支持服务质量机制安全的策略防火墙设计与实现*)

Research and Realization of QoS Security Based on Policy Firewall Technology

郭乐深　刘锦德

(电子科技大学计算机学院微机所　成都610054)

Abstract With the increasing development of broadband and Multimedia technology, the implement of IP QoS is inevitable. But the security in IP-QoS network is insufficient. It is a great challenge for the future IP-QoS network. In this article, the authors present a solution, which realizes the security of IP QoS network by defining the QoS policy in policy firewall system. The QoS policy structure is given in the end of paper. We solve the difficulty question totally.

Keywords Intserv, Diffserv, Security policy, Firewall, Security QoS policy

1. IP服务质量机制的安全性隐患

现在Internet上的应用层出不穷，多媒体信息的数量与日俱增。Internet已经逐步由单一的数据传送网络向数据、语音、图像等多媒体信息的综合传输网络演化。因此，以提高网络资源利用率、为用户提供更高的服务质量(QoS)为目标的研究领域目前极其活跃。近几年Internet的IETF相应的工作小组提出的RFC2115，RFC2117以及1998，1999年提出的RFC26xx系列中的Intserv(Integrated Service[1])和Diffserv(Differentiated Service[2~4])等用于解决IP QoS控制问题。

在上述标准中提供用户的服务质量方式安全性还不能令人满意，易于受到网络攻击，这些攻击包括：一种是主动攻击，它以各种方式有选择地破坏资源预留请求(RSVP数据包)信息的有效性和完整性，来破坏资源的请求、延迟或丢弃资源请求与响应，尤其是近一段的DOS(Denial of Service)攻击；另一类是被动攻击，它是在用户正常工作的情况下，进行截获、窃取、破译以获得用户资源预留的用户认证重要信息，然后恶意地过度消费正常用户的资源，使用未认证的用户的资源，所以IP QoS机制的安全性必须解决。

面对高速发展的多媒体技术、IP QoS技术和越来越多的用户需求，传统设计的防火墙系统的伸缩性和可扩展性较差，所以无法灵活满足用户这些日益发展的需求，导致大多数防火墙系统仍然基于传统IP数据包设计安全保护，没有针对IP服务质量体系结构进行安全保护，从而导致IP QoS技术难于在Internet网络实施的原因之一。本文基于可伸缩、可扩展的策略防火墙系统上，通过定义面向IP QoS体系结构的QoS安全策略及其结构，来设计与实现支持IP服务质量机制的防火墙系统来解决这些问题。

2. 基于策略防火墙的框架

2.1 防火墙综述

防火墙是近期发展起来的一种保护计算机网络安全的技术性措施，是一个用以阻止网络中的黑客访问某个机构网络的屏障，也可称之为控制进/出两个方向通信的门槛。在网络边界上通过建立起来的相应网络通信监控系统来隔离内部和外部网络，以阻档外部网络的侵入。目前的防火墙主要有以下三种类型：

(1)包过滤防火墙：设置在网络层，可以在路由器上实现包过滤。首先应建立一定数量的信息过滤表，信息过滤表是以其收到的数据包头信息为基础而建成的。信息包头含有数据包源IP地址、目的IP地址、传输协议类型(TCP、UDP、ICMP等)、协议源端口号、协议目的端口号、连接请求方向、ICMP报文类型等。当一个数据包满足过滤表中的规则时，则允许数据包通过，否则禁止通过。这种防火墙可以用于禁止外部不合法用户对内部的访问，也可以用来禁止访问某些服务类型。但包过滤技术不能识别有危险的信息包，无法实施对应用级协议的处理，也无法处理UDP、RPC或动态的协议。

(2)代理防火墙：又称应用层网关级防火墙，由代

*)本文得到电子科学研究院预研项目资助。郭乐深　博士研究生，主要研究方向为开放系统、多媒体技术和系统可靠性。刘锦德　教授，博士导师，主要研究方向为开放系统技术、虚拟现实和多媒体应用。

理服务器和过滤路由器组成，是目前较流行的一种防火墙，它将过滤路由器和软件代理技术结合在一起。

(3)双穴主机防火墙：是用主机来执行安全控制功能。一台双穴主机配有多个网卡，分别连接不同的网络。双穴主机从一个网络收集数据，并且有选择地把它发送到另一个网络上。网络服务由双穴主机上的服务代理来提供。内部网和外部网的用户可通过双穴主机的共享数据区传递数据，从而保护了内部网络不被非法访问。

2.2 基于策略防火墙

上述单一型防火墙系统已经不能完全地满足分布式信息系统的安全要求，于是人们寻求一种在逻辑和物理上统一的实现多种类型混合型防火墙的实现框架结构，因此产生了基于策略防火墙。

基于策略防火墙是一种防火墙实现模型体系结构，其目的是建立一个可伸缩、分布式、逻辑与物理上统一、高效的防火墙系统。其核心思想是：无论是那一种类型的防火墙(包过滤型防火墙、代理防火墙、双穴主机防火墙)，都可以通过定义不同安全策略实现，即当防火墙系统中定义包过滤、代理、双穴主机等不同策略时，防火墙成为混合型滤防火墙，同样道理，当防火墙策略定义安全服务质量策略时，就成为支持服务质量机制安全的防火墙系统。

基于策略的防火墙体系结构分为两个组件：策略实施点(Policy Enforcement Point，PEP)和策略决定点(Policy Decision Point，PDP)。其中策略实施点和策略决定点可以比喻成警察和法官的关系，策略实施点是具体安全策略实施者，策略决定点则根据安全策略数据库，也可能是其他的认证服务器上的策略信息(比如 RADIUS、LDAP 数据库信息等等)，其系统结构见图1。

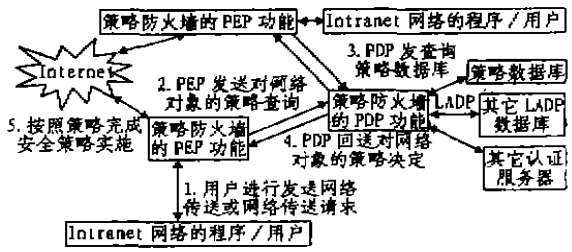

图1 基于策略的防火墙的体系结构

在策略防火墙中 PEP 和 PDP 在逻辑功能上是分开的，在物理上可以是在同一设备上或分别在不同两台机器上执行，实际上当 PDP 和 PEP 同处于一台设备上时，我们称这种 PDP 为本地 PDP(简称 LPDP)。对于 PEP 和 PDP 在不同机器上时，机器之间通过 IPSec 加密技术进行策略对象信息的传输。

基于公共的 Internet 网络来组建复杂的分布式系统时，基于策略防火墙的 PEP 设备按照域划分，同一个域中的 PEP 对应同一个 PDP 设备，而 PDP 设备维护了一致的网络安全策略，这样，虽然 PEP 是分散在网络各个角落，但是同一域内的网络策略是统一、完整的，于是基于策略防火墙系统可以较好解决大型、分布式、企业级网络的信息安全问题。基于策略防火墙系统的执行过程如下：

1)用户程序发送网络传送或网络传送请求(包括 RSVP 申请、多媒体数据流、WWW 连接申请、FTP 数据传输等等)。

2)数据包在经过 PEP 进行检查时，PEP 根据数据包内容生成相应的条件，并且把该条件发向 PDP。

3)PDP 接到 PEP 的条件查询申请，查找自己的策略数据库(本地的策略数据库，LADP 数据库、其他认证服务器上信息等)。

4)PDP 根据 PEP 发送的条件和策略数据库的网络对象的策略，产生策略决定，并且把决定回送该 PEP。

5)PEP 按照 PDP 策略决定，完成安全策略实施，即执行接受、拒绝和丢弃等动作。

2.3 基于策略防火墙中组件功能与框架

基于策略防火墙包括主要功能为决策、策略实施、条件度量三个方面，其中 PDP 主要执行决策，而 PEP 完成策略实施、条件度量功能，下面详细论述这三个方面。

策略决定点(PDP)完成策略决策包括：查询策略、解释策略、探测策略冲突、查询策略数据库界面与接受 PEP 的条件界面、判定 PEP 的条件与策略是否相关、向 PEP 返回策略决策等功能。

策略实施点(PEP)实现的策略实施的主要功能：根据网络度量生成条件，并且把条件发送给 PDP，接受 PDP 的策略决定，执行 PDP 的策略决定。

另外 PEP 还要对网络状态进行度量，度量是为了生成 PEP 的条件，度量的内容分为静态和动态两种，静态度量主要针对数据包内容和用户信息(如数据的目的节点、源节点、端口号、协议等)、用户名(对于 RSVP 协议包)等静态信息产生度量；动态度量不仅根据数据包内容和用户信息，还要结合当前网络状态(网络的可用带宽大小、网络时间、网络延迟大小等)等动态变化信息共同产生度量。

基于策略防火墙框架见图2，该框架进一步反映基于策略防火墙的体系结构和功能，框架包括策略管理工具、策略数据库、PDP 和 PEP 等四个方面，其中策略管理工具和策略数据库与 PDP 之间交互采用标准的 SNMP 协议，而 PDP 与策略数据库采用数据库接口或

者是 LDAP 协议交互，而 PDP 和 PEP 之间交互采用是基于 IPSec 安全协议上的 COPS[7]协议进行交互。

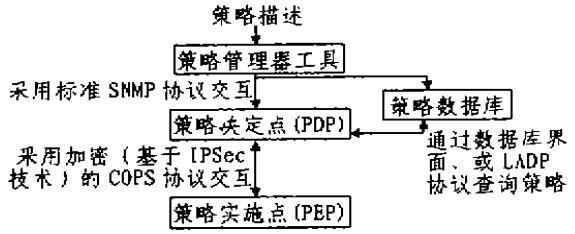

图2 基于策略防火墙框架

3. 基于策略防火墙实现 QoS 保证机制的安全性

3.1 提供端到端 QoS 保证机制的结构

在 IP 网络的 QoS 研究中存在不同两种体系结构：Intserv 体系结构及其相应的信令协议 RSVP 和 Diffserv 体系结构，为了更好地提供端到端的 QoS 提供机制，通常考虑将 Intserv、RSVP、Diffserv 相结合、相协同，文[5]描述如何将两者结合，为用户提供统一的端到端的 QoS 方法，其核心思想是在支持 Intserv/RSVP 的端到端网络中央含有一个 Diffserv 区，发送方与接受方都使用 RSVP 协议传达用户的定量 QoS 请求，RSVP 请求由 Intserv 的边缘路由器/边缘防火墙(ER)和 Diffserv 的边界路由器/边界防火墙(BR)截取，进行不同方式资源预留处理，资源预留处理内包括安全性检查，策略加纳控制、资源接纳控制和实际资源预留，具体如图3。

图3 Intserv、RSVP、Diffserv 为用户提供统一的端到端的 QoS

Diffserv 与 Intserv/RSVP 协同工作的好处是[5]：使用 RSVP 为信令的 Intserv 网络区和使用 RSVP 代理的 Diffserv 网络区网络可以识别端系统用户的 RSVP 数据包，而资源请求可以通过识别的两个不同的网络区的网络元素（如基于策略的防火墙系统、Intserv 的边缘路由器 ER、Diffserv 的边界路由器 BR 等）截取，而在资源请求数据包中存在标识流（per-flow）的服务质量参数、用户或应用程序的信息，通过 RSVP 数据包中的信息参数，PEP 可以生成基于策略防火墙的条件，PDP 按照 PEP 生成的条件和基于策略防火墙中策略数据库中定义的支持 QoS 机制的 QoS 安全策略进行安全性检查，同时按照 QoS 安全策略产生对应的动作，PDP 把对应动作传输给 PEP 进行处理用户或程序的服务质量请求（即接受、拒绝和丢弃等）。

3.2 基于策略防火墙的 QoS 安全策略

由于基于策略防火墙是可伸缩、分布式、逻辑与物理上统一、高效的防火墙系统体系结构，我们针对第1节所论述的服务质量机制的安全隐患和第3.1节所论述的提供端到端 QoS 保证机制的结构，通过在策略数据库中增加支持服务质量的策略，可以实现支持服务质量机制安全性的防火墙系统。服务质量策略是针对非法用户的攻击制定，其策略结构详见图4。下面详细描述服务质量策略含义。

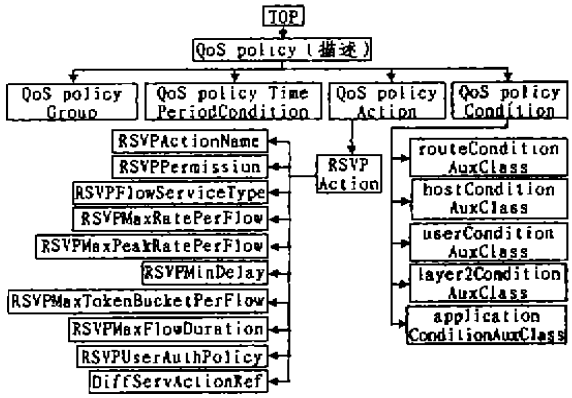

图4 支持服务质量(QoS)的策略防火墙的策略结构

在图4的策略结构中 QoS policy 是对服务质量策略的一般性描述；QoS policyGroup 表示服务质量策略所属的策略组信息；QoS policy TimePeriodCondition 描述该条策略的有效时间；最重要是 QoS policy Decision 和 QoS policy Condition 结构，QoS policy Decision 表示服务质量策略的条件(Condition)，QoS policy Condition 表示满足该服务质量策略的条件下，PDP 要求 PEP 所要执行的决定。

QoS policy Condition 的内容包括：1) hostConditionAuxClass：表示本 QoS 策略适用的源 IP 地址和目标 IP 地址范围；2) userConditionAuxClass：表示本 QoS 策略适用的用户信息（在 RSVP 包中含有用户信息）范围；3) applicationConditionAuxClass：表示本 QoS 策略适用的端口号范围，以及通信协议（如 TCP、UDP、ICMP、RSVP 等）；4) routeConditionAuxClass：表示本策略适用的防火墙的资源情况（即可用带宽，延迟、抖动、拥塞情况）；5) layer2ConditionAuxClass：表示本 QoS 策略适用的源 MAC 地址和目标 MAC 地址

（下转第56页）

IDS 具有一些共同特征，由于 IDS 在分布式环境中得到了应用，所以也包含了一些如远程设置、安全通信和认证之类的特征。IDS 产品中通常都能发现一些系统管理功能问题，比如集中式事件通知、日志记录、模板和自动响应报告问题。在 NT 系统中需要对所有的攻击进行监控。为防止 NT 中用户优先权的非正常改变，必须监视非常重要的两类事件：优先级变化和假冒。以下是几个比较有名的用于 NT 的 IDS 产品。

①Centrax 公司的主导产品 eNTrax，向组织提供以下四种关键业务：检测威胁和误用并且作出响应；制止将要发生的误用；破坏性估计；可能的预防措施支持。

②IIS SAFESuite 和 RealSecure for NT，前者产品系列进行本地和远程脆弱性评价。RealSecure 是一种通过检查网络数据包来寻找攻击的智能网络监视器。IIS SAFESuite 和 RealSecure 具有许多十分有用的特点，如远程管理、综合报告、自动响应、目标结点的可配置策略模板以及网络控制台和目标结点间的安全通信。

③Security Dynamics 公司的 KSA 和 KSM。KSA 是一捕捉脆弱性的评价工具，其基础就是通过咨询获得最优方法。KSM 是一种 NT 事件日志监控器，重点是事件日志分析和报警。

结束语 本文结合计算机系统的主要安全目标和安全体系结构，提出了 NT 安全性模型。通过对该安全模型的研究分析，提出了一些改善和提高 NT 站点安全性的切实可行的技术措施和策略，改善了传统安全方法。这些安全措施或策略已在企业和高校中得到成功应用。

参 考 文 献

1 Hancock B. Security Views. Computers Security, 1999, 18: 646～659
2 Cheswick W R. Firewalls and Internet security repelling the wily hacker. Reading, MA: Addison-Wesley, 1994
3 Okuntseff N. Windows NT security: programming easy-to-use security options. Lawrence, KA: R&D Books, 1998
4 Abrams M D. Network security, protocol reference model and the trusted computer system evaluation criteria. IEEE Network Magazine, 1987, 1(2): 24～33
5 Sheldon T. Windows NT security handbook. Berkeley, CA: Osborne McGraw-Hill, 1997
6 Needham R M. The changing environment for security protocols. IEEE Network, 1997, 11(3): 12～15
7 Cooper & Lybrand. Microsoft Windows NT server: security features and future direction. Available at: http://www.microsoft.com/security, 2000
8 Available at: http://www.microsft.com/ntserver/windowsnt5/exec/overview/whatsNew.asp; http://www.mcom.com/info

（上接第42页）

范围，以及子网的类型（以太网、令牌网、ATM 网等）和网段是否支持802.1P，802.1Q 协议。

QoS policy Decision 表示对应的 QoS policy Condition 条件下，PDP 作出的决定（Decision），即要求 PEP 采取的动作，其中包括一个子树——RSVP Decision，而 RSVP Decision 包括的策略动作有：1）RSVPActionName 指定本 QoS 策略条件的动作名字；2）RSVPPermission：指定本 QoS 策略的条件是否执行接受动作；3）RSVPFlowServiceType：描述本 QoS 策略条件的多媒体流，指定其服务类型（Guaratee，ControlledLoad，Besteffort）；4）RSVPMaxRatePerFlow：指定本 QoS 策略条件的多媒体流的平均速率；5）RSVPMaxPeakRatePerFlow 指定本 QoS 策略条件的多媒体流的峰值速率；6）RSVPMaxTokenBucketPerFlow 指定本 QoS 策略条件的多媒体流的缓冲区大小；7）RSVPMinDelay 指定本 QoS 策略条件的多媒体流的延迟大小；8）RSVPMaxFlowDuration 指定本 QoS 策略条件的多媒体流的持续时间；9）RSVPUserAuthPolicy 指定本 QoS 策略条件的多媒体流的用户认证协议（Kerberos、RADIUS）；10）DiffServActionRef：指定本 QoS 策略条件的 RSVP 数据包由 Interserv 域进入 Diffserv 域或反之时，指定 RSVP 与 Differserv 之间的映射关系。

结束语 随着 IP 网络互联规模不断扩大，用户对多媒体业务、实时业务需求增加，网络中服务质量机制必然得到广泛应用和实施，本文深入研究近几年防火墙技术和服务质量技术的最新发展，并且结合策略防火墙技术的可伸缩、可扩展基础上，通过定义面向 IP QoS 体系结构的安全 QoS 策略，来设计与实现支持 IP 服务质量机制安全的策略防火墙系统，从而解决了这一棘手问题。

参 考 文 献

1 Braden R, Clark D, Shenker S. Integrated Services in the Internet Architecture. IETF RFC 1633, June 1994
2 Black D, et al. An Architecture for Differentiated Service, Internet Draft, Mar. 1998
3 Nichols K, Jacobson V, Zhang L. A Two-bit Differentiated Services. Internet Draft, Nov. 1997
4 Rosen E, Viswanathan A, Callon R. Multi-protocol Label Switching Architecture. Internet Draft, Mar. 1998
5 Bernet Y, Yavatkar R, Ford P, et al. A Framework for integrated services operation over diffserv network. IETF Internet Draft (draft-ietf-issll-diffserv-rsvp-03.txt), September 1999
6 Yavatkar R, Pendarakis D, Guerin R. A Framework for police-based Admission Control. IETF Internet Draft (draft-ietf-rap-framework-03.txt), April 1999
7 Boyle J, et al. The COPS (Common Open Policy Service Protocol. IETF Internet Draft (draft-ietf-rap-cops-06.txt), February 1999