

第9章 Cisco PIX 防火墙翻译

本章包含下列主题：

- ❖ 传输协议
- ❖ PIX防火墙

传输协议

一个会话通常是由下列两种传输层协议之一进行承载：

- TCP（传输控制协议），这种协议容易检查。
- UDP（用户数据报协议），这种协议难以进行适当地检查。

可能被PIX检查的其他协议有ICMP（Internet控制消息协议/Internet Control Message Protocol）和GRE（通用路由封装/Generic Routing Encapsulation）。

❖ 传输控制协议

TCP是一种面向连接的协议。当从位于PIX防火墙的一个相对安全的接口侧的主机上发起一个对话是，PIX会在它的绘画状态表中产生一个表项。

PIX防火墙能够从网络流中提取网络会话信息，并实时地主动验证会话的有效性。这种状态型过滤器维护者每条网络连接的参数（或状态），并根据它的预期，检查后继的信息（比如，源和目的端口号与IP地址，但是不只限于这些信息）。

当发起一个穿过PIX防火墙的TCP会话时，PIX防火墙会纪录该网络流，并寻找来自目的设备的确认。然后PIX防火墙将根据三次握手机制，允许数据流在两个设备之间流动。

当穿过PIX防火墙建立一个TCP会话时，发生了：

- 1、当PIX防火墙从内部收到一个IP包时，PIX检查现有的翻译槽位，如果没有对应的翻译槽位，PIX防火墙就为之产生一个（如果在检验过配置之后认为应该产生一个翻译槽位的话）。PIX防火墙中的翻译槽位是内部IP地址和被分配的全球唯一的IP地址。这个信息被保留在内存中，从而可以对后继的数据包流进行检查(见图5-2)。
- 2、连接槽位被标记为未完成（还没有被建立）。
- 3、PIX防火墙对连接的初始序列号进行随机化处理，并将数据包转发到输出接口上。

- 4、现在PIX防火墙期望收到来自目的主机的SYN/ACK数据包。PIX防火墙将收到的数据包与连接槽位匹配，计算序列信息，并将返回的数据包转发到内部主机。任何数据包，如果他们匹配源和目的地址和/或端口，但是不匹配协议的正确步骤，都将被丢弃并被记录下来。
- 5、内部主机用ACK完成连接建立过程（三次握手过程）（见图5-3）。
- 6、PIX防火墙上的连接槽位被标记为已连接（活动的已建立状态），并传送数据。然后将这条连接的未完成计数器复位。

❖ 用户数据报协议

UDP是一种无连接的协议，所以PIX防火墙必须采取其它措施来确保UDP的安全。采用UDP的应用很难被保证安全，这是因为它没有握手或排序机制。很难确定一次UDP交易的当前状态。

由于会话没有清楚地开始、流状态、或结束状态，所以维持会话的状态也很难。但是，当从相对安全的接口向不太安全的接口发送发送UDP数据包时，PIX防火墙会为之产生一个UDP连接槽位。所有匹配连接槽位的后继返回UDP数据包可以被转发到内部网络。保证UDP安全的固有问题就是由于UDP应用（NFS、DNS、RPC等）经常被攻击，所以对于这类应用采用限制性的防火墙规则是很重要的。图5-4显示了PIX如何对一个UDP会话处理。

PIX防火墙接受向内的UDP数据包的前提条件是，此前它已经看到过一个来自相同目的和源IP地址的向外的UDP数据包。当UDP连接槽位的空闲时间超过了我们所配置的空闲时间（缺省时两分钟）时，连接槽位将被从连接表中删除。

UDP的一些特性：

- *UDP是一种不可靠的（无连接），但是高效的传输协议
- *伪造UDP数据包氏非常容易的（没有握手或排序）。
由于没有状态机，事物/交易de发起者和当前的状态都不能被确定
- *UDP没有传输保证机制
- *没有连接的建立和终止（由应用程序来实现状态机）
- *UDP没有拥塞管理或避免机制

PIX防火墙翻译

在PIX防火墙上设置地址翻译时，可以有两种选择。内部地址可以被翻译成一个指定的全局地址，这被称为静态地址翻译。第二种选择是，在数据穿越PIX防火墙时，将内部地址翻译到一个全局地址池中的某个地址。这种翻译类型是动态地址翻译。

❖ 静态地址翻译

如果每次通过PIX防火墙建立一个向外的会话时，要求同一台主机都被翻译成相同的地址，就需要采用静态地址翻译。它也可以用来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。对于由同一个源地址创建的每条连接，PIX防火墙为之建立的翻译槽位都将具有相同的源IP地址和相同的翻译地址。

语法：static [(internal_if_name,external_if_name)] global_ip
local_ip [netmask network_mask] [max_conns [em_limit]]
[norandomseq]

其中，internal_if_name：内部网络接口名称。我们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。我们正在访问的较高安全级别的接口。

global_ip：全局IP地址。这个地址不可以是一个PAT（端口地址翻译）IP地址。我们正在访问的较低安全级别的接口上的IP地址。

local_ip：内部网络的本地IP地址。我们正在访问的较高安全级别的接口上的IP地址。

netmask：在制定网络掩码之前所需的保留字。

network_mask：用于global_ip和local_ip的网络掩码。对于主机地址，总采用255.255.255.255。对于网络地址，使用适当类别的掩码或子网掩码；例如，对于A类网络，使用255.0.0.0。一个掩码的例子是 255.255.255.224

`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。

`em_limit`：未完成连接限制数。设置这个限制，以防止未完成连接风暴攻击。缺省是0，这意味着不限制连接数。

`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。

例如：如图5-5，当通过PIX防火墙建立一个会话时，来自10.0.1.10(本地地址)的数据包含有的源地址是192.168.1.101（全局地址）。static命令将本地地址永久地映射到全局地址。相应的static命令语法是：

```
static (inside,outside)192.168.1.101 10.0.1.10
```

当允许通过PIX防火墙访问一台特定的内部主机时，必须为外部的用户定义该主机的外部IP地址。外部主机必须用内部主机的静态全局地址（翻译地址），作为目的IP地址。conduit命令允许通过PIX防火墙的访问，对于图5-6中的网络，命令如下：

```
Static (inside,outside) 192.168.1.101 10.0.1.10
```

```
Conduit permit tcp host 192.168.1.101 eq telnet host  
172.16.1.1
```

在这个Telnet会话中，具有外部IP地址172.16.1.1的主机正在建立一个会话，其目的地是具有全局IP地址192.168.1.101的一台内部主机。PIX防火墙将全局IP地址192.168.1.101翻译成本地IP地址10.0.1.10。

我们还可以用static命令翻译一段地址范围。如果要将A类网络的一个子网10.1.1.0 255.255.255.0翻译成C类网络192.168.1.0 255.255.255.0，相应的命令语法是：

```
static ( inside , outside ) 192.168.1.0 10.1.1.0
```

这被称为网络静态netstatic翻译。在这个例子中，子网10.1.1.0/24中的每个具体IP地址每次被翻译成相同的全局IP地址。例如，IP地址为10.1.1.100的主机，对于通过PIX建立的每个会话，都被翻译成192.168.1.100。

我们还可以用static命令将地址翻译成自身。在这种情况下，本地IP地址和全局地址是一样的：

```
static ( inside , outside ) 192.168.1.10 192.168.1.10
```

❖ 动态地址翻译

动态地址翻译用来将一段本地地址范围翻译成一段全局地址范围，或者一个全局地址。将一段本地地址范围翻译成一段全局地址范围，这被称为网络地址翻译（NAT）。将一段本地地址范围翻译成一个全局地址，这被称为端口地址翻译（PAT）。

一、网络地址翻译

对于采用NAT的动态地址翻译，必须用nat命令来定义本地主机。然后必须用global命令定义全局地址池。根据用nat命令选择的nat_id，在输出接口上选择用于地址翻译的全局地址池。用户指定的IP全局地址池的数量可以多达256个。

图5-7的具体语法如下：

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

```
global (outside) 1 192.168.1.10-192.168.1.254 netmask
```

如果主机10.0.1.10是通过PIX向Internet发起第一条连接的主机，它就会被翻译成全局地址192.168.1.10

二、端口地址翻译

当采用端口地址翻译时，所有的本地地址都被翻译到同一个全局地址。PAT的配置与NAT的配置很相似。其中一个区别是，“global”命令语句中只包含一个IP地址，而不是在图5-8所示一段IP地址范围，语法：

```
nat (inside)1 0.0.0.0 0.0.0.0  
global (outside)1 193.168.1.10 netmask  
255.255.255.255
```

当连接到Internet时，所有的内部IP地址都将被翻译到同一个地址192.168.1.10

下面是关于PAT的一些重要的考虑：

- *PAT让多个向外的会话看起来像是源自同一个IP地址。启用PAT后，防火墙为每个向外的xlate（翻译槽位），从PAT的IP地址中，选择一个唯一的端口号。当ISP不能为我们的向外连接分配足够多的唯一IP地址时，这个功能特性就非常有价值。
- *我们为PAT指定的那个IP地址不能被用于另一个全局地址池。
- *当PAT被用于扩充全局地址池时，首先使用的是全局池中的地址，当全局地址池中的地址被用尽后，下一条连接将选取PAT地址。如果全局地址池中有一个地址变成可用的，下一条连接就采用那个地址。全局地址池中的地址总是先于PAT地址被使用。可以通过在产生全局地址池和PAT的global命令语句中使用相同的“nat_id”，用PAT来扩充全局地址池。例如：

```
global (outside) 1 172.16.201.1-172.16.201.10 netmask  
255.255.255.224
```

```
global (outside) 1 172.16.201.22 netmask 255.255.255.224
```

- *对于H.323应用和高速缓存名字服务器来说，不能使用PAT。在多媒体应用需要通过防火墙运行时，也不要使用PAT。多媒体应用可能会与PAT提供的端口映射发生冲突。
- *PAT不能与established命令一起工作。
- *对于DNS、FTP和被动FTP、HTTP、e-mail、RPC、rshell、Telnet、URL过滤和向外的traceroute，PAT可以工作。

❖ 翻译和连接

翻译时在TCP/IP协议栈的IP层，连接是在传输层。连接时翻译的子集。在一个翻译之下，我们可以有许多连接。

xlate命令让我们可以显示或清除翻译槽位的内容。当建立一个通过PIX防火墙的会话时，将产生一个翻译槽位。在修改了配置之后，翻译槽位仍然会保留。在我们的配置中增加、改变或删除alias、conduit、global、nat、route或static命令之后，最好使用clear xlate命令。对PIX防火墙应用reload命令，或者重新开关电源，也可以达到清除翻译槽位的目的。clear xlate和show xlate命令如下：

```
show xlate [global | local ip1 [-ip2] [netmask mask]]  
          lport | gport port [-port]] [interface if1 [,if2] [,ifn]]  
          [state static [,dump] [,portmap] [,norandomseq]  
          [,identity]]
```

```
clear xlate [global | local ip1 [-ip2] [netmask mask]]  
    lport |gport port [-port]] [interface if1 [,if2] [,ifn]]  
    [state static [,dump] [,portmap] [,norandomseq]  
    [,identity]]
```

其中：

[global | local ip1 [-ip2]] [netmask mask]：根据全局IP地址或本地IP地址，显示活动的翻译，用网络掩码限定IP地址的范围；

lport |gport port [-port]：根据指定的本地和全局端口，显示活动的翻译；

interface if1 [,if2][ifn]：根据接口，显示活动的翻译；

state：根据状态，显示活动的翻译；static翻译（static），dump（cleanup），PAT global（portmap），具有norandomseq设置（norandomseq）的nat或static翻译，或nat 0标识特性的使用（identity）。