

## 知 某局点防火墙限制web登录无法生效的经典案例

ACL 域间策略/安全域 郝聚显 2019-10-22 发表

### 组网及说明

SecPath防火墙除了提供常见的命令行管理外，为了管理的快捷和直观，专门开发了WEB网管方式，管理的方式为http://防火墙地址/。但在使用WEB网管的过程中，客户经常有如下要求：只允许部分内网和个别外网用户具有登录权限，禁止来自其他外网及内网用户的访问。默认设置下，所有和防火墙接口路由可达的用户都可以登陆防火墙的WEB管理界面，一旦Web网管密码泄露或用户通过暴力破解获取账号密码，非法用户将直接登陆防火墙WEB网管界面，进行任意篡改。为了防止这种情况，我们可以将WEB网管只授权给管理员。

### 问题描述

客户反馈配置限制web登录后无法生效，未配置时所有主机都可以登录，配置限制acl后所有主机都无法登陆

### 过程分析

#### 配置检查

管理口配置：

```
#
interface GigabitEthernet 1/0/0
ip binding vpn-instance ceshi
ip address 10.10.10.10 255.255.255.0
```

限制登录的ACL定义

```
#
acl basic 2999
rule 0 permit source 1.1.1.1 0
rule 5 permit source 2.2.2.2 0
rule 10 deny
```

应用WEB管理页面登录控制

//将ACL绑定到HTTP网管上

```
# ip http acl 2999
```

检查配置发现客户实际上是把管理口绑定了vpn实例，此时acl限制需要绑定vpn实例，否则主机访问防火墙时防火墙查找的为全局路由表，从而出现上述故障现象，同时需要保证防火墙上配置vpn路由

### 解决方法

#### 1、限制acl绑定vpn实例

```
rule 0 permit vpn-instance ceshi source 1.1.1.1 0
```

#### 2、利用防火墙的安全策略实现

对于访问管理口的流量限制源目ip地址，服务类型配置为http和https，同时注意更改管理口所属安全域，因为man到local域的策略默认是放通的，如下面会话（管理口未更改安全域会话）。

```
dis session table ipv4 source-ip 1.1.1.1 verbose
```

Slot 1:

Initiator:

```
Source IP/port:1.1.1.1/57221
Destination IP/port: x.x.x.x/443
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: mgt/-/
Protocol: TCP(6)
Inbound interface: GigabitEthernet1/0/0
Source security zone: Management
```

Responder:

```
Source IP/port: x.x.x.x/443
Destination IP/port:1.1.1.1/57221
DS-Lite tunnel peer: -
VPN instance/VLAN ID/Inline ID: mgt/-/
Protocol: TCP(6)
Inbound interface: InLoopBack0
Source security zone: Local
```

State: TCP\_ESTABLISHED

Application: HTTPS

Start time: 2019-10-17 15:08:28 TTL: 597s

Initiator->Responder: 49 packets 6689 bytes

Responder->Initiator: 86 packets 100379 bytes

