防火墙核心技术的研究和高安全等级防火墙的设计*)

Research for the Critical Technology of Firewall and Implementation in a High Level Security Firewall

黄登玺　卿斯汉　蒙　杨

(中国科学院信息安全技术工程研究中心　北京100080)

Abstract　This paper studies the current critical technology of firewall. Considering the total solution for network security, we design and implement a high level security firewall. In the process of design, we take a few of new technology such as Status Inspection, 2-dimension PATRIE algorithm, Key Management protocol IKE, and Authentication technology. We structurize the functional modules based on the correlation among the policies of security. After a strict test, we find our firewall is a compromise of functions and performance.

Keywords　Stateful inspection, Packet classification, NAT, VPN, Security association, IKE, Security OS

一、引言

随着信息安全越来越受到人们的重视，防火墙作为一种有效的网络安全技术，也越来越受到人们的注意。在从90年代初开始的近十年的研究中，防火墙本身的技术也逐渐完善起来。但无论是包过滤还是应用代理防火墙，都是基于规则和状态的。而密码和加密作为经典和终极的安全技术，也成为现在流行的防火墙技术。另外，当前的防火墙类型是建立在早期的网络安全需求基础上的，它考虑的对象主要是单个的子网，并且各种类型的防火墙都存在其相应的弱点，包过滤是一个无状态的概念，不能根据通讯的上下文或应用的上下文来进行过滤；同时难于配置、监视和审计，只有极弱的包信息处理能力。应用代理发生在应用层，最大的优点是有状态的，但每一个服务都需要一个代理，不易扩展，并且性能很低。总之，已有的防火墙系统是一个静态的网络攻击防御，其对新协议和新服务的支持不能动态地扩展，所以很难提供个性化的服务。根据上面的分析，我们提出了新的防火墙系统，该系统以防火墙设备为安全核心，来提供面向企业尤其是 Intranet 的网络安全整体解决方案。本文首先将对从配置、检测和基于密码学两方面的技术进行研究，并给出我们在技术实现上的考虑，最后本文从各安全技术的策略管理的角度出发，介绍我们在安全操作系统上的防火墙的体系结构，并试图给出应用于未来电子商务中的整体网络安全解决方案。

二、基于规则和状态的核心技术

2.1　连接跟踪和状态检测

网络状态检测技术普遍被认为是新一代防火墙的核心技术。与传统的包过滤技术类似，状态检测对新建的应用连接，检查预先设置的安全规则，允许符合规则的连接通过，并在内存中记录下该连接的相关信息，生成状态检测表。对该连接的后续数据包，只要符合状态表，就可以通过。这种方式的好处在于：由于不需要对每个数据包进行规则检查，而是一个连接的后续数据包(通常是大量的数据包)通过哈稀算法，直接进行状态检查，从而使得性能得到了较大提高；而且，由于状态表是动态的，因而可以有选择地、动态地开通1024号以上的端口，使得安全性得到进一步的提高。此外，部分状态检测型防火墙还支持多种用户认证方式，提供了应用级的安全认证手段，增加了某些应用的代理功能，使得安全控制粒度更为细致。

状态检测一般以连接跟踪为其技术基础，对所有经过防火墙的流量都进行跟踪，对所有经过的 IP 包 的各协议层进行分析，对于 TCP 层进行状态机分析，对 UDP 建立虚拟的连接，对其建立方向的概念。同时对 ICMP 包进行分析，决定其与已有的 TCP 或 UDP 连接之间的关系。同时，根据系统配置，来决定对上层应用的分析，比如对 FTP，HTTP 的分析。而状态检测是存取控制、入侵探测以及网络地址转换的基础。

我们在实现状态检测时也以连接跟踪为基础，对网络流量进行监视，以达到实时反应。连接是指具有一定方向的数据流量，会话被定义为往返于固定源和目的地址间的数据流的集合，连接控制块和会话控制块是最基本的数据结构。连接跟踪一般工作在链路层和 IP 层之间，其效率与整个防火墙的效率密切相关。是防火墙的瓶颈之一。而如何组织连接控制块和会话控制块十分关键。面向连接的哈希组织为每一个方向有一个连接控制块，所有的连接控制块通过哈希表组织起来，同一个会话的每一个方向的连接控制块通过连接指针指向会话控制块。其查询效率为：假设系统最多能有 N 个会话，每一个会话有3个方向的连接(原始方向，应答方向，相关方向)，则哈希表中有3 * N 个项。当每收到一个包时，通过包中的内容去查找相应的控制块。假设每一次包中的选择器与哈希表项比较所需的时间是 t，则最坏情况下查询所需时间为(3 * N * t/2)。面向会话的哈希组织则把会话控制块通过哈希表组织起来，但是，连接控制块在堆中是随机的存放，它们之间通过指针连接。其效率分析为假设每次得到一个包后计算该包是否属于该连接所需的时间平均约为 t_0，则最坏情况下查询所需时间是 (t_0 * N/2)。但由于连接跟踪是状态检测与地址转换以及其他功能的基础，因此在计算一个包是否属于一个连接时所需的时间 t_0要大于 t，经过我们的分析发现，在有 NAT 和状态检测功能时，t_0远大于 t。所以，我们选择了面向连接的组织方式。

2.2　包分类

*)国家重点基础研究发展规划资助项目(G1999035810)、国家自然科学基金资助项目(60083007)。黄登玺　硕士研究生。卿斯汉　研究员，博士生导师，中科院信息安全中心主任。蒙　杨　博士，信息安全中心防火墙开发组组长。

防火墙的各项控制策略大多是一个个规则集合，通过对数据包和规则的匹配来决定如何处理此包，大量的规则匹配导致策略查询成为防火墙的主要瓶颈，所以寻找最佳的策略查询算法成为关键。防火墙的策略匹配实际上就是包分类，其常用的算法为 PATRIE 搜索，这是 BSD 的 NET/3中使用的一个算法。其中，PATRIE 结构是一个将2进制 TRIE 结构中只有一个分枝的节点移走而形成的一个结构。它由内部节点和叶子节点组成，内部节点含一比特测试位，其中有些节点包含掩码列表。叶子则对应一个路由项及相应的掩码。其查询过程是一个向下与回溯的重复，向下指从根开始，测试内部节点测试位，如果该位开，则向下搜索其右子树。如果相应位关，则搜索其左子树。如果到达叶子，则判断是否是所需要的路由，如果不是，则进入回溯。回溯则进入叶子节点的父节点，如果该节点的掩码列表非空，则以该节点为根节点，计算新的查询键值，在此树中按上述算法继续搜索。否则，继续回溯，直到缺省节点。

防火墙的规则匹配主要依据数据包的几个字段：源 ip 地址，目的 ip 地址，协议号，协议相关字段，用 src，dst，pro，propart 来表示。我们在实现的过程中，采用2维的 PATRIE 结构来存储 dst 和 src，其他的部分用线性表表示，即把 dst 用一个 PATRIE 表示，把每一个 dst 对应的 src 用一个 PATRIE 结构表示。如图1所示，根为 DH0的 dst 树包含目的地址 D1、D2、D3和缺省节点。而目的节点 D1对应根节点为 SH0的 PATRIE 结构，该 PATRIE 结构包含源地址节点 S1、S2以及缺省节点。同样，目的节点 D2对应根为 SH1的 PATRIE 结构。同样缺省节点对应根为 DH0的 PATRIE 结构。查询时在找到(源，目的)对应的节点后，从线性表中根据其他部分来进行匹配，最后根据匹配结果找到相应的规则数据结构块。

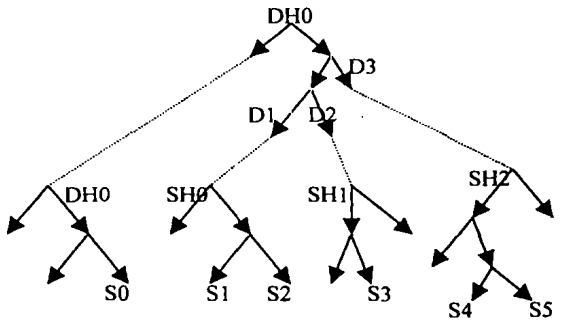

图1

2.3 NAT 及其相关技术

网络地址转换(NAT)是防火墙的一个重要功能，它能够将内部地址转换为外部地址，使仅具备内部地址的计算机通过少量的外部地址访问外部网络，缓解了 IP 地址紧缺的问题。同样外部网络访问防火墙拥有的某一外部地址时，防火墙能将其转发到该地址映射的内部地址的计算机上。网络地址转换技术已成熟，但是由网络地址转换发展而来的技术，如负载平衡、地址伪装以及透明代理，成为大家关注的热点。

2.4 审计

防火墙的审计系统就是对系统中有关安全的活动进行记录、检查及审核。它的主要目的就是检测和阻止非法用户对防火墙所保护的服务以及防火墙本身的入侵，并显示合法用户的误操作。审计是安全系统的重要组成部分，在美国国防部的 TCSEC(Trusted Computer System Evaluation Criteria)中要求 C2级以上的安全操作系统必须包含审计功能，在计算机信息系统安全保护等级划分准则(GB 17859-1999)中也有相应的要求。

审计点是审计程序的入口，也是审计信息的收集点。内核中的审计通常是在系统调用的入口处增加审计点，尽管这样实现起来简洁统一，但是我们的防火墙审计系统不同于操作系统的审计系统，我们只关心部分的系统调用，所以我们没有采用在入口处增加审计点，而是在系统调用内部，对于特权命令，在特权命令的相关系统调用的内部增加审计点。审计事件是系统审计用户动作的最基本单位，根据其性质的不同，可分为基本事件、系统运行状态警告与错误事件、报警事件、开发人员相关事件几类。对于各审计事件，我们采用面向策略的方法，每个策略有自己的待审计事件集，称为策略事件标准，一旦其行为落入待审计事件集，系统就会将事件信息记录下来，另外每个系统都需审计的公共部分称为基本事件集，它由审计管理和系统安全的要求设定。基本事件集和策略事件集作并集运算，结果才是真实的审计事件标准。其中在基本事件集中有部分安全相关事件与系统安全性关系非常大，任何时候都不应免于审计，被称为固定事件集。为了保障安全，固定审计事件是不可更改的，管理员不能改变它，除非修改审计子系统。

符合审计策略的事件以文件形式被记录下来，审计数据可能会增长得很快，为防止空间的增长破坏整个文件系统，必须限制审计文件占用的文件系统空间。审计管理员事先申明为文件系统预留的空间(如10%)，在写磁盘时检查文件系统超级块中指示的可用空间，若低于预留值，则视为异常情况，需要紧急处理。另外审计系统自身的安全性也至关重要，审计的代码和进程，及包括系统和用户审计标准、审计系统的运行参数、审计事件的定义的配置文件应采取存取控制，确保只有审计管理员才能使用。另外，系统应能够监督审计管理员，防止其权力过大可以为所欲为。防火墙操作系统中引入了角色分配机制，使特权分离，从而限制审计管理员的权力。一个可行的方案是，增加一个系统安全管理员角色，赋予他开审计特权，而审计管理员只拥有关审计特权，这样，即使审计管理员可以随时关闭审计，却无法再次打开审计，而且他的关审计动作也在审计文件中被记录。当然，也可以分配多个审计员角色，达到相互制约。

三、基于加密和认证的核心技术

3.1 密钥管理

数据加密作为安全的最终解决方法，在防火墙系统中也得到广泛应用，而密钥管理是其中的关键部分。常用的密钥管理模型有：公钥模型，协议双方拥有对方的公共密钥，其目的是在即使没有共享密钥的基础上建立双方的共享密钥。协议的安全性取决于对公钥的认证，而认证本身取决于基于第三方的公钥证书的存在。这是最灵活、最易扩展的模型。密钥分发中心，该模型是一种容易建立的且被广泛采用的一种模型，这种模型通过 KERBEROS 协议而流行起来。人工密钥分发，该模型是最原始的一种密钥分发手段，但它仍是许多系统中安装初始密钥的基本方法。而在防火墙中，密钥管理分为两部分内容，一是防火墙的各分布式部件之间的通讯的密钥管理，另外则是加密网关间的密钥管理(如 IPSEC 中的 IKE)。

在防火墙系统实现中，密钥管理主要保证防火墙的各部件之间的数据通讯的安全，我们构造了适合防火墙的密钥管理协议，而加密网关间的密钥管理则在 VPN 技术中介绍。由

于在内部网中缺乏可行的第三方的支持，我们采用密钥分发中心与人工密钥分发相结合的模型。考虑到通讯双方的会话维持从理论上讲是无限的，对于每一个会话密钥，我们应规定一定的生存周期，以防止给密钥分析提供足够的信息量。系统中我们采用时间生命周期与使用生命周期相结合的办法以自动的方式提供更新。另外为了保证算法的可替换性，我们要求协议中协议描述与算法之间的相互分离，而在我们的协议实现中，消息是由消息头和消息实体构成，消息实体包含不同的荷载类型，并用下一荷载类别来标识。

密钥管理协议的过程如图2所示，其具体描述为假设 $k_{a,b}$ 为 a，b 间的预共享密钥，防火墙部件 F 通过 $k_{f,KDC}$ 向密钥管理中心(KDC)用发送 Cookie(过程1)，KDC 验证其正确性，若通过，则产生 F，C 的共享密钥 $K_{f,c}$ 分别用 $k_{f,KDC}$ $k_{c,KDC}$ 发送给 F，C(过程2)。F，C 则通过 $K_{f,c}$ 进行验证和产生后续会话密钥(过程3，4，5)。

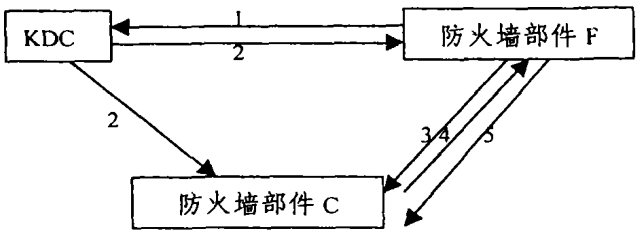

图2

3.2 认证

认证是防火墙安全的第一道门槛，我们采用体制与协议分离的技术，可以根据需要提供不同的认证协议。在这里，认证体制指认证实现的体制，是一工程实现的概念。认证过程的流程一般为：系统开始工作时，首先调用认证客户端，该过程可以也可以不通过防火墙访问认证服务器。同时，防火墙不应拒绝客户端通过它访问认证服务器。认证服务器告诉防火墙其认证结果，然后客户端通过防火墙访问内部网的服务。我们系统已支持的认证协议有 S/KEY、FWN1，其中 S/key 是典型的一次一密的认证协议。口令为一个单向的前后相关的序列，系统只用记录第 N 个口令。用户用第 N－1个口令登录时，系统用单向算法算出第 N 个口令与自己保存的第 N 个口令匹配，以判断用户的合法性。由于 N 是有限的，用户登录 N 次后必须重新初始化口令序列。

由于我们采用认证体制与认证协议分离的体制，同时采用认证模块与防火墙的其他功能模块之间的独立设计，因此我们必须有防火墙的认证通讯协议，来完成认证部件与防火墙其他部件之间的通讯，并在其基础上实现一次性认证技术。

因为只有认证服务器是面向不可信网络的，所以要考虑认证服务器的安全性。对于拒绝服务攻击，对处于悬挂状态的连接进行限制，在我们的系统里，采用的阈值为20，也就是说，当悬挂值超过20时，系统不再接受后续的认证请求。但这种做法易造成拒绝服务攻击。而由于我们采用的认证协议本身防止重放攻击，而通讯协议采用 nonce 技术，因此重放攻击不再有效。

3.3 VPN 技术

虚拟专用网(VPN)是一种保护信息数据通过公网安全传输的技术，它运行在广域网上，而不必建立昂贵的专线网，对各个站点，网络之间的连接进行透明加密。通过 VPN 可以将分布在各地的结点安全连接起来，保证数据的完整性、可靠性、可信任性。

VPN 技术的协议基础是 IPSec 协议，IPSec 从网络层提供加密和认证的安全保障，屏蔽了上层应用协议的多样性和下层链路的差异，使得安全机制通用、透明，而且网络层安全具有较大的灵活性，可配置成端到端、路径到路径、网络到网络或端到网络等各种形式。安全关联(SA)是构成 IPSec 的基础，它是发送者和接受者之间协商的一种安全协定，它决定了用来保护数据包安全的转码方式，密钥和密钥的有效存在时间等，同时它是一单向的关系。如果进行双向的 IP 端对端安全服务，就必须有两个安全关联。每一个安全关联只为单向单独提供服务。IPSec 协议有两种方式(AH 和 ESP)来保护一个完整的 IP 载荷，其中 AH 用于提供数据源鉴别、无连接的数据完整性以及数据的防重传保护；而 ESP 用于提供信息保密、有限的流量保密以及可选的数据源鉴别、无连接的数据完整性和数据的防重传保护。而这两种保护是由 IPSec 的两种模式提供的，其中传输模式用来保护上层协议，而通道模式用来保护整个 IP 数据包。在传输模式中，IP 头与上层协议头之间需插入一个特殊的 IPSec 头，而通道模式中，要保护的整个 IP 包都需封装到另一个 IP 数据包中，同时在外部和内部 IP 头之间插入一个 IPSec 头。

IPSec 的主要功能是在网络层对数据包提供加密和认证等安全的网络层服务，除了核心层的加密和认证处理等模块外，最重要的就是应用层的密钥管理 IKE 模块。IKE 也采用了安全关联的概念，用它定义如何对一个特定的 IP 数据包进行处理。IKE 使用了两个阶段的 ISAKMP，第一阶段建立 IKE 安全关联，第二阶段利用这个既定的安全关联，为 IPSec 协商具体的安全关联。在阶段1，可选择两种交换方式(主模式，野蛮方式)，主模式将 SA 的建立和对端身份的鉴别以及密钥协商结合起来，这种连接的好处在于能够抵抗中间人攻击。野蛮方式使得协商更加快捷，但抵抗攻击的能力较差，也不能提供身份保护，所以我们只实现了主模式交换。在阶段2仅提供了一种交换方式，即快速模式，它在特定的 IKE SA 的保护下，协商拟定 IPSec SA。

IPSEC 的实现方式有两种，一是将 IPSEC 集成到操作系统的协议栈处理中，这种方式需要访问 IP 的源码，适用于主机和安全网关的场合，二是协议栈肿块法实现，在 TCP/IP 协议栈的网络层和网络接口驱动程序之间实现、该方式无需访问 IP 的源码，通常只适用于主机场合。由于我们采用具有自主产权的安全操作系统，因此采用 IPSec 的第一种实现方式，通过修改内核中的 TCP/IP 协议源码而实现。这种将 IPSec 集成到 IP 源码中的实现提高了网络处理的效率，直接利用 IP 模块的分片与重组、路由选择功能，避免相同功能的重复实现。同时可以利用防火墙中的其他安全功能，提高了 VPN 的安全性和工作效率。另外通过修改 TCP/IP 的协议实体来实现 VPN 将是系统更容易控制对 ICMP 报文的处理，因为在协议栈肿块实现在网关应用场合会丢弃许多发往主机的 ICMP 报文。

四、高安全等级防火墙的实现

4.1 安全操作系统

上面我们从各项技术的实现角度，给出了我们防火墙设计的考虑。在给出我们防火墙的总体设计前，我们先介绍其操作系统基础，即我们自主开发的安全操作系统。该系统的安全级达到 B1级，同时满足在系统设计中进程调度和文件系统是

为网络服务的，并考虑到网络安全部分，如设计安全的 Socket，listen 等函数，且系统的新增功能不影响系统的网络性能。下面就防火墙在设计时利用安全操作系统的功能和机制方面做一描述。

强制存取控制(MAC)机制，系统中的信息分密级和类进行管理，它对系统中的每个进程、每个文件、每个 IPC 客体赋予相应的安全级，当一进程访问一个客体时，根据进程的安全标识和访问方式，比较进程的安全级和文件的安全级，从而确定是否允许进程对文件的访问。另外根据 TCSEC 的规定，B1 以上级安全操作系统将系统信息划分三个区，即系统管理区，用户空间区，病毒保护区。它们通过 MAC 机制的控制被分隔，来保持系统的安全性，系统管理区不能被用户读和写。用户空间区包含用户的数据和应用，用户可以进行读和写。病毒保护区包含不能被用户区的进程写的数据、文件，但可被用户区的进程读。而防火墙中的关键数据有安全策略数据、系统用户数据、审计数据、记账数据，由于病毒保护区所具有的特点，把关键数据放在该区，利用域间的隔离机制实现数据保护。

最小特权管理，其思想是将超级用户的特权划分为一组细粒度的特权，分别授给不同的系统操作员/管理员，使各种系统管理员/操作员只具有完成其任务所需的特权，从而满足最小特权原理。我们知道，攻击防火墙的技术之一便是修改防火墙的规则使得防火墙的规则对其攻击无效，而要修改规则，则修改者须有一定的特权即可。在实际的安全操作系统设计中，普通用户和特权用户的操作在特权判断之前是一样的，但是到了特权判断时，普通用户的操作请求被拒绝。同时，根据防火墙操作系统的特点，将系统的对防火墙的本机管理的特权赋予安全管理员。这样，经过权限分割，系统的安全性大大的提高。我们给该管理员一定的安全级别，同时该防火墙的相关关键数据目录文件也具有该安全级。

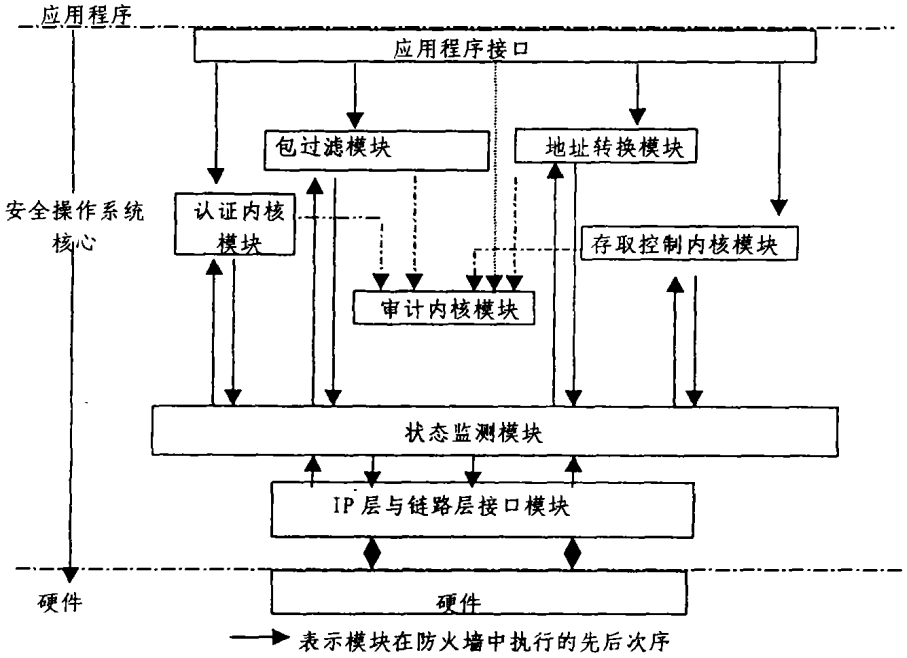

图3

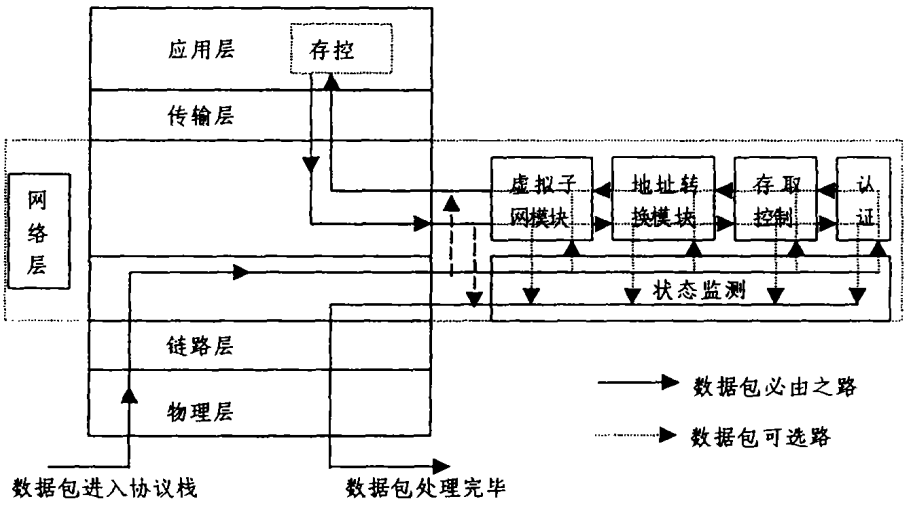

图4

4.2 策略管理

安全策略一般指根据具体的安全需求，对数据所进行的处理方法。我们的防火墙由多个功能模块构成，每个模块都有

(下转封四)

(上接第 84 页)

自己的安全策略,为了统一管理,防止策略之间的相互冲突,我们采用中心策略管理模块,所有的功能策略在增加、删除时受制于中心策略管理。

在策略管理时,必须考虑策略之间的各种关系。主要包括功能模块内部的策略关系和功能模块之间的策略关系。此处主要考虑功能模块之间互斥关系和先后关系。在我们的系统中,所有的策略除地址转换与加密(VPN)之外不存在互斥关系,而加密具有最低的优先级,过滤具有最高的优先级。

4.3 体系结构

我们的防火墙提供了认证功能、存取控制功能、密钥管理功能、快速的包分类功能、虚拟子网功能、状态检测功能、地址转换功能和系统审计与纪录功能,各功能模块间的组织框架结构如图 3 所示。

另外各模块在协议栈中出现的位置如图 4 所示,从中看出,我们的防火墙系列模块中状态监测模块是必需的,数据包是否经过其他模块的处理关键看策略的要求,同时,数据包可能不经过任何其他处理模块,大多模块是并行存在。

4.4 性能评测

在本地的实验环境中,我们给出各功能策略在单独运行下的性能测试数据,可看出系统功能还是不错的。

过滤规则条数	0	50	100	200	400	500	600
吞吐率(M/s)	93.6	93.1	92.0	91.7	90.3	87.5	86.1

认证规则条数	0	20	40	60	80	100	120
吞吐率(M/s)	93.6	92.7	91.4	90.3	84.5	83.3	82.1

目的地址转换	0	20	40	60	80	100	120
吞吐率(M/s)	93.6	92.7	91.4	90.3	84.5	83.3	81.2

VPN(AH)	0	20	40	60	80	100	120
吞吐率(M/s)	93.6	83.7	76.5	73.5	70.5	68.5	65.5

VPN(ESP)	0	20	40	60	80	100	120
吞吐率(M/s)	93.6	81.6	76.4	70.3	65.5	65.4	60.4

结束语 本文从设计一个高安全等级防火墙的角度出发,对当前重要的防火墙核心技术进行了研究和实现考虑,并对防火墙所依赖的高安全级操作系统作了介绍。我们的防火墙对各协议和策略的实现时,考虑了其间的相互关系,并注意了各模块间的独立性和可扩展性。能够根据应用环境的需求动态管理支持协议与服务。另外从实测数据中也可以看出,防火墙在安全与性能间作出了合理的折中,达到了我们的预计要求。

参 考 文 献

1 Cheswick B. The Design of a Secure Internet Gateway. USENIX proceedings. Available for FTP from research. att. com: /dist/secure-internet-gateway. ps

2 Guttman J D. Filtering postures: Local enforcement for global policies. In: Proc. IEEE Symp. on Security and Privacy, Oakland, CA, 1997

3 Rubin A, Geer D, Ranum M. Web Security Sourcebook. Wiley Computer Publishing

4 http://WWW. checkpoint. com/techsupport

5 van Rooij G. Real Stateful TCP Packet Filtering in IP filter. In: 2nd Intl. SANE Conf. March 2000

6 Lopatic T, McDonald J, Song D. A Stateful Inspection of Firewall-1. Black Hat Briefings 2000

7 Andersson A, Nilsson S. Faster searching in tries and quadtrees - analysis of level compression. In: Proc. of the Second Annual European Symposium on Algorithms, LNCS 855, 1994. 82～93

8 Andersson A, Nilsson S. Improved behaviour of tries by adaptive branching. Information Proceeding Letters, 1993, 46(6): 295～300

9 Gupta, Lin, McKeown. Routing lookups in hardware at memory access speeds. In: Proc. of IEEE INFOCOM, April 1998

10 Egevang K, Francis P. The IP Network Address Translator. RFC 1631, May 1994

11 Srisuresh P, Holdrege M, NAT Terminology and Considerations. RFC 2663, Aug. 1999

12 Carpenter B. Internet Transparency. RFC 2775, Feb. 2000

13 Krawcyzk, Hugo. SKEME: A Versatile Secure Key Exchange Mechanism for Internet, ISOC Secure Networks and Distributed Systems Symposium, San Diego, 1996

14 Diffie, Oorschot P C V, Wiener M J. Authentication and Authenticated Key Exchanges. in Designs, Codes and Cryptography, Kluwer Academic Publishers, 1992. 107

15 Kent S. Security Architecture for the Internet Protocol, RFC2401

16 Kent S. IP Authentication Header, RFC2402

17 Harkins. The Internet Key Exchange, RFC2409

18 Kent S. Security Architecture for the Internet Protocol, RFC2403

计算机科学

(1974 年 1 月创刊)
第 29 卷第 10 期 (月刊)
2002 年 10 月 25 日出版

中国标准刊号: ISSN 1002-137X / CN50—1075/TP

定价: 18.00 元 国外定价: 5 美元
邮发代号: 78—68
发行范围: 国内外公开

主管单位: 国家科学技术部
主办单位: 国家科技部西南信息中心
编辑出版: 《计算机科学》杂志社
重庆市渝中区胜利路 132 号 邮政编码: 400013
电话: (023) 63500828 E-mail: jsjkx@swic.ac.cn
社 长: 牟炳林
主 编: 朱宗元
印 刷 者: 重庆科情印务有限公司
总发行处: 重庆市邮政局
订 购 处: 全国各地邮政局
国外总发行: 中国国际图书贸易总公司 (北京399信箱)
国外代号: 6210—MO