SecPath1800F SYN攻击防范功能的配置

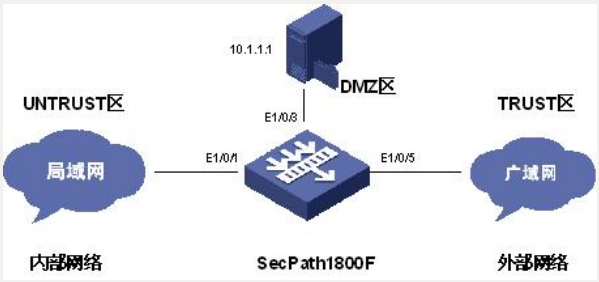
王刚 2006-10-30 发表

SecPath1800F SYN攻击防范功能的配置

一、 组网需求：

SecPath1800F可以阻止基于SYN的攻击防范，保护内部的服务器。

二、 组网图：



三、 配置步骤：

适用版本： SecPath1800F 当前所有版本

```
sysname SecPath
#                                                    // 配置域间规则
 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
#
 firewall mode route
#
 firewall defend syn-flood enable          // 开启syn攻击防范功能
 firewall defend syn-flood zone trust max-rate 600 tcp-proxy on
// 基于域的防范
 firewall defend syn-flood ip 10.1.1.1 max-rate 600 tcp-proxy on
// 基于ip的防范
 firewall defend syn-flood interface Ethernet1/0/0 max-rate 500 tcp-proxy on
// 基于接口的防范方式
 firewall defend syn-flood interface Ethernet1/0/5 max-rate 500 tcp-proxy on
#
 firewall statistic system enable
#
interface Aux0
 async mode flow
 link-protocol ppp
#
interface Ethernet0/0/0
#
interface Ethernet0/0/1
```

```
#
interface Ethernet1/0/0
#
interface Ethernet1/0/1
 ip address 10.1.1.254 255.255.255.0
#
interface Ethernet1/0/2
#
interface Ethernet1/0/3
 ip address 192.168.1.254 255.255.255.0
#
interface Ethernet1/0/4
#
interface Ethernet1/0/5
 ip address 202.96.199.254 255.255.255.0
#
interface Ethernet1/0/6
#
interface Ethernet1/0/7
#
interface NULL0
#
firewall zone local
 set priority 100
#
firewall zone trust
 set priority 85
 add interface Ethernet1/0/1
#
firewall zone untrust
 set priority 5
 add interface Ethernet1/0/5
#
firewall zone dmz
 set priority 50
 add interface Ethernet1/0/3
 statistics enable ip inbound     // 在入域的方向上开启统计功能
#
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
#
#
 ip route-static 0.0.0.0 0.0.0.0 202.96.199.253     // 指向外部网络的静态路由
#
user-interface con 0
user-interface aux 0
```

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

四、 配置关键点：

SecPath1800F对于SYN方式的攻击防范可以在三个层面上配置：基于ip的；基于端口的；基于域的，其中基于端口的最为有效。在配置防范的阀值时可以根据网络中的实际情况尽行设置。全局统计及域上的统计都要打开该功能才能生效。