关于S8500系列交换机 ARP防攻击的一种方法

齐楠 2006-02-08 发表

S8500 ARP防攻击的一种方法

ARP攻击简介

这里，我们将利用ARP报文发起的攻击的行为，统称为“ARP攻击”，其常见的攻击方式有如下两种：

其一，由于ARP协议没有任何验证方式，在网络监听过程中，攻击者抢先合法目的主机应答源主机发起的ARP请求，源主机被误导建立一个错误的映射并保存一段时间，在这段时间内，源主机发送给目的主机的信息被误导致攻击者。如果攻击者模拟网络出口路由器发动ARP攻击，内部网络的所有出口信息都将被接管。

其二：攻击者向三层交换机发送大量的ARP报文，由于设备的处理能力和资源有限，当冲击设备的报文达到一定数量的时候，会导致合法主机的ARP报文被“淹没”于其中而得不到处理，结果无法生成正常的ARP表项，从而导致三层转发异常。

从实施难度和危害程度来说，第二种方式操作较为容易，并且危害也更为严重，也是我们在交换机侧需要予以重点关注和预防的攻击方式，因此我们这里所说的ARP攻击，特指这种攻击方式。

S8500 ARP防攻击机制

为了增加产品的健壮性，S8500设计并实现了ARP的攻击检测及抑制功能，该功能通过以下命令进行控制：

anti-attack arp {enable | disable }

当使能了该功能后，系统自动检测冲击设备的ARP报文，在检测到攻击报文时，提取出该报文的源MAC，然后自动下发一条抑制表项，在一段时间内抑制相同源MAC的报文转发。抑制定时器超时后，自动解除，恢复转发。

其次，我们可以通过使用ACL规则对各端口接收到的ARP报文进行流量监管，下面采用一个实际的例子给大家示范一下。如果S8500上的Ethernet2/1/7受到了ARP攻击，我们可以采用下面的配置步骤解决这个问题：

1、配置流模板如下：

[8512D]flow-template user-defined ethernet-protocol ip-protocol

2、配置ACL规则如下：

[8512D]acl name robust_arp link

[8512D-acl-link-robust_arp]rule permit arp

3、在受攻击的端口E2/1/7上，利用ACL规则下发流量监管功能。

[8512D-Ethernet2/1/7]flow-template user-defined

[8512D-Ethernet2/1/7]raffic-limit inbound link-group robust_arp 128 512 512 exceed drop

在端口上进行这样的配置可以使其他端口的用户在该端口受到ARP攻击之后，本端口的ARP学习不受影响。

我们通过灵活运用ARP防攻击功能和流量监管，85对于ARP攻击是可以有效预防的。