基于移动 IPv6 的防火墙的研究与设计①

Research and Design of Firewall Based on Mobile IPv6

聂　哲　温晓军　（深圳职业技术学院计算中心 广东深圳 518055）

摘　要：随着 IPv6 的推广应用的不断普及，原有的基于移动 IPv4 的防火墙技术已不能适应移动 IPv6 的需求。在深入分析移动 IPv6 下原有防火墙技术存在的问题后，提出了相应的防火墙设计模型，通过利用 Linux 和 Netfilter 内核机制来实现 IPSec 处理，从而解决了在外的移动节点与本地节点直接通信的问题。

关键词：移动 IPv6 防火墙 安全机制 认证

1　引言

随着 Internet 技术的迅速发展，IP 地址匮乏、网络安全机制不健全等问题突显出来，于是 IPv6 的使用成为可能。但由于原有的各种网络应用均基于 IPv4 协议，因此如何让 IPv4 下的应用能低成本地移植到 IPv6，并能够充分利用 IPv6 的新特性，是目前急需解决的问题。

基于 IPv4 的防火墙要能够在 IPv6 下正常运行，在技术上就需要解决：

（1）由于 IPv6 包格式的变化，防火墙对数据包的处理方式需要重新解析。

（2）如何解决由于 IPv6 对移动 IP 的更强支持而导致的防火墙无法判断一个节点是否为本地节点的问题。

2　IPv6 协议给防火墙设计带来的问题

移动 IP 技术是移动节点以固定的网络 IP 地址，实现跨越不同网段的漫游功能，并保证网络权限在漫游过程中不发生任何改变，实现数据的无缝和不间断的传输。

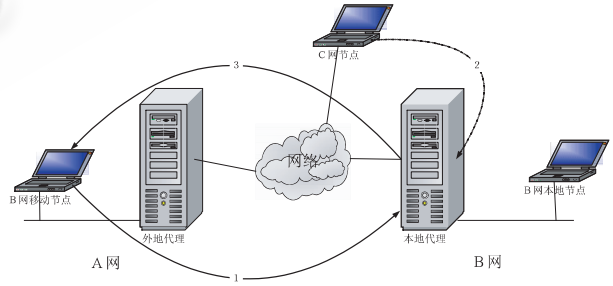
2.1　IPv4 下移动 IP 的工作机制

移动 IPv4 通过移动节点、外地代理和本地代理 3 个功能实体来完协同完成移动节点的路由问题。如图 1 所示。

在移动 IP 协议中，每个移动节点都有 1 个唯一的本地地址。当移动节点移动时，它的本地地址不变。在本地网络上，每一个本地节点还有一个本地代理来维护当前的位置信息，即转交地址。当移动节点连接到外地网络时，转交地址就用来标识移动节点现在所在的位置。移动节点的本地地址与当前转交地址的联合称为绑定。当移动节点得到一个新的转交地址时，通过绑定向本地代理进行注册，以让本地代理即时了解节点的当前位置。

当移动节点连接到外地网络时，移动节点使用一个称为“代理发现”的规则在外地网络上发现外地代理并注册，把这个外地代理的 IP 地址作为自己的转交地址。移动节点获得转交地址后，再通过注册规程把该转交地址告诉本地代理。

这样，当有发往移动节点本地地址的数据包时，本地代理便截取该数据包，并根据注册的转交地址，通过隧道将数据报传送给移动节点。



1－B 网移动节点移动到 A 网，将转交地址告诉本地代理
2－C网节点发网B网在外的移动节点的信息，先发往本地代理
3－本地代理将信息发往在外移动节点的转交地址

图 1　IPv4 下的移动 IP 工作机制

① 基金项目：深圳市科技计划项目（06KJce037）

2.2 IPv6 下移动 IP 的工作机制

在 IPv6 网络中，路由器会周期性地发出广播信息。当一个移动节点连接到网络时，其就会收到路由器广播信息。移动节点检查接收到的广播信息的网络前缀，如果其中的前缀与移动节点的本地地址相匹配，移动节点就连接到它的本地网络，否则，移动节点就连接到一个外地网络，此时移动节点向该路由器所在网络上的一个服务器申请一个地址作为自己的转换地址。

移动节点采用移动 IPv6 进行连接外地网络的通信过程如图 2 所示。

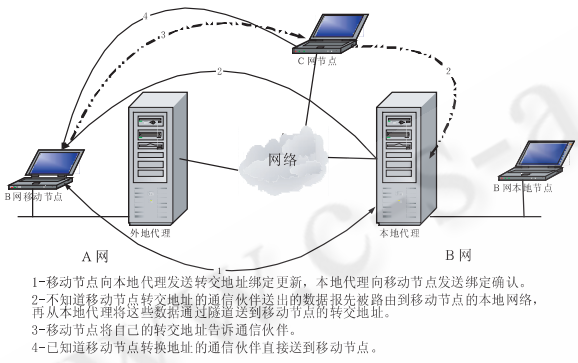


图 2　IPv6 下的移动 IP 工作机制

2.3 IPv4 转向 IPv6 给移动 IP 防火墙设计带来的问题

从图 2 可以看出，由于 IPv6 下的移动 IP 可以不通过本地代理而直接使用转交地址和其他通信节点通信，这就对基于 IPv4 的防火墙带来安全问题。由于出现本地的移动节点移动到本地防火墙之外，异地的移动节点移动到本地防火墙之内的情况，就会导致包过滤型防火墙无法识别一个连接是合法还是恶意的，如图 3、图 4 所示。

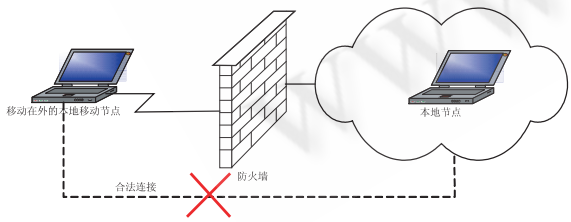


图 3　本地移动节点在外时与本地的连接被防火墙阻断

3　基于移动 IPv6 的防火墙设计方案

从图 3 可以看出，由于移动节点连接到外地网络，防火墙可能截断移动节点和本地节点的通信。我们采

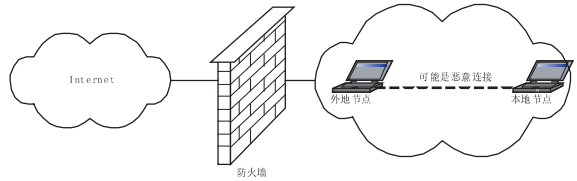


图 4　外地移动节点在与本地节点的连接逃过防火墙检查

用的解决方案是在防火墙中加入对移动节点的状态分析以及认证及授权机制，其拓扑图如图 5 所示。

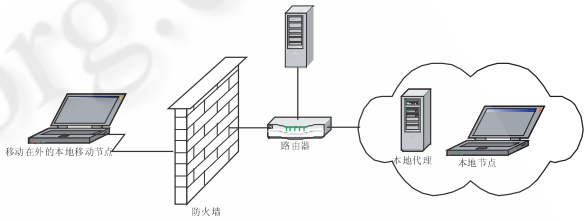


图 5　基于移动 IPv6 的防火墙拓扑图

对移动节点的通信状态分析的目的就是让防火墙能够识别出一个外部节点是否是本地的一个在外的移动节点。其解决方法是在防火墙上建立一个移动节点转交地址表，当一个移动节点连接到外地网络，在向本地代理进行绑定注册时，本地代理将其转交 IP 地址发送到防火墙的移动节点转交地址表中。这样，防火墙可以通过检查一个数据包的源地址是否在该表中而判定一个外地节点是否为本地移动节点。

但由于外地恶意节点可能会伪造源 IP 地址让而躲过防火墙的检查，因此还必须对移动节点进行认证与授权。

而对于图 4 所示的外地节点与本地节点的通信逃过防火墙安全检查的问题，必须通过将防火墙功能分布到各节点来解决，具体做法为：在外地移动节点申请转交地址时，防火墙记录下该外地移动节点，然后通过路由广播的方式通告给本地的节点主机。各主机采取相应措施来保证安全。

4　防火墙协议设计

移动认证主机的主要作用是对移动节点进行认证与授权。通过采用 IPSec 协议实现，IPSec 协议包括网络认证协议 Authentication Header（AH）、封装安全载荷协议 Encapsulating Security Payload（ESP）、密钥管理协议 Internet Key Exchange（IKE）和用于网络认证及加

密的一些算法等。基于 IPSec 协议的数据包格式设计如图 6 所示。

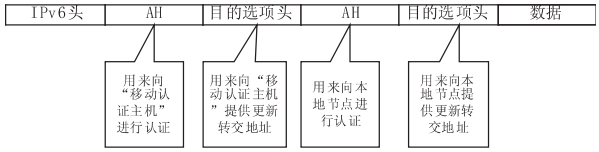


图 6　双重认证数据

在防火墙接收到一个数据包后，查看该数据包是否含有 AH 头，如果有则将该数据报转交给移动认证主机，如果没有 AH 头，则对数据包进行安全性检查，若该数据包没有通过安全性检查，则防火墙将其丢弃。

移动认证主机接收到防火墙转发过来的数据后，通过查看扩展头是否为“转交地址绑定更新”信息。如果是，说明这个数据包是地址更新包，则需要对这个数据包进行认证，如果认证通过，则更新本机的移动节点转交地址表，然后将这个数据包发给相应的目的节点（本地代理或本地节点）；如果没有扩展头，或者扩展头信息不是“转交地址绑定更新”信息，则查看该数据包的源地址是否记录在移动节点转交地址表中。如果表中找到匹配项，则说明这个数据包是移动节点和本地节点的一般通信，直接转发给相应的节点。

5　设计实现

针对所提出的设计方案，我们在 Linux 操作系统下实现了基于移动 IPv6 的防火墙，其设计模型如图 7 所示。

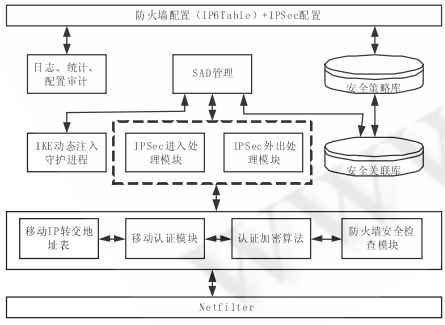


图 7　防火墙设计模型

方案的具体实现充分利用 Linux 的 IPv6 协议栈和 Netfilter 框架。在 Netfilter 的 NF_IP6 – FORWARD 点处加入移动认证模块，通过对数据包的认证分析，来确认数据包是否是本地在外的移动节点，从而确认其通信的合理性，具体处理流程如图 8 所示。

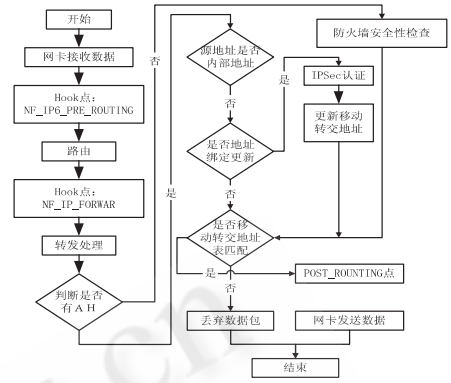


图 8　数据包处理流程

6　结语

针对基于移动 IPv4 的防火墙方案已不能适应移动 IPv6 协议的要求，我们提出了就如何解决 IPv6 下移动节点在外地与本地节点之间的通信穿越防火墙的方案。

（1）由于系统利用了 Linux 和 Netfilter 内核机制来实现 IPSec 处理，并在 IP6table 基础上实现防火墙的过滤功能，配置灵活，效率较高。

（2）该防火墙模型对防火墙外部节点完全透明，可推广性强。

（3）根据该防火墙模型的模块划分，移动认证模块可满足更强的性能要求。

参考文献

1　郭强，朱杰，徐向华. 下一代全 IP 通信网移动多媒体业务的仿真研究 . 计算机仿真，2005，22（5）：98 – 101.

2　周金和，焦瑞莉，李丹. 移动 IPv6 的嵌入式系统实现 . 北京机械工业学院学报，2006，21（3）：21 – 24.

3　施新刚，吴建平，尹霞，崔武成. 移动 IPv6 协议的测试研究 . 小型微型计算机系统，2006，27（7）：1185 – 1188.

4　王承文，陈志刚. 移动 Ipv6 的安全威胁及对策 . 长沙航空职业技术学院学报，2006，6（3）：48 – 50.

5　修志华，卢汉成，李津生，洪佩琳. 一种支持移动 IPv6 的防火墙模型 . 计算机工程与应用，2006，42（6）：116 – 119.

6　李波，钟本善. 移动 IPv6 切换技术 . 电信快报：网络与通信，2006，9：30 – 32.