目 录

1 ALG配置

1.1 ALG简介

ALG（Application Level Gateway，应用层网关）主要完成对应用层报文的处理。通常情况下，NAT只对报文头中的IP地址和端口信息进行转换，不对应用层数据载荷中的字段进行分析。然而一些特殊协议，它们报文的数据载荷中可能包含IP地址或端口信息，这些内容不能被NAT进行有效的转换，就可能导致问题。

例如，FTP应用就由数据连接和控制连接共同完成，而且数据连接的建立动态地由控制连接中的载荷字段信息决定，这就需要ALG来完成载荷字段信息的转换，以保证后续数据连接的正确建立。

ALG在与NAT（Network Address Translation，网络地址转换）、ASPF（Application Specific Packet Filter，基于应用层状态的包过滤）配合使用的情况下，可以实现地址转换、数据通道检测和应用层状态检查的功能。

- 地址转换

对报文应用层数据载荷中携带的IP地址、端口、协议类型（TCP或者UDP）、对端地址（在数据载荷中带有对端的地址）进行地址转换。

- 数据通道检测

提取数据通道信息，为后续的报文连接建立数据通道。此处的数据通道为相对于用户的控制连接而言的数据连接。

- 应用层状态检查

对报文的应用层协议状态进行检查，若正确则更新报文状态机进行下一步处理，否则丢弃报文。

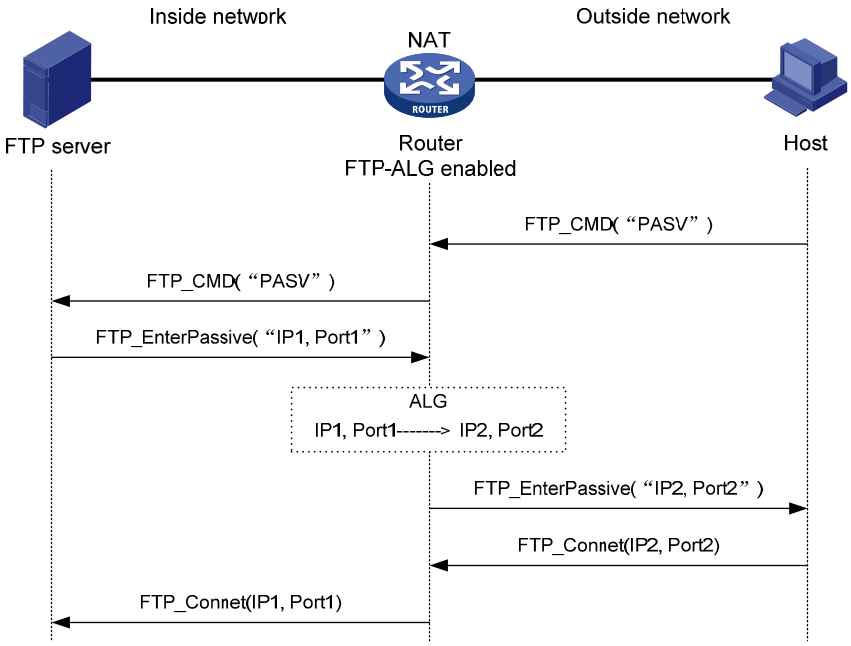
本特性支持对多种应用层协议的ALG处理，不同的协议对以上三种功能的支持情况有所不同，实际中根据具体需要选择支持全部或部分功能。

目前实现ALG功能的常用应用层协议包括：

- DNS（Domain Name System，域名系统）
- FTP（File Transfer Protocol，文件传输协议）
- GTP（GPRS Tunneling Protocol，GPRS隧道协议）
- H.323（包括RAS、H.225、H.245），一种多媒体会话协议
- ILS（Internet Locator Server，Internet定位服务）
- MSN/QQ，两种常见的语音视频通讯协议
- NBT（Network Basic Input/Output System，网络基本输入/输出系统）
- PPTP（Point-to-Point Tunneling Protocol，点到点隧道协议）
- RTSP（Real-Time Streaming Protocol，实时流协议）
- SCCP（Skinny Client Control Protocol，瘦小客户端控制协议）
- SIP（Session Initiation Protocol，会话发起协议）
- SQLNET，一种Oracle数据库语言
- TFTP（Trivial File Transfer Protocol，简单文件传输协议）

下面以FTP协议为例，简单描述使能ALG特性的设备在网络中的工作过程。如 图 1-1所示，位于外部网络的客户端以PASV方式访问内部网络的FTP服务器，经过中间的设备Router进行NAT转换，该设备上使能了ALG特性。

图1-1 PASV 方式的 FTP-ALG



整个通信过程包括如下四个阶段：

(1) 建立控制通道

客户端向服务器发送 TCP 连接请求。TCP 连接建立成功后，服务器和客户端进入用户认证阶段。若 TCP 连接失败，服务器会断开与客户端的连接。

(2) 用户认证

客户端向服务器发送认证请求，报文中包含 FTP 命令（USER、PASSWORD）及命令所对应的内容。

客户端发送的认证请求报文在通过配置了 ALG 的设备时，报文载荷中携带的命令字将会被解析出来，用于进行状态机转换过程是否正确的检查。若状态机转换发生错误，则丢弃报文。这样可防止客户端发送状态机错误的报文攻击服务器或者非法登陆服务器，起到保护服务器的作用。

客户端的认证请求报文通过 ALG 处理之后，到达服务器端，服务器将对其进行响应。

(3) 创建数据通道

认证状态正确且用户是服务器已经授权的客户端，才能和服务器建立数据连接，进行数据的交互。

如 图 1-1所示，当客户端发送“PASV”命令发起连接时，服务器会在发送给客户端的PASV响应报文中携带自己的私网地址和端口号（IP1，Port1），响应报文经过ALG设备时被解析，其中携带的服务器的私网地址和端口号被转换成其对应的公网地址和端口号（IP2，Port2），之后在该地址和端口与客户端的地址和端口之间将建立起数据通道。

(4) 数据交互

客户端和服务器之间的数据交互可以直接通过数据通道来进行。

1.2 配置使能ALG功能

操作	命令	说明
进入系统视图	**system-view**	-
使能指定协议的 ALG 功能	**alg** { **all** | **dns** | **ftp** | **gtp** | **h323** | **ils** | **msn** | **nbt** | **pptp** | **qq** | **rtsp** | **sccp** | **sip** | **sqlnet** | **tftp** }	可选 缺省情况下，所有协议的 ALG 功能均处于使能状态

1.3 ALG典型配置举例

说明

以下典型配置举例中，需保证服务器和客户端的配置已经完成，本节只介绍设备端的 ALG 配置，其它配置略。

1.3.1 ALG支持FTP典型配置举例

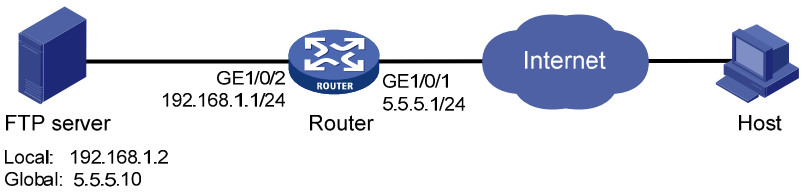
1. 组网需求

如 图 1-2所示，某公司通过启用了NAT和ALG功能的设备连接到Internet。公司内部对外提供FTP服务。公司内部网络地址为 192.168.1.0/24。其中，内部FTP服务器的IP地址为 192.168.1.2。通过配置NAT和ALG，满足如下要求：

- 外部网络的 Host 可以访问内部的 FTP 服务器。
- 公司具有 5.5.5.1、5.5.5.9～5.5.5.11 四个合法的公网 IP 地址。FTP 服务器使用 5.5.5.10 作为对外的 IP 地址。

2. 组网图

图1-2 ALG 应用组网图



3. 配置步骤

配置地址池和访问控制列表。

```
<Router> system-view
[Router] nat address-group 1 5.5.5.9 5.5.5.11
[Router] acl number 2001
[Router-acl-basic-2001] rule permit
[Router-acl-basic-2001] quit
```

使能 FTP 协议的 ALG 功能。

```
[Router] alg ftp
```

配置 NAT 转换。

```
[Router] interface gigabitethernet 1/0/1
[Router-GigabitEthernet1/0/1] nat outbound 2001 address-group 1
```

配置内部 FTP 服务器。

```
[Router-GigabitEthernet1/0/1] nat server protocol tcp global 5.5.5.10 ftp inside 192.168.1.2
ftp
```

1.3.2 ALG支持SIP/H.323 典型配置举例

说明

ALG 支持 H.323 的典型配置方法与支持 SIP 的类似，下面仅以 SIP 为例。

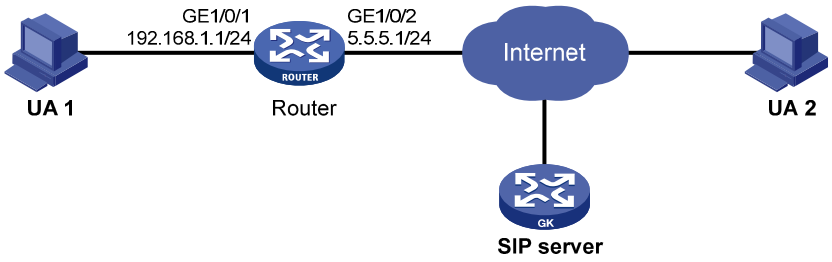
1. 组网需求

如 图 1-3所示，某公司通过启用了NAT和ALG功能的设备连接到Internet。公司内部网络地址为192.168.1.0/24。通过配置NAT和ALG，满足如下要求：

- 公司内部的 SIP UA 1 和外部网络的 SIP UA 2 均可以通过别名与对方成功建立通信。
- 公司具有 5.5.5.1、5.5.5.9～5.5.5.11 四个合法的公网 IP 地址。公司内部 SIP UA 1 在向外部的 SIP server 注册时选择 5.5.5.9～5.5.5.11 中的一个地址作为其公网地址。

2. 组网图

图1-3 ALG 支持 SIP 应用组网图



3. 配置步骤

配置地址池和访问控制列表。

```
<Router> system-view
[Router] nat address-group 1 5.5.5.9 5.5.5.11
[Router] acl number 2001
[Router-acl-basic-2001] rule permit source 192.168.1.0 0.0.0.255
[Router-acl-basic-2001] rule deny
[Router-acl-basic-2001] quit
```

使能 SIP 协议的 ALG 功能。

```
[Router] alg sip
```

配置 NAT 转换。

```
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] nat outbound 2001 address-group 1
```

1.3.3 ALG支持NBT典型配置举例

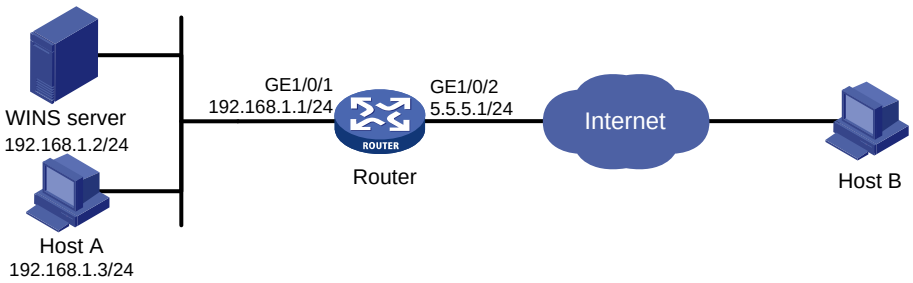
1. 组网需求

如 图 1-4所示，某公司通过启用了NAT和ALG功能的设备连接到Internet。公司内部对外提供NBT服务。公司内部网络地址为 192.168.1.0/24。其中，内部服务器通过配置NAT和ALG，满足如下要求：

- 外部网络的主机可以通过主机名访问内部的 WINS 服务器和主机。
- Host A 使用 5.5.5.9 作为对外的 IP 地址。WINS 服务器使用 5.5.5.10 作为对外的 IP 地址。

2. 组网图

图1-4 ALG 支持 NBT 应用组网图



3. 配置步骤

配置静态地址转换。

```
<Router> system-view
[Router] nat static 192.168.1.3 5.5.5.9
```

使能 NBT 协议的 ALG 功能。

```
[Router] alg nbt
```

配置 NAT 转换。

```
[Router] interface gigabitethernet 1/0/2
[Router-GigabitEthernet1/0/2] nat outbound static
```

配置内部 WINS 服务器。

```
[Router-GigabitEthernet1/0/2] nat server protocol udp global 5.5.5.10 137 inside 192.168.1.2
137
[Router-GigabitEthernet1/0/2] nat server protocol udp global 5.5.5.10 138 inside 192.168.1.2
138
[Router-GigabitEthernet1/0/2] nat server protocol tcp global 5.5.5.10 139 inside 192.168.1.2
139
```