

XE200私网与公网之间NAT_FW 隧道穿越业务的配置

一、组网需求

一台NAT/FW设备将公网隔开，公网中布置一台语音网关和两台XE语音服务器（分别作为位置服务器和处理服务器），私网中布置一台语音网关和一台XE语音服务器（作为处理服务器）。

二、组网图

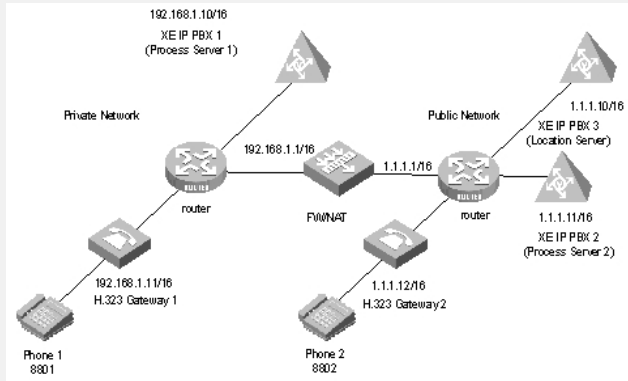


图1-1 公网之间NAT/FW隧道穿越配置举例组网图

三、配置步骤

1. 配置H.323 Gateway 1 (私网语音网关)

```
# 配置以太网接口
[VG1] interface ethernet 0
[VG1-Ethernet0] ip address 192.168.1.11 255.255.0.0
[VG1-Ethernet0] quit
# 配置语音实体
[VG1] voice-setup
[VG1-voice] dial-program
[VG1-voice-dial] entity 8888 voip
[VG1-voice-dial-entity8888] address ras
[VG1-voice-dial-entity8888] match-template ....
[VG1-voice-dial-entity8888] quit
[VG1-voice-dial] entity 8801 pots
[VG1-voice-dial-entity8801] line 0
[VG1-voice-dial-entity8801] match-template 8801
[VG1-voice-dial-entity8801] return
# 配置GK-Client
[VG1] voice-setup
[VG1-voice] gk-client
[VG1-voice-gk] gw-id h323gateway1
[VG1-voice-gk] gw-address ip 192.168.1.11
[VG1-voice-gk] gk-id xeippbx1 gk-addr 192.168.1.10 1719
[VG1-voice-gk] ras-on
```

2. 配置H.323 Gateway 2 (公网语音网关)

```
# 配置以太网接口
[VG2] interface ethernet 0
[VG2-Ethernet0] ip address 1.1.1.12 255.255.0.0
[VG2-Ethernet0] quit
# 配置语音实体
[VG2] voice-setup
[VG2-voice] dial-program
[VG2-voice-dial] entity 8888 voip
[VG2-voice-dial-entity8888] address ras
[VG2-voice-dial-entity8888] match-template ....
[VG2-voice-dial] entity 8802 pots
[VG2-voice-dial-entity8802] line 0
```

```

[VG2-voice-dial-entity8802] match-template 8802
[VG2-voice-dial-entity8802] return
# 配置GK-Client
[VG2] voice-setup
[VG2-voice] gk-client
[VG2-voice-gk] gw-id h323gateway2
[VG2-voice-gk] gw-address ip 1.1.1.12
[VG2-voice-gk] gk-id xeippbx2 gk-addr 1.1.1.11 1719
[VG2-voice-gk] ras-on
3. 配置处理服务器1 (私网process-server)
# 配置以太网接口
[XE] interface ethernet 0/0
[XE-Ethernet0/0] ip address 192.168.1.10 255.255.0.0
[XE-Ethernet0/0] quit
[XE] ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
# 配置网守
[XE] process-server
[XE-ps] ps-config xeippbx1 interface Ethernet 0/0
[XE-ps] heartbeat password xe200
[XE-ps] ls-mode remote ip-address 1.1.1.10
[XE-ps] start
[XE-ps] gatekeeper // 启用处理服务器的GK功能
[XE-ps-gk] start
4. 配置处理服务器2 (公网process-server)
# 配置以太网接口
[XE] interface ethernet 0/0
[XE-Ethernet0/0] ip address 1.1.1.11 255.255.0.0
[XE-Ethernet0/0] quit
# 配置网守
[XE] process-server
[XE-ps] ps-config xeippbx2 interface Ethernet 0/0
[XE-ps] heartbeat password xe200
[XE-ps] ls-mode remote ip-address 1.1.1.10
[XE-ps] start
[XE-ps] gatekeeper // 启用处理服务器的GK功能
[XE-ps-gk] start
5. 配置位置服务器 (公网location-server)
# 配置以太网接口
[XE] interface ethernet 0/0
[XE-Ethernet0/0] ip address 1.1.1.10 255.255.0.0
[XE-Ethernet0/0] quit
# 配置位置服务器
[XE] location-server
[XE-ls] ls-config interface Ethernet 0/0
[XE-ls] call-mode h323 routed // 配置网守为路由呼叫模式
[XE-ls] start
[XE-ls] domain PriDomain // 设定域的名称
[XE-ls-domain-PriDomain] attribute private // 配置域的私有属性
[XE-ls-domain-PriDomain] quit
[XE-ls] domain PubDomain // 设定域的名称
[XE-ls-domain-PubDomain] attribute public // 配置域的公有属性
[XE-ls-domain-PubDomain] quit
[XE-ls] process-server xeippbx1
[XE-ls-ps-xeippbx1] ip-address 1.1.1.1
[XE-ls-ps-xeippbx1] heartbeat password xe200
[XE-ls-ps-xeippbx1] belongto PriDomain // 配置process-server所有//域的名称 (私有域)
[XE-ls-ps-xeippbx1] quit
[XE-ls] process-server xeippbx2
[XE-ls-ps-xeippbx2] ip address 1.1.1.11
[XE-ls-ps-xeippbx2] heartbeat password xe200
[XE-ls-ps-xeippbx2] belongto PubDomain // 配置process-server所有域//的名称 (私有域)
[XE-ls-ps-xeippbx2] quit

```

```

[XE-ls] nat&fw // 进入隧道穿越视图
[XE-ls-nat&fw] tunnelpeer tunnelpeer01 private xeipbpx1 1.1.1.11 port 9600 public xe
ipbpx2 1.1.1.1 port 9700 // 在公网处理服务器和私网处理服务器之间建立隧道
[XE-ls-nat&fw] quit
[XE-ls] process-server xeipbpx1
[XE-ls-ps-xeipbpx2] tunnel enable // 启用process-server的隧道功能
[XE-ls-ps-xeipbpx1] quit
[XE-ls] process-server xeipbpx2
[XE-ls-ps-xeipbpx2] tunnel enable // 启用process-server的隧道功能
[XE-ls-ps-xeipbpx2] quit
[XE-ls] gateway h323gateway1 // 配置私网注册网关
[XE-ls-gw-h323gateway1] device-type h323
[XE-ls-gw-h323gateway1] dynamic-ip enable
[XE-ls-gw-h323gateway1] quit
[XE-ls] gateway h323gateway2 // 配置公网注册网关
[XE-ls-gw-h323gateway2] device-type h323
[XE-ls-gw-h323gateway2] dynamic-ip enable

```

6. NAT/FW的配置

```

# 配置以太网接口
<Quidway> system-view
[Quidway] interface GigabitEthernet 0/0
[Quidway-GigabitEthernet0/0] ip address 1.1.1.1 255.255.0.0
[Quidway-GigabitEthernet0/0] quit
[Quidway] interface GigabitEthernet 0/1
[Quidway-GigabitEthernet0/1] ip address 192.168.1.1 255.255.0.0
[Quidway-GigabitEthernet0/1] quit
# 配置访问控制列表。
[Quidway] acl number 2001
[Quidway-acl-basic-2001] rule permit source 192.168.1.0 0.0.0.255 // 配置ACL
[Quidway-acl-basic-2001] quit
[Quidway] interface GigabitEthernet 0/0
[Quidway-GigabitEthernet0/0] nat outbound 2001 // 在接口下绑定nat到公网的ACL
[Quidway-GigabitEthernet0/0] nat server protocol udp global 1.1.1.1 9700 inside 192.
168.1.10 9700 // 将公网process-server映射到私网的process-server上

```

四、配置关键点

如果需要公、私网之间隧道穿越，首要条件是公网和私网都必须有process-server，而公网的process-server可以和location-server位于同一台XE上。其次需要在location-server上配置公有域public和私有域private，然后分别指定公、私网的process-server所属的域，并且location-server采用h323路由呼叫。最后要在隧道穿越视图下配置隧道穿越的规则，如：

```
tunnelpeer tunnelpeer01 private xeipbpx1 1.1.1.11 port 9600 public xeipbpx2 1.1.1.1
port 9700
```

其中1.1.1.11是指私网PS看到的公网PS的IP地址，即公网PS的IP地址，而1.1.1.1是公网PS侧看到的私网PS的IP地址，一般为防火墙的WAN口IP地址。此规则与NAT/FW设备上的映射规则是对应的，如：

```
nat server protocol udp global 1.1.1.1 9700 inside 192.168.1.10 9700
```

同时还需要在NAT/FW设备上配置私网外出访问公网的nat outbound，保证私网能够访问公网。