大型企业网 IPv6 多节点协同机制与安全策略①

郭文刚

(中国电子科技集团公司 电子科学研究院, 北京 100041)

摘 要: 摘要大型企业网结构复杂庞大, 各部门之间需要协同合作, 构建一个多节点协同机制的安全策略体统可以有效解决大型企业网的协同安全管理问题. 针对这种情况, 通过采用 C/S 结构, 引入蚁群原理, 引进入侵检测的算法, 设计并实现了一个基于 IPv6 的多节点协同机制与安全系统框架, 并对本文设计的系统进行了一定的测试实验, 结果表明这一系统可以很好的解决大型企业网安全问题, 实现大型企业网间的有效协同合作, 并较好的解决了大型企业网的协同安全管理问题.

关键词: 大型企业网; IPv6; 多节点协同机制; 安全策略系统; 实现

Large Enterprises Network Security Strategy and Multi-Node Coordination Mechanism Based on IPv6

GUO Wen-Gang

(China Academy of Electronics and Information Technology, China Electronic Science & Technology Group Inc., Beijing 100041, China)

Abstract: The network structure of large enterprises is complex. It requires cooperation between every department. Building a security policy system of multi-node cooperative mechanism can efficiently solve the problem onthe cooperative security management for large enterprises network. Based on the above background, this paper uses C/S structure, introduces the principle of ant colony and the algorithm of intrusion detection, to carry out a research on the coordination mechanism and security system of multi-node based on IPv6. The designed system in this paper is tested. The result shows it can handle the security problem of the large enterprises network well. It also implements the effective collaboration between large enterprises networks, and solves the problem on the cooperative security management of large enterprises network.

Key words: large enterprise network; IPv6; multi-node cooperative mechanism; security policy system; implement

IPv6 (Internet Protocol Version6)也就是下一代互联网协议. IPv6 技术是在 IPv4 技术的基础之上发展而来的. 它定义了归属代理, 通信节点和移动节点三种操作实体[1]. IPv6 定义了两种 ICMP 消息类型: 即归属代理地址发现应答消息和归属代理地址发现请求消息. 另外还定义了两种“邻居发现”选项: 归属代理信息选项和宣告消息间隔. 在传统的 IPv4 网络环境下, 多层软件体系已经发展的十分成熟和丰富, 尤其是发展快速的中间件, 当前大量的企业级计算要实现数据中心的丰富业务都要依靠中间件[2]. IPv6 中通信的安全性的保证主要借助强制实施的 IPSec 协议, 而 IPSec 的实现完全依赖于 SPD 的正确配置和安全策略. IPSec 实现的入口是安全策略, 这在整个 IPSec 体系中发挥着十分重要的作用. IPSec 中的 SPD 所存储的主要是 IPSec 策略[3]. 然而, 基于 IPv6 底层通信的大规模计算体系并未真正成熟, 如各种数据库对 IPv6 操作的支持也是在近两年才开始成熟, 企业核心系统软件的通信层面处于刚刚开始的 IPv6 转换期. 怎样搭建一个跨地区的由多个节点组成的大型企业网, 体现其安全性, 先进性, 协同性, 示范性, 则是本文需要研究的主要内容.

目前, 大多数大型企业网是异构的, 大部分情况下运行在不同的协议上支持不同的功能或应用, 这严重阻碍了企业之间, 企业内部各部门之间及企业与分支企业之间信息沟通与交流, 不利于企业网信息的有

① 收稿时间:2014-07-21:收到修改稿时间:2014-09-10

效快速的传达, 也不利于企业整体安全策略系统的构建. 本文通过对大型企业网中基于 IPv6 的多节点协同机制与安全策略的研究来解决这一现实问题.

1 大型企业网IPv6多节点可协同安全策略系统分析

1.1 大型企业网中 IPv6 的基本应用情况

在传统 IPv4 的网络环境下, 多层软件体系已经发展的十分成熟和丰富, 尤其是发展快速的中间件, 当前大量的企业级计算要实现数据中心的丰富业务都要依靠中间件. IPv6 虽然对上层应用而言, 只是在网络通信层面做了替代, 只是涉及到底层协议栈的修改, 但是, 基于 IPv6 底层通信的大规模计算体系尚未真正成熟, 如各种数据库对 IPv6 操作的支持也是在近两年才开始成熟, 企业核心系统软件的通信层面处于刚刚开始的 IPv6 转换期[4].

IPv6 网络中, 提供一个可扩展的分布式框架来发现、协商和管理 IPSec 策略是 IPSec 策略管理的目标. 它要解决的中心问题是采取一种适应大量的 IPSec 应用和操作模式的方法来控制安全策略, 单独的 SPS 系统不可能做到这点. 而且在大型的分布式网络中, 因为 IPv6 地址空间的强大, 一旦单独配置每一个通信节点的安全策略, 大量的人力资源不仅会浪费, 安全策略配置不一致的问题也会更加容易引起[5]. 随着网络规模地不断扩大及应用地增加, 网络系统及其应用扩展范围也会越来越广阔, 网络的脆弱性也在不断增加. 因此, 网络安全问题的解决不可能一劳永逸.

1.2 大型企业网 IPv6 多节点的划分

在多节点协同机制的安全策略系统中, 本文是以域为单位进行策略的管理与实施的, 本文主要通过以下三种方式来划分大型企业网域: 一是按照大型企业网安全需求进行划分; 二是基于网络拓扑结构进行划分; 三是把安全需求和网络拓扑结构二者综合进行划分, 尽量减少跨域的安全需求[6]. 安全策略在域的划分基础之上, 又可细分为两大策略: 即域内和域间策略. 一台策略管理服务器在多节点分布式环境下, 应具备的功能主要包括以下几方面:

在域内:

(1)执行策略可根据目标策略自动生成;

(2)具备查询执行策略和目标策略的功能;

(3)具有对域内全部安全节点的策略信息进行管理和维护功能, 执行策略和目标策略也包括在内;

(4)保证在安全节点上对执行策略所发送的进行实施;

(5)当目标策略发生冲突时, 向管理员反馈结果, 为其提供候选方案.

在域间:

(1)邻域的策略信息无权直接更改, 由邻域策略管理, 但对于变更所需的策略可以通知邻域;

(2)是否更改由服务器决定, 对邻域服务器所返回的应答进行接收;

(3)向邻域在必要时查询相关的策略信息, 邻域所返回的应答进行接收;

(4)对由邻域发来的变更策略的通知要求进行接收, 是否需要变更要根据域的具体情况而定, 返回应答;

(5)对领域发来的查询进行接收, 之后作出应答.

在网络环境下, 任何一个数据包在离开路由选择域时都必须抵达其中的一个路由器. 一般情况下, 可以控制某一数据包所穿过哪一路由器. 但对于主机而言, 尤其是在链路已经中断的情况, 倘若选择域不止一个退出点, 退出时使用哪个路由器很难进行控制. 为应对这种情况, 对一个域级策略进行定义并把它分发给所有的边界路由器就显得很重要[7].

1.3 安全策略服务器的选取

目前网络中 IPv6 应用以 FTP、WEB 服务、视频点播、文件共享等服务为主, 这类服务对网络带宽有一定要求, 对服务器本身的计算能力并无较高要求. 从更为成熟的行业化应用计算角度来看, 一般的应用都是多层(N-tier)架构, 如常见的 C/S 架构和 B/S 多层应用方式, C/S 的优点是能充分发挥客户端 PC 的处理能力, 很多工作可以在客户端处理后再提交给服务器. 对应的优点就是客户端响应速度快. C/S 一般建立在专用的网络上, 小范围里的网络环境, 局域网之间再通过专门服务器提供连接和数据交换服务, 这符合大型企业网的专用特点[8].

本文所要构建的策略系统模型是基于现有的网络拓扑结构建立的, 而 C/S 模型就是现有的网络模型所采用的. 此外, 本文是对大型企业网安全策略进行研究, 这就决定了安全策略本身所具有的安全性是非常关键的, 所以就需要加强有效控制信息安全的能力. 而在对 C/S 结构与 B/S 结构服务器性能进行比较后, 本文选择 C/S 结构对策略服务器进行配置.

策略服务器压力因多层次多节点的出现而获得了有效分流, 但是任何一个域策略服务器出现了故障都可能影响整个下属域策略的实施[9]. 所以需要构建一个多节点协同机制的框架模型. 当大型企业网工作机出现异常, 协同机制内的其他关键主机主动接管工作机的工作, 快速接管对方机器的数据库, 支持关键应用服务, 保证系统不间断的运行[10].

2　基于IPv6的多节点协同机制安全策略大型企业网构建

2.1 协同机制安全策略系统总体框架

上文已经对大型企业网 IPv6 安全策略系统的数据中心进行了部署, 但还需要构建一个基于这个数据中心的安全策略系统. 本框架主要采取分步实施、分级管理及协同合作的原则. 网络本身就是一个分层次的拓扑结构, 所以网络的安全防护必然要采用分层次的防范保护措施.

一个完整的网络安全解决方案应该对网络的各个层次进行覆盖, 并且与安全管理相结合. 我国的纯 IPv6 网络将网络划分为许多地区, 每个地区中的接入结点又可以细分为普通结点和核心结点[11]. 基于 IPv6 网络的这种安全需求和结构, 本文将网络划分为多个相互之间无交集的安全域, 根节点是数据中心策略库, 在数据中心策略库中, 整个系统手工配置的策略全部存储其中, 发挥协同作用, 并根据各级的具体层次需求逐级从各自安全域策略服务器中下载, 由此得到的这个系统我们称为多级多节点协同安全策略系统, 框架图如下图 1 所示.

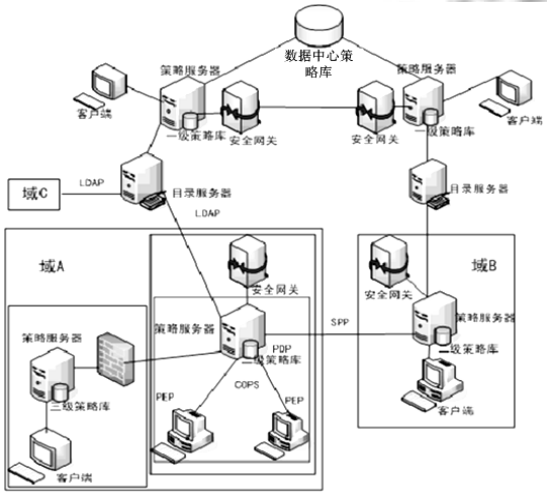

图 1　多节点协同安全策略系统框架

2.2 协同机制安全策略系统设计流程

企业网具备 MPLS 网络, 为实现 IPv6 分支的接入, 可将 PE 路由器升级为双栈. 新建 IPv6 分支节点出口设备作为 CE 设备, 采用双栈路由器.

域在网络环境中一般指的是一个路由选择域, 这也就是说任何一个数据包离开该选择域都必须抵达其中的一个路由器. 一般而言, 控制某一数据包所要穿过哪一个路由器也是可能的[12]. 但如果不止一个选择域的退出点, 对于主机来说很难对哪个路由器退出控制使用, 尤其是在链路已经中断的情况下.

所以, 企业总部与分支采用星型连接, 通过 N×E1 专线的方式, 各分支出口路由器分别汇接至企业总部汇聚路由器. 如果新建了部分 IPv6 分支, 为了达到与分支节点的 IPv6 实现连接的目的, 可将作为汇聚节点的企业总部路由器设备升级为双栈. 双栈的 WEB 服务器, 相对而言其后台支持的 APP 将更为灵活, 既可以是 IPv4, 也可以是 IPv6. 这样一来, 原有的 IPv4 分支与总部的连接保持不变, 而出口设备采用双栈路由器的新建 IPv6 分支节点也可接入到总部的双栈设备上. 根据实际企业组网需要, 分支与总部之间可运行 OSPFv3 路由协议. 如图 2 所示.

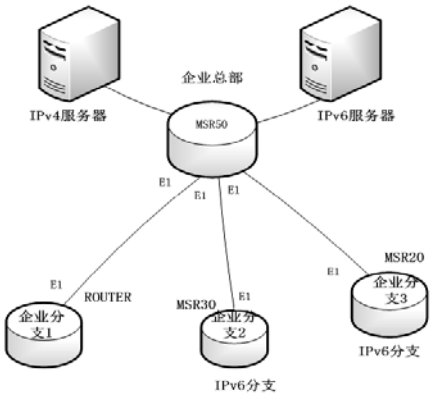

图 2　企业分支节点接入图

在操作安全策略系统中, 一种策略描述语言必须要有, 因为这是管理者对整个分布式系统的管理思想的体现, 可以表达访问控制、身份认证、IPSec 和信息流过滤等多种策略. SPSL 和 Keynote 是目前两种流行的安全策略规范语言,其中 SPSL 语言是 SPS 系统自带的安全策略规范语言, 目前支持包 IPSec 策略、过滤策略和 IKE 策略, 而且可以很容易的被扩展以描述其他类型的策略[13]. 用 SPSL 语言描述 IPSec 策略定义如下:

*policy-name: <object-name>
*association:<mode-name>|mode-set-name>
|<gateway-name>|gateway-set-name>
|<domain-name>
*cache-expiry: <integer>
*policy: Dst,port;src, port; xport-proto
directioninbound|outboundpermit|deny
*userid: * | any | list of [not] n822 <email-addr>
| list of [not] dn<distinguished-name>
* systemname: * |any| list of [not] <general-name>
|list of [not] dn<distinguished-name>
* ipv6-class: * |any| list of [not] <integer-range>
* ipv6-flow: * |any| list of [not] <integer-range>
* seclabel: * |any| list of [not] <seclabel>
*tfr-action:
ipsec-action: see below
isakmp-action: see below
*mnt-by: list of <mntner-name>
*changed: <mntner-name><date>

2.3 Ipv6 攻击方法检测算法设计

网络技术的发展日新月异,所以对于当前的企业而言, 其必须要面对企业内部数据信息以及企业网的安全问题. 网络安全问题在网络技术的不断发展的情况下也变得日益突出,在网络安全防御技术中, 各种主动式的安全防御技术是这些技术中的主流, 其中较为成熟的技术之一便是入侵检测. 基于 IPv6 的多节点协同机制同样需要维护大型企业网的安全, 在分析协同机制安全策略系统框架的基础上还需要对基于IPv6的企业网安全攻击行为特征进行分析[14]. 所以本文引进入侵检测的算法来掌控基于 IPv6 的大型企业网的安全.

当前在大型企业网络上的IPv6的攻击事件相对较少,所以在研究基于 IPv6 漏洞攻击事件的特征和行为时,首要的便是构造一个 IPv6 环境,开发出基于大型企业网 IPv6 的攻击集成平台,进而能对整个 IPv6 环境下的攻击行为进行较为全面地模拟. 本节在入侵检测当中引入蚁群原理, 在建立特征和检测中利用其协作、启发式、信息素等, 使入侵检测的检测率更加有效而智能[15].

在入侵检测中, 蚁群原理的应用主要通过蚁群原理与聚类分析结合来实现, 也就是聚类入侵检测技术. 进行入侵检测在利用聚类分析时, 主要经过数据标准化、标记实例数据、聚类分析、实时入侵检测等几个过程. 在这些过程的基础之上得到聚类结果之后, 就可以对正常数据以及异常数据进行有效的区分. 一般而言, 在网络中正常数据流占据绝大部分, 大大多于入侵数据[16]. 所以可以认为各种体现攻击行为的类及其子类数量要远远少于正常行为的类及其子类数据的数量. 正常行为和异常行为可以根据聚类的划分进行区分, 这可以借助于全部的聚类中所包含的数据数量大小进行排序, 设定一个阈值 β, 对大于 β 的聚类就判定为正常行为, 否则就被认为是异常行为.

本文中的入侵检测算法主要是在蚁群聚类基础上展开的, 数据可以被看作是不同属性的蚂蚁, 聚类中心可以看作是蚂蚁所要寻找的“食物源”. 所以, 数据聚类过程实际上是一种蚂蚁对“食物源”进行寻找的过程. 设$X=\{Xi|Xi=(xi1,xi2,...,xim),i=l,2,...,N\}$是将要进行聚类分析的数据实例集合, 令

$$d_{ij}=\| P(X_i - X_j)\|_2 = \sqrt{\sum_{k=1}^{m} P_k (X_{ik} - X_{jk})^2},$$

d_{ij} 表示 X_i 到 X_j 之间的加权欧氏距离,其中加权因子为p,可以根据在聚类中各分量的贡献不同而设定.

聚类半径设为 r,统计误差用 ε 表示,$r_{ij}(t)$是 t 时刻数据 X_i 到数据 X_j 路径上残留的信息量,设 $\tau_{ij}(0)=0$, 即各条路径上的信息量在初始时刻相等且为 0. 路径 ij 上的信息量有下式给出:

$$\tau_{ij}(t)=\begin{cases}1, d_{ij} \le r\\ 0, d_{ij} > r\end{cases}$$

是否将 Xi 归并到 Xj 由下式给出:

$$P_{ij}(t)=\frac{\tau_{ij}^{\alpha}(t)\eta_{ij}^{\beta}(t)}{\sum_{s\in S}\tau_{sj}^{\alpha}\eta_{sj}^{\beta}(t)}$$

其中, $S=\{Xs|dij\le r,s=1,2,...,j,j+l,...,N\}$. 若 $P_{ij}(t)\ge P_0$,则 X 归并到 X_j 邻域. 令

$$Cj=\{Xk|dkj\le r,k=1,2,...,J\}$$

所有归并到 X_j 邻域的数据集合用 C_j 表示. 理想聚类中心的求出主要根据下式:

$$\overline{C_j}=\frac{1}{J}\sum_{k=1}^{J} X_k$$

其中, $X_k \in C_j$.

审计在入侵检测系统(IDS)中扮演着十分关键的角色,但是为了有效的分析入侵, 审计中大量的数据要

收集. 在入侵检测系统当中, 完整的特征库被建立以后,接下来就要利用它来实现入侵检测. 对于系统收集的审计数据库当中各种入侵审计数据,要实时进行处理,这样才能在第一时间里知道入侵,给出对策[17]. 具体的处理过程如图 3 所示:

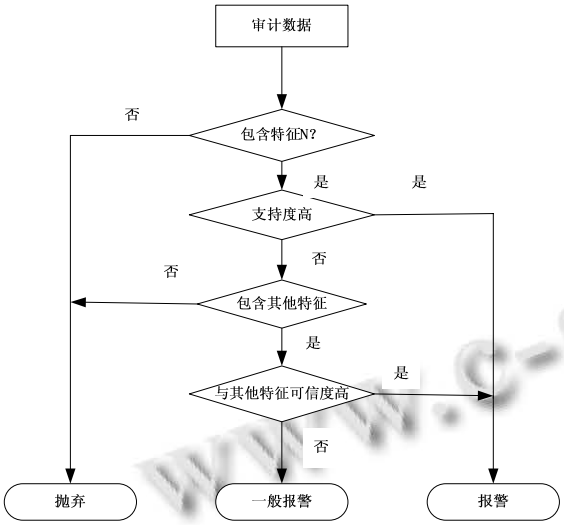

图 3　审计处理过程

```
算法: IF INCLUDED_CHARACTER_N
      IF DATA_SUPPORD_HIGH
      ALARM()
      ELSE IF INCLUDED_OTHER_ CHARACTER
      IF HAS_HIGH_CONFIDENCE_WITH_OTHERS
      NOTICE();
      ELSEALARM();
      ELSEALARM();
      ELSEABANDON();
      ELSE ABANDON();
       RETURN();
```

3　基于IPv6的多节点协同安全策略系统设计实现

3.1 系统实现

总部的 IPv6 网络以及 IPv6 业务, 可被分支内的 IPv6 用户直接访问. 同时, 由于总部双栈路由器可以作为 NAT-PT 设备, 所以借助于 NAT-PT 设备, 分支的 IPv6 用户也可以访问企业原有的 IPv4 网络和 IPv4 业务. 企业网能兼容 IPv4 的目的就可以达到.

由于保存 SPD 在内核, 所以在具体实施 IPSec 方案中, 需要有一个合适的接口来对内核进行操作. 图 4 为多节点可协同多域安全策略系统的 IPSec 实现框. PF KEY 在 IPSec 密钥管理应用中, 是其进程接口. 对 SAD 进行与 SA 相关的操作是它的基本作用. 因为没有具体指定 SPD 接口, PF KEY v2 的功能因此可以得到扩展, 并对内核中 SPD 进行操作.

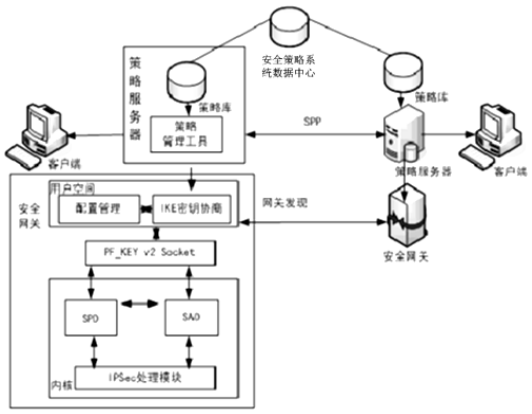

图 4　多节点可协同安全策略系统在 IPSec 中的实现

有效检测可以说是安全问题的核心. 构建新协议下的IPv6特征库,以实现检测的准确快捷. 在当前IPv4与 IPv6 共存情况下,IPv6 库的建立是否完备,将直接决定入侵检测能否成功. 入侵检测系统在 IPv6 环境下,描述网络数据报文所使用的规则语言非常灵活,因此对网络攻击行为可以做出快速的翻译. 攻击方法检测处理实现流程如图 5 所示.

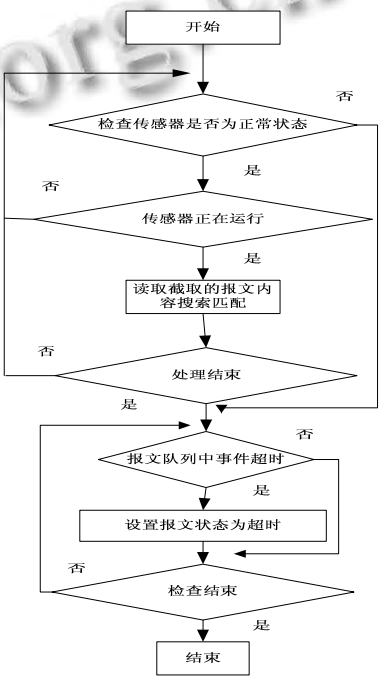

图 5　攻击方法检测处理流程

3.2 系统应用实例分析

本文提出的基于 IPv6 协议一致性协同测试框架, 不同于传统的测试结构, 是基于实例进行的测试. 不再对测试系统和测试方法所要实现功能的界限进行明确的定义, IPv6 协议测试的需求在基于物理测试的所有测试功能能上可以得到充分满足[18]. 以下是对系统测试分析的通信节点进行的几点说明.

(1)在检查移动报头有效性上存在些许问题: 即使收到与协议标准所规定不相符的字段, Code 为 0 的 ICMP 参数错误消息在被测移动节点上也没有返回;

(2)在注册过程中, 收到的 Code=2、Type=4 的 ICMP 错误消息不能够正确处理. 移动节点应该在过一段时间后试图重新注册. 但是测试发现在这种情况下在测试中, 被测移动节点并不会试图重新注册;

(3)动态家乡代理地址发现机制不受支持: 在进行家乡注册时, 被测移动节点收到状态为 133 的绑定确认消息, 动态家乡代理地址发现请求消息没有发送;

根据以上的说明, 做一个假设: 在大型企业网中心策略库可以把域 IPSec 策略描述为: 安全域内的任何被允许的端到端的通信安全利用 IPSec 来保护, 假设在大型企业网中汇聚点部署 A 和 B 两台安全策略主机. 为了实现应用 IPSec 策略后的 IPv6 通信, 需要对每台主机的安全关联数据库 (SAD)和安全策略数据库(SPD)进行正确的关联和策略配置. HTTP 协议的数据包通信在两台主机开始通信时, 将被 ESP 和 AH 传输模式保护起来. ESP 传输模式还将保护其它数据包通信.

下图 6 所示的是在外地链路移动到新的外地链路后, 移动节点重新向家乡代理注册测试例的测试结果图. 图 6 中被测协议实现移动节点 MN 由 SYSTEM 代表; component 1 是创建的并行测试成分, 在新外地链路时, 其代表移动节点是家乡代理 HA; 在外地链路时, MTC 成为家乡代理 HA 的代表移动节点. 可以从下图 6 中看到测试结果为 pass(通过).

所以, 本应用实例测试中假设的两台主机都有关联和本地环回(loopback)策略, 在仅有一台主机的可用的情况下, 可作为测试之用. 每个安全策略需要进出两个安全关联, 所以一共需要八个安全关联. 包含数据的文件需要在两台主机进行创建, 其中的数据用来创建和验证关于每个 IPSec 保护的数据包的“报文摘要 (MD) ”键入散列数据. 两台主机如果只有一台主机应用了 IPSec 策略时, 他们之间不能进行通信. 一台应用了 IPSec 策略的主机也不能与其它没有应用 IPSec 策略的主机进行通信. 倘若试图与一台应用了 IPSec 策略的主机进行通信, Ping 命令的返回信息为 Request timed out. 对于本测试来讲, 由于应用了 IPSec 策略在环路本地地址上, 所以当 Ping6: 1 时, 通信正常.

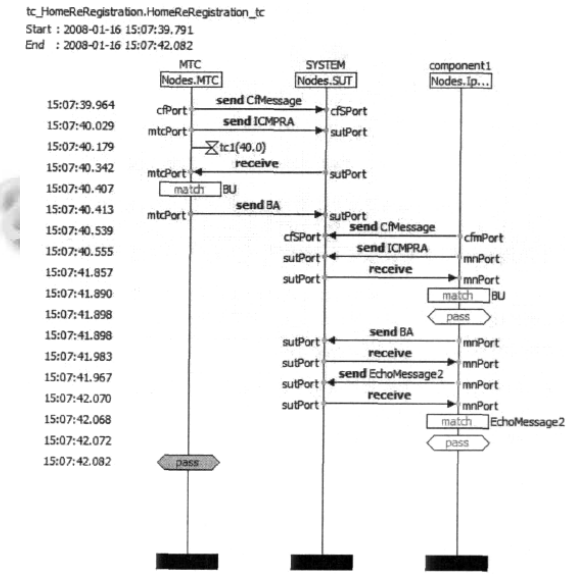

图 6 移动节点主转交地址重新注册测试结果

4 结语

IPv6 在数据中心的具体实践应用可以说是 IPv6 发展首要表现. 双栈数据中心在 IPv4 向 IPv6 的长期过渡周期内会成为最基本的建设模式, 而当前 IPv6 时代新 IT 建设能够持续有效的最佳方式便是要不断实践、深入探索[19]. 构建快捷、稳定、高效的 IPv6 安全策略数据系统中心基础架构, 是实现大型企业网安全有效协调重要保障.

基于 IPV6 技术的下一代互联网的安全已经不仅仅局限于对网络传输安全、数据安全的关注,还要关注管理方面的安全,要基于管理观念并结合体系结构来制定网络的管理和安全体系,要有有效的网络安全防护机制,还要重视网络管理所发挥的基础性作用[20]. 本文把蚁群原理引入到入侵的规则建立与检测中,对安全检测研究的深入提供了新的思路和方法. 这对于大型企业网而言, 更是如此, 本文基于 IPv6 的多节点协同机制与安全策略体系为其提供了一个可供参考的框架, 具有一定的实践意义.

参考文献

1 伍孝金.IPv6 技术与应用.北京:清华大学,2010.

2 杨国良,李阳春,伍佑明.IPv6 技术、部署与业务应用.北京:人民邮电出版社,2011.

3 约瑟夫·戴维斯,杨轶,苏啸鸣,吴超译.深入解析 IPv6.第 2 版.北京:人民邮电出版社,2009.

4 郑红霞,田军,张玉军,等.IPv6 协议一致性测试例的设计.计算机应用,2011,23(4):62–64.

5 杭州华三通信技术有限公司.IPv6 技术.北京:清华大学出版社,2010.

6 苏金树,涂睿,王宝生,刘亚萍.互联网新型安全和管理体系结构研究展望.计算机应用研究,2009,21(10):35–38.

7 Wu JP, et al. CNGI－CERNET2: An IPv6 deployment in China. Computer Communication Review, 2011, 41(2): 48–52.

8 邱全杰.一种 IPv6 网络可用带宽测量方法及分析.计算机科学,2011,24(3):84–86.

9 张栋,黄成.Linux 服务器配置与管理.第 2 版.北京:电子工业出版社,2012.

10 Desmeules R. Cisco self-study: Implementing Cisco IPv6 networks(IPv6). Published by: Cisco Press, USA, 2013. 1011–1012.

11 周晓娟.IPv6 从网络到应用的蝶变.中国教育网络,2010,16(8):12–15.

12 刘灏.浅谈 IPv6 技术的发展前景及影响.价值工程,2010,23(36):152–152.

13 Wu JP, Wang JH. CNGI-CERNET2: An IPv6 deployment in China. Computer Communication Review, 2011, 41(2): 48 –52.

14 Yang ZJ, Yu JC. Research and Implementation of IPv6 ControllableMulticast in the Campus Network. Beijing, Beijing Jiaotong University, 2010.

15 张雅琼.浅谈 IPv4 向 IPv6 过渡技术.科技传播,2010,26(18):25–28.

16 武萍.IPv6 在网络中的应用.内蒙古科技与经济,2010,20(8):31–33.

17 姜晓琳.IPv6 在企业网中的部署.硅谷,2013,26(11):123.

18 桑文辉.互联网协议中 IPv6 过渡机制的探讨.硅谷,2009,30(18):105–106.

19 李哲夫.基于 IPv6 的校园网用户管理系统设计.微计算机应用,2011,21(4):62–63.

20 吴斌.IPv4 与 IPv6 混合网间的 SIP 通信解决方案.现代计算机(专业版),2011,18(29):42–43.