首页 Cisco 微语 HuaWei H3C 网工工具 网工经验 进制转换 运营商IP段 报文格式大全 手气不错

如何判断交换机是否受到ARP攻击以及处理方式

时间：2015-10-21 16:18 评论：0 条

如何判断交换机是否受到ARP攻击以及处理方式

一、如果网络受到了ARP攻击，可能会出现如下现象：

1、用户掉线、频繁断网、上网慢、业务中断或无法上网。

2、设备CPU占用率较高、设备托管、下挂设备掉线、设备主备状态震荡、设备端口指示灯红色快闪。

3、Ping有时延、丢包或不通。

定位ARP攻击时，请先排除链路、环路或路由问题，排除后再执行下面的步骤。执行过程中请保存以下步骤的执行结果，以便在故障无法解决时快速收集和反馈信息。

1、在网关上执行命令display cpu-defend statistics all，查看ARP Request、ARP Reply或ARP Miss报文的“Drop”计数是否增长。

如果计数为0，设备没有丢弃ARP报文。

如果有计数，表示设备收到的ARP报文由于超过了CPCAR的速率限制而被丢弃。

如果是ARP Miss报文丢弃很多，设备很可能受到了ARP Miss攻击。

如果是ARP Request或ARP Reply报文丢弃很多，设备很可能受到了ARP Request或ARP Reply报文攻击。

2、在网关上执行命令display arp all，查看用户的ARP表项是否存在。

如果ARP表项还在，请再查看用户的ARP表项，然后确定是否有用户或网关的ARP表项被改变。

如果是网关上用户ARP表项被改变，设备受到了ARP欺骗网关攻击。

在设备与用户连接的接口上获取报文头，分析ARP报文的源地址，找出攻击者。

建议找出攻击者后进行杀毒或卸载攻击工具。也可以在网关设备上配置防攻击功能，请根据情况选择配置。

3、系统视图下执行命令arp static，配置静态ARP表项。

如果下挂用户较少，可以通过配置静态ARP表项，绑定MAC地址和IP地址，确保IP地址不会被伪用户盗用。

4、系统视图或接口视图下执行命令arp anti-attack entry-check { fixed-mac | fixed-all | send-ack } enable，配置ARP表项固化功能。

fixed-mac方式适用于用户MAC地址固定，但用户接入位置频繁变动的场景。当用户从不同接口接入设备时，设备上该用户对应的ARP表项中的接口信息可以及时更新。

fixed-all方式适用于用户MAC地址固定，并且用户接入位置相对固定的场景。

send-ack方式适用于用户的MAC地址和接入位置均频繁变动的场景。

二、处理方式：

1、配置黑名单或黑洞MAC对攻击源的报文进行丢弃处理。

如果是用户的网关ARP表项被改变，设备受到了ARP仿冒网关攻击。

在设备与用户连接的接口上获取报文头，分析ARP报文的源地址，找出攻击者。

建议找出攻击者后进行杀毒或卸载攻击工具。也可以在网关设备上配置防攻击功能，请根据情况选择配置。

2、在网关的下行接口配置端口隔离，防止同一VLAN的用户收到攻击的ARP。

系统视图下执行命令arp anti-attack gateway-duplicate enable，使能ARP防网关冲突攻击功能。

3、在接口或VLAN视图下执行命令arp anti-attack check user-bind enable，使能动态ARP检测功能（即对ARP报文进行绑定表匹配检查功能）。

动态ARP检测功能主要用于防御中间人攻击的场景，避免合法用户的数据被中间人窃取。

4、在系统视图下执行命令arp anti-attack packet-check { ip | dst-mac | sender-mac }*，使能ARP报文合法性检查功能，并指定ARP报文合法性检查项。

配置后，还需应用该防攻击策略才能生效。

用户视图下执行命令display arp anti-attack configuration arp-speed-limit，查看是否配置了ARP报文限速。

系统视图下执行命令arp speed-limit source-ip [ip-address] maximum maximum，调整根据源IP地址进行ARP报文限速的限速值。

系统视图下执行命令arp speed-limit source-mac [mac-address] maximum maximum，调整根据源MAC地址进行ARP限速的限速值。

系统视图、VLAN视图或接口视图下执行命令arp anti-attack rate-limit packet packet-number，调整ARP报文的限速值。

正文部分到此结束

上一篇 交换机配置文件备份与恢复示例 MAC地址理论知识与配置步骤 下一篇

相关文章

最简单的MAC地址大小比较方法
ARP理论知识详解（三）
ARP配置教程（三）
ARP配置教程（二）
路由式ARP Proxy（arp代理）配置示例
华为交换机静态ARP与动态ARP结合使用配置示例
如何判断交换机是否受到ARP攻击以及处理方式
华为交换机VLAN之间Proxy ARP示例
服务器集群（多端口）ARP配置示例
华为交换机VLAN内Proxy ARP配置示例

交换机 arp攻击 处理方式

二维码加载中...技术交流：欢迎在本文下方留言或加入QQ群:859273036 互相学习。

本文地址：http://www.023wg.com/arp/34.html

版权声明：若无注明，本文皆为“Swiers思唯网络博客”原创，转载请保留文章出处。

昵称

邮件地址 (选填)

个人主页 (选填)

发表评论

清歌妙音

热门文章

- 华为交换机ping命令详解
- 华为交换机CPU占用率高原因判...
- 华为交换机堆叠介绍（一）
- ping丢包故障处理方法
- 华为交换机SSH（stelnet...
- 最全的华为交换机vlan配置教程
- 最新国内各运营商（ISP）IP段...
- 华为策略路由详解
- 华为交换机CPU占用率高原因判...

随机文章

- 思唯网络VIP学员学习特权 思科...
- 【思唯网络】CISCO VRRP...
- 【思唯网络】CISCO VRRP...
- 【思唯网络】华为通用路由封装...
- 【思唯网络】华为通用路由封装...
- 【思唯网络】HSRP（热备份路由...
- 【思唯网络】网络故障排查之tra...
- 【思唯网络】HSRP+DHCP实...
- 【思唯网络】华为交换机系统启...

分类

- 思唯动态（2）
- Cisco（1）
- HuaWei（3）
  - 基础配置（59）
  - 路由配置（60）
  - 组播配置（24）
  - 破坏配置（9）
  - 故障处理（18）
  - 可靠性配置（17）
  - VPN（9）
  - QoS（15）
  - ACL（8）
  - ARP（15）
  - VLAN（34）
- H3C（1）
- 网工工具（2）
- 视频教程（0）
- 网工经验（6）

标签

arp欺骗 1篇 Tracert 1篇 AS_Path 1篇
拥塞管理 2篇 cac 3篇 离职 1篇
console配置 2篇 交换机监控 1篇
历史命令 1篇 华为路由器 4篇
BFD配置 1篇 默认密码 1篇
vlink-peer 1篇 e-trunk 1篇
网络环路 1篇 log 2篇 客户端 1篇
日志 2篇 BGP与BFD 1篇 GR 3篇
UP 1篇 域名系统 1篇 组播协议 1篇
QoS 15篇 crc 1篇 IS-IS主机名映射 1篇
报文 1篇 网络工程师 6篇 经验 2篇
radius 1篇 模拟器 1篇 icmp 1篇
BGP平滑重启 1篇 单板重启 1篇
命令行帮助 1篇 svf 1篇

最新评论

enomothem 说:
是的，证书需要于你的实力匹配

墨殃 说:
谢谢楼主分享很详细 祝您工作愉快

冰尘 说:
我当年上学的时候也这么考虑过，不过没有你...

你好 说:
在交换机B上ping 172.16.2网...

随梦而追 说:
博主大人您好，我是2017年毕业的小伙子...

燃灯大师 说:
我刚好参加此次比赛

曲别针 说:
多谢分享，赞!

agony 说:
谢谢，受益匪浅

陈Huid 说:
谢谢分享

美股指数 说:
谢谢您的分享!