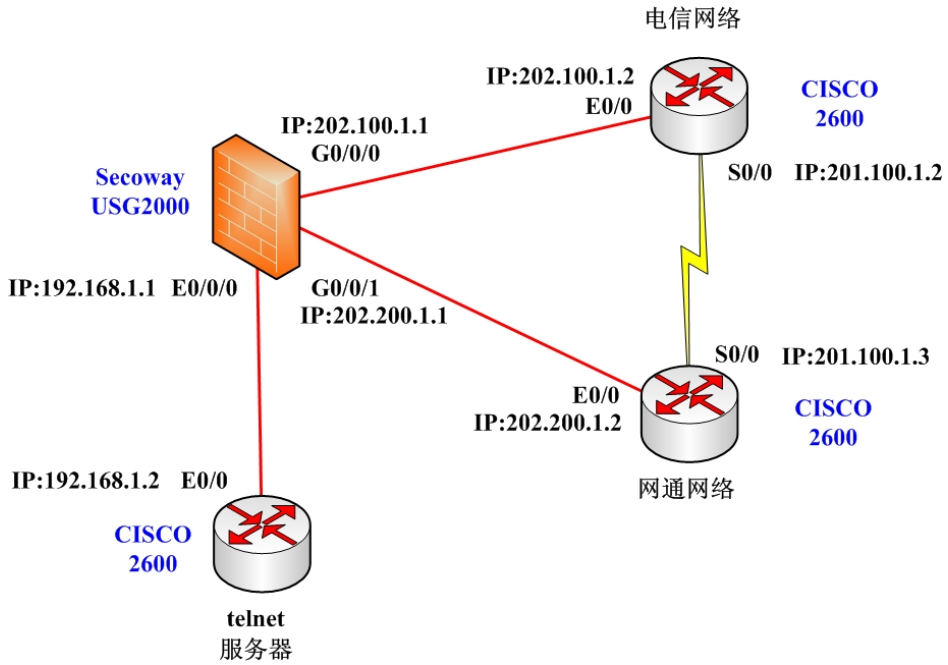
华为防火墙 USG2000 实验文档



要求:通过配置华为防火墙实现本地 telnet 服务器能够通过 NAT 上网.并且,访问电信网络链路时走电信,访问网通链路时走网通.

具体配置如下:

华为 USG 2000

Username:admin

Password:Admin@123

批注 [canhong1]: 默认用户名和密码

<USG2205BSR>system-view

批注 [canhong2]: 进入配置模式

[USG2205BSR]sysname huawei

批注 [canhong3]: 命名

[huawei]interface GigabitEthernet 0/0/0

批注 [canhong4]: 进入接口

[huawei-GigabitEthernet0/0/0]description ###conn to dianxin link###

批注 [canhong5]: 对接口描述

[huawei-GigabitEthernet0/0/0]ip address 202.100.1.1 255.255.255.0

批注 [canhong6]: 配置 IP

[huawei-GigabitEthernet0/0/0]undo shutdown

批注 [canhong7]: 启用接口

[huawei-GigabitEthernet0/0/0]quit

批注 [canhong8]: 退出接口模式

[huawei]interface GigabitEthernet 0/0/1

[huawei-GigabitEthernet0/0/1]description ###conn to yidong link###

[huawei-GigabitEthernet0/0/1]ip address 202.200.1.1 255.255.255.0

[huawei-GigabitEthernet0/0/1]undo shutdown

[huawei-GigabitEthernet0/0/1]quit

[huawei]interface Vlanif 1

[huawei-Vlanif1]description ###conn to local###

[huawei-Vlanif1]ip address 192.168.1.1 255.255.255.0

[huawei-Vlanif1]undo shutdown

[huawei-Vlanif1]quit

[huawei]firewall zone trust

批注 [canhong9]: 进入信认区域,信认区域默认安全等级为 85

[huawei-zone-trust]undo add interface GigabitEthernet 0/0/0

[huawei-zone-trust]undo add interface GigabitEthernet 0/0/1

批注 [canhong10]: 默认 G0/0/0 和 G0/0/1 属于信认区域,由于本实验,这两个接口连接外网,应把这两个接口从信认区域移出,加入到非信认区域中.

[huawei-zone-trust]add interface Vlanif 1

批注 [canhong11]: 把 VLANIF 1 加入信认区域

[huawei]firewall zone name Dianxin

批注 [canhong12]: 重新建个新的区域,命名为 dianxin,设置安全等级为 4,并把 G0/0/0 加入该区域

[huawei-zone-dianxin]set priority 4

[huawei-zone-dianxin]add interface GigabitEthernet 0/0/0

[huawei-zone-dianxin]quit

[huawei]firewall zone name Yidong

[huawei-zone-yidong]set priority 3

[huawei-zone-yidong]add interface GigabitEthernet 0/0/1

批注 [canhong13]: 重新建个新的区域,命名为 yidong,设置安全等级为 3,并把 G0/0/1 加入该区域

[huawei-zone-yidong]quit

[huawei]acl number 2000

批注 [canhong14]: 配置一个 ACL 2000, 设置规则允许内网 192.168.1.0 的网段

[huawei-acl-basic-2000]rule 10 permit source 192.168.1.0 0.0.0.255

[huawei-acl-basic-2000]quit

[huawei]firewall interzone trust dianxin

批注 [canhong15]: 进入信认区域和 dianxin

[huawei-interzone-trust-dianxin]packet-filter 2000 outbound

批注 [canhong16]: 包过滤的出口方向应用 ACL 2000

[huawei-interzone-trust-dianxin]nat outbound 2000 interface GigabitEthernet 0/0/0

批注 [canhong17]: ACL 2000 与接口 G0/0/0 做 PAT

[huawei-interzone-trust-dianxin]quit

[huawei]firewall interzone trust yidong

[huawei-interzone-trust-yidong]nat outbound 2000 interface GigabitEthernet 0/0/1

批注 [canhong18]: 同上

[huawei-interzone-trust-yidong]quit

[huawei]user-interface vty 0 4

批注 [canhong19]: 进入接口 VTY, 启用验证模式为密码模式

[huawei-ui-vty0-4]authentication-mode password

[huawei-ui-vty0-4]quit

[huawei]ip route-static 0.0.0.0 0.0.0.0 202.100.1.2

批注 [canhong20]: 配置默认路由到达电信.

[huawei]ip route-static 27.8.0.0 255.248.0.0 202.200.1.2

[huawei]ip route-static …… …… 202.200.1.2

[huawei]ip route-static 222.160.0.0 255.252.0.0 202.200.1.2

批注 [canhong21]: 配置明细路由到网通的路由，约有 683 条明细路由.

[huawei] firewall packet-filter default permit interzone local dianxin direction inbound

[huawei] firewall packet-filter default permit interzone local dianxin direction outbound

[huawei] firewall packet-filter default permit interzone trust dianxin direction inbound

[huawei] firewall packet-filter default permit interzone trust dianxin direction outbound

[huawei] firewall packet-filter default permit interzone local yidong direction inbound

[huawei] firewall packet-filter default permit interzone local yidong direction outbound

[huawei] firewall packet-filter default permit interzone trust yidong direction inbound

[huawei] firewall packet-filter default permit interzone trust yidong direction outbound

批注 [canhong22]: 配置包过滤,允许 dianxin 、yidong 与 local 、trust 之间的入方向和出方向。没有允许的话，则外网无法 PING 通防火墙的出接口。

如图：电信网络、网通网络和 telnet　服务器配置　略！

验证：

内网 192.168.1.2 分别 PING 电信与网通.

inside#ping 202.100.1.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 202.100.1.2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/4 ms

inside#ping 202.200.1.2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 202.200.1.2, timeout is 2 seconds:

!!!!!

<huawei>display firewall session table

批注 [canhong23]: 查看 NAT 转换列表

11:38:23 2010/11/06

Current total sessions: 3

icmp VPN: public -> public

192.168.1.2:3[202.100.1.1:23088]-->202.100.1.2:3

tcp VPN: public -> public 192.168.1.1:1024-->192.168.1.2:23

icmp VPN: public -> public

192.168.1.2:4[202.200.1.1:43288]-->202.200.1.2:4

验证成功!!!

[huawei]display current-configuration

批注 [canhong24]: 查看当前配置

11:54:30 2010/11/06

#

acl number 2000

rule 10 permit source 192.168.1.0 0.0.0.255

#

sysname huawei

#

super password level 3 cipher ^]S*H+DFHFSQ=^Q`MAF4<1!!

#

web-manager enable

#

info-center timestamp debugging date

#

firewall packet-filter default permit interzone local trust direction inbound

firewall packet-filter default permit interzone local trust direction outbound

firewall packet-filter default permit interzone local untrust direction inbound

```
 firewall packet-filter default permit interzone local untrust direction outbound
 firewall packet-filter default permit interzone local dmz direction inbound
 firewall packet-filter default permit interzone local dmz direction outbound
 firewall packet-filter default permit interzone local vzone direction inbound
 firewall packet-filter default permit interzone local vzone direction outbound
 firewall packet-filter default permit interzone local dianxin direction inbound
 firewall packet-filter default permit interzone local dianxin direction outbound
 firewall packet-filter default permit interzone local yidong direction inbound
 firewall packet-filter default permit interzone local yidong direction outbound
 firewall packet-filter default permit interzone trust untrust direction inbound
 firewall packet-filter default permit interzone trust untrust direction outbound
 firewall packet-filter default permit interzone trust dmz direction inbound
 firewall packet-filter default permit interzone trust dmz direction outbound
 firewall packet-filter default permit interzone trust vzone direction inbound
 firewall packet-filter default permit interzone trust vzone direction outbound
 firewall packet-filter default permit interzone trust dianxin direction inbound
 firewall packet-filter default permit interzone trust dianxin direction outbound
 firewall packet-filter default permit interzone trust yidong direction inbound
 firewall packet-filter default permit interzone trust yidong direction outbound
 firewall packet-filter default permit interzone dmz untrust direction inbound
 firewall packet-filter default permit interzone dmz untrust direction outbound
 firewall packet-filter default permit interzone untrust vzone direction inbound
 firewall packet-filter default permit interzone untrust vzone direction outbound
 firewall packet-filter default permit interzone dmz vzone direction inbound
 firewall packet-filter default permit interzone dmz vzone direction outbound
#
 dhcp enable
#
 firewall statistic system enable
#
vlan 1
```

```
#
interface Cellular0/1/0
 link-protocol ppp
#
interface Vlanif1
 description ###conn to local###
 ip address 192.168.1.1 255.255.255.0
#
interface Ethernet1/0/0
 port link-type access
#
interface Ethernet1/0/1
 port link-type access
#
interface Ethernet1/0/2
 port link-type access
#
interface Ethernet1/0/3
 port link-type access
#
interface Ethernet1/0/4
 port link-type access
#
interface GigabitEthernet0/0/0
 description ###conn to dianxin link###
 ip address 202.100.1.1 255.255.255.0
#
interface GigabitEthernet0/0/1
 description ###conn to yidong link###
 ip address 202.200.1.1 255.255.255.0
#
```

```
interface NULL0
#
firewall zone local
 set priority 100
#
firewall zone trust
 set priority 85
 add interface Vlanif1
#
firewall zone untrust
 set priority 5
#
firewall zone dmz
 set priority 50
#
firewall zone vzone
 set priority 0
#
firewall zone name dianxin
 set priority 4
 add interface GigabitEthernet0/0/0
#
firewall zone name yidong
 set priority 3
 add interface GigabitEthernet0/0/1
#
firewall interzone trust dianxin
 packet-filter 2000 outbound
 nat outbound 2000 interface GigabitEthernet0/0/0
#
firewall interzone trust yidong
```

```
 packet-filter 2000 outbound
 nat outbound 2000 interface GigabitEthernet0/0/1
#
aaa
 local-user admin password cipher ]MQ;4\]B+4Z,YWX*NZ55OA!!
 local-user admin service-type web telnet
 local-user admin level 3
 authentication-scheme default
#
 authorization-scheme default
#
 accounting-scheme default
#
 domain default
#
#
right-manager server-group
#
 slb
#
 ip route-static 0.0.0.0 0.0.0.0 202.100.1.2
 ip route-static 27.8.0.0 255.248.0.0 202.200.1.2
 ip route-static ……  ……  202.200.1.2
 ip route-static 222.160.0.0 255.252.0.0 202.200.1.2
#
user-interface con 0
user-interface tty 9
 authentication-mode none
 modem both
user-interface vty 0 4
 user privilege level 3
```

#

return

[huawei]