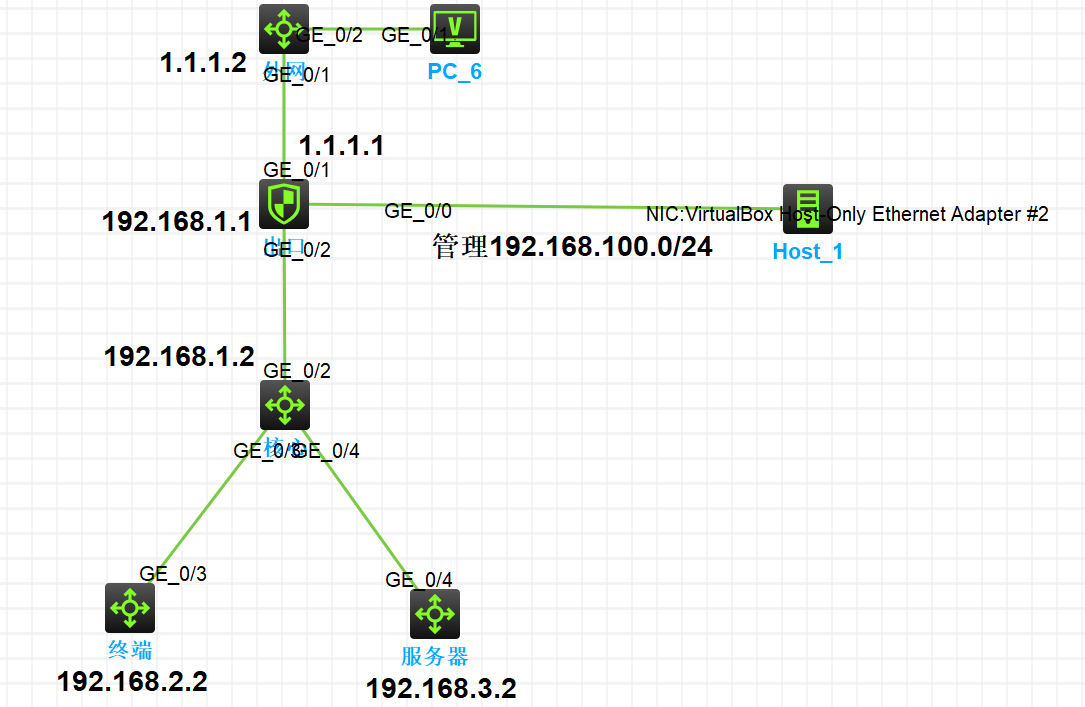
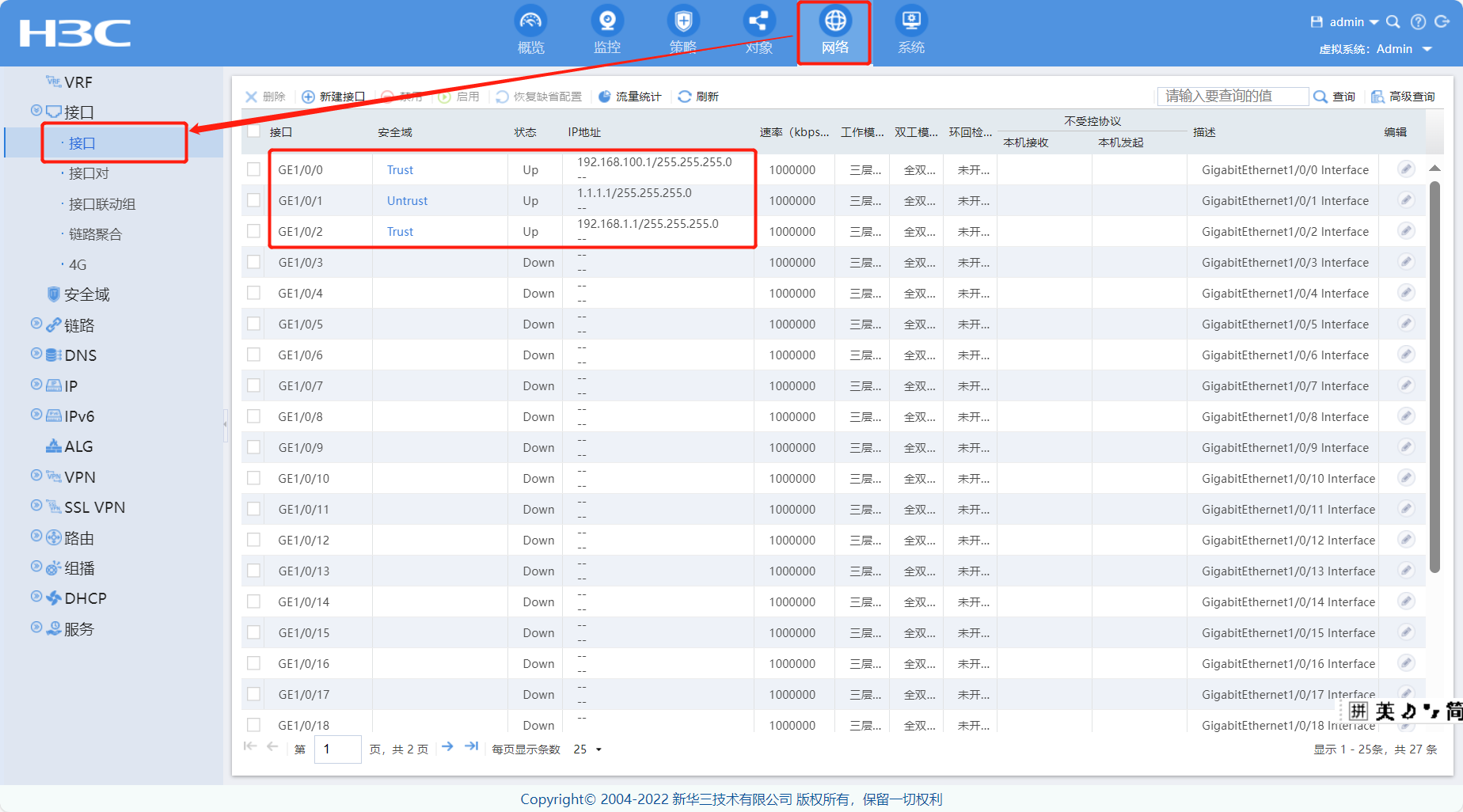
组网图：



防火墙web界面配置

接口地址与安全域的配置



#

interface GigabitEthernet1/0/0

port link-mode route

combo enable copper

ip address 192.168.100.1 255.255.255.0

#

interface GigabitEthernet1/0/1

port link-mode route

combo enable copper

ip address 1.1.1.1 255.255.255.0

#

interface GigabitEthernet1/0/2

port link-mode route

combo enable copper

ip address 192.168.1.1 255.255.255.0

#

<H3C>dis security-zone

Name: Local

Members:

None

Name: Trust

Members:

GigabitEthernet1/0/0

GigabitEthernet1/0/2

Name: DMZ

Members:

None

Name: Untrust

Members:

GigabitEthernet1/0/1

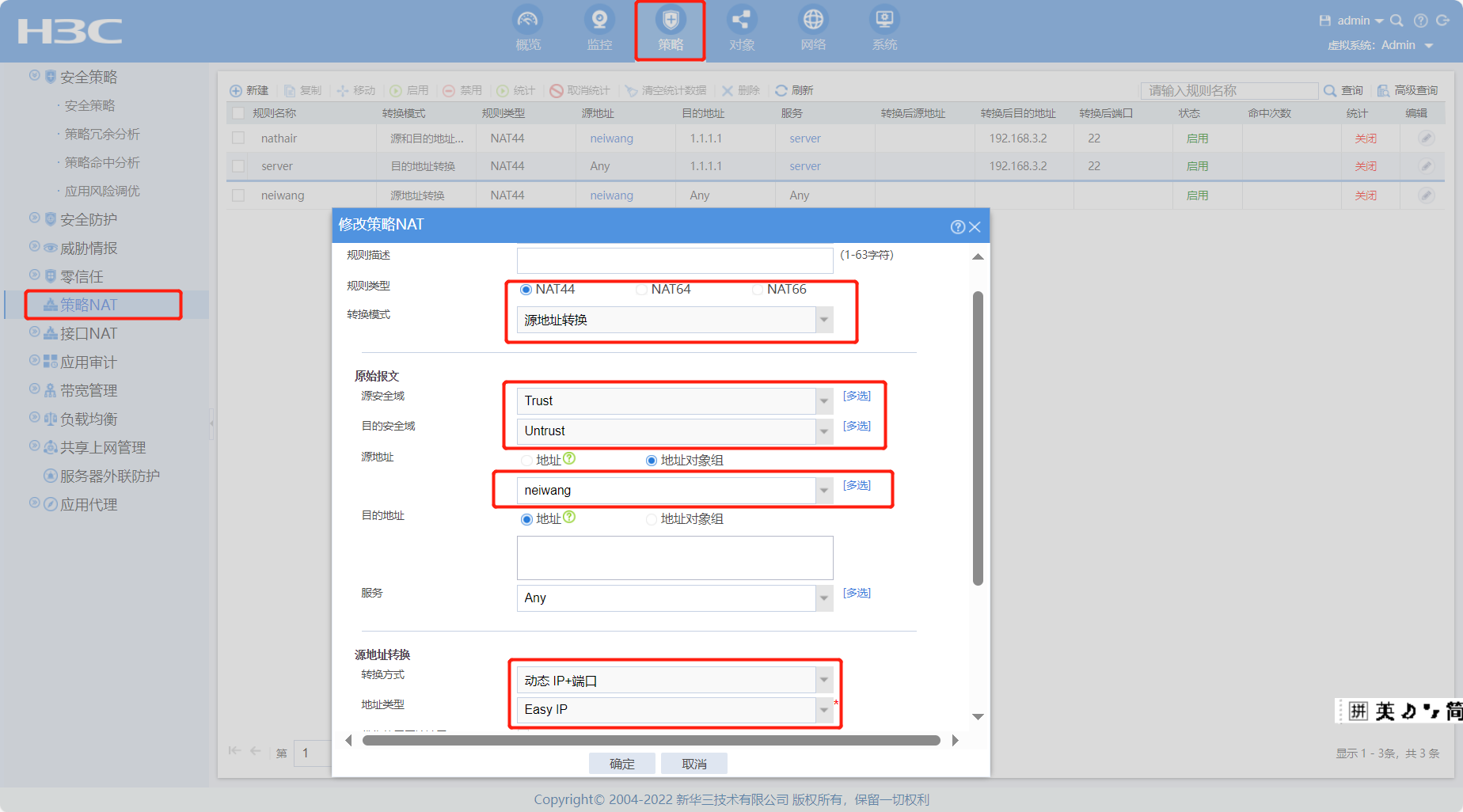
Name: Management

Members:

None

全局nat的配置

内网用户访问公网nat策略配置



rule name neiwang

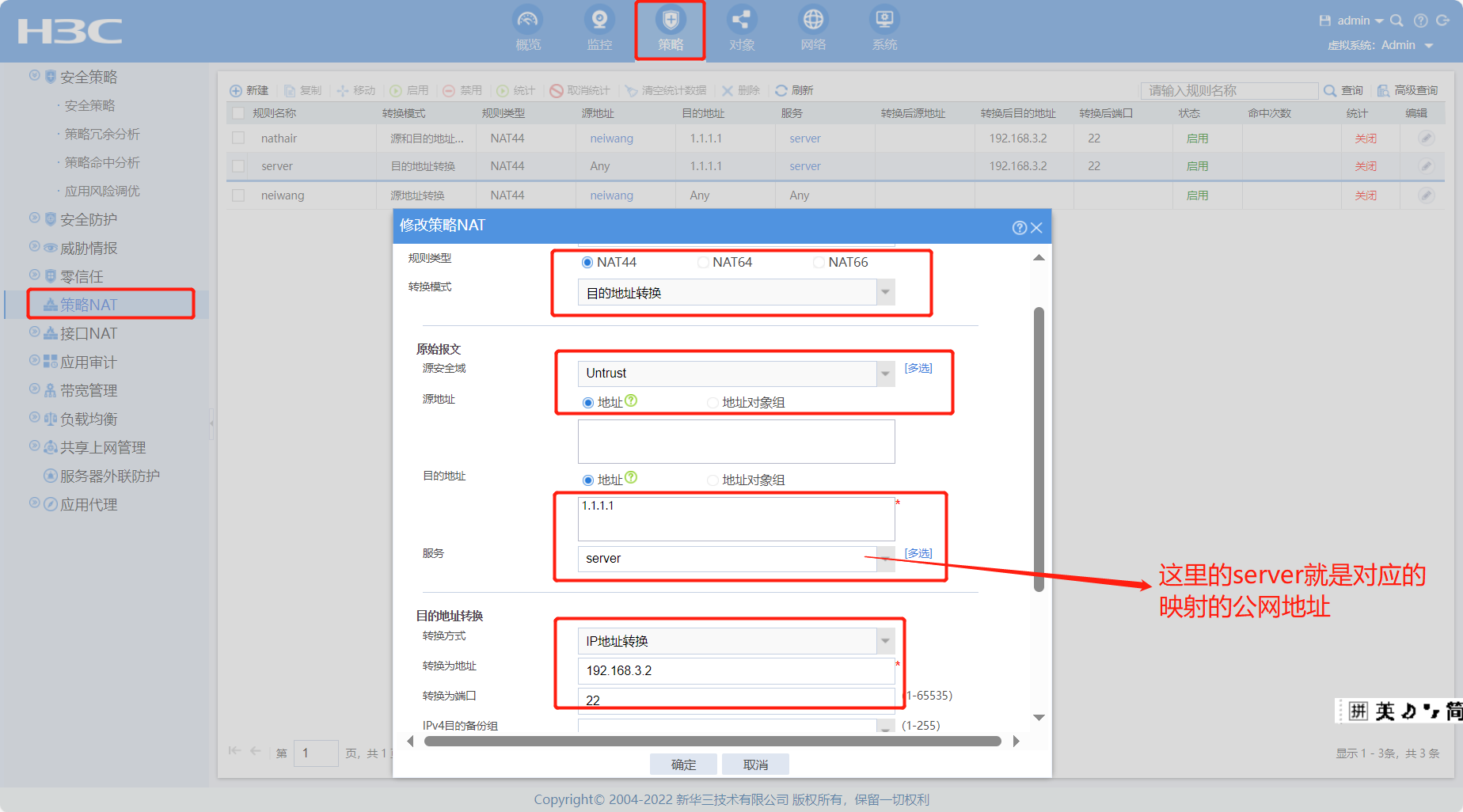
source-zone Trust

destination-zone Untrust

source-ip neiwang

action snat easy-ip

外网用户访问内网服务器的配置：



rule name server

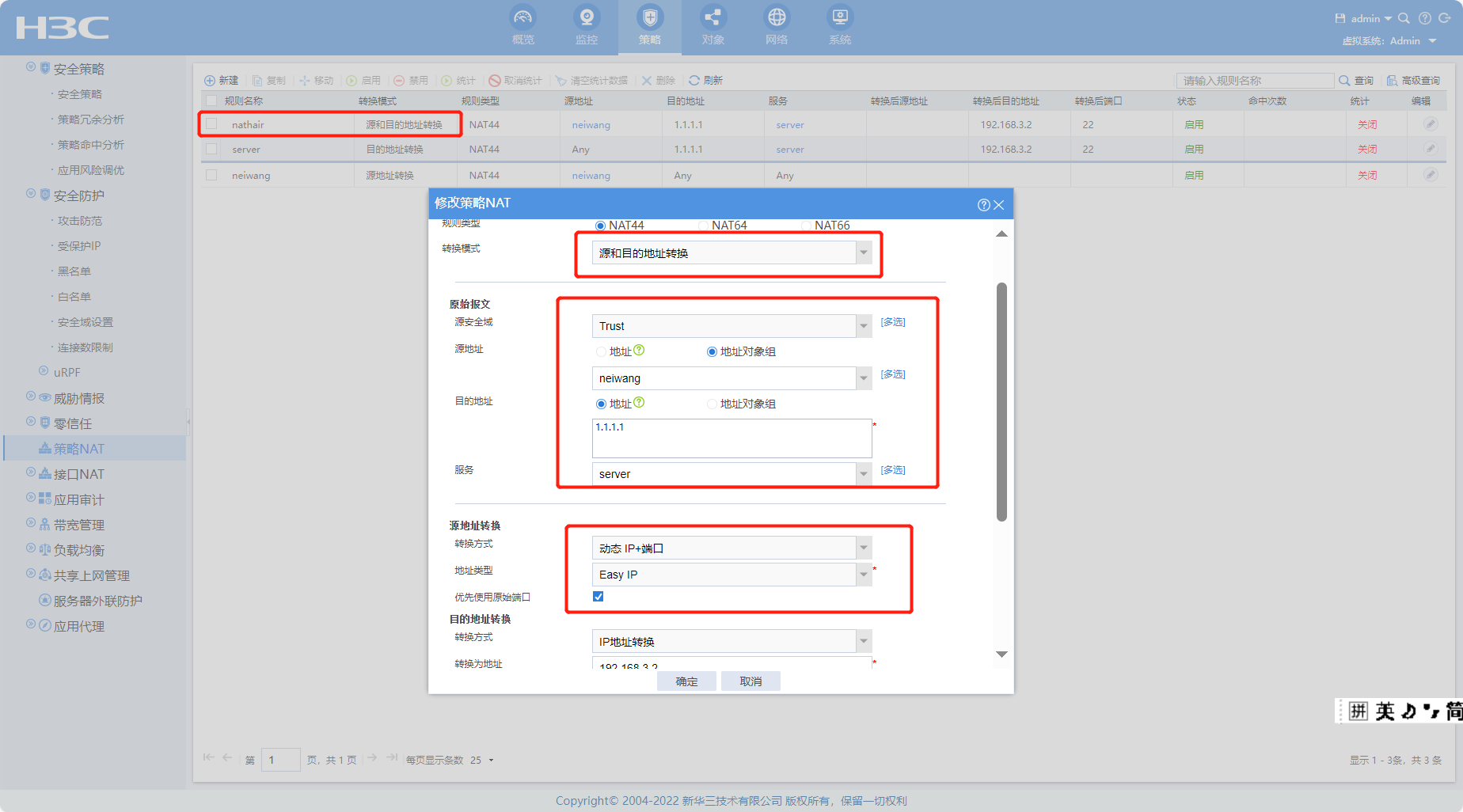
service server

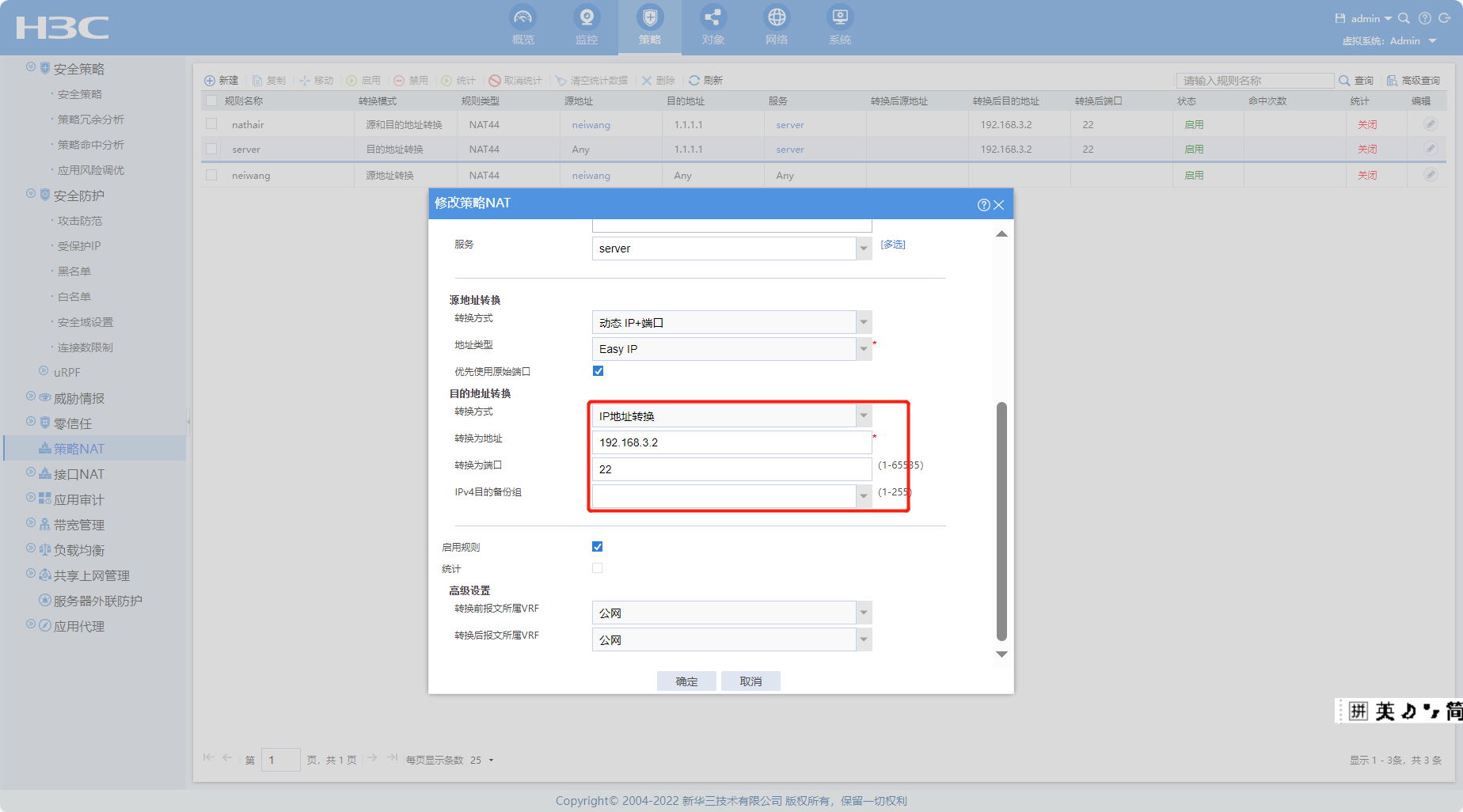
source-zone Untrust

destination-ip host 1.1.1.1

action dnat ip-address 192.168.3.2 local-port 22

内网用户通过公网地址访问内网服务器：





rule name nathair

service server

source-zone Trust

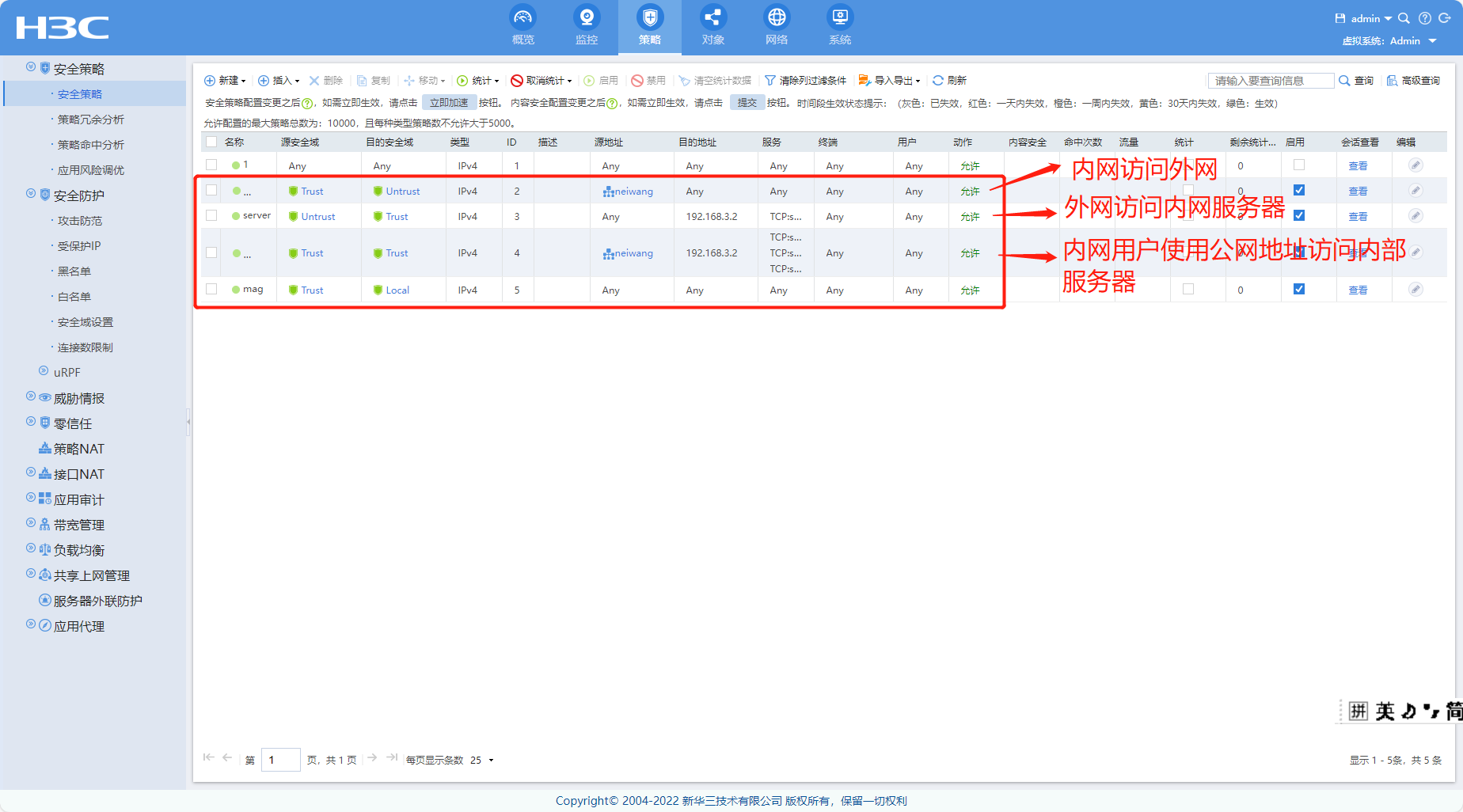
source-ip neiwang

destination-ip host 1.1.1.1

action snat easy-ip port-preserved

action dnat ip-address 192.168.3.2 local-port 22

安全策略配置



Security-policy ip

rule 1 name 1

action pass

disable

rule 2 name internet

action pass

source-zone Trust

destination-zone Untrust

source-ip neiwang

rule 3 name server

action pass

source-zone Untrust

destination-zone Trust

destination-ip-host 192.168.3.2

service-port tcp destination eq 22

rule 4 name nathairpin

action pass

source-zone Trust

destination-zone Trust

source-ip neiwang

destination-ip-host 192.168.3.2

service-port tcp destination eq 23

service-port tcp destination eq 2222

service-port tcp destination eq 22

rule 5 name mag

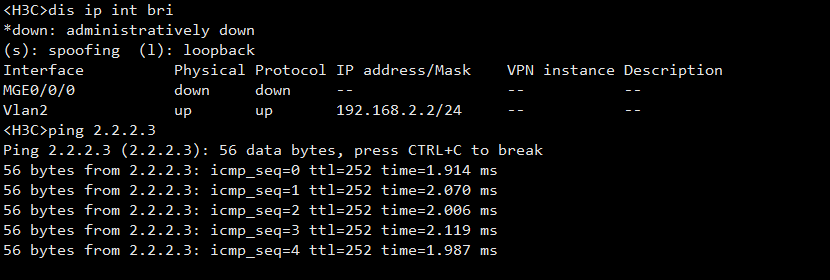
action pass

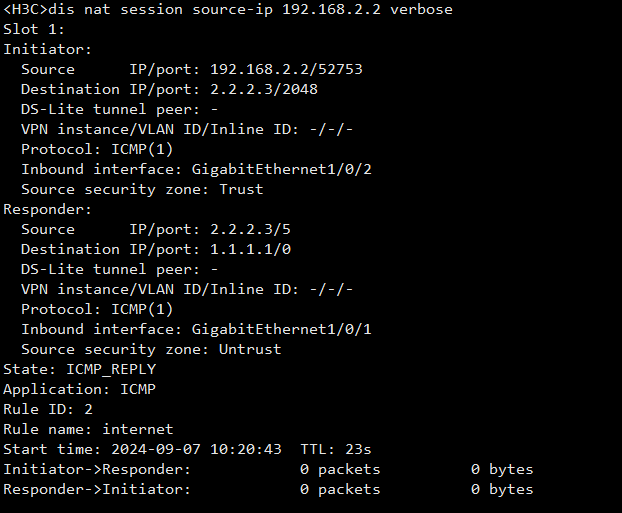
source-zone Trust

destination-zone Local

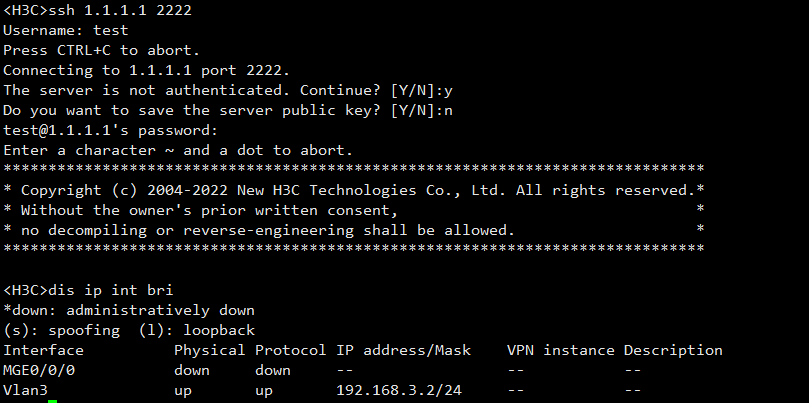
测试结果：

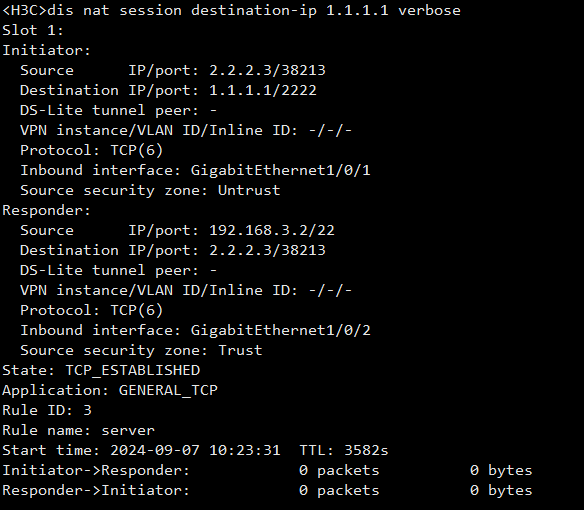
内网用户访问外网，外网地址是2.2.2.3





外网用户使用公网地址访问内部服务器，测试公网地址2.2.2.3





内网用户使用公网地址访问内网服务器测试的终端192.168.2.2

