防止同网段arp欺骗攻击配置

彭天付 2006-04-25 发表

防止同网段ARP欺骗攻击的配置方法

二层交换机实现仿冒网关的ARP防攻击：

一、组网需求：

1. 二层交换机阻止网络用户仿冒网关IP的ARP攻击

二、组网图：

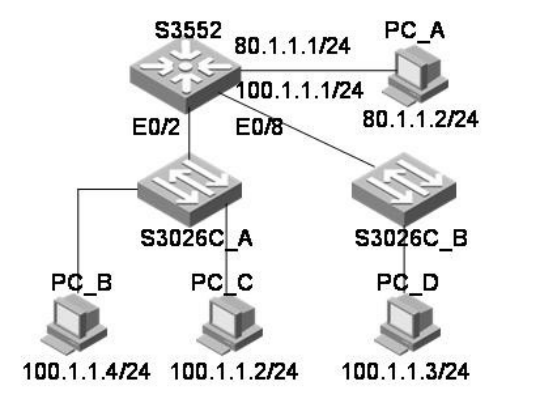

图1二层交换机防ARP攻击组网

S3552P是三层设备，其中IP：100.1.1.1是所有PC的网关，S3552P上的网关MAC地址为000f-e200-3999。PC-B上装有ARP攻击软件。现在需要对S3026C_A进行一些特殊配置，目的是过滤掉仿冒网关IP的ARP报文。

三、配置步骤

对于二层交换机如S3026C等支持用户自定义ACL（number为5000到5999）的交换机，可以配置ACL来进行ARP报文过滤。

全局配置ACL禁止所有Sender ip address字段是网关IP地址的ARP报文

acl num 5000

rule 0 deny 0806 ffff 24 *64010101* ffffffff 40

rule 1 permit 0806 ffff 24 *000fe2003999* ffffffffffff 34

其中rule0把整个S3026C_A的端口冒充网关的ARP Reply报文禁掉，其中斜体部分64010101是网关IP地址100.1.1.1的16进制表示形式。Rule1允许通过网关发送的ARP报文，斜体部分为网关的mac地址000f-e200-3999。

注意：配置Rule时的配置顺序，上述配置为先下发后生效的情况。

在S3026C-A系统视图下发acl规则：

[S3026C-A] packet-filter user-group 5000

这样只有S3026C_A上连网关设备才能够发送网关的ARP报文，其它主机都不能发送假冒网关的arp响应报文。

三层交换机实现仿冒网关的ARP防攻击

一、组网需求：

1. 三层交换机实现防止同网段的用户仿冒网关IP的ARP攻击

二、组网图

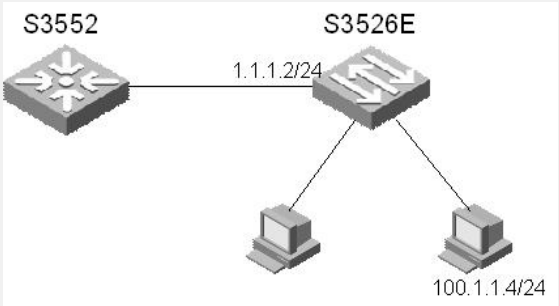

图2 三层交换机防ARP攻击组网

三、配置步骤

1. 对于三层设备自己作为网关，需要配置过滤Sender ip address字段是网关的ARP报文的ACL规则，配置如下ACL规则：

acl number 5000

rule 0 deny 0806 ffff 24 *64010105* ffffffff 40
rule0禁止S3526E的所有端口接收冒充网关的ARP报文，其中斜体部分64010105是网关IP地址100.1.1.5的16进制表示形式。
2. 下发ACL到全局
[S3526E] packet-filter user-group 5000

仿冒他人IP的ARP防攻击
一、组网需求：
作为网关的设备有可能会出现错误ARP的表项，因此在网关设备上还需对用户仿冒他人IP的ARP攻击报文进行过滤。
二、组网图：
参见图1和图2
三、配置步骤：
1. 如图1所示，当PC-B发送源IP地址为PC-D的arp reply攻击报文，源mac是PC-B的mac (000d-88f8-09fa)，源ip是PC-D的ip(100.1.1.3)，目的ip和mac是网关（3552P）的，这样3552上就会学习到错误的arp，如下所示：
---------- 错误 arp 表项 ----------
IP Address MAC Address VLAN ID Port Name Aging Type
100.1.1.4 000d-88f8-09fa 1 Ethernet0/2 20 Dynamic
100.1.1.3 000f-3d81-45b4 1 Ethernet0/2 20 Dynamic
从网络连接可以知道PC-D的arp表项应该学习到端口E0/8上，而不应该学习到E0/2端口上。但实际上交换机上学习到该ARP表项在E0/2。上述现象可以在S3552上配置静态ARP实现防攻击：
arp static 100.1.1.3 000f-3d81-45b4 1 e0/8
2. 在图2 S3526C上也可以配置静态ARP来防止设备学习到错误的ARP表项。
3. 对于二层设备（S3050C和S3026E系列），除了可以配置静态ARP外，还可以配置IP+MAC+port绑定，比如在S3026C端口E0/4上做如下操作：
am user-bind ip-addr 100.1.1.4 mac-addr 000d-88f8-09fa int e0/4
则IP为100.1.1.4并且MAC为000d-88f8-09fa的ARP报文可以通过E0/4端口，仿冒其它设备的ARP报文则无法通过，从而不会出现错误ARP表项。
四、配置关键点：
此处仅仅列举了部分Quidway S系列以太网交换机的应用。在实际的网络应用中，请根据配置手册确认该产品是否支持用户自定义ACL和地址绑定。仅仅具有上述功能的交换机才能防止ARP欺骗。