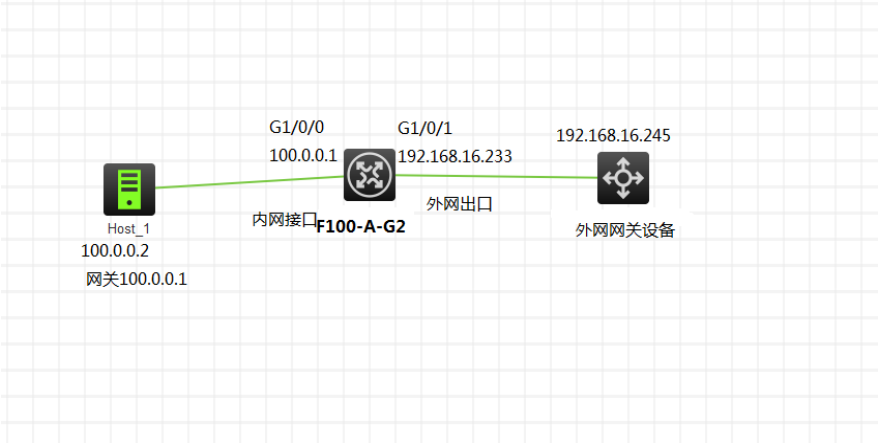
V7防火墙内部nat服务器配置

NAT　付琪琪　2016-02-22 发表

外网的电脑能通过防火墙G1/0/1的ip和3389端口号访问内网100.0.0.2的3389服务



1 先需要在命令行配置如下，可以实现web登入防火墙

```
sys
security-zone name Trust
 import interface GigabitEthernet1/0/0
interface GigabitEthernet1/0/0
 port link-mode route
 ip address 100.0.0.1 255.255.255.0
acl advanced 3333
 rule 0 permit ip
zone-pair security source Trust destination local
 packet-filter 3333
zone-pair security source local destination Trust
 packet-filter 3333
local-user admin class manage
 password hash admin
 service-type telnet terminal http https
 authorization-attribute user-role level-3
 authorization-attribute user-role network-admin
 ip http enable
 ip https enable
```

配置后，电脑连接G1/0/0，电脑配置100.0.0.2 ip地址。使用web的用户名和密码为admin admin 登入防火墙

2 配置内网接口的dhcp

2 配置外网接口

3 外网接G1/0/1口加入安全域

4 配置trust到trust的互访

5 nat动态地址转换

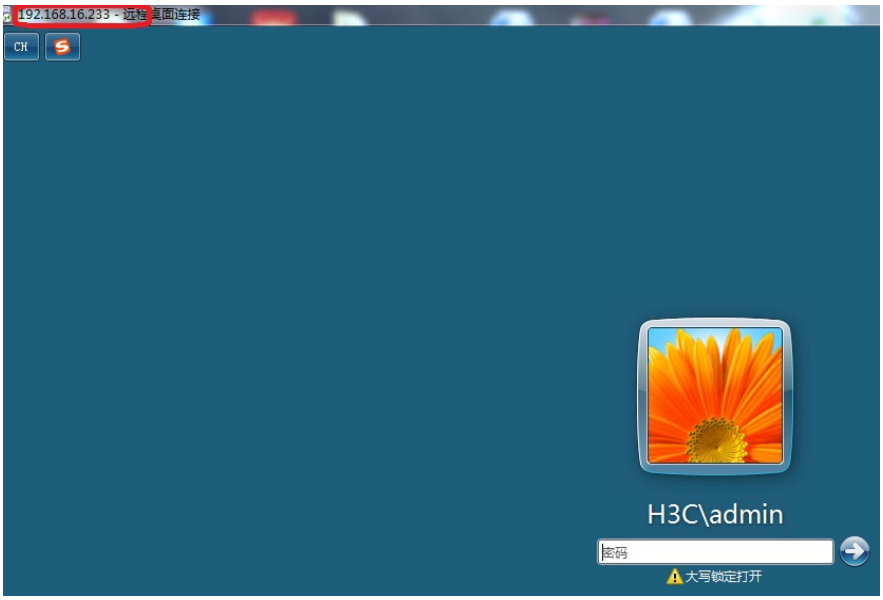
6 配置去外网的静态默认路由

7 dns 配置，开启dns服务器和dns代理

8 配置nat内部服务器

四 配置测试结果

外网电脑（192.168.16.1）能通过192.168.16.233:3389远程到内部pc机100.0.0.2



1 V7防火墙的菜单和V5差别很大，新增的菜单基本都是标示符+
2 要用的接口都要加入安全域，而且也要配置同级安全域的互访，同一安全域内报文过滤的缺省动作为deny。
3 基本配置要点：nat动态地址转换，静态默认路由，dns服务器器，nat内部服务器
4 内网电脑的网关要指向防火墙的内网接口
5 内部服务器配置和V5的差别比较大，根据实际情况选择好映射方式

六 命令行配置

```
dhcp server ip-pool qq1
 gateway-list 100.0.0.1
 network 100.0.0.0 mask 255.255.255.0


interface GigabitEthernet1/0/0
 port link-mode route
 ip address 100.0.0.1 255.255.255.0

interface GigabitEthernet1/0/1
 port link-mode route
 ip address 192.168.16.233 255.255.255.0
 nat outbound 2000
nat server protocol tcp global current-interface 3389 inside 100.0.0.2 3389

security-zone name Trust
 import interface GigabitEthernet1/0/0
 import interface GigabitEthernet1/0/1

zone-pair security source Trust destination local
 packet-filter 3333
zone-pair security source local destination Trust
 packet-filter 3333

security-zone intra-zone default permit
zone-pair security source Trust destination Trust
 object-policy apply ip Trust-Trust

 ip route-static 0.0.0.0 0 192.168.16.254

acl basic 2000
 rule 5 permit source 100.0.0.0 0.0.0.255 logging counting

acl advanced 3333
 rule 0 permit ip

local-user admin class manage
```

password hash admin
service-type telnet terminal http https
authorization-attribute user-role level-3
authorization-attribute user-role network-admin

ip http enable
ip https enable