S7500交换机防arp攻击特性

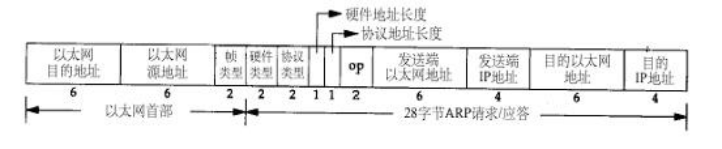
杨超 2007-12-26 发表

S7500交换机防arp攻击特性

一、 ARP协议及ARP攻击类型

1. ARP协议简介

ARP协议提供了从硬件地址（MAC地址）到三层地址（IP地址）之间的对应。通常情况下，当设备收到arp报文后，会更新相应arp表项。



ARP报文中帧类型字段固定为0x0806，硬件类型字段指明了发送方想知道的硬件接口类型，以太网的值为1。协议类型字段指明了发送方提供的高层协议类型，IP为0x0800。硬件地址长度和协议长度指明了硬件地址和高层协议地址的长度，这样ARP报文就可以在任意硬件和任意协议的网络中使用。操作字段用来表示这个报文的目的，ARP请求为1，ARP响应为2，RARP请求为3，RARP响应为4。除了目的以太网地址外，其他字段都要有填充值。

当发出ARP请求时，发送方填好发送方首部和发送方IP地址，还要填写目标IP地址。当目标机器收到这个ARP广播包时，就会在响应报文中填上自己的48位主机地址。ARP还包括有免费ARP和代理ARP。

2. ARP攻击

如果有一个不被信任的节点对本地网络具有写访问许可权，那么也会有某种风险。这样一台机器可以发布虚假的ARP报文并将所有通信都转向它自己，然后它就可以扮演某些机器，或者顺便对数据流进行简单的修改。

2.1. 假冒ARP应答

假冒的B主动向A发应答包，这时A会更新其ARP表中主机B的MAC地址。主机A向主机B的所有主动的通讯都将中断。我司交换机在ARP老化之前，会向其目的主机发送ARP请求，如果假冒的B的IP地址与实际B的IP地址不同，则交换机中的ARP会老化掉。如果假冒的B的IP地址与实际B的IP地址相同，则会出现IP相同的报警信息，因此在真实的B未向A主动发送报文的情况下，假冒ARP造成的中断会在ARP老化时间内起作用。

2.2 点对点的假冒查询

假冒的主机A点对点方式直接向主机B发送单播的ARP查询包，主机B收到主机A的查询包后，会更新MAC地址缓冲区中主机A的MAC地址。主机B主动向主机A的所有IP通讯都将中断。同样造成的中断会在ARP老化时间内起作用。

2.3 定时ARP欺骗

由于假冒ARP造成的中断会在ARP老化时间内起作用，且被假冒的主机主动向其他主机发送报文后，也会使通信正常，为了使得欺骗能持续更长时间，因此在MAC地址更新前再次发送ARP欺骗包。

2.4 对网关的干扰

如果在以太网上发送一个IP地址为网关的免费ARP欺骗包，则使得这个网上的主机都不能访问这个局域网外的所有IP。

二、S7500交换机防ARP攻击的策略

1 IP和MAC地址绑定

我司设备支持配置IP地址和mac地址已经vlan、接口的绑定

[H3C]arp static 10.10.12.20 0013-3042-1820

使用该方法可以防止arp仿冒，但是该方法对用户地址频繁变化的场合不适用。

2 ARP源抑制功能

如果网络中有主机通过向交换机发送大量目的IP地址不能解析的IP报文来攻击交换机，会增加CPU的负担，也会增加目的网段的负载。

为避免这种攻击所带来的危害，系统提供了ARP源地址抑制功能。缺省情况下， ARP源抑制功能是开启的。交换机在单位时间间隔内可以接收到的源IP地址相同，本地ARP最多为3个，过路ARP为3个，总共ARP数量为100个，可以通过命令修改阈值：

[H3C]arp source-suppression limit ?

local Specify ARP source suppression limit that destination IP is local

through Specify ARP source suppression limit that destination IP isn't local

total Specify ARP source suppression limit

3 限制全局和端口下arp表的大小

交换机支持限制在全局和端口下学习arp表项的最大值。

[H3C]arp max-entry ?

INTEGER<4096-8192> Value of maximum ARP entry number

缺省值是8K。

[H3C]inter g 5/0/1

[H3C-GigabitEthernet5/0/1]arp max-dynamic-entry ?

INTEGER<0-8192> Value of maximum port dynamic ARP entry number

缺省值是2K。设置的阈值可以由下面的命令察看：

[H3C]dis arp entry-limit

The maximum ARP entry number is 8192

The maximum dynamic ARP entry number of the port GigabitEthernet0/0/1 is 2048

The maximum dynamic ARP entry number of the port GigabitEthernet0/0/2 is 2048

The maximum dynamic ARP entry number of the port GigabitEthernet0/0/3 is 2048

The maximum dynamic ARP entry number of the port GigabitEthernet0/0/4 is 2048

The maximum dynamic ARP entry number of the port Ethernet2/0/1 is 2048

The maximum dynamic ARP entry number of the port Ethernet2/0/2 is 2048

The maximum dynamic ARP entry number of the port Ethernet2/0/3 is 2048

The maximum dynamic ARP entry number of the port Ethernet2/0/4 is 2048

The maximum dynamic ARP entry number of the port Ethernet2/0/5 is 2048

The maximum dynamic ARP entry number of the port Ethernet2/0/6 is 2048

此方法可以防范ARP table attacks:

[H3C]dis arp attack-list

MAC ADDR VLAN IP ADDR PORT NAME LAST-ATTACK COUNT

4 限制相同MAC不同IP的ARP学习个数

[H3C]arp mac-arp-map limit ?

INTEGER<1-8192> Attack list of the ARP attacker

默认相同的MAC对应的不同IP不能超过2个。可以通过dis arp attack-list命令查看超出限制的表项。

该命令在V3.10 R3133及之后版本才提供，可以防止对仿冒其它用户的arp欺骗。但是对于存在nat转换或者F5均衡设备的网络，以及VRRP有多个备份组时，BACKUP会把收到免费ARP当成攻击报文处理, 另外还存在与SUPER VLAN配合使用的问题等。

5 通过ACL 5000限制禁止某些异常用户仿冒网关

对于非ft48e的bcm单板

acl number 5000

rule deny 0806 ffff 16 网关ip地址（16进制） ffffffff 32

对于ft48e单板

acl num 5000

rule deny 0806 ffff 20 网关ip地址（16进制） ffffffff 36

在所有与终端直连的端口配置。

例如网关地址为192.168.1.1 防止e4/0/1端口下设备仿冒网关的配置为

对于非ft48e的bcm单板：

acl num 5000

rule 0 deny 0806 ffff 16 c0a80101 ffffffff 32

对于ft48e单板：

acl num 5000

rule 0 deny 0806 ffff 20 c0a80101 ffffffff 36

ft48e比其他单板多偏移4个字。

6 限制单位时间内上送接口板cpu的arp报文数量

75交换机在软件上还有softcar机制，软件限制单位时间内上送接口板CPU的arp报文的数目。