

SecPath防火墙限制WEB网管典型配置

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：

1. 关闭WEB网管

系统视图下，关闭http网管功能：

```
#  
ip http shutdown
```

2. 限制WEB网管用户地址

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。

假设管理员的主机地址为202.1.1.1，则我们只授权此地址可以通过WEB管理防火墙：

```
//创建过滤ACL，只能使用2000系列的ACL
```

```
#  
acl number 2000  
rule 1 permit source 202.1.1.1 0  
rule 10 deny
```

```
//将ACL绑定到HTTP网管上
```

```
#  
ip http acl 2000
```