UTM内部服务器(NAT Server)典型配置指导

万欣 2008-11-25 发表

UTM内部服务器(NAT Server)典型配置

1 配置举例

1.1 外网访问私网的服务器

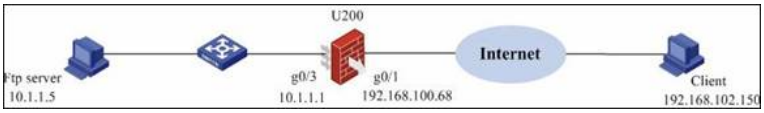
1、组网需求

某公司内部对外提供FTP服务，公司内部网址为10.1.1.0/24。其中，内部FTP服务器地址为10.1.1.5/24。公司拥有192.168.100.68/22至192.168.100.70/22三个IP地址。需要实现如下功能：

？ 外部的主机可以访问内部的服务器。

选用192.168.100.68作为公司对外的接口IP地址， FTP服务器使用192.168.100.70作为对外的IP地址

2、 组网图



具体配置可通过命令行或WEB方式进行配置：

3、命令行配置（接口已经配置IP地址，并加入安全域）

配置访问控制列表。//定义内网流量

<U200A> system-view

[U200A] acl number 3010

[U200A-acl-adv-3010] rule permit ip source 10.1.1.0 0.0.0.255

[U200A-acl-adv-3010] quit

配置NAT转换。 //定义内网用户访问外网时需要将源地址转换为G0/1的地址

[U200A] interface inter GigabitEthernet 0/1

[U200A-GigabitEthernet0/1] nat outbound 3010

配置内部FTP服务器。//定义内网服务器被外网用户访问时将地址转换成192.168.100.70

[U200A-GigabitEthernet0/1] nat server protocol tcp global 192.168.100.70 ftp inside 10.1.1.5 ftp

4、WEB配置

配置访问控制列表ACL 3010。

在导航栏中选择“策略管理 > ACL”，新建ID为3010的ACL，配置允许源IP地址为“10.1.1.0”，通配符为“0.0.0.255”的流通过。

配置动态地址转换

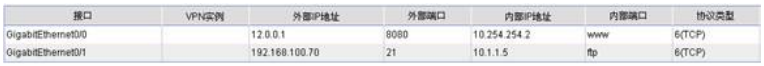
在导航栏中选择“策略管理 > 地址转换策略 > 动态地址转换”，在对外的接口g0/1上引用ACL3010。

& 注：

如上采用Easy-IP方式，即直接使用该接口的IP地址作为转换后的公网地址。

也可以在该接口上配置ACL3010和NAT地址池（192.168.100.69-192.168.100.70）相关联（在“对象管理”中配置），即PAT方式，符合ACL规则的报文的源IP地址可以使用地址池中的地址进行地址转换。

配置内部FTP服务器，选择“策略管理>地址转换策略>内部服务器”，在对外的接口g0/1上配置FTP服务器的地址转换。



1.2 私网用户通过公网地址访问内部服务器

1.2.1 私网用户和内部服务器在不同网段

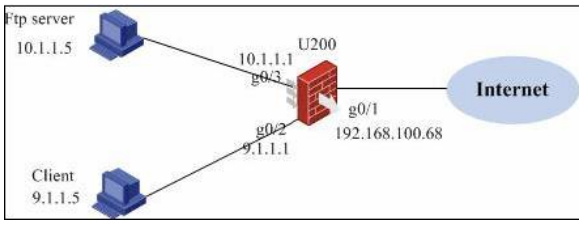
1、组网需求

需要实现如下功能：

l 选用192.168.100.68作为公司对外的接口IP地址， FTP服务器使用192.168.100.70作为对外的IP地址

l 内部的主机与内部服务器在不同网段，可以通过FTP服务器的公网地址来访问它。

2、组网图



3、命令行配置

配置内部FTP服务器，在Client端连接的接口g0/2上配置nat server。

[U200A-GigabitEthernet0/2] nat server protocol tcp global 192.168.100.70 ftp inside 10.1.1.5 ftp

4、WEB配置

配置内部FTP服务器。

选择“策略管理>地址转换策略>内部服务器”, 选择“策略管理>地址转换策略>内部服务器”

接口	VPN实例	外部IP地址	外部端口	内部IP地址	内部端口	协议类型	操作
GigabitEthernet0/0		12.0.0.1	8080	10.254.254.2	www	6(TCP)	
GigabitEthernet0/2		192.168.100.70	21	10.1.1.5	ftp	6(TCP)	

1.2.2 私网用户和内部服务器在同一网段

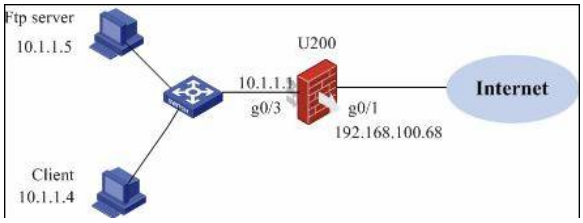
1、组网需求

需要实现如下功能：

l 选用192.168.100.68作为公司对外的接口IP地址， FTP服务器使用192.168.100.70作为对外的IP地址

l 内部的主机和内部FTP服务器在同一网段，可以通过FTP服务器的公网地址来访问它。

2、组网图



3、命令行配置

配置访问控制列表。

<U200A> system-view

[U200A] acl number 3010

[U200A-acl-adv-3010] rule permit ip source 10.1.1.0 0.0.0.255

[U200A-acl-adv-3010] quit

在内部连接主机的接口g0/3上配置NAT转换。 //注意，此处在内部接口上要配置nat outbound。

[U200A] interface inter GigabitEthernet 0/3

[U200A-GigabitEthernet0/3] nat outbound 3010

配置内部FTP服务器，在内部主机连接的接口g0/3上配置nat server。

[U200A-GigabitEthernet0/3] nat server protocol tcp global 192.168.100.70 ftp inside 10.1.1.5 ftp

4、WEB配置

配置访问控制列表ACL 3010。

高级ACL 3010

规则ID	操作	描述	时间段	操作
0	permit	ip source 10.1.1.0 0.0.0.255	无限制	

配置动态地址转换

在导航栏中选择“策略管理 > 地址转换策略 > 动态地址转换”。

接口	ACL	地址池索引	地址转换方式	操作
GigabitEthernet0/3	3010		Easy IP	

配置内部FTP服务器，选择“策略管理>地址转换策略>内部服务器”。

接口	VPN实例	外部IP地址	外部端口	内部IP地址	内部端口	协议类型
GigabitEthernet0/0		12.0.0.1	8080	10.254.254.2	www	6(TCP)
GigabitEthernet0/1		192.168.100.70	21	10.1.1.5	ftp	6(TCP)

1.3 验证配置结果

Client可以访问内部FTP服务器。