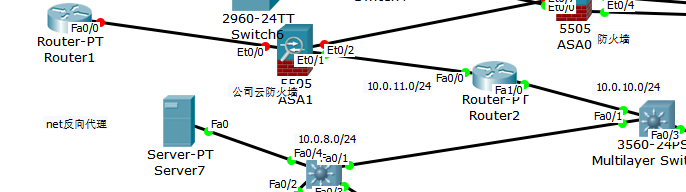
**技术原理**

NAT将网络划分为内部网络和外部网络两部分，局域网主机利用NAT访问网络时，是将局域网内部的本地地址转换为全局地址(互联网合法的IP地址)后转发数据包；

NAT分为两种类型：NAT(网络地址转换)和NAPT(网络端口地址转换IP地址对应一个全局地址)。

NAPT：使用不同的端口来映射多个内网IP地址到一个指定的外网IP地址，多对一。

NAPT采用端口多路复用方式。内部网络的所有主机均可共享一个合法外部IP地址实现对Internet的访问，从而可以最大限度地节约IP地址资源。又可隐藏网络内部的所有主机，有效避免来自Internet的攻击。因此，目前网络中应用最多的就是端口多路复用方式。



反向代理拓扑结构

ROUTE 2 进行NAPT 反向代理

命令：

Router>

Router>enable

Router>enable

Router#conf t

Enter configuration commands, one per line. End with CNTL/Z.

Router(config)#int fa1/0

Router(config-if)#ip nat inside

Router(config-if)#exit

Router(config)#int fa 0/0

Router(config-if)#ip nat dmz

^

% Invalid input detected at '^' marker.

Router(config-if)#ip nat outside

Router(config-if)#exit

Router(config)#access-list 1 permit 10.0.10.0 0.0.0.255

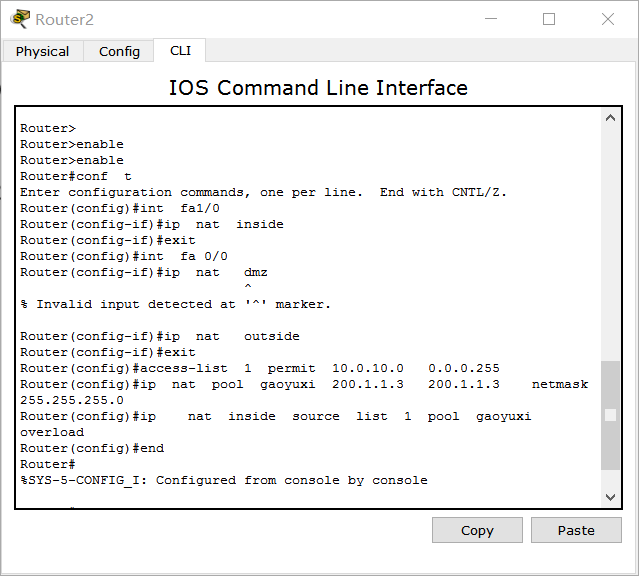
Router(config)#ip nat pool gaoyuxi 200.1.1.3 200.1.1.3 netmask 255.255.255.0

Router(config)#ip nat inside source list 1 pool gaoyuxi overload

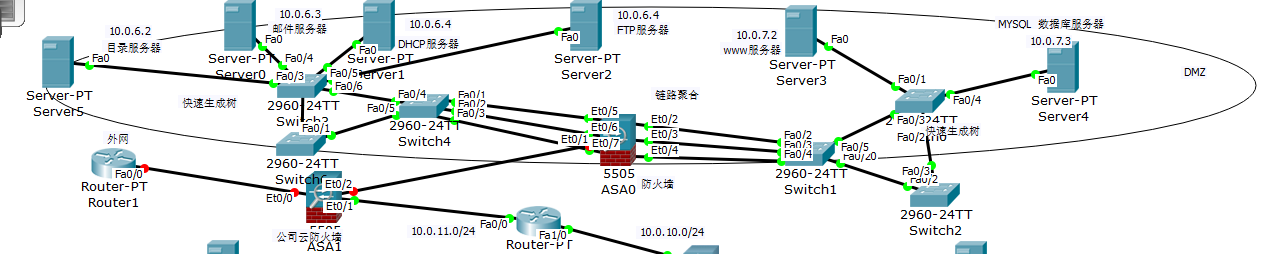
Router(config)#end

Router#

Rouer#show ip nat translations



防火墙：



防火墙体系结构：

**硬件防火墙的优点：**

 硬件防火墙功能强大，且明确是为了抵御威胁而设计的；

 硬件防火墙比软件防火墙的漏洞少。

Cisco**硬件防火墙技术应用于以下三个领域：**

PIX 500系列安全设备；

ASA 5500系列自适应安全设备；

Catalyst 6500系统交换机和Cisco 7600系统路由器的防火墙服务模块（FWSM，Firewall Services Module）；

**ASA安全设备**:

Cisco ASA 系列5500系列自适应安全设备室最新的cisco防火墙技术产品，它提供了整合防火墙，入侵保护系统（IPS，Intrusion Prevention System）、高级自适应威胁防御服务，其中包括应用安全和简化网络安全解决方案的VPN服务。

2.

ASA**的安全算法**:

**状态化防火墙：**ASA **是一个状态化防火墙，状态化防火墙维护一个关于用户信息的连接表，称为**Conn**表。**

**表中的关键信息：**

源IP地址。

目的IP地址。

IP协议（eg：TCP 或UDP）。

IP协议信息（eg：TCP/UDP端口号,TCP序列号，TCP控制位）

**默认情况下，**ASA

**对**TCP

**和**UDP

**协议提供状态化连接，但**ICMP

**协议是非状态化的。**

ciscoasa> enable

ciscoasa# config terminal

ciscoasa(config)# hostname ASA1

配置密码：

ASA(config)# enable password 666     ——配置特权密码

ASA(config)# passwd 666

ASA的每个接口都有一个安全级别，范围是0~100，数值越大其安全级别越高。

不同安全级别的接口之间互相访问时，遵循的规则：

**允许出站连接**：即允许从高安全级别接口道低安全级别接口的流量通过，eg：从inside到outside时允许的；

**禁止入站连接**：即禁止从低安全级别接口到高安全级别接口的流量通过，eg：从outside到inside是禁止的；

**禁止相同安全级别的接口之间通信**。

接口的配置：

**配置接口的名称**：

ciscoasa(config-if)# nameif  name

**配置接口的安全级别：**

ciscoasa(config-if)# security-level  number

number的范围： 0~100

Ethernet 0/0接口的配置：

ciscoasa(config)# int e0/0

ciscoasa(config-if)# nameif outside

INFO: Security level for "outside" set to 0 by default.

ciscoasa(config-if)# security-level 0

ciscoasa(config-if)# ip add 200.1.1.3 255.255.255.0

ciscoasa(config-if)# no sh

Ethernet 0/1接口的配置：

ciscoasa(config)# int e0/1

ciscoasa(config-if)# nameif inside

INFO: Security level for "inside" set to 100 by default.

ciscoasa(config-if)# security-level 100

ciscoasa(config-if)# ip add 10.1.1.1 255.255.255.0

ciscoasa(config-if)# no sh

ACL：

允许入站连接：

ciscoasa(config)# access-list out\_to\_in permit ip host 172.16.1.1 host 10.1.1.1

ciscoasa(config)# access-group out\_to\_in in int outside

控制出站连接的流量：

ciscoasa(config)# access-list  in\_to\_out  deny  ip 10.1.1.0  255.255.255.0  any

ciscoasa(config)# access-list  in\_to\_out  permit  ip  any  any

ciscoasa(config)# access-group  in\_to\_out  in  int  inside

ICMP协议：默认情况下，禁止ICMP报文穿越ASA是基本的安全性考虑。

保存running configuration 配置到startup configuration ：

ciscoasa(config)# **write memory**

ciscoasa(config)# **copy running-config startup-config**

清除running configuration 所有的配置

ciscoasa(config)# **clear configure all**

清除running configuration中指定命令的配置：

eg：清除所有access-list命令的配置：

ciscoasa(config)# **clear configure access-list**

eg：只删除access-listin\_to\_out的配置：

ciscoasa(config)# clear configure access-list in\_to\_out

删除startup-config配置文件：

ciscoasa# **write erase**

**4.**多安全区域:

DMZ区域概述:

DMZ：称为“隔离区”，也称“非军事化区”，是位于企业内部网络和外部网络之间的一个网络区域。

DMZ内通常放置一些不含机密信息的公用服务器，这样来自外网的访问DMZ中的服务，但不能访问内网中的公司机密等信息。

DMZ的默认访问规则：

Inside**可以访问**outside**；**

Inside**可以访问**DMZ**；**

DMZ**可以访问**outside**；**

DMZ**不能访问**inside**；**

Outside**不能访问**inside**；**

Outside**不能访问**DMZ