连接数限制典型配置

雷浩【技术大咖】 2006-09-13 发表

Eudemon防火墙IP带宽限制配置

一、组网需求:

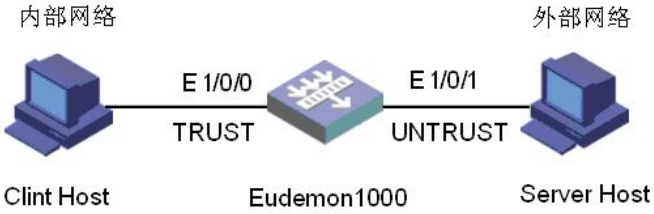
PC两台，Eudemon 1000一台。

Client host地址： 100.1.1.100 在防火墙的trust域。

Server host地址：110.1.1.110 在防火墙的untrust域。

对clint host发起的连接数数量进行限制。

二、组网图:



Eudemon 1000软件版本：VRP 3.30 RELEASE 0336.01(08)

三、配置步骤:

```
[Eudemon]display current-configuration
#
acl number 2000                          //定义基本ACL组
 rule 0 permit source 100.1.1.100 0
#
acl number 3000                          //定义高级ACL组
rule 0 permit udp source 100.1.1.100 0 destination 110.1.1.110 0
#
 sysname Eudemon
#
 firewall mode route
#
 firewall statistic system enable
 firewall conn-class 1 100               // ip连接数等级配置
#
interface Aux0
 async mode flow
 link-protocol ppp
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
#
interface Ethernet1/0/0
 ip address 100.1.1.1 255.255.255.0
#
interface Ethernet1/0/1
 ip address 110.1.1.1 255.255.255.0
#
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
#
firewall zone local
 set priority 100
#
firewall zone trust
 set priority 85
 add interface Ethernet1/0/0
 statistic enable ip outzone                    //使得域IP统计
 statistic ip-stat outbound acl-number 3000   //高级acl来指定要做连接数限制的流
statistic connect-number ip tcp outbound 1 acl 2000//IP 连接数统计限制
#
firewall zone untrust
 set priority 5
 add interface Ethernet1/0/1
#
firewall zone dmz
 set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local dmz
#
firewall interzone trust untrust
#
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:

高级ACL的连接报文进行连接数限制，这主要是为拓宽应用范围，有些应用，需要对由该IP发起的特定连接，或者向该IP发起的特定连接数量进行限制（例如对邮件服务器，有时候要限制外面一个IP对其发起的连接数，否则邮件服务器可能速度很慢，这个有应用实例）。

连接会话数量的多少，可以全局定义7个等级，每个等级可以对应不同的会话数量。使用命令**firewall conn-class** *conn-class conn-num*配置。