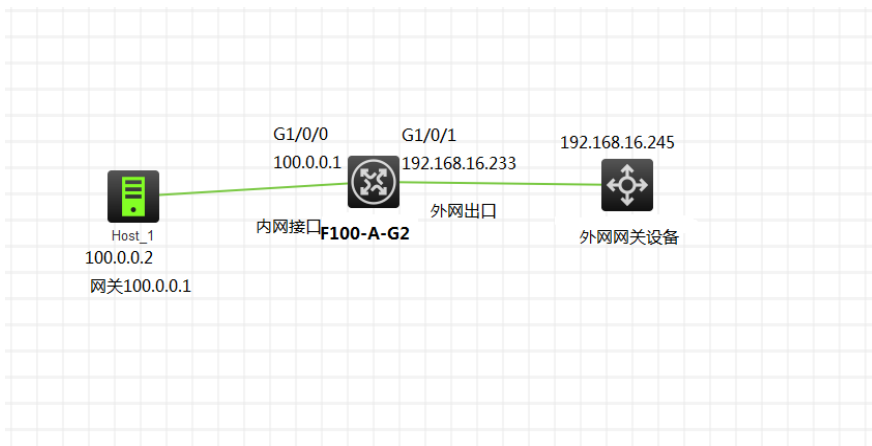


知 V7防火墙内部nat服务器配置

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

The screenshot shows the H3C web management interface. On the left is a navigation menu with options like 概览, 监控, 设备, 资源, 用户, 防火墙, 应用安全, NAT, VPN, 负载均衡, and 网络. The '网络' (Network) option is selected. The main area is titled 'DHCP' and contains a table for configuring DHCP services on various interfaces.

接口	DHCP服务	中继服务器
GE1/0/0	DHCP服务器	
GE1/0/1	关闭	
GE1/0/2	关闭	
GE1/0/3	关闭	
GE1/0/4	关闭	
GE1/0/5	关闭	
GE1/0/6	关闭	
GE1/0/7	关闭	
GE1/0/8	关闭	
GE1/0/9	DHCP服务器	
GE1/0/10	DHCP服务器	
GE1/0/11	DHCP服务器	

H3C

admin

f100-a-g2

概览

监控

设备

资源

用户

防火墙

应用安全

NAT

VPN

负载均衡

网络

DHCP

DHCP (Dynamic Host Configuration Protocol , 动态主机配置协议) 用来为网络设备动态地分配IP地址等网络配置参数。

服务地址地

QQ1

删除

添加地址地

地址分配地址地选项已分配地址

租约有效期限

无限制

1天0小时0分0秒

域名后缀

(1-50字符)

网关

100.0.0.1

DNS 服务器

100.0.0.1

WINS服务器

NetBIOS节点类型

请选择...

DHCP选项

DHCP选项类型选项内容

2 - 254十六进制数串1 - 256个字符

DHCP选项取值范围为2-254, 不包括50-54, 56, 58, 59, 61, 62。

DHCP选项类型为十六进制数串时, 选项内容为2-255个字符且位数为偶数。

确定

2 配置外网接口

H3C

admin

f100-a-g2

概览

监控

设备

资源

用户

防火墙

应用安全

NAT

VPN

负载均衡

网络

修改接口设置

接口

GigabitEthernet1/0/1 (GE1/0/1)

链路状态

up禁用

描述

GigabitEthernet1/0/1 Interface (1-255字符)

MAC地址

3C-8C-40-B4-B9-F3 (HH-HH-HH-HH-HH-HH)

IP地址

IP地址/掩码

192.168.16.233/255.255.255.0

IPv6地址/前缀长度

速率

(当前 : 1000000Kbps)

自协商

双工模式

(当前 : 全双工)

自协商

带宽

(当前 : 10000000kb/s)

选择 接口 G1/0/1的最后

一个菜单选择详细

工作模式

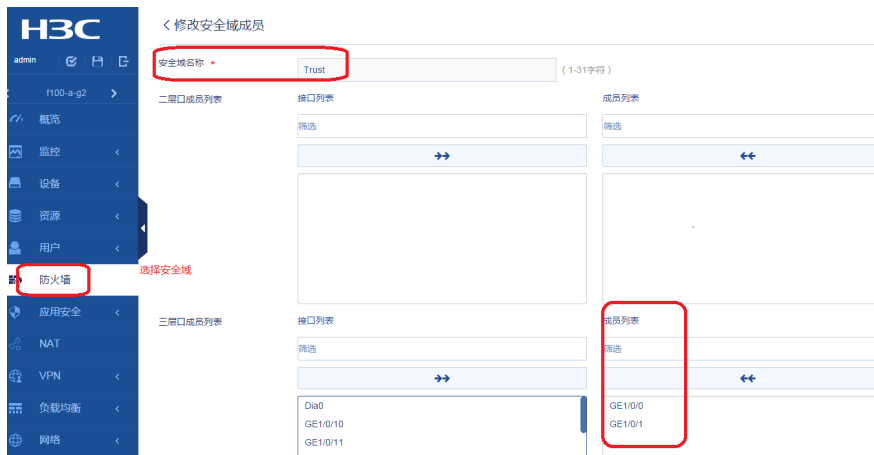
允许超长帧通过

二层模式三层模式

不允许

1600 (1600-1600)

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



The image shows the H3C web management interface for configuring NAT for internal servers. The left sidebar contains navigation menus for 'NAT' (selected), 'VPN', '负载均衡', and '网络'. The main configuration area is titled 'NAT 选择内部服务器'. It includes fields for '映射方式' (Mapping Method) set to '外网地址单一, 外网端口连续', '外网地址' (External Address) with radio buttons for '指定IP地址' (selected), '使用当前接口的主IP地址作为内部服务器的外网地址 (Easy IP)', and '使用Loopback接口的主IP地址作为内部服务器的外网地址'. Below this are '端口范围' (Port Range) and 'VRF' (Public Network) fields. The '内部服务器' (Internal Server) section includes 'IP地址范围' (IP Address Range) and '端口范围' (Port Range) fields, with a 'VRF' dropdown set to '公网'. At the bottom, there is a '报文匹配规则 (ACL)' section with a '启用' (Enable) checkbox checked.

映射方式 * 外网地址单一, 外网端口连续

外网地址 *

IP地址

☐ 指定IP地址 使用外网接口的ip

☒ 使用当前接口的主IP地址作为内部服务器的外网地址 (Easy IP)

☐ 使用Loopback接口的主IP地址作为内部服务器的外网地址

端口范围 3389 - 3389 (最多256个)

VRF 公网 外部端口号

IP地址范围 100.0.0.2 - 100.0.0.2 内部服务器的内网ip

端口范围 3389 - 3389 (最多256个)

VRF 公网 内部服务器开放的内部端口号

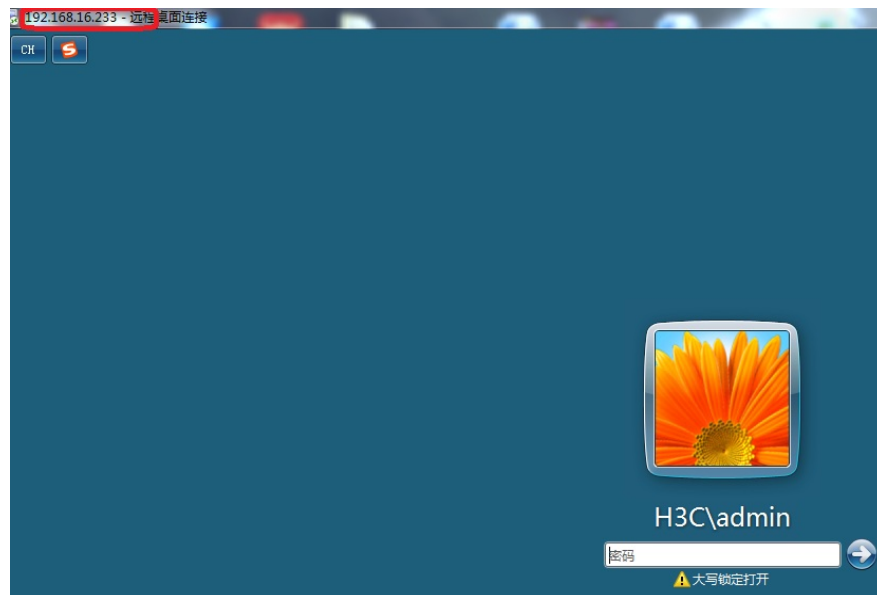
报文匹配规则 (ACL)

启用 ☒ 启用此条规则

确定 取消

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