由，转发给22.1。

回程路径中vsys2会收到目的地址为10.0网段的路由，转发给12.5.1.5全局，随后vsys1会收到路由，转发给11.1。

以下是通过disp cu | include route-static 查询的路由，因此不显示在哪个虚拟系统内。

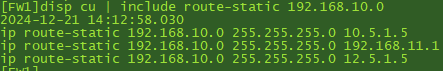


图3 - 7 PC1-PC3防火墙静态路由 1



图3 - 8 PC1-PC3防火墙静态路由2

这是PC1pingPC3的现象：

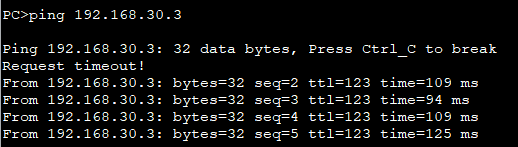


图3 - 9 PC1pingPC3

这是tracert现象：

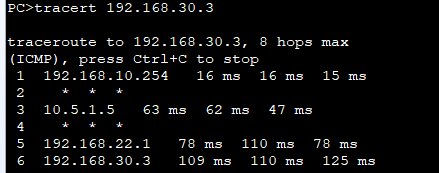


图3 - 10 tracert

# 3.4 PC2-PC4的流量路径控制

SW1上配置如下路由，实例1内收到前往40.0网段的路由，转发给11.2，随后防火墙会转发给实例2，实例2收到后直连路径不用静态。

回程路径实例2收到前往20.0网段路由，转发给22.2，随后防火墙转发给实例1收到后直连路由不用静态。



图3 - 11 PC2-PC4交换机静态路由

防火墙上配置如下路由，防火墙的虚拟系统1收到前往40.0网段路由后转发给虚拟系统2，虚拟系统2收到后转发给22.1。

回程路径虚拟系统2收到前往10.0网段路由后转发给虚拟系统1，虚拟系统1转发给11.1。



图3 - 12 PC2-PC4防火墙静态路由1

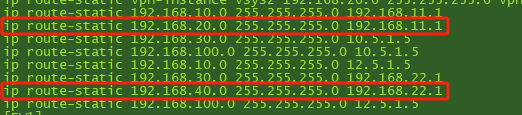


图3 - 13 PC2-PC4防火墙静态路由2

这是PC2pingPC4的现象：

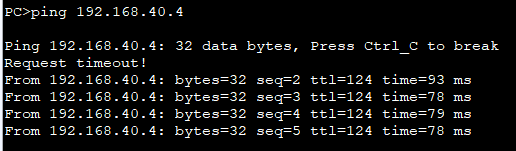


图3 - 14 PC2pingPC4

这是tracert现象：

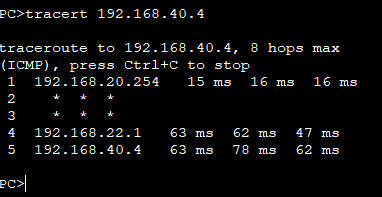


图3 - 15 tracert

# 3.5 PC1、PC2、PC3、PC4访问Server的流量路径控制

SW1上配置如下路由，实例1实例2收到前往100.0网段的路由后分别转发给实例1/2对应的虚拟系统1虚拟系统2，随后防火墙转发给交换机全局，全局收到后不用做静态路由因为直连。

回程路径在全局收到前往PC1234网段的路由后转发给对应实例对应的虚拟系统，再由虚拟系统转发给交换机的实例1/2，然后通过直连路由转发给对应网段。

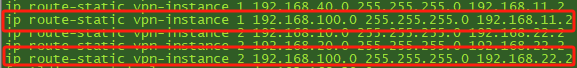


图3 - 16 PC-Server交换机静态路由 1



图3 - 17 PC-Server交换机静态路由2

防火墙上配置如下路由，虚拟系统1、2分别从交换机收到前往100.0网段的路由后转发给交换机的全局。

回程路径无需配置，因为之前已经配置过对应虚拟系统内回到10/20/30/40网段的静态路由，这会转发给交换机对应的实例。

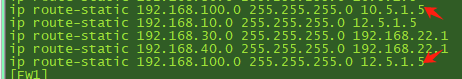


图3 - 18 PC-Server防火墙静态路由

PC1pingServer的现象：

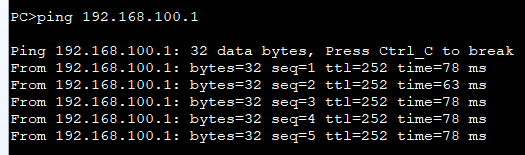


图3 - 19 PC1-Server ping

PC3pingServer的现象：

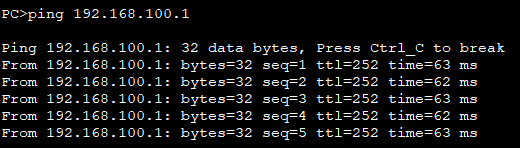


图3 - 20 PC3-Server ping

两者的tracert现象：

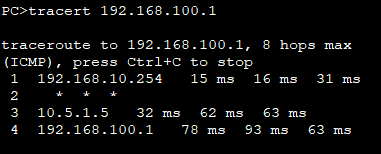


图3 - 21 PC1-Server tracert

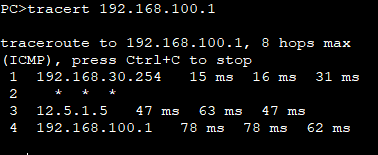


图3 - 22 PC3-Server tracert

# 结论

# 4.1 遇到的问题

该次实验，我感到一定的不熟练，加上vlan实验长时间未配置，导致一些低级错误的产生，外加上防火墙的策略一开始我十分混淆，源目区域源目地址的规划不合理，浪费了长时间在构思策略上，加上首次对防火墙配置如此多的命令，算是正式的开始配置防火墙，以至于很多问题的产生需要我不断地switch虚拟系统，外加二层三层接口时不时地混淆，导致一开始虽在交换机上配置了trunk口，但是在防火墙上的三层接口切换为二层接口耗费了一段时间，但其实最多的问题还是在虚拟系统之间的路由配置和该创建多少vlanif上，最后还是迎刃而解了。

# 4.2 心得体会

此次实验对有一定的逻辑性，需要静心配置以及思考流量的路径该如何选择，初始不熟练的时候要想上许久的时间，熟悉后才开始得心应手，这确实提升了我对流量的感知，这也是张总要我们一开始配置静态的初心，对我的提升很大，也让我对防火墙配置有一定的熟练度，也再次熟稔了交换机的配置。