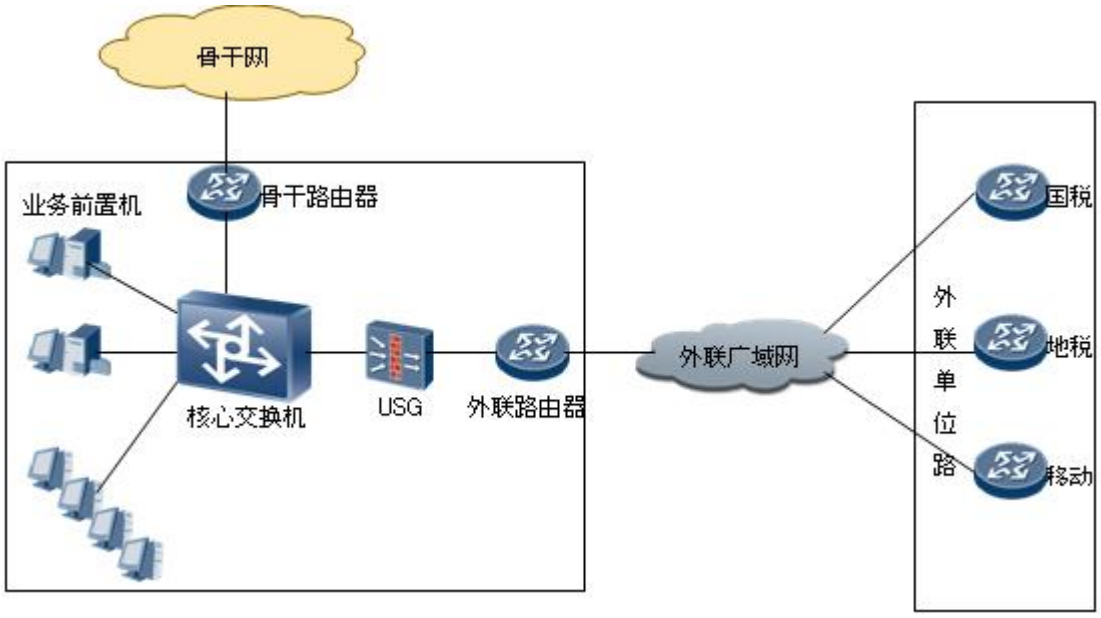
防火墙透明模式下做双向 NAT 典型配置

一、组网需求

如下图所示：某市银行通过外联路由器连接国税，地税等外联单位，通过骨干路由器连接银行骨干网。为了保证内网的安全，在外联单位和内网之间部署了一台 USG 防火墙，通过严格的规则限制内网和外联单位之间的互相访问。



具体需求如下：

- 防火墙采用透明模式接入，不影响原有的网络结构和地址规划。G0/0/0 连接内网核心交换，TRUST 区域，G0/0/1 连接外联路由器，UNTRUST 区域。
- 业务访问需求：外联单位只能够访问内网的业务前置机的特定端口。内网的业务前置机和某些终端可以访问外联单位的业务主机。
- 对外联单位发布一个业务前置机的虚地址，对内网用户发布一个外联单位业务主机的虚地址。
- 外联单位业务主机只允许固定的某个地址可以访问。
- 为了保证内网安全，不能在内网的核心三层交换机上配置到到外联单位的路由。
- 为了保证路由器性能，外联路由器只做路由转发，通过防火墙做 NAT 策略。

二、IP 地址，NAT 地址规划：

项目	数据	备注
	接口编号：G/0/0/0 接口编号：G/0/0/1 接口加入 VLAN10 Ip 地址;无	防火墙透明模式下可以使用额外的接口配置地址进行管理。也可以配置 VLAN 地址，来进行管理
安全区域	Trust：GigabitEthernet 0/0/0 Untrust：GigabitEthernet 0/0/1	
业务前置机	真实地址：10.112.0.1/24 对外发布地址：9.108.101.10/24	外联国税服务器只允许源地址为 9.108.101.10 的地址访问
外联单位服务器（国税）	真实地址：9.108.100.1/24 对内发布地址：10.112.100.1/24	内部用户通过访问 10.112.100.1 来访问外联单位国税服务器

三、配置思路

配置 USG 的工作模式，并将接口加入相应安全区域。

配置域间防火墙策略。

配置 Trust 到 Untrust 的 NAT Outbound.

配置 Untrust 到 Trust 的 NAT Inbound.

配置 NAT Server

四、操作步骤

1. 配置 USG5310 的工作模式并将接口加入对应安全区域。

```
<USG5310>system-view
[USG5310]firewall mode  transparent
```

2. 将接口加入安全区域

```
[USG5310]firewall zone  trust
[USG5310-zone-trust]add  interface GigabitEthernet 0/0/0
[USG5310-zone-trust]quit

[USG5310]firewall zone  untrust
[USG5310-zone-untrust]add  interface GigabitEthernet 0/0/1
[USG5310-zone-untrust]quit
```

3． 配置域间防火墙策略

略

4． 配置 NAT 地址池

[USG5310]nat address-group 1 9.108.101.10 9.108.101.10 此 nat 地址池用于内网终端和业务前置机访问外联服务器时的 nat outbound 规则

[USG5310]nat address-group 2 10.112.100.1 10.112.100.1 此 nat 地址池用于外联服务器访问内网业务前置机时的 nat inbound 规则

配置 trust 到 untrust 的 NAT Outbound 规则

[USG5310]nat-policy interzone trust untrust outbound

[USG5310-nat-policy-interzone-trust-untrust-outbound]policy 1

[USG5310-nat-policy-interzone-trust-untrust-outbound-1]policy source 10.112.0.0 0.0.0.255

[USG5310-nat-policy-interzone-trust-untrust-outbound-1]action source-nat

[USG5310-nat-policy-interzone-trust-untrust-outbound-1]address-group 1

[USG5310-nat-policy-interzone-trust-untrust-outbound-1quit

配置 trust 到 untrust 的 NAT Inbound 规则

[USG5310]nat-policy interzone trust untrust inbound

[USG5310-nat-policy-interzone-trust-untrust-inbound]policy 1

[USG5310-nat-policy-interzone-trust-untrust-inbound-1]policy source 9.108.100.10 0

[USG5310-nat-policy-interzone-trust-untrust-inbound-1]action source-nat

[USG5310-nat-policy-interzone-trust-untrust-inbound-1]address-group 2

[USG5310-nat-policy-interzone-trust-untrust-inbound-1]quit

配置 NAT Server 规则

[USG5310]nat server global 9.108.101.10 inside 10.112.0.1

[USG5310]nat server global 10.112.100.1 inside 9.108.100.10

从外联单位服务器(9.108.100.10)上 ping 9.108.101.10,在防火墙上看到会话表如下：

[USG5310]disp firewall session table

17:49:38 2011/02/22

Current Total Sessions : 2

icmp VPN: public -> public

9.108.101.10:768[10.112.0.1:12838]<--9.108.100.10:768[10.112.100.1:12838]

从内网业务服务器(10.112.0.1)ping 10.112.100.1,在防火墙看到会话表如下：

10.112.0.1:44000[9.108.101.10:44000]-->10.112.100.1:44000[9.108.100.10:44000]

配置脚本：

```
<USG5310>disp cu
18:08:23  2011/02/22
#
acl number 2000
 rule 0 permit
#
 sysname USG5310
#
 ftp server enable
#
 web-manager enable
 web-manager security enable
#
 firewall packet-filter default permit interzone local t
 firewall packet-filter default permit interzone local t
 firewall packet-filter default permit interzone local u
 firewall packet-filter default permit interzone local u
d
 firewall packet-filter default permit interzone local d
 firewall packet-filter default permit interzone local d
 firewall packet-filter default permit interzone trust u
 firewall packet-filter default permit interzone trust u
d
 firewall packet-filter default permit interzone trust d
 firewall packet-filter default permit interzone trust d
 firewall packet-filter default permit interzone dmz unt
 firewall packet-filter default permit interzone dmz unt
#
 nat address-group 1 9.108.101.10 9.108.101.10
 nat address-group 2 10.112.100.1 10.112.100.1
 nat server 0 global 9.108.101.10 inside 10.112.0.1
 nat server 1 global 10.112.100.1 inside 9.108.100.10
#
 firewall statistic system enable
#
interface Vlanif10   (如果核心交换机和路由器之间互联地址为 30 为掩码，可以不用配置 VLAN 地址，采用额外的一个防火墙接口进行管理)
 ip address 9.107.1.3 255.255.255.0
#
interface GigabitEthernet0/0/0
 port default vlan 10
#
interface GigabitEthernet0/0/1
```

```
 port default vlan 10
#
interface GigabitEthernet0/0/2
#
interface GigabitEthernet0/0/3
#
interface NULL0
#
firewall zone local
 set priority 100
#
firewall zone trust
 set priority 85
 add interface GigabitEthernet0/0/0
#
firewall zone untrust
 set priority 5
 add interface GigabitEthernet0/0/1
#
firewall zone dmz
 set priority 50
#
firewall interzone local untrust
 detect ftp
#
policy interzone local untrust inbound
 policy 1
 action permit
 policy source 192.168.1.2 0
#
nat-policy interzone trust untrust inbound
 policy 1
 action source-nat
 policy source 9.108.100.0 0.0.0.255
 address-group 2
#
aaa
 local-user admin password cipher ]MQ;4\]B+4Z,YWX*NZ55OA
 local-user admin service-type web telnet
 local-user admin level 3
 local-user ftp password simple Admin@123
 local-user ftp service-type ftp
 local-user ftp ftp-directory flash:/
```

```
 authentication-scheme default
#
 authorization-scheme default
#
 accounting-scheme default
#
 domain default
#
right-manager server-group
#
rip
#
 ip route-static 10.112.0.0 255.255.255.0 9.107.1.1
#
user-interface con 0
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 3
 protocol inbound telnet
#
Return
```

外联路由器，核心交换机配置略。