

## SecPath防火墙分片报文攻击防范典型配置

### 一、组网需求

部署SecPath防火墙，对IP分片报文攻击进行防范，以保护FTP Server 11.0.0.1/24。

### 二、组网图



软件版本如下：

SecPath10F: VRP 3.40 ESS 1604;

### 三、配置步骤

```
[DOWN] dis cur
#
sysname DOWN
#
firewall packet-filter enable
firewall packet-filter default permit
#
undo connection-limit enable
connection-limit default deny
connection-limit default amount upper-limit 50 lower-limit 20
#
firewall statistic system enable
#
radius scheme system
#
domain system
#
local-user admin
password cipher .]@USE=B,53Q=^Q`MAF4<1!!
service-type telnet terminal
level 3
service-type ftp
#
acl number 3000
//阻止到达server的IP分片报文
rule 1 deny ip destination 11.0.0.1 0 fragment
//允许ftp分片报文通过
rule 2 permit tcp destination 11.0.0.1 0 destination-port eq ftp fragment
#
interface Ethernet1/0
ip address 10.0.0.254 255.255.0.0
firewall packet-filter 3000 inbound //在接口上应用acl
#
interface Ethernet2/0
speed 10
duplex full
ip address 11.0.0.254 255.255.255.0
#
interface NULL0
#
firewall zone local
set priority 100
```

```

#
firewall zone trust
add interface Ethernet2/0
set priority 85
#
firewall zone untrust
add interface Ethernet1/0
set priority 5
#
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
#
FTP server enable
#
user-interface con 0
user-interface vty 0 4
authentication-mode scheme
#
return

```

#### **四、配置关键点**

1. 在ACL中配置对分片报文的阻断;
2. 在接口上应用ACL。

#### **五、验证结果**

在攻击机Attacker: 10.0.0.1上对11.0.0.1进行ping大包，PC会对ping报文进行分片，结果无法ping通11.0.0.1。

在攻击机上ftp 11.0.0.1，正常。

```
[DOWN]dis acl 3000
Advanced ACL 3000, 2 rules
Acl's step is 1
rule 1 deny ip destination 11.0.0.1 0 fragment (0 times matched)
rule 2 permit tcp destination 11.0.0.1 0 destination-port eq ftp fragment (0 times matched)
```

```
[DOWN]dis acl 3000
Advanced ACL 3000, 2 rules
Acl's step is 1
rule 1 deny ip destination 11.0.0.1 0 fragment (108 times matched)
rule 2 permit tcp destination 11.0.0.1 0 destination-port eq ftp fragment (0 times matched)
```