H3C SecPath系列面向对象管理特性典型配置

王思军 2007-06-14 发表

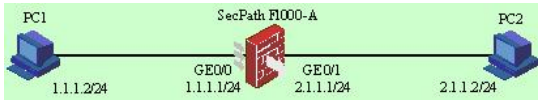
H3C SecPath系列面向对象管理特性典型配置

一、 组网需求：

用一台防火墙（SecPath F1000A）连接两台PC，PC1模拟局域网（内网）用户，PC2模拟Internet（外网）上的Server，F1000-A上对内网地址段做NAT转换，访问外网的服务器。

要求用地址对象、服务对象、流对象来代替真实的地址。

二、 组网图：



适用版本：

Comware software, Version 3.40, ESS 1621及以上

支持产品：

SecPath V1000-A/F1000-A/F1000-S/F100-E/F100-A

三、 配置步骤：

面向对象的基本配置需要配置以下内容：

1、创建地址（组）对象。

将IP地址和域名简化为地址对象和地址组对象；将多个地址对象添加到同一个地址组对象。

2、创建服务（组）对象。

将协议号、源端口、目的端口、ICMP消息类型简化为服务对象；将多个服务对象添加到同一个服务组对象。

3、创建时间对象。

配置时间范围，创建一个时间对象。

4、创建流对象。

将通常的五元组简化为流对象，一个流对象中可以引用包括地址（组）对象、服务（组）对象和时间段对象三类对象信息。

4、包过滤引用流对象/NAT引用流对象。

对数据流进行过滤/对指定的数据流进行地址转换。

1、 命令行配置方法：

当前视图	配置命令	简单说明
<H3C>	system	进入系统视图
[H3C]	interface GigabitEthernet 0/0	进入GigabitEthernet0/0接口视图
[H3C-GigabitEthernet0/0]	ip address 1.1.1.1 255.255.255.0	配置接口地址
[H3C-GigabitEthernet0/0]	interface GigabitEthernet 0/1	进入GigabitEthernet0/1接口视图
[H3C-GigabitEthernet0/1]	ip address 2.1.1.1 255.255.255.0	配置接口地址
[H3C-GigabitEthernet0/1]	quit	退出接口视图
[H3C]	firewall zone trust	进入trust安全区域视图
[H3C-zone-trust]	add interface GigabitEthernet0/0	将GigabitEthernet0/0接口加入trust安全区域
[H3C-zone-trust]	firewall zone untrust	进入untrust安全区域视图
[H3C-zone-untrust]	add interface GigabitEthernet0/1	将GigabitEthernet0/1接口加入untrust安全区域
[H3C-zone-untrust]	quit	退出接口视图
[H3C]	object address truadd 1.1.1.0 255.255.255.0	创建地址对象truadd
[H3C]	object address untruadd 2.1.1.0 255.255.255.0	创建地址对象untruadd

当前视图	配置命令	简单说明
[H3C]	object address-group trugrp	创建地址组对象trugrp，并进入地址组对象视图
[H3C-obj-addr-group-trugrp]	add truadd	添加地址对象truadd到地址组对象trugrp
[H3C-obj-addr-group-trugrp]	object service-group ipgrp	添加服务组对象ipgrp，进入服务组对象视图
[H3C-obj-srv-group-ipgrp]	add ip	添加预定义服务ip到服务组对象ipgrp中
[H3C-obj-srv-group-ipgrp]	quit	退到系统视图
[H3C]	time-range tm 09:00 to 18:00 Tue	创建时间对象tm（注：时间对象的创建请根据需求）
[H3C]	acl name ipflow	创建流对象ipflow，进入流对象视图
[H3C-acl-name-ipflow]	rule 0 permit source truadd destination untruadd service ipgrp time-range tm	添加流规则
[H3C-acl-name-ipflow]	acl name untruipflow	创建流对象untruipflow，进入流对象视图
[H3C-acl-name-untruipflow]	rule 0 permit source untruadd destination truadd service ipgrp time-range tm	添加流规则
[H3C-acl-name-untruipflow]	acl name perall	创建流对象perall，进入流对象视图
[H3C-acl-name-perall]	rule 0 permit	添加流规则
[H3C-acl-name-perall]	quit	退到系统视图
[H3C]	interface GigabitEthernet0/0	进入GigabitEthernet0/0接口视图
[H3C-GigabitEthernet0/0]	firewall packet-filter ipflow inbound	在GigabitEthernet0/0入方向，包过滤引用流对象ipflow
[H3C-GigabitEthernet0/0]	firewall packet-filter perall outbound	在GigabitEthernet0/0出方向，包过滤引用流对象perall
[H3C-GigabitEthernet0/0]	interface GigabitEthernet0/1	进入GigabitEthernet0/1接口视图
[H3C-GigabitEthernet0/1]	firewall packet-filter untruipflow inbound	在GigabitEthernet0/1入方向，包过滤引用流对象untruipflow
[H3C-GigabitEthernet0/1]	firewall packet-filter perall outbound	在GigabitEthernet0/1出方向，包过滤引用流对象perall
[H3C-GigabitEthernet0/1]	nat outbound ipflow	在GigabitEthernet0/1出方向，NAT引用流对象ipflow

2、 WEB配置方法：

创建地址对象：

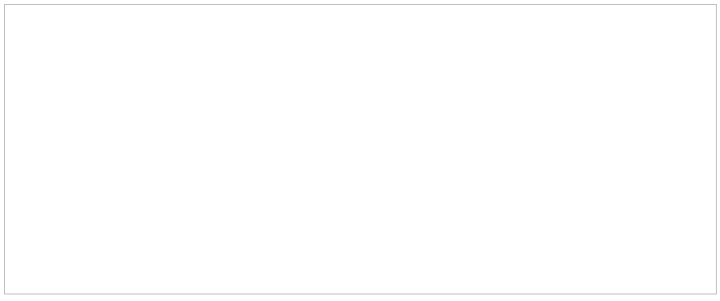


图1 地址对象

创建地址组对象：

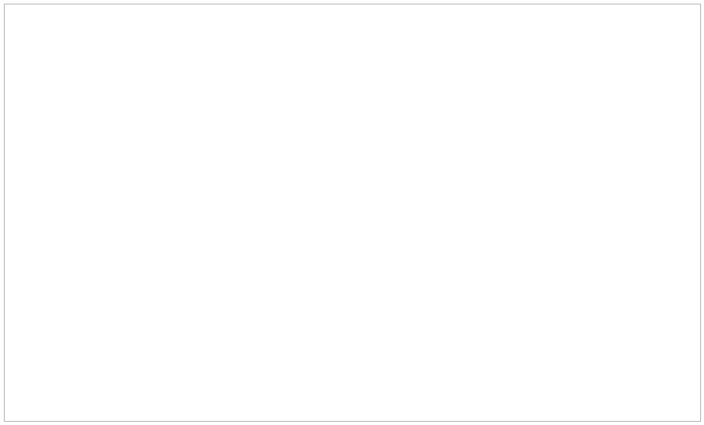


图2 地址组对象

创建服务对象：

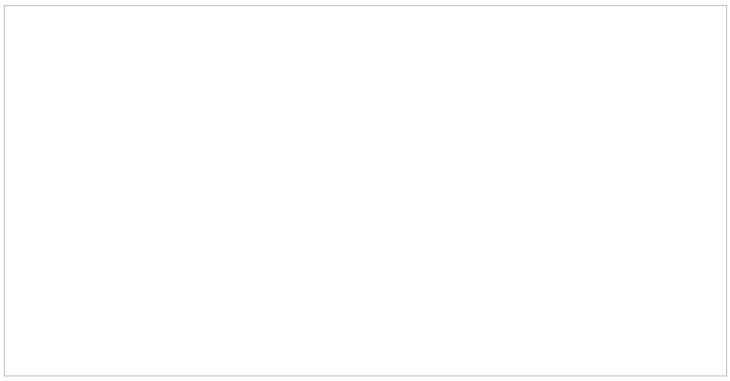


图3 服务对象

创建服务组对象：

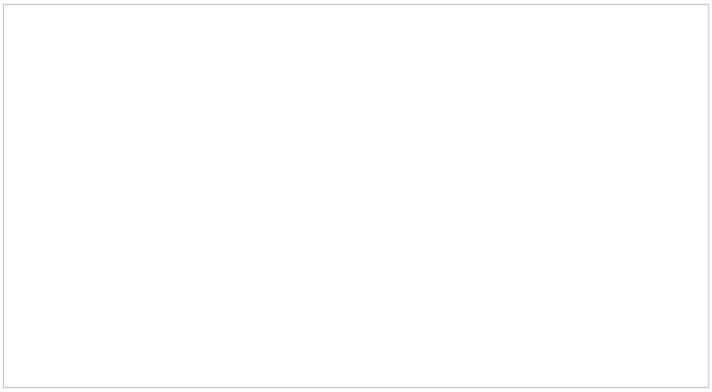


图4 服务组对象

创建时间对象：

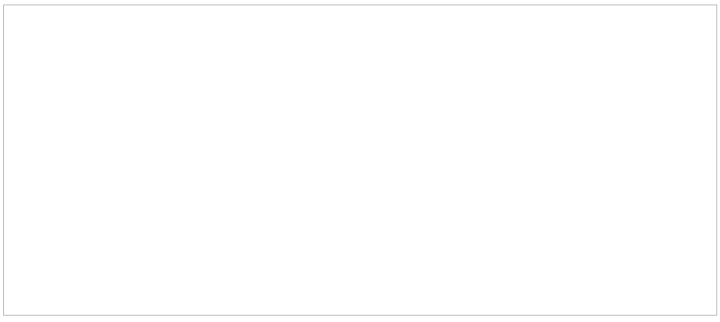


图5 时间对象

设置时间段范围：

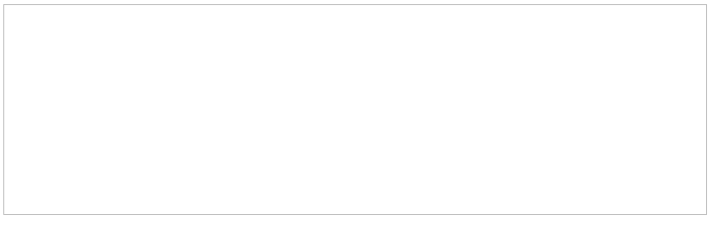


图6 设置时间段范围

创建流对象：

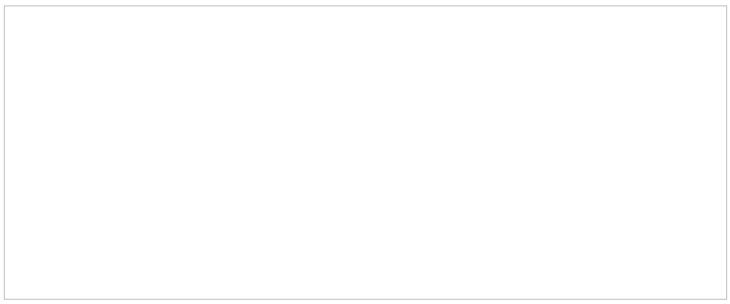


图7 创建流对象

添加流规则：

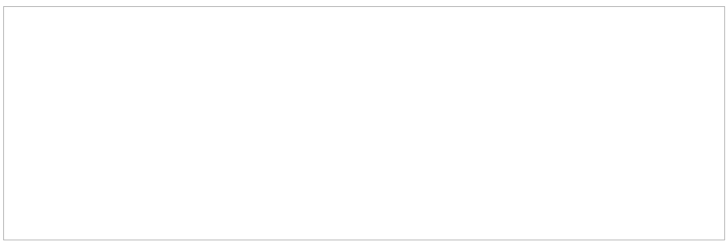


图8 添加流规则

包过滤引用流对象：

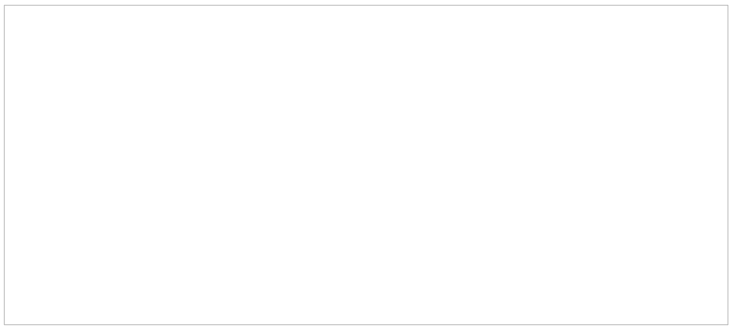


图9 包过滤引用流对象

NAT引用流对象：

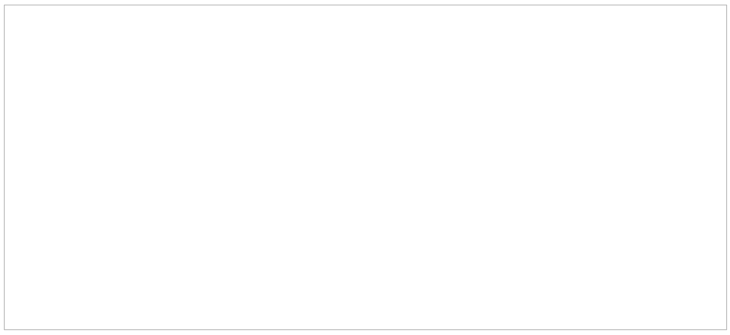


图10 NAT引用流对象

四、 配置关键点：

面向对象的配置管理需要注意以下几点：

1) 目前面向对象只支持包过滤引用流对象和NAT引用流对象，其他模块暂不支持。

2) 系统预定义了常用服务对象，方便管理员使用，如服务对象ftp代表ftp服务（可以通过display object predefined service查看预定义服务）。

3) 如果创建的地址对象是域名，需要配置如下命令：

dns resolve （进行地址解析）

dns server X.X.X.X （dns服务器地址）