第5章

网络连接和地址转换

本章要点

- 了解防火墙对 IP 地址翻译、连接的网络流量处理过程。
- 掌握防火墙的网络地址转换技术和配置命令。通过 NAT 和 PAT 功能，保障内部网络地址在网络通信中隐藏网络结构和地址，从而提升网络安全性。
- 理解防火墙通过 NAT 和 PAT 功能，采用一个互联网 IP 地址（或全局 IP 地址），使内部网络主机可以连接到互联网（或外部网络）。

防火墙外网访问 DMZ 和内网

5.1 网络连接

网络会话是 IP 数据包的流动，随之产生的网络流量，是端到端的数据流动，理解这个数据流动方式对理解互联网通信技术是必要的，对理解防火墙运行原理、防火墙技术而言也很重要。理解数据流的流动方式后，更容易理解如何保护数据流的安全性。网络会话通常是由 TCP、UDP 两种协议承载的。TCP 传输控制协议容易检查，UDP 用户数据报协议检查相对困难。防火墙内的数据流动有两个方向，数据向外传输，意味着网络会话是由相对信任的安全区域所发起，流动到相对不信任的安全区域；数据向内传输，意味着网络会话是由相对不信任的安全区域发起，流动到相对信任的安全区域。

网络会话过程中，数据经过 TCP/IP 协议栈，会逐层封装、逐层拆封，形成一个数据帧在网络传送。经由防火墙时，将在数据帧中读取特定的信息，对这个数据流做出处理，决定丢弃或者转发。为了加深理解防火墙是如何处理向内和向外的数据传输，以两个 TCP/IP 传输协议，TCP 和 UDP 分析流动方式。

5.1.1 TCP 穿越防火墙

TCP 是面向连接的协议。如图 5.1 所示，当位于 PIX 防火墙内部一台比较安全的主机发起会话时，防火墙在会话状态过滤器上创建一个日志。PIX 防火墙能够从网络流里抽取出网络会话，实时地主动验证其合法性，维护每个网络连接的状态信息，并对这个网络会话随后的数据包进行检查，判断数据是否符合期望。TCP 数据包经过防火墙发起一个会话连接时，防火墙将记录该网络流，并等待对方确认数据包。此后，防火墙在 TCP 三次握手之后允许该网络连接之间的数据传输。

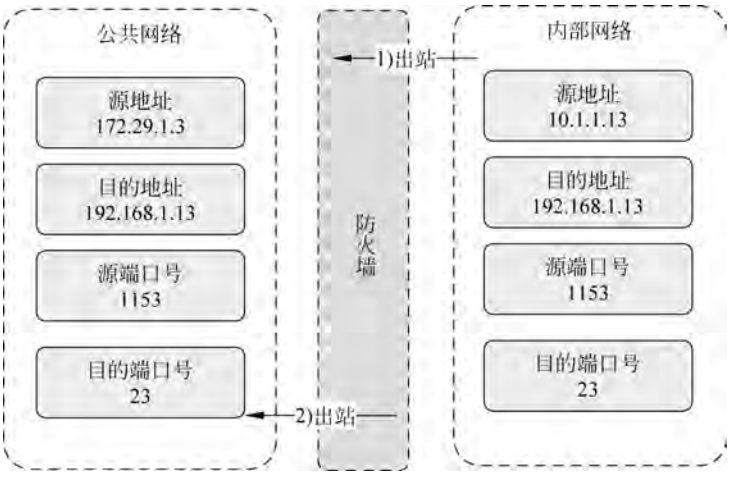

图 5.1 内部网络请求网络通信的出站行为

TCP 是一个面向连接的传输协议，实现了节点间通信的可靠性。TCP 通过创建称作虚电路的连接来完成数据双向通信的传输任务。TCP 协议具有可靠性，保证了节点间的数据传输。TCP 还能够根据网络状况的变化动态地改变连接的传输参数。TCP 数据包头中包含的 TCP 序号和 TCP 应答号，保障了源端和目的端能够有序、准确地传送数据，但这些开销也会使传输速度变慢。图 5.2 描述了 TCP 数据包经过防火墙建立一个 TCP 会话时，防火墙收到入站请求的 IP 数据包处理流程。

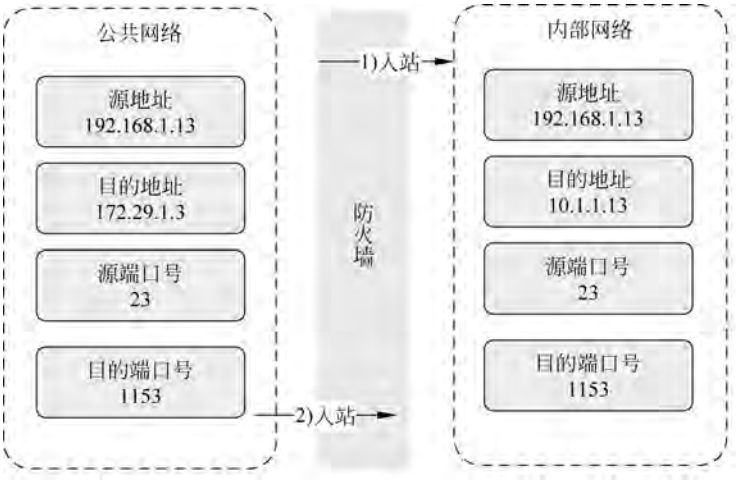

图 5.2 公共网络响应网络通信的入站行为

当防火墙收到一个 IP 数据包时，先检查防火墙的地址映射关系表。如果没有找到地址映射，防火墙将生成一个地址映射。防火墙的地址映射关系表是内部地址（私有 IP 地址）和全局地址（公共 IP 地址）。地址映射关系表的信息保留在内存中，可以对后继的数据包流进行检查。例如，某服务器内部 IP 地址 10.1.1.113 映射成全局地址 222.18.1.101，对外以全局地址访问。

完成三次握手后建立 TCP 会话，并传送数据，否则是一条未完成的半开 TCP 会话。防火墙采用了多种方式限制未完成连接的数量，以防御 TCP 半连接攻击。例如：可以在一个给定的时间内，限定时间范围内防火墙里半开 TCP 会话数的最大值，或半开 TCP 会话完成连接的最大时间跨度，限制“未完成”连接的数量。防火墙将接收的数据包与日志信息进行匹配，匹配到的源地址（端口）和目的地址（端口）时，将数据包转发给内部主机，不匹配的数据包则丢弃并记录。

5.1.2 UDP 穿越防火墙

UPD 会话没有状态信息，缺乏安全性保证，导致 DNS、RPC、NFS 等协议受到攻击，必须通过防火墙保证 UDP 协议的安全性。UDP 协议是一个非连接的传输协议，用于向目的端发送数据。UDP 协议没有提供错误校验、错误校正和发送检验等措施，而是将保障数据可靠性传输的任务交给了上层协议解决，UDP 协议只负责发送数据而不对传输数据进行查验，具有简单和快速的特性，防火墙针对 UDP 数据传输无状态的特性，当 UDP 数据包从在防火墙接口之间穿越时，同样会保存 UDP 连接信息，需要对每一个 UDP 数据包进行检查，根据存储的源目的信息进行匹配，匹配成功会转发到内部网络，否则丢弃。在 PIX 防火墙上关于 UDP 传输的流程如下：

防火墙入口放行 UDP 数据包的条件是，出口方转发了相同目的和源 IP 地址的 UDP 数据包，针对 UDP 数据包而言，防火墙内部存储的这条 UPD 连接的信息只保留有限时间，这个 UDP 连接的数据传输空闲时间超时时会自动失效，并从内存中删除，缺省时间是 2min。

5.2 网络地址转换

防火墙通过地址转换功能处理网络连接数据，采用网络地址转换（Network Address Translation，NAT）命令和端口地址转换（Port Address Translation，PAT）命令实现本地地址和全局地址之间的地址映射。

网络通信的地址转换示意图如图 5.3 所示。内部网络的主机 172.16.1.4 与外部主机 192.168.1.4 通信，序号 1 时可见内部地址 172.16.1.4，进入防火墙后，序号 2 时通过地址转换池，获取外部地址 192.168.1.9，并与外部主机进行通信，序号 3 是出防火墙后的可见地址 192.168.1.9。

安全设备地址转换的规则是：根据地址转换规则创建转换表里的记录，对网络设备配置地址转换，如果 IP 数据包没有匹配上转换表的记录，则无法通过安全设备，安全设备的内部接口将丢弃 IP 数据包。从内部网络发起的会话数据包，经过防火墙出站时，防火墙将内部采用的私有地址转换为全局地址，否则该会话无法连接成功。从互联网发起的会话，经过防火墙出站时，如果该网络连接的目的地址是一个私有地址，网络会话将无法建立，除非防火墙配置了这个会话的放行规则。

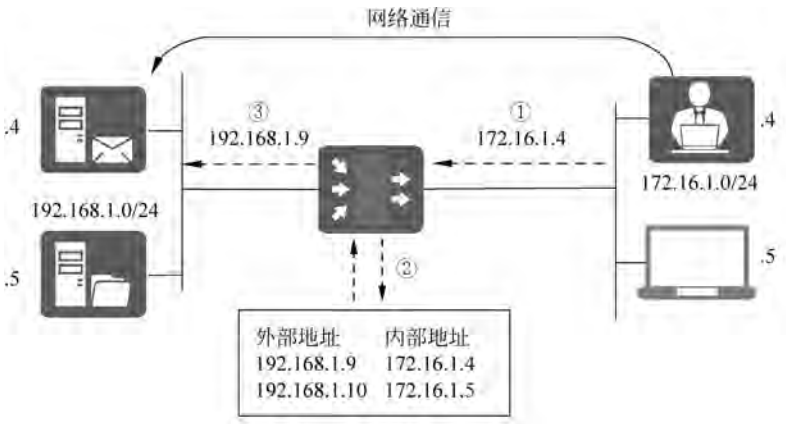

图 5.3 网络通信的地址转换示意图

5.2.1 地址转换分类

数据包从安全级别高的内部接口穿越防火墙时，可以根据应用场景设置不同的地址转换方式：静态网络地址转换和动态网络地址转换。防火墙将一段内部地址范围转换成一段全局地址范围，这是一种多对多的地址映射关系，一个内部地址转换为一个全局地址，需要配置与内部 IP 地址数量相等的全局 IP 地址，称为网络地址转换；防火墙将一段本地地址范围转换为一个全局地址，这是一种多对一的地址映射关系，多个内部地址转换为一个全局地址，通过端口号区分不同的内部地址，最多可以转换端口数 65535 个内部地址，称为端口地址转换。NAT 和 PAT 既可以静态转换，又可以动态转换。

防火墙将内部地址固定转换为一个全局 IP 地址，这种方式称为静态网络地址转换；防火墙为内部地址随机分配一个全局 IP 地址，称为动态网络地址转换。防火墙内部接口的数据包是转换前的地址，在内部接口配置需要进行地址转换的内部地址；外部接口看到的是转换后的地址，在外部接口配置全局地址，如图 5.4 所示。

图 5.4 NAT-Global 动态地址转换示意图

如图 5.5 所示，防火墙实现地址转换可以隐藏内部网络拓扑和地址信息，通过地址映射关系实现内部网络与外部网络的通信，实现数据包穿越防火墙。命令 NAT(PAT)和

Global 适用于配置本地网络的终端用户，将内部地址随机转换为一个全局地址；命令 Static 适用于配置对外开放的服务器，将内部地址固定转换为一个全局地址。

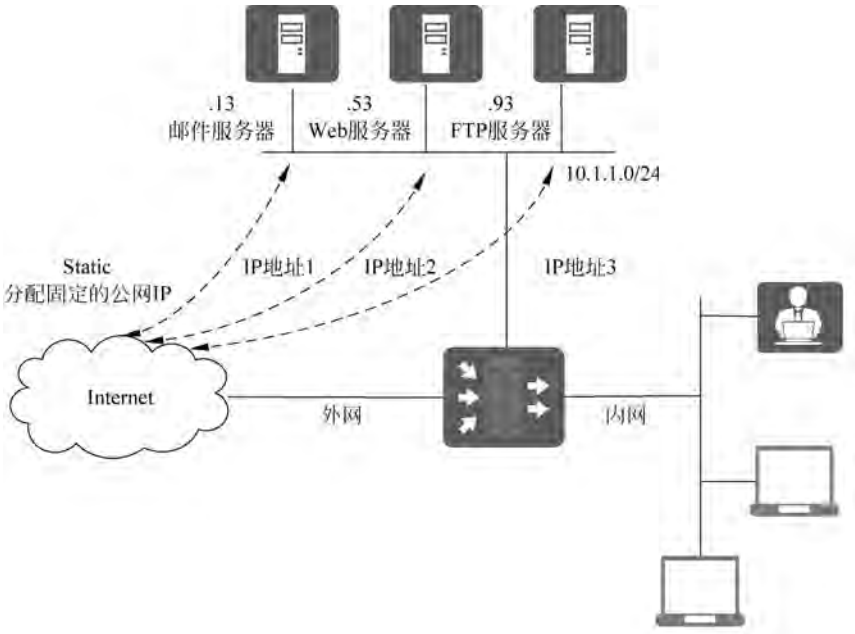

图 5.5　静态地址转换示意图

在防火墙安全级别低的外部接口，数据包出站前要转换为全局地址。防火墙的内部接口需要配置执行地址转换的内部地址；防火墙的外部接口需要配置地址转换后的全局地址，不符合配置规则的数据包无法穿越防火墙。因此，通过 nat 命令和 global 命令协同工作，使网络内部与外部保持通信。防火墙的数据包流动取决于安全级别，安全级别较高的接口可以访问安全级别较低的接口，除非明确拒绝，否则允许网络连接。安全级别较低的接口无法访问安全级别较高的接口，除非配置静态地址转换和访问列表命令对来明确允许，如图 5.6 所示。

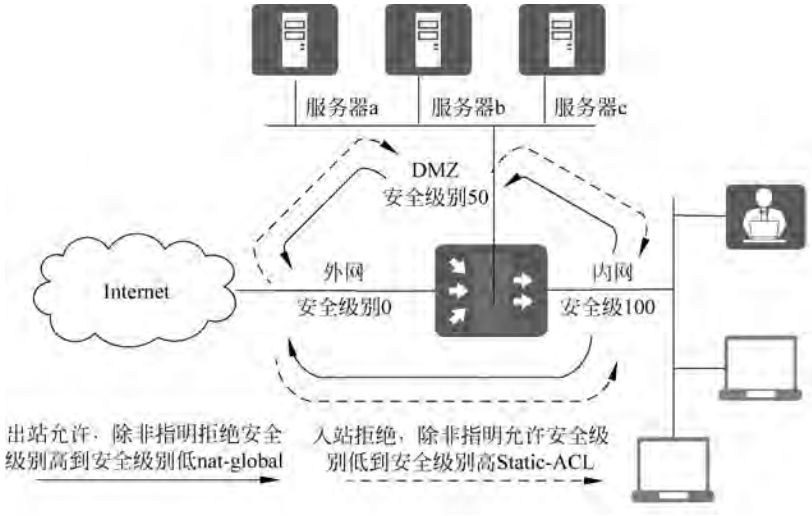

图 5.6　安全级别出站入站示意图

5.2.2 nat 命令

1. nat 命令使用说明

启用防火墙的 NAT 功能时，所有穿越防火墙的数据包都要遵循相应的转换规则。防火墙会创建一个地址映射关系，将安全级别高接口接收的 IP 地址转换为安全级别低接口的 IP 地址。NAT 功能可以将防火墙后边的内部 IP 地址对外隐藏起来。nat 命令的主要任务就是在转发数据包到外部网络之前，将全球不唯一的内部 IP 地址转换成全球公认的全局 IP 地址。完成这个任务需要 nat-global 命令对联合使用；先用 nat 命令配置内部网络需要被转换的 IP 地址，再用 global 命令配置可使用的全局 IP 地址。这个转换关系可以是多个，通过设置 nat 命令中的标识 nat_id 来进行区分，出站接口就是用标识 nat_id 决定查找的地址转换规则。

当一台内部网络中的主机或服务器等网络设备发送了一个出站数据包，到达启动 NAT 功能的防火墙时，将提取数据包的源地址、访问地址转换表并进行比较。如果当前地址转换表中没有该内部地址的映射关系，那转换时将为该内部地址创建一条记录，并为它分配一个可用的全局 IP 地址，这个任务是使用 global 命令配置完成的，数据包转换后，防火墙转发转换后的 IP 数据包。

考虑到资源有限性和网络连接的合法性，防火墙的内存并不会一直保留地址转换表的记录。将会通过超时设置删除不使用的映射关系，缺省时间是 3 小时，意味着在这个时间内没有使用该记录中的地址转换的数据包穿越，则会从地址转换表中删除该记录，释放的全局地址则可以给其他的内部地址转换使用。

在内部网络中使用私有地址与外部网络进行通信，需要将内部网络数据包转发到外部网络时，通过 NAT 功能将私有地址转换成全局 IP 地址。这样可以应对全局 IP 地址紧缺的问题，减少了所需的地址数量；而从安全角度看，这是一种保护内部地址、隐藏内部网络拓扑的安全措施。

通过网络地址转换将防火墙后边的内部 IP 地址对外隐藏起来。nat 命令语法格式如下：

```
nat [(if_name)] nat_id address [netmask] [dns] [[tcp] tcp_max_conns [emb_limit]
[norandomseq]]] [udp udp_max_conns]
nat [(if_name)] nat_id address [netmask] [timeout hh:mm:ss]
```

nat 命令参数说明如表 5.1 所示。

表 5.1 nat 命令参数说明

参　数	说　明
if_name	接口名称，该接口连接的网络地址进行地址转换
nat_id	大于 0，指定用于动态地址转换的全局地址池
address	要进行转换的 IP 地址，0.0.0.0 允许所有主机发起出站连接

续表

参　数	说　明
netmask	地址的网络掩码，0.0.0.0 表示允许所有的出站连接使用全局地址池中的地址进行转换
timeout	改变缺省 xlate 超时值，默认 3 小时
hh：mm：ss：	转换槽的超时时间，没有 tcp 或者 udp 连接使用转换，将发生超时

如图 5.7 所示的 NAT 示例中，主机 172.16.1.4 发起一个出站的网络连接。防火墙收到该出站连接的数据包后，将源地址 172.16.1.4 转换为 192.168.1.9。从主机 172.16.1.4 发出的数据包，对外部网络而言就是与 192.168.1.9 地址进行通信。从外部网络返回的数据包的目的地址是 192.168.1.9，再通过防火墙转换为地址 172.16.1.4。从而完成数据包的发送和接收过程。

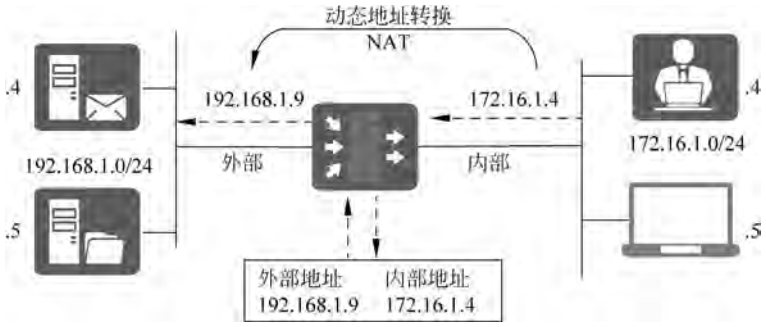

图 5.7　NAT 示例

通过 nat 命令可以配置转换一个内部 IP 地址、一段内部地址。通常情况下会根据内部网络的地理位置、行政单位、网络功能等方式划分地址段，配置相应的映射关系，并与其他安全策略实施联动。当网络规模不大，或者不需要区分时，可以使用命令 nat 1 0.0.0.0 0.0.0.0 ，实现对内部所有 IP 地址进行转换。其中，0.0.0.0 可以使用 0 代替，以简化 nat 命令参数。防火墙配置 nat 命令意味着启用了 NAT 功能。

示例 5.1：防火墙 inside 区域的所有 IP 地址都要进行网络地址转换，命令如下所示：

```
# nat (inside) 1 0.0.0.0 0.0.0.0 0 0
```

2. nat 0 命令使用说明

地址转换隐藏了内部网络地址和网络拓扑，还控制了可以出站的内部 IP 地址。通过 nat 0 命令则可以关闭地址转换功能，使所有内部网络的 IP 地址对外不可见。当内部网络中拥有 NIC 注册的 IP 地址，并且这个地址要被外部网络访问的时候，就要使用这个特性，nat 0 命令关闭内部地址转换。

示例 5.2：启用内部网段 10.0.0.0 出站连接的地址转换功能，关闭内部网段 192.168.0.0 出站连接的地址转换功能，命令如下所示：

```
# nat (inside) 1 10.0.0.0 255.0.0.0
# nat (inside) 0 192.168.0.0 255.255.255.0
```

nat 命令可以控制哪些内部 IP 地址需要进行地址转换，内部对外部不可见；还可以通过 nat 0 命令控制哪些 IP 地址不需要地址转换，内部 IP 地址就是实际通信地址。当内部网络的网络设备配置了全局 IP 地址，并允许被外部网络访问的时候，可以通过 nat 0 命令实现。

示例 5.3：设置防火墙 dmz 接口收到 IP 地址是 192.168.0.9 的所有数据包，都不做网络地址转换，命令如下所示：

```
# nat (dmz) 0 192.168.0.9 255.255.255.255
```

使用 nat 0 命令意味着 IP 地址对外可见，用于网络通信时，将不会对 IP 地址 192.168.0.9 进行地址转换。

5.2.3 global 命令

内部网络的主机发起出站连接，穿越防火墙请求访问外部网络的服务时，无法使用内部 IP 地址与外部通信，需要转换成外部 IP 地址；外部服务发起入站连接，响应内部主机的访问请求时，需要通过外部 IP 地址找到内部主机。防火墙通过配置成对 nat 命令和 global 命令实现，nat 命令指明哪些 IP 地址做网络地址转换，是转换前地址；global 命令指明转换成哪些 IP 地址，通过 nat 命令标识号 nat_id 匹配成对。命令如下所示：

```
global [(if_name)] nat_id {global_ip [-global_ip] [netmask global_mask]} |interface
```

global 命令参数说明如表 5.2 所示。

表 5.2 global 命令参数说明

参　数	说　明
if_name	使用全局地址的外部网络接口名称
nat_id	标识全局地址池，要与 nat 命令的 nat_id 匹配
global_ip	一个 IP 地址或一个全局地址范围的起始 IP 地址
global_mask	用于 global_ip 地址的网络掩码
interface	指定 PAT 使用接口上的地址

删除配置的命令，单个命令都是使用 no 命令，这里使用 no global 命令可以删除已经配置了 nat 相应的可供分配使用的全局 IP 地址。

```
# no global(outside) 1 192.168.1.20-192 168.1.254 netmask 255.255.255.0
```

示例 5.4：防火墙二接口通信。允许内部网络的所有设备发起出站连接，并分配全局 IP 地址进行通信，如图 5.8 所示。

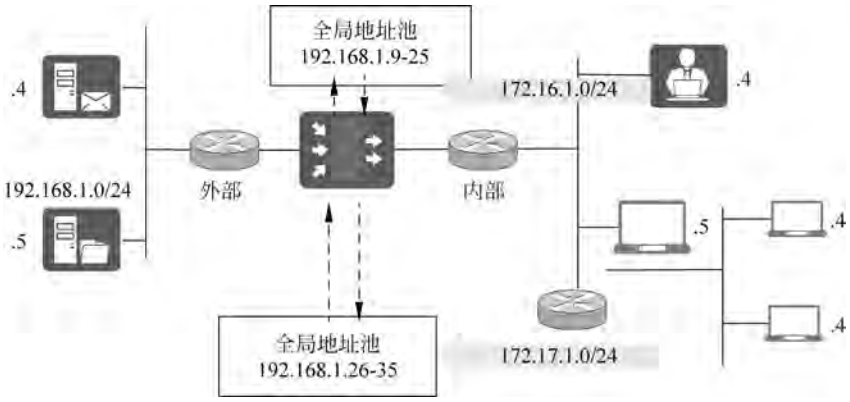

图 5.8　防火墙二接口 nat 命令示意图

命令如下所示：

```
# nat (inside) 1 172.16.1.0 255.255.255.0
# nat (inside) 2 172.17.1.0 255.255.255.0
# global (outside) 1 192.168.1.9 - 192.168.1.25 netmask 255.255.255.0
# global (outside) 2 192.168.1.26 - 192.168.1.35 netmask 255.255.255.0
```

第 1 条 nat 命令，标识符是 1，配置防火墙 inside 接口的网络地址转换，指定转换范围是 172.16.1.0/24 网段的数据包。

第 2 条 nat 命令，标识符是 2，配置防火墙 inside 接口的网络地址转换，指定转换范围是 172.17.1.0/24 网段的数据包。

第 3 条 global 命令，指定防火墙 outside 接口，转换 nat 标识符是 1 的所有数据包源 IP 地址，分配出站的全局地址。防火墙 inside 接口 172.16.1.0/24 网段的数据包，从 outside 接口出站，将从全局地址池 192.168.1.9 到 192.168.1.25 分配 IP 地址，共计 14 个地址可供网络地址转换使用。

第 4 条 global 命令，指定防火墙 outside 接口，转换 nat 标识符是 2 的所有数据包源 IP 地址，分配出站的全局地址。防火墙 inside 接口 172.17.1.0/24 网段的数据包，从 outside 接口出站，将从全局地址池 192.168.1.26 到 192.168.1.35 分配 IP 地址，共计 16 个地址可供网络地址转换使用。

示例 5.5：防火墙三接口通信。允许内部用户访问 DMZ 和 Internet，DMZ 的主机可以访问外网，如图 5.9 所示。

命令如下所示：

```
# nat (dmz) 1 10.1.1.0 255.255.255.0
# nat (inside) 1 172.16.1.0 255.255.255.0
# global (outside) 1 192.168.1.9 - 192.168.1.25 netmask 255.255.255.0
# global (dmz) 1 10.1.1.9 - 10.1.1.25 netmask 255.255.255.0
```

第 1 条 nat 命令，网络地址转换的标识符是 1，配置防火墙 dmz 接口的网络地址转换，指定转换范围是 10.1.1.0/24 网段的数据包。

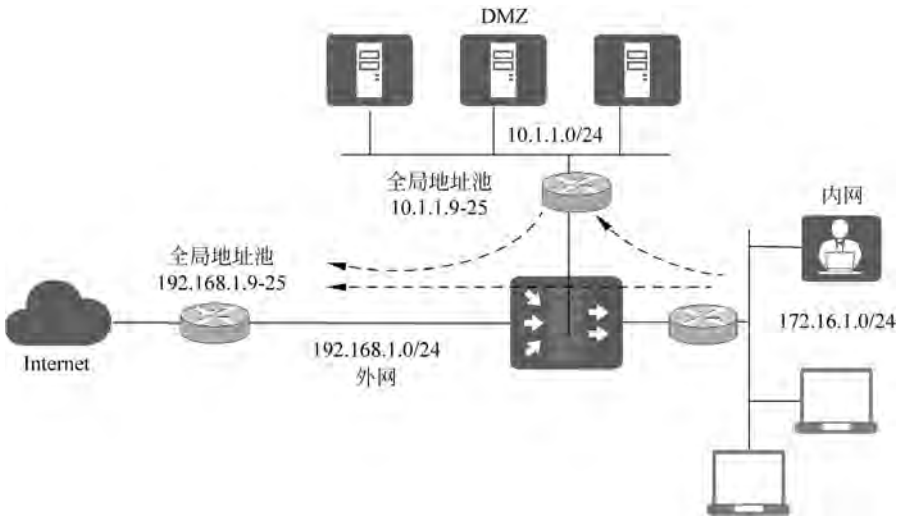

图 5.9 防火墙三接口 nat 命令示意图

第 2 条 nat 命令，网络地址转换的标识符是 1，配置防火墙 inside 接口的网络地址转换，指定转换范围是 172.16.1.0/24 网段的数据包。

第 3 条 global 命令，指定防火墙 outside 接口用于转换的全局地址池，要与 nat 命令标识是 1 的进行匹配，转换其所有出站数据包的源 IP 地址，可供分配的全局地址是 192.168.1.9 到 192.168.1.25。实现防火墙内网用户和防火墙 DMZ 区域的网络设备发起出站请求时，共享这个全局地址段。

第 4 条 global 命令，指定防火墙 dmz 接口用于转换的全局地址池，要与 nat 命令标识是 1 的进行匹配，转换其所有出站数据包的源 IP 地址，可供分配的全局地址是 10.1.1.9 到 10.1.1.25。实现防火墙内网用户发起访问防火墙 DMZ 区域网络请求时，共享这个全局地址段。

5.2.4 pat 命令

针对可分配全局地址资源不足的情况，可以利用端口地址转换功能，实现内网多台网络设备共用一个全局地址进行网络通信。对外可见的只有一个全局地址，所有网络通信看起来是一个 IP 地址。启用 pat 功能后，将为每个发起外部连接的内部地址分配一个可用端口号。pat 命令配置的全局地址不能被其他的全局地址池使用。

同时配置多对多的地址转换 nat 命令和多对一的地址转换 pat 命令时，内部地址出站时的分配顺序是，先使用 nat 命令对转换的全局地址，全局地址用尽后，再选取 pat 命令对转换的地址。即当 nat 全局地址池中有一个可用地址，下一次使用的就是这个地址，总是先于 pat 地址使用。因此，地址资源有限的情况下，可以通过配置相同 nat_id 标识的 global 命令，实现全局地址的扩充。规划地址资源时，考虑到需要使用特定端口号的服务，为了避免端口冲突则不使用 pat 命令。总计 65 535 个端口，除了知名端口分配给特定的服务，可供地址转换使用的端口是 64 000 个。

采用 pat 命令，待转换的内部地址(或称本地地址)转换为同一个全局地址。pat 命令配置与 nat 命令配置的区别是，成对使用的 global 命令中只有一个 IP 地址，而不是 IP 地址范围。

示例 5.6：内部网络 172.16.1.0 的主机发起外部访问的时候，共享一个全局 IP 地址 192.168.1.9，命令如下所示：

```
#nat (inside) 1 172.16.1.0 255.255.255.0
#global (outside) 1 192.168.1.9 netmask 255.255.255.255
```

如图 5.10 所示，采用 pat 命令时，内部地址的出站地址都是相同的，只是增加了一个端口号对内部地址加以区分。两个客户端 172.16.1.3 和 172.16.1.5 发起到外网的连接请求，根据高到底的安全级别，默认允许出站，使用 pat 命令定义地址转换规则。地址 172.16.1.3 转换为了 192.168.1.9，为了保持会话的可区分性，源端口使用端口号 1025 区分；地址 172.16.1.5 同样转换为了 192.168.1.9，源端口使用端口号 1027 区分。

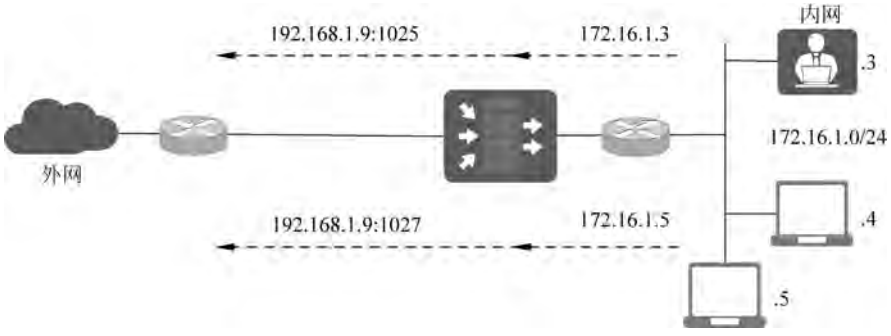

图 5.10　防护墙 pat 命令示意图

示例 5.7：使用 pat 命令来扩大全局地址。内部网络的网段是 172.16.1.0/24，可供使用的全局地址范围是 192.168.1.20 至 192.168.1.254，请确保内部网络中的所有网络设备出站连接都可以分配到全局地址。

```
# nat (inside) 1 10.0.0.0 255.255.255.0
# global (outside) 1 192.168.1.20 - 192.168.1.253 netmask 255.255.255.0
# global (outside) 1 192.168.1.254 netmask 255.255.255.255
```

第 1 条 nat 命令，网络地址转换的标识符是 1，配置防火墙 inside 接口的网络地址转换，指定转换范围是 10.0.0.0 /24 网段的数据包。

第 2 条 global 命令，指定防火墙 outside 接口用于转换的全局地址池，要与 nat 命令标识是 1 的进行匹配，转换其所有出站数据包的源 IP 地址，可供分配的全局地址是 192.168.1.20 到 192.168.1.253。

第 3 条 global 命令，指定防火墙 outside 接口用于转换的全局地址池，要与 nat 命令标识是 1 的进行匹配，转换其所有出站数据包的源 IP 地址，可供分配的全局地址是 192.168.1.254，以端口号区分不同网络设备。只有上一条 global 命令的全局地址全部分配后，才使用这条 global 命令配置的全局地址池。

5.2.5 static 命令

在实际应用中可通过 static 命令实现静态网络地址转换。例如，对外提供服务的服务器，如要从因特网访问该服务器资源，就需要将服务器的地址配置为固定的全局地址。根据从低到高的安全策略，默认拒绝入站，因此除了通过 static 命令配置静态地址外，还要对网络安全设备配置访问控制策略，允许到该服务器的流量入站，从而穿越防火墙，让较低安全级别接口上的设备能够访问位于较高安全级别接口上的 IP 地址。

静态网络地址转换实现了将一个内部地址映射为一个固定的全局地址，使这个内部节点可以允许外部网络(Internet)访问。

```
static [(internal_if_name,external_if_name)] global_ip local_ip[netmask network_mask][max_
conns [em_limit]] [norandomseq]
```

static 命令参数说明如表 5.3 所示。

表 5.3 static 命令参数说明

参　数	说　明
internal_if_name	内部网络接口名称。正在访问的较高安全级别的接口
external_if_name	外部网络接口名称。正在访问的较低安全级别的接口
global_ip	较低安全级别的接口上的 IP 地址
local_ip	较高安全级别的接口上的 IP 地址。内部网络的本地 IP 地址
netmask	指定网络掩码之前所需的保留字
max_conns	每个 IP 地址的最大连接数量，允许同时通过该静态地址翻译的连接数量
network_mask	用于 global_ip 和 local_ip 的网络掩码。对于主机地址，总是采用 255.255.255.255。对于网络地址，使用适当类别的掩码或子网掩码
em_limit	未完成连接限制数。以防止未完成连接风暴攻击。缺省是 0，意味着不限制连接
norandomseq	不对 TCP/IP 数据包的序列号进行随机化处理。如果另一台在线防火墙也在对序列号进行随机化，结果就会扰乱数据，只有这时才使用这个选项

示例 5.8：内部地址 10.10.10.9 是一台服务器，要求对外提供服务，并分配了全局地址 192.168.0.9，请使用 static 命令配置地址转换，命令如下所示：

```
# static (inside, outside) 192.168.0.9 10.10.10.9
```

示例 5.9：在防火墙 DMZ 区域，有 1 台 FTP 服务器和 1 台 Web 服务器，防火墙接口命名是 dmz，服务器 IP 地址分别是 172.16.1.9 和 172.16.1.10；允许防火墙外部区域使用这两个服务器的资源，可用 IP 地址网段是 192.168.1.0/24，防火墙接口命名是 outside。请使用 static 命令给服务器配置一个固定 IP 地址，可以与防火墙外部区域的主机进行通信，命令如下所示：

```
# static (dmz,outside) 192.168.1.3 172.16.1.9 netmask 255.255.255.255
# static (dmz,outside) 192.168.1.4 172.16.1.10 netmask 255.255.255.255
```

第 1 条 static 命令，指定防火墙 DMZ 区域的 IP 地址 172.16.1.9，转换为防火墙外部区域的 IP 地址 192.168.1.3，FTP 服务器使用 IP 地址 192.168.1.3，与防火墙外部区域的主机进行通信。

第 2 条 static 命令，指定防火墙 DMZ 区域的 IP 地址 172.16.1.10，转换为防火墙外部区域的 IP 地址 192.168.1.4，Web 服务器使用 IP 地址 192.168.1.4，与防火墙外部区域的主机进行通信。

注意，这里只考虑静态地址转换，还需要配置防火墙的安全访问策略，才可以实现网络流入站。

示例 5.10：在防火墙 DMZ 区域有 2 台 FTP 服务器，防火墙接口命名是 dmz，服务器 IP 地址是 172.16.1.9 和 172.16.1.10；允许防火墙外部区域使用这 2 个 FTP 服务器的资源，只有一个可用 IP 地址 192.168.1.9，防火墙接口命名是 outside。请使用 static 命令给服务器配置一个固定 IP 地址，可以与防火墙外部区域的主机进行通信。命令如下所示：

```
static (dmz,outside) tcp 192.168.1.9 ftp 172.16.1.9 ftp netmask 255.255.255.255
static (dmz,outside) tcp 192.168.1.9 3131 172.16.1.10 ftp netmask 255.255.255.255
```

第 1 条 static 命令，指定防火墙 DMZ 区域的 IP 地址 172.16.1.9，转换为防火墙外部区域的 IP 地址 192.168.1.9，FTP 服务器使用 IP 地址 192.168.1.3 和 21 端口号，与防火墙外部区域的主机进行通信。

第 2 条 static 命令，指定防火墙 DMZ 区域的 IP 地址 172.16.1.10，转换为防火墙外部区域的 IP 地址 192.168.1.9，FTP 服务器使用 IP 地址 192.168.1.4 和 3131 端口号，与防火墙外部区域的主机进行通信。由于第 1 条 static 命令，FTP 服务器使用了 21 号端口号，另一台 FTP 服务器要使用不同的端口号。

5.3 route 命令

防火墙是网络安全设备，还具有路由器的路由选择功能。防火墙为了将数据包发送到特定的目的地，需要配置功能，从而使数据包可以转发给指定的路由器、网关，到达目的地址。根据网络复杂程度选择配置静态路由、动态路由。静态路由适用于小规模的网络实施，使用 route 命令对接口配置静态路由、默认路由。命令如下所示：

```
#route if_name ip_address netmask gateway_ip [metric]
```

route 命令参数说明如表 5.4 所示。

表 5.4 route 命令参数说明

参 数	说 明
if_name	内部或外部网络接口名字，数据将通过这个接口离开 PIX
ip_address	内部或外部网络 IP 地址，默认 0 表示所有目标网络
netmask	指定应用到 in_address 的网络掩码。0 表示默认路由
gateway_ip	指定网关路由器的 IP 地址(路由的下一跳地址)
metric	指定到 gateway_ip 的跳数。默认 1

防火墙可以使用 route 命令配置多个不同的静态路由，不可以配置多条静态路由到相同的网络，有且仅有一条默认路由。

示例 5.11：通过路由器 192.168.1.31 转发所有出站数据包，到达 10.0.1.0 网段的数据包通过路由器 172.16.0.21 转发，如图 5.11 所示。

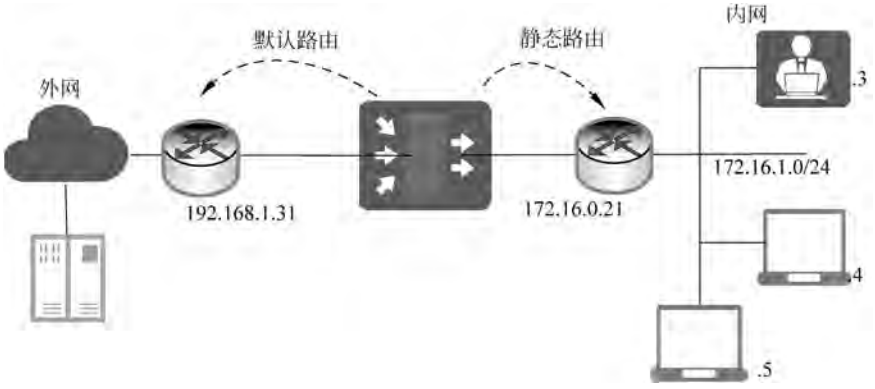

图 5.11　route 命令拓扑示例

```
# route outside 0.0.0.0 0.0.0.0 192.168.1.31 1
# route inside 172.16.1.0 255.255.255.0 172.16.0.21 1
```

第 1 条 route 命令，配置防火墙默认路由，从防火墙 outside 接口出站的所有数据包，通过默认路由到达外网，默认路由的 IP 地址是 192.168.1.31。

第 2 条 route 命令，配置防火墙静态路由，从防火墙 inside 接口到 172.16.1.0/24 网段的所有数据包，通过静态路由到达内网，静态路由的 IP 地址是 172.16.0.21。

IP 地址和网络掩码组合 0.0.0.0，此处可以缩写为 0，等同于上面配置命令，命令如下所示：

```
# route outside 0 0 192.168.1.31 1
```

示例 5.12：DMZ 区域有 10.1.1.0 和 10.1.2.0 这两个网段，都连接到同一台路由器 10.0.1.11，如图 5.12 所示。请配置到达这两个网络的静态路由。

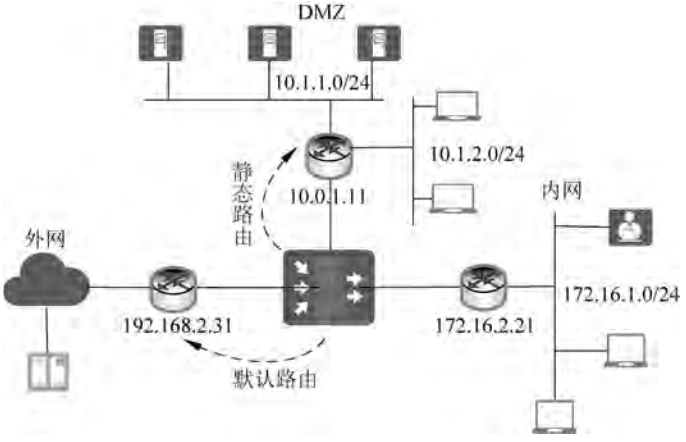

图 5.12　防火墙三接口拓扑示例

防火墙的路由配置命令如下所示：

```
# route dmz 10.1.1.0 255.255.255.0 10.0.1.11 1
# route dmz 10.1.2.0 255.255.255.0 10.0.1.11 1
```

第 1 条 route 命令，配置防火墙静态路由，从防火墙 dmz 接口到 10.1.1.0/24 网段的所有数据包，通过静态路由到达 DMZ 区域，静态路由的 IP 地址是 10.0.1.11。

第 2 条 route 命令，配置防火墙静态路由，从防火墙 dmz 接口到 10.1.2.0/24 网段的所有数据包，通过静态路由到达 DMZ 区域，静态路由的 IP 地址是 10.0.1.11。

5.4　防火墙二接口配置实训

5.4.1　实验目的与任务

1. 实验目的

通过本实验了解 PIX 防火墙的软硬件组成结构，掌握 PIX 防火墙的工作模式，熟悉 PIX 防火墙的 6 条基本命令，掌握 PIX 防火墙的动态、静态地址映射技术，熟悉 PIX 防火墙在小型局域网中的应用。实训需要 PIX 防火墙 1 台，路由器 2 台，网络连接线若干。

2. 实验任务

本实验主要任务如下：

(1) 观察 PIX 防火墙的二接口硬件结构，掌握硬连线方法；

(2) 掌握模拟器下防火墙设备的配置，理解和配置 PIX 防火墙的基本命令，实现内网访问外网；

(3) 查看 PIX 防火墙的配置信息。

5.4.2　实验拓扑图和设备接口

根据实验任务，规划设计实验的网络拓扑图，如图 5.13 所示。通过网络设备、路由器执行 ping 命令或 telnet 命令，发起位于防火墙不同安全区域网络设备的通信，验证防火墙功能是否配置正确。

图 5.13　防火墙二接口实验拓扑图

根据实验任务和实验拓扑图，为每个网络设备及其接口规划相关配置，防火墙 PIX 的配置信息如表 5.5 所示。

表 5.5 防火墙 PIX 的配置信息

序号	interface	Type	nameif	Security level	IP Address
1	e0	☑physical☐logical	inside	100	10.9.9.1
2	e1	☑physical☐logical	outside	0	192.168.9.1

位于防火墙外部网络的路由器 R1 的配置信息如表 5.6 所示。

表 5.6 路由器 R1 的配置信息

序　　号	interface	IP Address
1	f0/0	192.168.9.2

位于防火墙内部网络的路由器 R2 的配置信息如表 5.7 所示。

表 5.7 路由器 R2 的配置信息

序　　号	interface	IP Address
1	f0/0	10.9.9.2

5.4.3 实验步骤和命令

1. 防火墙主要命令

下面对实验中配置防火墙使用的主要命令进行说明。

```
# int e0
# ip add 10.9.9.1 255.255.255.0
# nameif outside
# security-level 0
# no sh
# nat (inside) 101 10.9.9.0 255.255.255.0
# global (outside) 101 192.168.9.101 netmask 255.255.255.255
# route outside 0 0 10.9.9.13
```

第 1 条命令，设置防火墙接口 e0，进入配置模式。

第 2 条命令，配置防火墙接口 e0 的 IP 地址为 10.9.9.1。

第 3 条命令，配置防火墙接口 e0 的命名为 outside。

第 4 条命令，配置防火墙接口 e0 的安全级别是 0。

第 5 条命令，启动防火墙接口 e0。

第 6 条命令，配置内部网络源地址为 10.9.9.0，穿越防火墙时将进行地址转换，NAT 标识 ID 为 101。

第 7 条命令，配置防火墙外部接口的全局地址池，转换 NAT 标识 ID 为 101 的源地址，共享 IP 地址 192.168.9.101。

第 8 条命令，配置防火墙默认路由为 10.9.9.13。

保存工程的路由器配置空，请使用导出配置文件，选择导出的路径，可看到配置文件如图 5.14 所示，据此可分别对路由器和防火墙进行配置。

图 5.14　GNS3 工程文件

2. 路由器 R1 的配置

路由器 R1 的配置信息包括接口、路由和密码访问配置，用于验证网络通信是否符合预期，命令如下所示：

```
R1#conf t
Enter configuration commands, one per line.   End with CNTL/Z.
R1(config)#int f0/0
R1(config-if)#ip add 192.168.9.2 255.255.255.0
R1(config-if)#no sh
R1(config-if)#end
R1#show ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            192.168.9.2     YES manual up                    up
R1#conf t
Enter configuration commands, one per line.   End with CNTL/Z.
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.9.1
R1(config)#end
R1#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 192.168.9.1 to network 0.0.0.0
C    192.168.9.0/24 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 192.168.9.1
R1#conf t
Enter configuration commands, one per line.   End with CNTL/Z.
R1(config)#line vty 0 4
R1(config-line)#password cisco
R1(config-line)#enable password cisco
R1(config)#end
```

```
R1#wr
Building configuration...
[OK]
R1#
```

3. 路由器 R2 的配置

路由器 R2 的配置信息包括接口、路由配置，用于验证网络通信是否符合预期，命令如下所示：

```
R2#
R2#conf t
Enter configuration commands, one per line.   End with CNTL/Z.
R2(config)#int f0/0
R2(config-if)#ip add 10.9.9.2 255.255.255.0
R2(config-if)#no sh
R2(config-if)#end
R2#show ip int br
Interface                  IP-Address      OK? Method Status                Protocol
FastEthernet0/0            10.9.9.2        YES manual up                    up
R2#conf t
Enter configuration commands, one per line.   End with CNTL/Z.
R2(config)#ip route 0.0.0.0 0.0.0.0 10.9.9.1
R2(config)#end
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 10.9.9.1 to network 0.0.0.0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.9.9.0 is directly connected, FastEthernet0/0
S*    0.0.0.0/0 [1/0] via 10.9.9.1
```

4. 防火墙的配置

可以对防火墙接口一次完成 IP 地址、命名和安全级别等信息的配置，也可以分别配置，重点是使用 no sh 命令启动接口，命令如下所示：

```
cuitfirewall>
cuitfirewall>en
Password:
cuitfirewall# conf t
cuitfirewall(config)# int e0
cuitfirewall(config-if)# ip add 10.9.9.1 255.255.255.0
```

```
cuitfirewall(config-if)# no sh
cuitfirewall(config-if)# end
cuitfirewall# conf t
cuitfirewall(config)# int e1
cuitfirewall(config-if)# ip add 192.168.9.1 255.255.255.0
cuitfirewall(config-if)# no sh
cuitfirewall(config-if)# end
cuitfirewall# conf t
cuitfirewall(config)# int e0
cuitfirewall(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
cuitfirewall(config-if)#
cuitfirewall(config-if)# end
cuitfirewall# conf t
cuitfirewall(config)# int e1
cuitfirewall(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.
cuitfirewall(config-if)# end
cuitfirewall# conf t
cuitfirewall(config)# nat (inside) 101 10.9.9.0 255.255.255.0
cuitfirewall(config)# global (outside) 101 192.168.9.101 netmask 255.255.255.255
INFO: Global 192.168.9.101 will be Port Address Translated
cuitfirewall(config)# end
cuitfirewall# wr
Building configuration...
Cryptochecksum: 5474d8a8 6437693a 730ccd8e 8f14f397
1633 bytes copied in 1.780 secs (1633 bytes/sec)
[OK]
cuitfirewall(config)# route outside 0 0 10.9.9.1
```

5. 防火墙配置显示

查看防火墙配置文件，使用 show 命令，其格式和内容如下所示：

```
cuitfirewall# show config
: Saved
: Written by enable_15 at 03:50:37.847 UTC Thu Mar 3 2022
!
PIX Version 8.0(2)
!
hostname cuitfirewall
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Ethernet0
 nameif inside
 security-level 100
 ip address 10.9.9.1 255.255.255.0
!
```

```
interface Ethernet1
 nameif outside
 security-level 0
 ip address 192.168.9.1 255.255.255.0
!
interface Ethernet2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Ethernet4
 shutdown
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
access-list 100 extended permit icmp any any echo-reply
access-list 100 extended permit icmp any any echo
pager lines 24
logging enable
logging console debugging
mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
global (outside) 101 192.168.9.101 netmask 255.255.255.255
nat (inside) 101 10.9.9.0 255.255.255.0
access-group 100 in interface outside
route outside 0.0.0.0 0.0.0.0 10.9.9.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
no crypto isakmp nat-traversal
```

```
telnet timeout 5
ssh timeout 5
console timeout 0
threat - detection basic - threat
threat - detection statistics access - list
!
!
prompt hostname context
Cryptochecksum:18fd9df96c1376a465ac76945f25cae0
```

完成上述配置后，验证网络通信是否可以穿越防火墙。路由器 R2 可以远程 telnet 路由器 R1，输入正确密码后如下所示：

```
R2#telnet 192.168.9.2
Trying 192.168.9.2 ... Open
User Access Verification
Password:
R1>en
Password:
R1#
```

★本章小结★

本章介绍了防火墙的不同安全区域之间是如何进行网络通信的，IP 数据包是如何从端到端流动的，从而理解防火墙对网络流的保护。通过回顾主要的 TCP/IP 传输协议，理解防火墙如何处理安全级别高的区域向安全级别低的区域进行数据传送的过程，以及安全级别低的区域向安全级别高的区域进行数据传送的过程。主要阐述了防火墙网络地址转换、该技术的安全特性和配置命令，以及普通用户和服务器如何选择网络地址转换的方式，还介绍了 pat 命令和 nat 命令的区别、使用方法和应用场景。最后，通过二接口实训任务，复习前面章节介绍的技术原理，为后续学习奠定了实验基础。

复习题

1. 动态地址转换和静态地址转换的应用场景分别是什么？
2. nat 命令和 pat 命令使用区别是什么？
3. 入站和出站时默认的访问控制策略是什么，何种情况配合使用 ACL？
4. 如何穿越防火墙，有哪些情况？