

### Eudemon防火墙IP带宽限制配置

#### 一、组网需求：

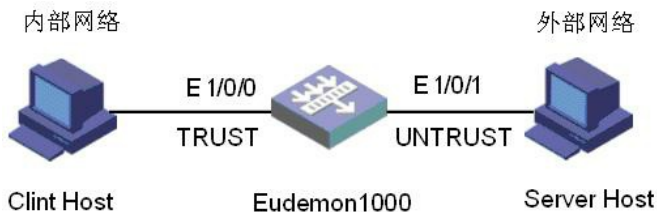
PC两台，Eudemon 1000一台。

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

由client发起去server的tcp连接，对这个流进行带宽限制。

#### 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 tcp source 100.1.1.100 0 destination 110.1.1.110 0
#
sysname Eudemon
#
firewall mode route
#
firewall statistic system enable
firewall car-class 1 100000                    // ip带宽等级配置
#
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 //基本acl来绑定ip带宽配置
statistic car ip outbound 1 acl 2000 //用高级acl来指定要做car的流
#
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：

client发起的到server的tcp连接的带宽限制，双向流量和为100000bps。如果是server发起去client的连接不受上面配置的限制。

```
[Eudemone-zone-untrust]statistic car ip outbound 2 acl 2000
```

指定从untrust域来的特定IP发起的会话的总带宽等级为2，指该IP发起的会话的双向流量之和。比如，如果untrust域穿过防火墙访问WWW服务器，则该会话中去服务器的流量加上WWW服务器回来的流量之和，不会超过设定的带宽等级。

如果服务器是FTP，因为服务器的Port方式下载，其FTP数据通道是由服务器发起，应增加如下配置

```
[Eudemone-zone-untrust]statistic car ip inbound 2 acl 2000
```

才能够限制住该用户的FTP下载流量。

注：IP CAR 中限制的流量，只包含IP包载荷，不包含二层头。

