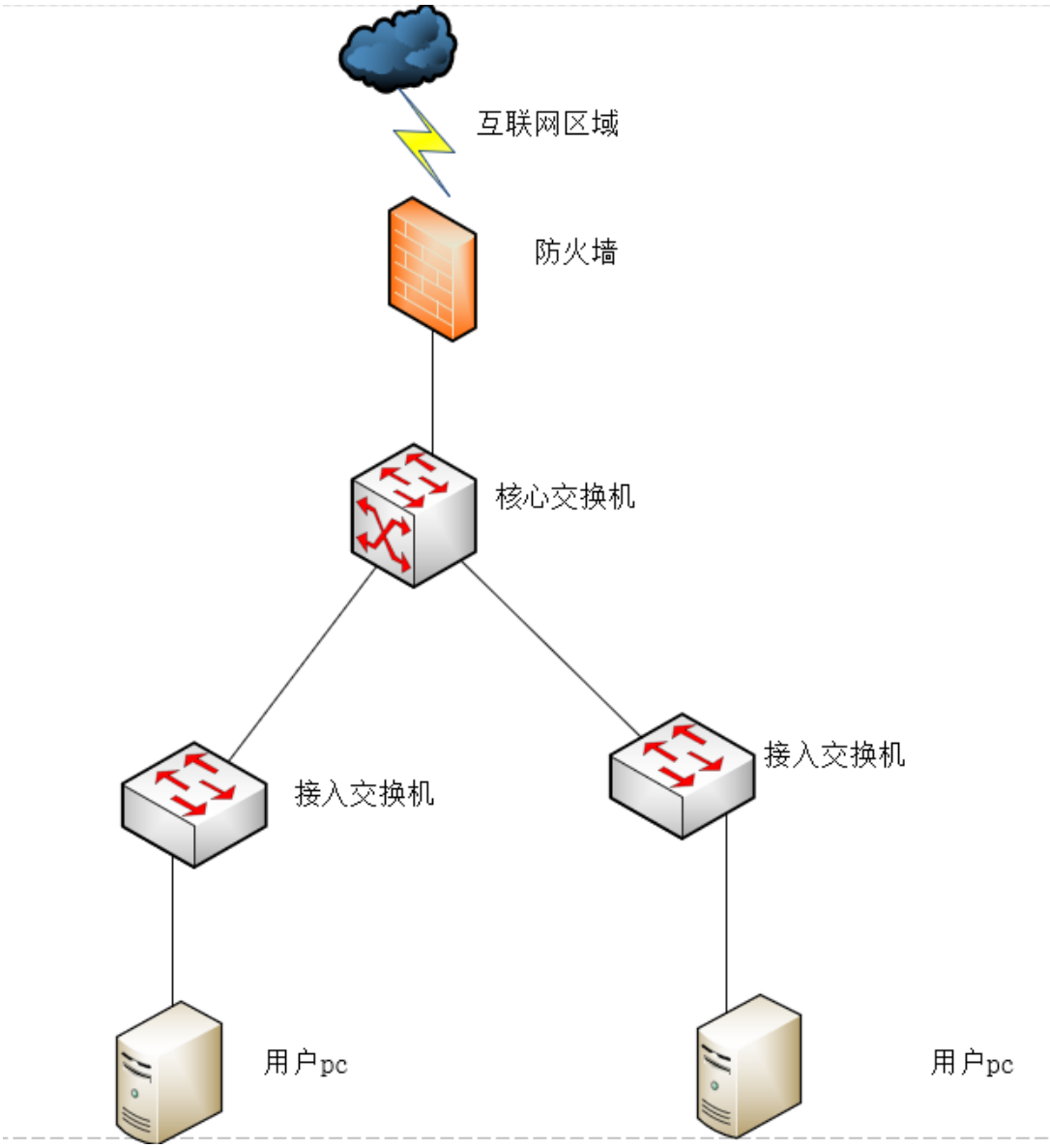
流量分析

笔记本： 应急
创建时间： 2022/10/18 9:12

1、概述

最近遇到的一个案例，某用户被监管机构通报，该企业内网存在一僵尸木马向境外某一ip发起访问，用户在接到通报后进行分析，进行内网排查，内网情况如下：
1、被通报的公网出口，主要是办公网出口，内网办公电脑大约200多台；
2、边界安全设备存在一台防火墙，但是防火墙没有上网行为管理功能，其访问日志记录的也不全；
3、内网内没有其他安全设备进行日志记录；
综合用户的描述，简单画出如下拓扑图，



从图中可看到，核心交换机上先是进行了vlan划分，然后用户被分为了不同的网段，最后通过防火墙出口访问互联网。

通报中也已经明确给出了，僵尸木马攻击的目标地址，常规思路是通过查看边界网络安全设备，确定是内网的哪个ip地址访问了目标地址，但是奈何内网没有能查看该条日志的设备，所以很难通过这个思路进行，客户内网机器上都装有杀毒软件，通过联系厂商，未发现相关杀毒软件的记录日志。

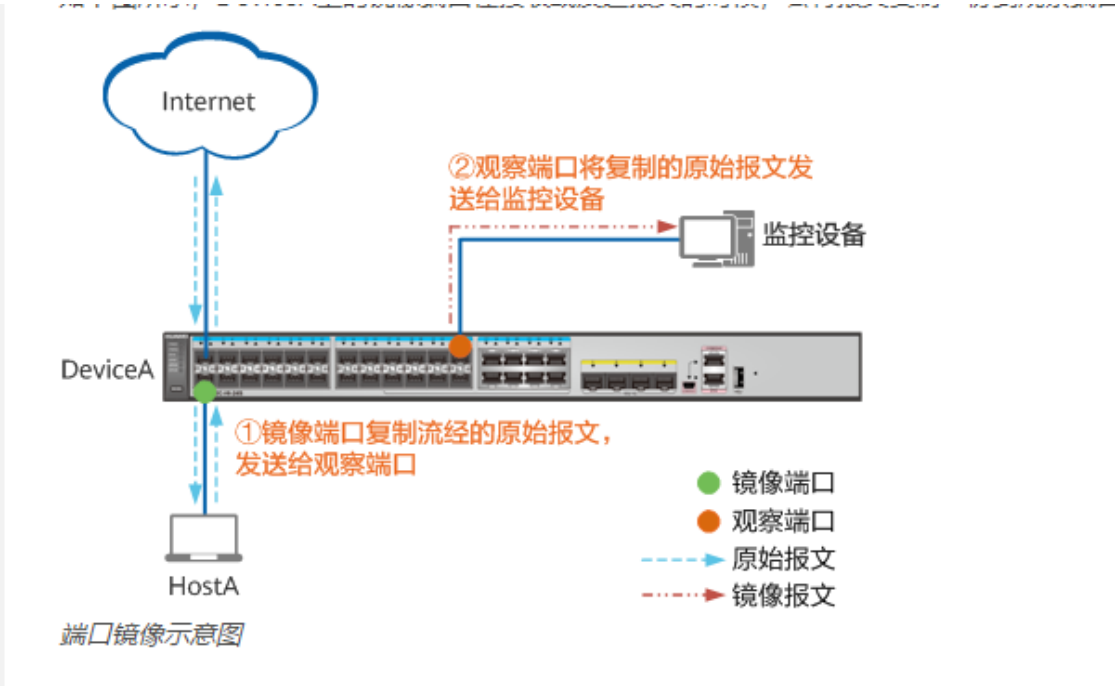
在遇到这种情况下怎么取处理呢，还有一种方法就是每台主机进行排查，但是200多台机器排查起来也是很费劲的，这时候可采用如下方法进行排查。

2、核心交换机进行端口镜像

镜像可以在不影响报文正常处理流程的情况下，将镜像端口的报文复制一份到观察端口，用户利用数据监控设备来分析复制到观察端口的报文，进行网络监控和故障排除。

端口镜像是将网络设备上指定端口接收或发送的报文复制到目的端口，可以只复制端口接收或者发送的报文，也可以同时复制接收和发送的报文。

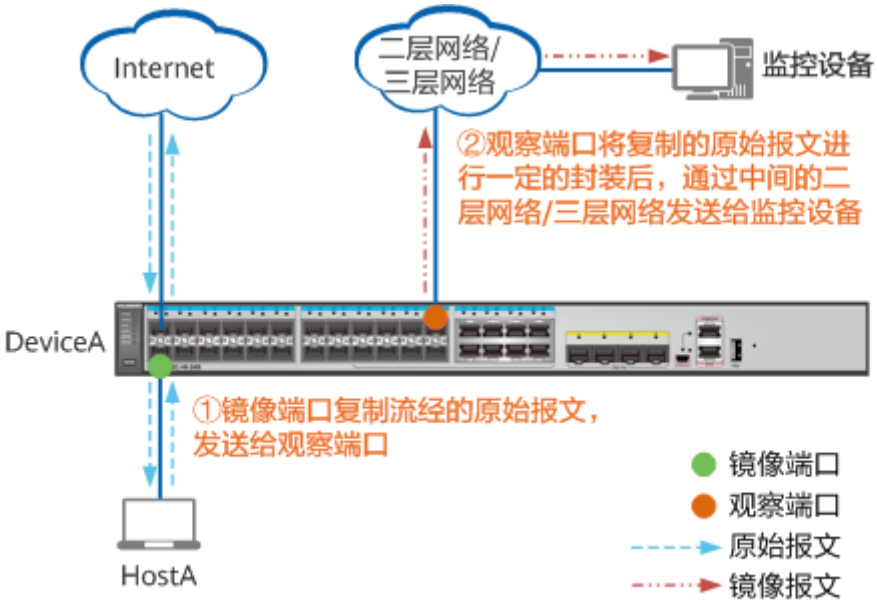
镜像可以在不影响交换机/路由器等网络设备报文正常处理流程的情况下，将指定源的报文复制一份到目的端口。目的端口与监控设备直接或间接相连，监控设备上安装了分析软件，可以对报文进行分析。当网络中存在攻击或出现故障时，网络管理员可以通过镜像功能对报文进行获取并分析，找到攻击源或故障原因。根据镜像源的不同，镜像可以分为端口镜像、流镜像、VLAN镜像、MAC镜像。例如端口镜像代表将指定端口入方向、出方向、或者出入方向的报文复制到目的端口。根据目的端口与监控设备间的连接方式，镜像可以分为本地镜像和远程镜像。
在核心交换机上采用了vlan划分的情况下，可进行vlan镜像，针对每个vlan进行分析，端口镜像工作示意图



端口镜像示意图

端口镜像是将网络设备上指定端口接收或发送的报文复制到目的端口，可以只复制端口接收或者发送的报文，也可以同时复制接收和发送的报文。指定端口称为镜像端口，目的端口称为观察端口。

当观察端口和监控设备直连时称为本地镜像。当观察端口和监控设备间不是直连，而是通过二层网络或三层网络相连时称为远程镜像。
目的端口通过二层网络与监控设备相连的场景称为二层远程镜像RSPAN（Remote Switched Port Analyzer）。目的端口通过三层网络与监控设备相连的场景称为三层远程镜像ERSPAN（Encapsulated Remote Switched Port Analyzer）。
如下图所示，远程端口镜像场景，观察端口将复制的报文发送给监控设备前会添加一层VLAN Tag或进行GRE封装，便于复制的报文能够穿过中间的二层网络/三层网络，到达监控设备。



远程端口镜像示意图

关于配置端口镜像的方法，不同的设备有不同的方法，就不在赘述，可参考具体设备的配置手册，下面连接给出了部分设备的配置手册

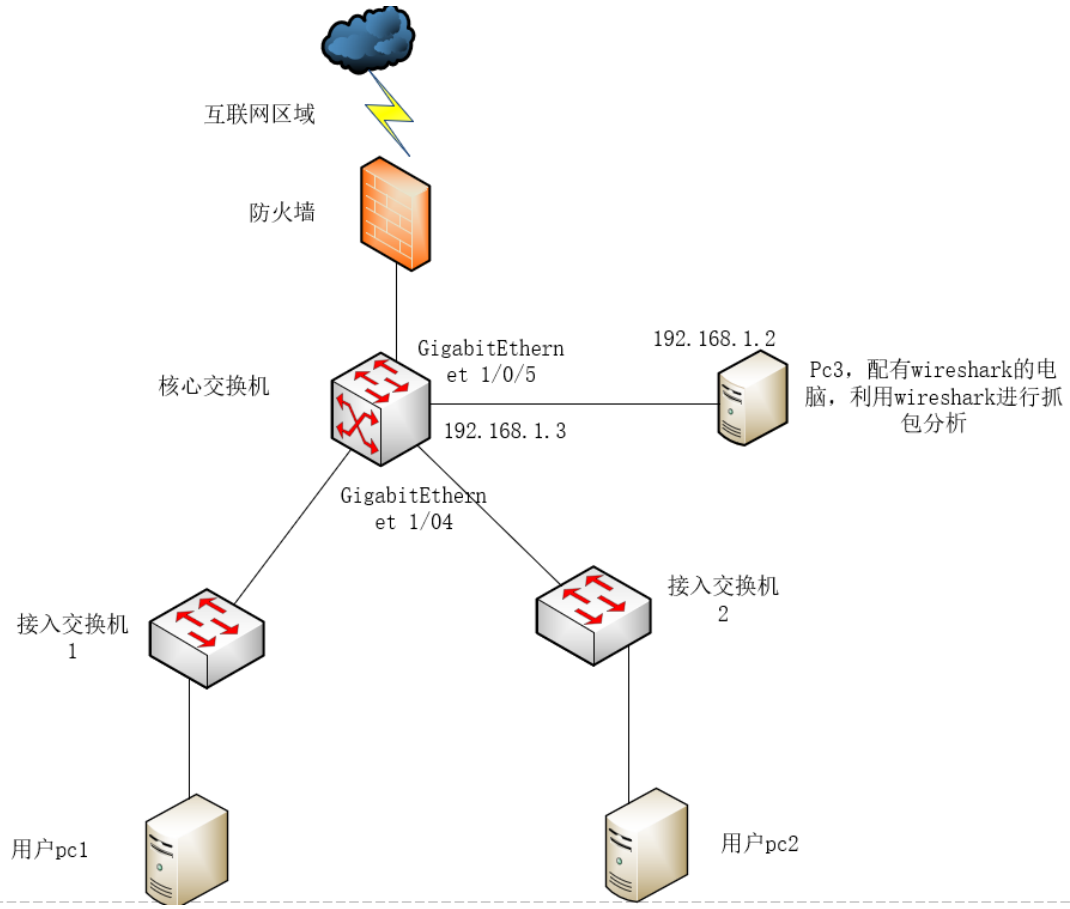
华为设备

备;https://support.huawei.com/enterprise/zh/doc/EDOC1100038439/5883765f

华三设备：

https://www.h3c.com/cn/d_201912/1249732_30005_0.htm#_Toc25856220

接下来重点说下，配置好端口镜像后如何进行抓包，如采用如下拓扑图

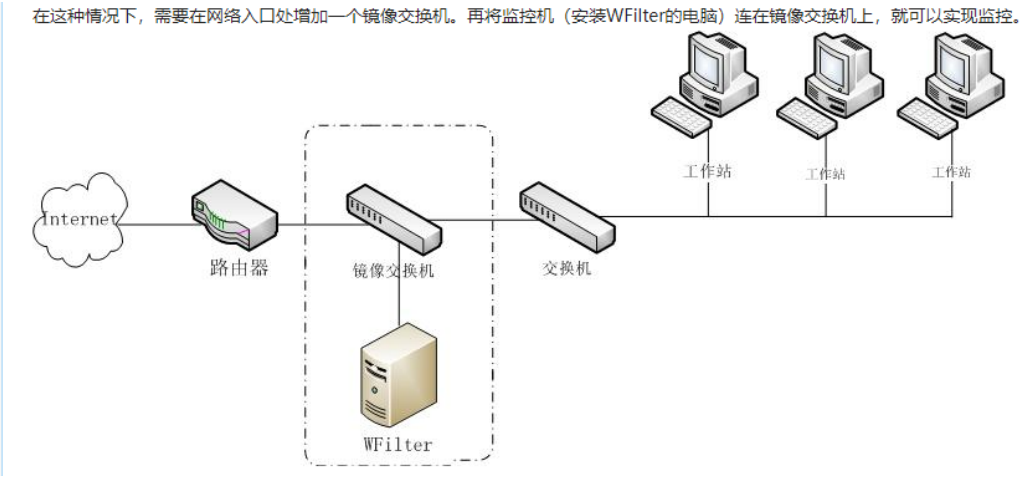


目的是实现，在核心交换机上抓取通过接入交换机2的流量，也就是端口4的流量，设置端

口4是源端口，端口5为目的端口IP地址为192.168.1.3，设置后好pc3装有wireshark等抓包工具，pc3连接端口5，并设置pc3 IP地址为192.168.1.2，此时观察wireshark可发现来自交换机2的数据流量。
通过这种方法就能通过抓到的数据包进行分析定位，判断是哪台机器出现了恶意链接，进而抓取恶意文件所在的机器。
这种方法还是相对比较好用的，但是存在的问题就是当应急处理完成后要及时将端口镜像取消，防止流量过大造成交换机卡顿。

3、其他软件

WFilter：
在搜索时在网上发现了另一个软件，WFilter感觉和wireshark类似，他的部署环境如下，也是分析的镜像端口的流量，通过对镜像端口的流量进行分析，分析局域网内的上网行为，好处是它是图形化页面展示，分析结果相对会更直观



它默认有10天的试用期，由于我是安装到虚拟机的，所以只能抓到我本机的一些的流量通信情况

感觉和wireshark原理类似，只是展示效果更直观一些，可视化更强。
科来分析系统：
科来网络分析系统相对都比较熟悉了，功能也强大，也是对流量进行分析，但是前提也是

基于流量进行分析，看网上有技术交流版
https://www.colasoft.com.cn/download/capsa.php

4、小结：

基于网上查的一些资料，都是要先获取相关流量然后在对流量进行分析，流量分析的软件有很多，难点就是如何获取相关流量，如果有安全设备、流量审计设备最好，直接就可以查看相关日志，但是没有的话就只能通过端口镜像等方式获取流量，然后在进行分析了，基于端口镜像是进行实时流量的分析，是无法查看历史流量了，所以感觉最靠谱的方式还是日志保存。