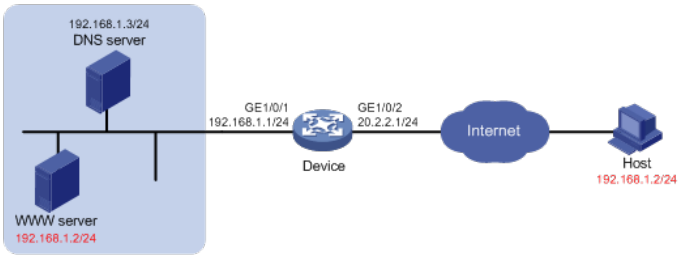
H3C Secpath M9000多业务安全网关入方向NAT典型配置

NAT 沈博文 2015-10-30 发表

主要应用需求：某公司分支局点主机可以通过专线连接到总部，但是使用私网地址同总部地址存在重叠，需要实现，分支可以通过域名访问与其地址重叠的总部Web服务器。



- 某公司总部使用的IP地址网段为192.168.1.0/24。
- 该公司总部针对分支提供Web服务，Web服务器地址为192.168.1.2/24。
- 该公司总部有一台DNS服务器，IP地址为192.168.1.3/24，用于解析Web服务器的域名。
- 该公司拥总部有三个外网IP地址：202.38.1.2、202.38.1.3和202.38.1.4。

按照组网图配置各接口的IP地址。

开启DNS协议的ALG功能。

[M9000] nat alg dns

配置ACL 2000，允许对总部网络中192.168.1.0/24网段的报文进行地址转换。

[M9000] acl number 2000

[M9000-acl-basic-2000] rule permit source 192.168.1.0 0.0.0.255

创建地址组1。

[M9000] nat address-group 1

添加地址组成员202.38.1.2。

[M9000-address-group-1] address 202.38.1.2 202.38.1.2

创建地址组2。

[M9000] nat address-group 2

添加地址组成员202.38.1.3。

[M9000-address-group-2] address 202.38.1.3 202.38.1.3

在接口GigabitEthernet1/0/2上配置NAT内部服务器，允许分支主机使用地址202.38.1.4访问总部DNS服务器。

[M9000] interface gigabitethernet 1/0/2

[M9000-GigabitEthernet1/0/2] nat server protocol udp global 202.38.1.4 inside 192.168.1.3 dns

在接口GigabitEthernet1/0/2上配置出方向动态地址转换，允许使用地址组1中的地址对DNS应答报文载荷中的内网地址进行转换，并在转换过程中不使用端口信息，以及允许反向地址转换，以使分支主机访问NAT之后的总部WEB服务器地址时可以匹配已建立的地址转换关系将目的地址转换为WEB服务器真实地址。

[M9000-GigabitEthernet1/0/2] nat outbound 2000 address-group 1 no-pat reversible

在接口GigabitEthernet1/0/2上配置入方向动态地址转换，允许使用地址组2中的地址对外网访问内网的报文进行源地址转换，并在转换过程中使用端口信息。

[M9000-GigabitEthernet1/0/2] nat inbound 2000 address-group 2

配置到达202.38.1.3地址的静态路由，出接口为GigabitEthernet1/0/2，下一跳地址为20.2.2.2（20.2.2.2为本例中的直连下一跳地址，实际使用中请以具体组网情况为准）。

这是一个典型的双向NAT应用，具体关键点如下。

- 分支主机通过域名访问Web服务器，首先需要访问总部的DNS服务器获取Web服务器的IP地址，因此需要通过配置NAT将内部服务器将DNS服务器的内网IP地址和DNS服务端口映射为一个外网地址和端口。
- DNS服务器回应给分支主机的DNS报文载荷中携带了Web服务器的总部内网IP地址，该地址与分支主机地址重叠，因此在出方向上需要为内网Web服务器动态分配一个NAT地址，并将载荷中的地址转换为该地址。NAT地址分配可以通过出方向动态地址转换功能实现，转换载荷信息可以通过DNS ALG功能实现。
- 分支主机得到总部Web服务器的IP地址之后（该地址为NAT后地址），使用该地址访问内网Web服务器，因为分支主机的地址与总部Web服务器的实际地址重叠，因此在入方向上也需要为外网主机动态分配一个NAT地址，可以通过入方向动态地址转换实现。
- NAT设备上没有目的地址为分支主机对应的NAT后地址的路由，因此需要手工添加静态路由，使得目的地址为分支主机NAT后地址的报文的出接口为GigabitEthernet1/0/2。