SecPathF1800-A 防火墙0332.28(08)BT限流典型配置

雷浩【技术大咖】 2006-08-31 发表

F1800-A 防火墙BT限流典型配置

一、组网需求：

两个PC,PC1作为BT客户端下载。PC2作为BT的服务器。

PC2上安装BT服务器软件 MYBT SERVER。PC2和PC1上分别安装一个BT客户端软件，如BITTORRENT 4.0。

对于trust-untrust域间ip为2.2.2.2用户除外的所有用户做BT限流，10:00~10:05的带宽为 400kbps，其他时间为 200kbps 。

二、组网图

F1800-A VRP版本：0332.26(08)

三、配置步骤：

```
[F1800-A]display current-configuration
#
acl number 2001                    // 定义ACL组
 rule 0 deny source 2.2.2.2 0
 rule 1 permit
#
 sysname F1800-A
#                                  // 域间安全策略
 firewall packet-filter default permit interzone local trust direction inbound
 firewall packet-filter default permit interzone local trust direction outbound
 firewall packet-filter default permit interzone local untrust direction inbound
 firewall packet-filter default permit interzone local untrust direction outbound
 firewall packet-filter default permit interzone local dmz direction inbound
 firewall packet-filter default permit interzone local dmz direction outbound
 firewall packet-filter default permit interzone trust untrust direction inbound
 firewall packet-filter default permit interzone trust untrust direction outbound
 firewall packet-filter default permit interzone trust dmz direction inbound
 firewall packet-filter default permit interzone trust dmz direction outbound
 firewall packet-filter default permit interzone dmz untrust direction inbound
 firewall packet-filter default permit interzone dmz untrust direction outbound
#
 bypass switch-back auto
#
 firewall mode route                // 防火墙工作模式
#
 firewall statistic system enable
 firewall p2p-car default-permit     // 打开BT限流功能
 firewall p2p include bt
 firewall p2p include edonkey
 firewall p2p include thunder
 undo firewall p2p include fasttrack
 undo firewall p2p include gnutella
 undo firewall p2p include pplive
 undo firewall p2p include ppstream
 undo firewall p2p include bt-dht
 undo firewall p2p include edk-kad
 firewall p2p-car class 0 cir 200        // 设定缺省BT带宽
 firewall p2p-car class 0 cir 400 1 timer      // 设定基于时间段的带宽
#
interface Aux0
 async mode flow
 link-protocol ppp
#
interface Ethernet0/0/0
 ip address 2.2.2.1 255.255.255.0
```

```
#
interface Ethernet0/0/1
 ip address 1.1.1.1 255.255.255.0
#
interface Ethernet1/0/0
#
interface Ethernet1/0/1
#
interface Ethernet1/0/2
#
interface Ethernet1/0/3
#
interface Ethernet1/0/4
#
interface Ethernet1/0/5
#
interface Ethernet1/0/6
#
interface Ethernet1/0/7
#
interface GigabitEthernet2/0/0
#
interface GigabitEthernet2/0/1
#
interface NULL0
#
 time-range timer 10:00 to 10:05 daily          // 配置时间段
#
firewall zone local
 set priority 100
#
firewall zone trust                            // 将端口加入安全域
 set priority 85
 add interface Ethernet0/0/0
#
firewall zone untrust                          // 将端口加入安全域
 set priority 5
 add interface Ethernet0/0/1
#
firewall zone dmz
 set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local dmz
#
firewall interzone trust untrust               // 域间配置限流带宽
 p2p-car 2001 class 0 inbound
 p2p-car 2001 class 0 outbound
#
firewall interzone trust dmz
#
firewall interzone dmz untrust
#
aaa
 authentication-scheme default
#
 authorization-scheme default
#
 accounting-scheme default
#
 domain default
```

```
#
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
#
return
```

四、配置关键点：

1）域间安全策略用 packet filter default permit all 配置成全通。

2）设定基于时间端的带宽firewall p2p-car class 0 cir 400 1 timer时，Class number of P2P car需设置与初始的一样（为0）。

3）通过display firewall p2p-car命令，查看限流设置：

```
[F1800-A]display firewall p2p-car
CLASS  ID    STATE    BANDTH(kbps)   TIME-RANGE
0    0    ACTIVE   200
0    1            400        timer
1    0    ACTIVE   100000
2    0    ACTIVE   100000
3    0    ACTIVE   100000
4    0    ACTIVE   100000
5    0    ACTIVE   100000
6    0    ACTIVE   100000
```