第 3 章　网络防火墙功能与结构解析

Internet 的出现给人们带来了全新的资源和信息共享方式，Internet 的快速发展和广泛应用给人们生活、工作，甚至整个社会的经济发展都带来了深远的影响。可以说 Internet 在很大程度上日益改变着人们的生活方式，甚至在改变整个社会的经济活动模式。例如，以此为基础发展出的电子商务，不仅改变数以亿计人们的购物方式和消费习惯，也对一些传统的经济实体（如各种实体商店、百货公司等）带来了极大的冲击。

另一方面，Internet 的网络互联也给网络黑客及其他网络攻击者远程攻击和控制目标网络与计算机系统提供了前提和基础。各种各样的机密信息窃取、信息篡改等网络安全事件层出不穷，网络和计算机系统的安全性面临着严峻的威胁。

为了应对信息安全威胁，多层次的信息安全技术以及相应的系统应运而生，如实现网络连接控制的防火墙系统，实现入侵发现的入侵检测系统，攻击响应及恢复系统等。网络防火墙对远程的网络访问进行检查和控制，是实现网络信息安全的第一道防线，也是目前最常用的信息安全技术，其相应的开发技术一直受到人们的重视。

3.1　网络防火墙的基本概念

Internet 的迅速发展，提供了发布信息和检索信息的场所，但也带来了信息失窃和数据破坏的危险。人们为了保护其数据和资源的安全，设计出了网络防火墙。防火墙原是建筑物大厦中采用的消防设施，以防止火灾从大厦的一部分扩散到另一部分。理论上网络防火墙的功能也属于类似目的，一般部署在内部网络接入 Internet 的出口处。网络防火墙作为要塞点、控制点能显著提高一个内部网络的安全性，通过对网间所传递的数据进行分析和控制，只有被认定为正常的网络协议数据才能通过防火墙，这样可防止 Internet 上的危险传播到网络内部，也能防止内部网络的数据被来自 Internet 的恶意用户窃取。

除了对内外网间的网络访问进行分析控制外，一般网络防火墙还具有审计功能，即对经过网络防火墙的所有网络访问作出日志记录，同时也能提供网络使用情况的统计数据。当发生可疑操作时，网络防火墙能进行适当的报警，并提供网络是否受到攻击的详细信息。

除具有网络访问控制和审计功能外，目前的网络防火墙产品还支持虚拟专用网（Virtual Private Network，VPN）功能，网络防火墙利用 VPN 功能可以创建安全连接，网络用户可以借助于该安全连接进行数据的安全传输，以保证数据在传输过程中不被偷听和篡改。

3.2　防火墙的网络访问控制功能

网络防火墙作为目前最为流行的网络安全技术，无论在学术界还是信息安全业界，其相关的研究、开发都受到广泛的关注和重视，各种新功能，如网络地址转换（Network Address

Translation,NAT)等,相继被开发并集成到相应的网络防火墙产品中。

尽管如此,网络访问的管理和控制功能仍然是网络防火墙最核心的基本功能。一方面,目前很多网络安全问题都是由不合理的网络连接或网络数据包传递引起的,任何对内部网络发起的攻击最终都要体现为恶意的网络连接和数据传递,因此阻断不必要的网络连接和网络数据包传递能够使内部网络躲避绝大多数的网络攻击。另一方面,网络防火墙的其他安全功能大多都要建立在对网络访问的管理和控制基础上。如果没有对网络访问的管理和控制,恶意的网络连接和网络数据包传递就可以任意通行,网络防火墙就失去了对网络最基本的安全保护能力,这时网络防火墙的其他安全功能就完全发挥不了作用。下文将网络连接以及网络数据包传递统称为网络访问,将对网络访问的管理和控制简称为网络访问控制。

网络防火墙要实现理想的网络访问控制功能,关键是如何甄别出哪些网络访问是正当的,应该让其通过的,而哪些网络访问是恶意的或者不正当的,应该阻断的。通常正常的网络连接或网络数据包不会在自身附上正当访问的标签,相反地,恶意的网络连接和数据包为了不被网络防火墙阻断,反而会尽可能地在形式或外表上将自己伪装成合法的网络连接或网络数据包。

甄别网络访问是否正当的过程实际上就是访问控制的决策过程,网络防火墙要完成该过程主要涉及到三个方面,即访问控制规则的设计、访问控制决策的形成以及访问控制决策的实施。①访问控制规则设计部分的功能体现为要按照什么规则和逻辑来判定网络访问是正当的、应该放行的,还是不正当的、应该阻断的,如根据网络数据包的源地址是否在指定的合法 IP 地址列表中来判定一个 IP 数据包是否放行,这就是一个常见的网络防火墙的访问控制规则;②访问控制决策形成部分的功能是对一个特定的网络访问,根据相应的访问控制规则,给出应该放行还是阻断该网络访问的判决或决策;③访问控制决策实施部分的功能是依据所形成的访问控制判决结果,对一个特定的网络访问进行控制,即放行或阻断该网络访问。

本书在讨论网络防火墙的实现技术中,重点关注如何实现网络防火墙的网络访问控制功能,对于网络防火墙的其他功能(如日志、VPN 等)不做具体的阐述。

3.3 访问控制功能的实现要素

综合上面的分析可知,网络防火墙要完成一个完整的网络访问控制功能,具体需要三个基本功能要素:访问控制规则的配置,基于访问控制规则的访问判决,访问判决的实施。下面的三个小节分别讨论这三个部分。

3.3.1 访问控制规则的配置

通常,网络防火墙不能完全智能地甄别出不当的或恶意的网络访问,并自动实现相应的网络访问阻断,毕竟防火墙所处的网络环境是多种多样的,甚至网络应用也处在动态变化之中。目前大多数网络防火墙都是依据网络管理员配置(或制定)好的规则进行网络访问控制,访问控制规则的制定是网络防火墙实现网络访问控制的前提和基础。因此在网络防火墙的实际应用中,访问控制规则的配置尤为重要。针对所在的网络应用环境,制定合适的网

络访问控制规则是网络防火墙对内部网络切实发挥安全保护作用的关键所在。

对具体的网络防火墙而言，为其配置合适的访问控制规则涉及到几个方面的现实问题。一是规则配置平台，即网络防火墙提供了什么样的方法来配置控制策略。二是访问控制规则的具体存在和表示形式，如控制规则中支持哪些控制要素以及运算逻辑等。另外安全管理员的作用也同样重要，安全管理员要配置出合适的安全规则还会涉及到很多因素，如安全管理员自身的安全素养，安全管理员对网络应用的熟悉程度，安全管理员对规则配置平台的理解程度等。安全管理员如果不能为网络防火墙配置出合适的访问控制规则，如默认放行所有的网络访问，网络防火墙就不能真正发挥作用。实际上，这些问题可归结为网络防火墙的管理和使用问题，本书从网络防火墙的开发角度出发，更关注如何实现或提供一个好的规则配置平台，以及如何组织访问控制规则。

对访问控制规则配置平台而言，良好的配置方式和界面非常重要，尤其是商用的网络防火墙。一个好的配置界面不但有利于系统被用户接受，而且还便于用户培训，节省培训费用等。但就其功能而言，访问控制规则配置平台的核心体现在能够配置出什么样的访问控制规则。网络防火墙所配置出的访问控制规则类似于一个运算结果为布尔值的函数，该类函数的关键特征体现在两个方面，一是其中所包含的数据种类，即所支持的数据类型、常量、变量等，二是对应所能支持数据种类的运算类型，如算术运算、逻辑运算等。相应地，网络防火墙规则配置平台的本质特征在于所支持的参量类型，即可以基于哪些要素来配置网络访问控制规则，以及所支持要素上的运算类型。通常运算类型依赖于所支持的参量，当规则配置支持的参量类型确定之后，其上所能进行的运算类型也就相应地确定下来，因此这里重点讨论防火墙规则配置所支持的参量类型。

网络防火墙的访问控制规则包含的元素可能会涉及到较多的数据类型，但从来源看，访问控制规则所依赖的要素可分为三类：网络访问参量、系统状态参量、自定义参量。目前大多数的网络防火墙都是在这三类参量上配置访问控制规则。

- 网络访问参量：不管是网络连接还是网络数据包传递，一个网络访问总会伴随着一定的上下文信息或者网络访问属性，如数据包的源 IP 地址、数据包的源端口、数据包的目标 IP 地址等，这些信息统称为网络访问参量。
- 系统状态参量：除了该次网络访问的属性外，有些网络防火墙的访问控制规则还涉及到一些全局性的系统状态变量，如系统时间等。商业化的防火墙多数都能配置出时间相关的网络访问控制规则，如工作日的 9:00～17:00 才能进行网络访问等。
- 自定义参量：这些参量通常体现为由安全管理员自己定义的一些常量，这些常量的值在规则配置阶段就已确定下来，如特定的网络 IP 地址段、合法的 URL 列表、URL 黑名单列表等。这些自定义参量对应了安全管理员的先验知识，安全管理员在配置网络访问控制规则时需要具备这些知识。

通常安全管理员在为网络防火墙配置访问控制规则时，配置出的可能不是单个规则，而是多条规则组成的规则集合，这些规则一般适用于不同场合下的网络访问。对于适用于相同场合的多条网络访问控制规则，网络防火墙应该包含规则冲突解决方案，即在对同一网络访问进行访问判决过程中，如出现有超过一条的访问控制规则适用于该访问，并且这些访问控制规则的判决结果不一致，这时应该以哪条判决结果对该网络访问进行控制。

3.3.2 基于访问控制规则的访问判决

网络访问控制规则给出了网络访问是否能够得到许可的静态约束和描述，即在什么条件下能够进行网络访问，什么条件下不能进行网络访问。而对一个特定的网络访问，需要根据其访问属性执行相应的访问控制规则，才能得出具体的访问判决结果。在网络防火墙中，基于控制规则的访问判决大致包含以下三个过程：

(1) 控制规则选取阶段。如果网络防火墙有多条访问控制规则，对一个特定的网络访问，需要找出对应本网络访问的(一条或几条)访问控制规则，然后解释或执行相应的访问控制规则以形成访问判决。一般情况下，在为一个网络访问选取相应的控制规则时，需要预先知道该网络访问的一些访问属性。假定防火墙中存在两条访问控制规则，分别用于 TCP 应用和 UDP 应用，因此只有明确该网络访问对应的具体业务类型(TCP 或 UDP)后，才可能为该网络访问找到合适的访问控制规则。如果网络防火墙只有一条访问控制规则，也就无所谓规则选取，在生成访问判决时会略过这个阶段。

(2) 单规则判决阶段。在为指定网络访问找到合适的控制规则后，解释或执行该控制规则，就能够得到关于该网络访问的判决结果。如果找到多条合适的控制规则，可能需要逐一解释或执行这些控制规则。

在控制规则的解释或执行过程中，如何获得该规则中所有的参量(或参量的取值)是最为核心的问题。在 3.3.1 节中提到的三种参量中，自定义参量的值如果包含在访问控制规则中，在解释或执行访问控制规则时不存在获得其参量值的问题，如果是保存在防火墙的配置文件中，只要读取相应的配置文件就能获得这些参量的值。

对于全局状态参量，通过访问全局数据结构或者状态查询函数，就能获得其参量的值，如调用操作系统的函数 gettimeofday()获得系统时间，用于解释什么时间段能够访问、什么时间段不能访问这样的访问控制规则。

对网络访问参量值的获取相对比较复杂，有些访问属性值可以从网络访问中直接得到，例如，从 IP 数据包中可以直接获得源 IP 地址，而有些访问属性值需要经过分析才能得到；从 IP 数据包中不能直接得到所对应的网络应用服务类型；是 FTP 应用还是 EMAIL 应用，网络应用服务类型可能需要将多个 IP 报文拼装分析后才能获得。

(3) 冲突判决仲裁阶段。对某网络访问，当有两条或两条以上访问控制规则的判决结果发生冲突时，需要对这些判决结果进行仲裁，以获得最终的判决结果。实际的网络防火墙可能会采用不同的方案来解决多条访问控制规则的判决冲突问题。多数防火墙采用“否定优先”的方式，即对一个网络访问的所有判决结果中，只要有一个是阻断的，防火墙就会阻断该网络访问。极少有防火墙采用“肯定优先”的方式来裁决不一致的判决。

3.3.3 网络访问判决的实施

在获得最终判决结果后，网络防火墙就能够对某网络访问进行管理和控制，即放行或阻断该网络访问。不难理解，要对一个网络访问进行控制，首先需要在机制上保证网络防火墙能够截获到该网络访问，如截获一个 TCP 连接或者一个 IP 数据包等。也就是网络防火墙必须运行在网络访问所经的结点(路由结点或某协议层次)上，或者至少有一个模块运行在相应的结点上，且该模块能够影响到该结点上的网络访问处理流程。如某防火墙要控制进

出一个局域网的 IP 数据包，该防火墙至少需要有模块运行在该局域网的网关（或路由器）上，且该模块能够根据访问判决结果，控制该网关是转发 IP 数据包还是阻断 IP 数据包。

显然在网络防火墙的实现中，网络访问判决的实施是一个非常关键的技术，直接决定了网络防火墙的实现方式和应用部署方式，3.5 节将结合具体的实现方式再进行详细阐述。

3.4　网络防火墙的逻辑结构

根据所实现功能的不同，网络防火墙在逻辑上可以分为三大模块，即访问控制规则配置模块、网络访问截获和控制模块、网络访问判决模块，此外还需一个保存访问控制规则的数据库。一个完整的网络防火墙的逻辑结构如图 3-1 所示。

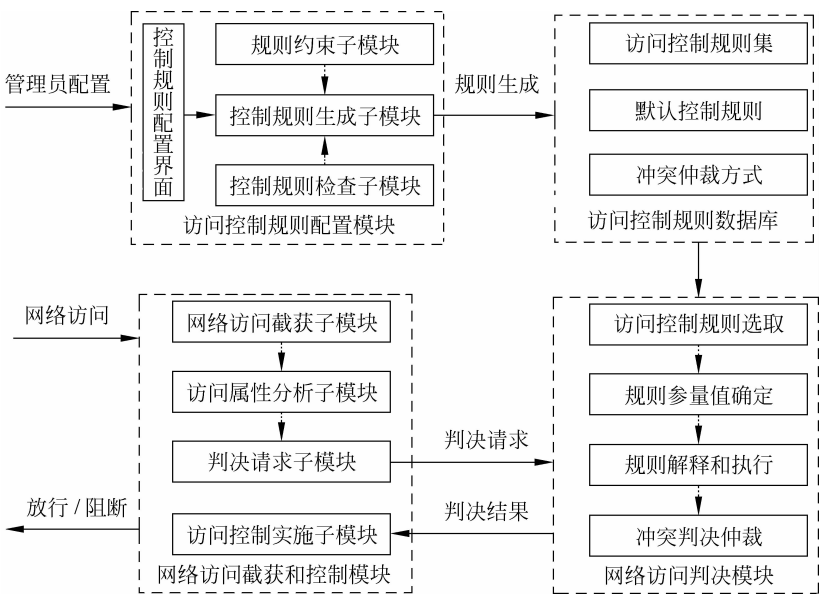

图 3-1　网络防火墙的逻辑结构

3.4.1　访问控制规则配置模块

该模块的主要功能是提供一个接口或者界面，供网络管理员配置相应的访问控制规则，并将配置结果保存在访问控制规则库中。在实现访问控制规则配置模块时，要预先确定访问控制规则所支持的参量种类，以及其上所能进行的运算类型。这些参量种类和运算类型要与后面（3.4.4 节）提到的访问控制规则解释和执行子模块所支持的参量种类和运算类型相一致。网络管理员只能在这些参量种类和运算类型基础上配置安全规则，否则所配置出的访问控制规则不能有效生成真正的访问控制判决。

有些网络防火墙的访问控制规则配置模块还具有附加功能，具体可能包括：访问控制规则的完整性检查，甚至自动添加一些默认规则，如默认禁止访问等；访问控制规则的冲突检查，或者以静态的方式预先消除规则冲突，或者指定规则冲突解决方式，以便于在适用于同一网络访问的多个规则出现判决不一致时形成最终的访问判决结果。

因此该模块从功能逻辑上可以划分为三个部分：规则约束子模块，其功能是约定用户如何配置出相应的访问控制规则，如约定可以配置的参量种类以及相应的运算类型等；控制规则生成子模块，该子模块为整个模块的功能核心，按照用户的配置生成相应的访问控制规则；控制规则检查子模块，即在生成访问控制规则前，对访问控制规则的完整性、一致性等进行检查。

3.4.2 访问控制规则数据库

访问控制规则数据库是联系访问控制规则配置模块和网络访问判决模块之间的纽带，保存访问控制规则配置模块的运行成果，用于网络访问判决模块对指定的网络访问形成相应的访问判决。

访问控制规则数据库中的规则内容和存在形式在不同的网络防火墙系统中差别很大，一个简单的网络防火墙可能只有一两条规则，而一些应用复杂的网络防火墙可能有几十条乃至上百条的规则。一般而言，访问控制规则数据库存储的内容主要包括：由一条条具体的访问控制规则组成的访问控制规则集合；默认的访问控制规则，该规则约定在没有合适的控制规则情况下如何对一个网络访问进行控制；规则冲突仲裁方式，用于在多个控制规则对同一个网络访问出现不同判决时产生最终的判决结果。

3.4.3 网络访问截获和控制模块

该模块的主要功能是截获网络访问，向网络访问判决模块询问如何处理该网络访问，待网络访问判决模块返回判决结果后，依据所得到的判决结果对该网络访问实施访问控制，即放行或者阻断该网络访问。

通常该模块在向访问判决模块询问判决结果时，需要将该网络访问的上下文信息，即各种访问属性，同时提交给访问判决模块，以便于访问判决模块形成对该网络访问的判决。因此该模块在逻辑上可分为四个子模块：访问截获子模块、访问属性分析子模块、判决请求子模块以及访问控制实施子模块。

- 访问截获子模块：该子模块截获网络中正在发生或将要发生的网络访问，包括网络连接、报文传递、应用会话等。开发和应用部署网络防火墙时，要保证所有的网络数据传递或者希望控制的网络数据传递全部经过该子模块，即该子模块不能被旁路，要能截获到所有需要控制的网络数据传递。
- 访问属性分析子模块：在截获网络访问后，需要将该网络访问发生的上下文信息进行收集，如数据包的来源、目的地址等。
- 判决请求子模块：依据分析出的访问属性信息（即访问上下文信息），形成访问判决请求，并将该访问判决请求连同访问属性信息一起发送给网络访问判决模块。
- 访问控制实施子模块：对已截获的网络访问，接收来自于网络访问判决模块的判决结果，并依据该判决结果对该网络访问进行处理，阻断或允许所传递的数据包（或网络连接）等。

3.4.4 网络访问判决模块

该模块的主要功能是针对网络访问截获和控制模块提交来的访问判决请求（附带有相

应的访问上下文信息),依据对应的访问控制规则形成访问判决,并将该判决结果返回给网络访问截获和控制模块。依据 3.3.2 节的讨论,该模块主要包含以下功能流程。

- 控制规则选取:根据待判决的访问控制请求及其访问属性信息,在访问控制规则库中选取适用于该访问的控制规则。对一些网络防火墙而言,可能会选取出多条适用的访问控制规则,也可能没有适用的访问控制规则,通常没有适用的访问控制规则意味着适用默认规则,或者直接生成默认的判决结果。
- 规则参量值提取:访问控制规则类似于一个布尔函数,访问控制规则的执行类似于计算函数的值,计算出函数结果的前提是需要知道函数参数的值。同样在执行选取出的访问控制规则时,需要知道该规则中所有参量的值。这些参量值可通过读取该网络访问伴随的访问属性值,查询全局状态,或者读取规则配置文件(或数据库)等来获得。
- 规则解释与执行:在获得访问控制规则涉及到的参量值后,就可以对该网络访问执行相应的规则解释,以对该网络访问形成访问判决结果。
- 判决结果仲裁:在出现多条访问控制规则的判决结果不一致时,如果管理员设置了不一致判决的仲裁方式,该模块将按此方式仲裁出最终的判决结果,否则需要按默认的方式,即“肯定优先”或“否定优先”等,仲裁出最终的判决结果。

3.5　网络防火墙接入的协议层次

从网络防火墙的逻辑结构不难看出,网络防火墙要在一个网络中实现真正的网络访问控制,需要能够截获针对该网络的网络访问,并且按照判决结果控制该网络访问的放行和阻断。换而言之,网络防火墙中的网络访问截获和控制模块(或者至少其中的一部分)应该嵌入到原有网络的协议处理流程中,这样才能截获到网络访问并获得网络访问的上下文信息,以及影响和改变网络访问的处理流程,从而真正落实网络防火墙的访问判决结果。因此,要实现网络防火墙,需要首先了解原有的网络协议处理流程。

网络访问对应为具体的网络通信,在 TCP/IP 体系结构下,通信双方以客户/服务器的形式存在。目前主要的应用层协议(FTP、HTTP 等)都支持代理模式,代理模式下的网络协议处理流程和一般模式下的网络协议处理流程存在根本性的不同,本节的一般模式是相对于代理模式而言的,即非代理模式。

本节首先用两小节分别介绍 TCP/IP 协议体系下一般模式和代理模式下的协议处理流程,然后讨论如何将防火墙嵌入到原有的网络协议处理流程中,即讨论防火墙的协议嵌入层次。

3.5.1　非代理模式下的协议处理流程

不失一般性,这里假定发出数据包的主机为客户端,接收数据包的主机为网络服务器。图 3-2 首先给出了非代理模式下的网络服务结构,这里假定客户端为局域网 LAN_A 中的 $HostA_i$,服务器为局域网 LAN_B 中的 $HostB_j$。

从客户端发出的代表网络访问的数据包要依次经过下列网络路径:客户机 $HostA_i$,局域网 LAN_A 的网关 GatewayA,Internet 上的各种中间设备(路由器、交换机等),局域网

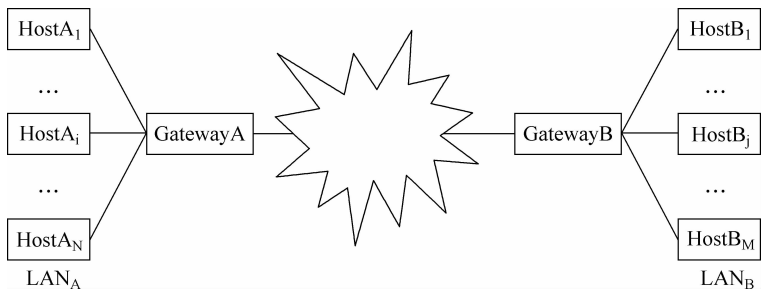

图 3-2 非代理模式下的网络服务结构

LAN_B 的网关 GatewayB，最后到达服务器主机 $HostB_j$。

从协议的处理层次角度来看，网络数据包经过的网络路径结点对应的处理方式存在区别。图 3-3 给出了各网络结点上协议的大概处理流程，这里假定客户端的 IP 地址和端口分别为 m 和 n(记作 m:n)，服务器的 IP 地址和端口分别为 x 和 y(记作 x:y)，各网络结点上的协议处理过程概括如下：

- 在客户端，应用层的数据经过 TCP/IP 协议的逐层处理，将会被封装成源 IP 地址和源端口为 m:n、目标 IP 地址和目标端口为 x:y 的 IP 数据包(记作 m:n->x:y)，然后封装在 MAC 帧中传输到硬件链路上。
- 在网络中间结点(包括局域网网关以及途径的 Internet 上的各种中间设备)，从所收到的 MAC 帧中提取出 IP 数据包，基于该数据包的目标 IP 地址，运行路由算法计算出下一跳的 IP 地址和连接该 IP 地址的网络接口，然后将该 IP 数据包再次封装成 MAC 帧，从相应的网络接口中转发出去。
- 在服务器端，IP 协议层从所收到的 MAC 帧中首先提取出 IP 数据包，根据该数据包的目标 IP 地址判断出该数据包是发往本机的。进行相应处理后，将 IP 包的数据部分交给上层协议，经传输层处理解析出应用层数据，并将这些数据交给应用层进行处理。

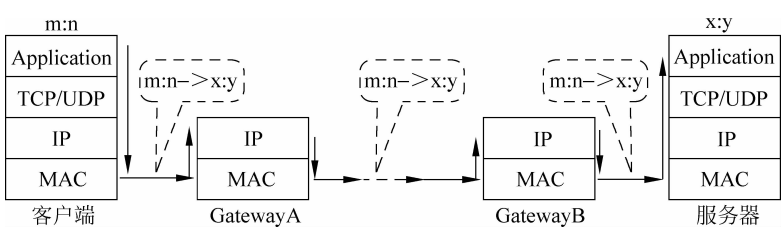

图 3-3 非代理模式下的网络协议处理流程

从图 3-3 可以看出，在一般模式的协议处理流程中，除非在端系统(客户端或服务器端)，所有网络中间结点都不会将途经的协议报文上升到应用层，网络中间结点只是对 IP 数据包进行路由和转发处理。一般情况下，IP 数据包在中间的传递环节是不做任何修改的，除非需要进行 IP 分片。

3.5.2 代理模式下的协议处理流程

为了一些特殊目的，如网络地址公用、安全控制等，一些应用层协议(FTP、HTTP 等)

开始支持代理模式下的网络访问，也就是说在客户端和服务器之间存在一个应用代理服务器。

理论上，从所处的物理结构来看，应用代理服务器并不一定要位于与客户端相同的局域网内，其也不一定要位于客户端和网关之间。但如果需要在应用代理服务器上实现安全控制功能，则该代理服务器就应位于客户端与服务器之间的访问路径中，这里只讨论这种网络结构，如图 3-4 所示。这里假定客户端为局域网 LAN_A 中的 $HostA_i$，服务器为局域网 LAN_B 中的 $HostB_j$，App_Proxy 为位于客户端和服务器间的应用代理服务器。

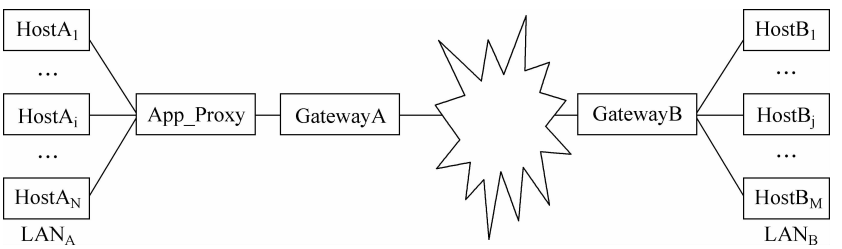

图 3-4　代理模式下的网络结构

从网络服务的逻辑关系上看，代理模式下的代理服务器对应两个角色：对内网的客户端而言，它相当于外网的服务器；对外网的服务器而言，它相当于请求服务的网络客户端。事实上，代理服务器的主要功能分为两个模块：一个是对内网客户端模拟服务器的代理服务器模块；另一个是对外网服务器模拟客户端的代理客户端模块。这里假定这两个模块对外提供的 IP 地址和端口分别为 s:t 和 p:q。

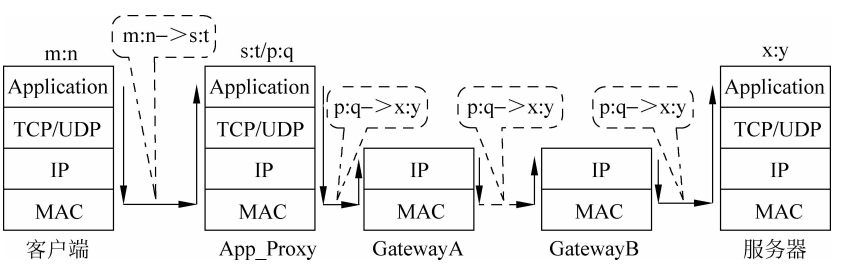

图 3-5　代理模式下的网络协议处理流程

代理模式下的协议处理流程如图 3-5 所示，这里假定客户端的 IP 地址和端口为 m:n，服务器的 IP 地址和端口为 x:y。各网络结点上的协议处理过程概括如下：

- 客户端：在应用层，与服务器的应用会话数据将会按照代理协议的格式和要求，被封装在发往代理服务器的应用会话中，然后该应用会话经过 TCP/IP 协议的逐层处理，被封装成源 IP 地址和源端口为 m:n、目标 IP 地址和目的端口为 s:t 的 IP 数据包（记作 m:n－>s:t），然后封装在 MAC 帧中传输到硬件链路上。
- 代理服务器端：从所收到的 MAC 帧中，IP 协议层首先提取出 IP 数据包，根据该数据包的目标 IP 地址判断出该数据包是发往本机的。进行相应处理后，将 IP 包中的数据部分交给上层协议，经传输层解析出应用层数据，并将这些数据交给应用层进行处理。应用代理服务器基于代理协议从中解析出所代理的应用会话数据，然后该

应用会话经过 TCP/IP 协议的逐层向下处理，先被封装成源 IP 地址和端口为 p:q、目标 IP 地址和端口为 x:y 的 IP 数据包（记作 p:q－＞x:y），最后封装在 MAC 帧中传输到硬件链路上。

- 网络中间结点：从所收到的 MAC 帧中，提取出 IP 数据包，基于该数据包的目标 IP 地址运行路由算法，计算出下一跳的 IP 地址和连接该 IP 地址的网络接口，然后将该 IP 数据包再次封装成 MAC 帧从相应的网络接口中转发出去。
- 服务器端：从所收到的 MAC 帧中，IP 协议层首先提取出 IP 数据包，根据该数据包的目标 IP 地址判断出该数据包是发往本机的。进行相应处理后，将 IP 包的数据部分交给上层协议，经传输层处理解析出应用层数据，并将这些数据交给应用层进行处理。

从上面的协议处理流程可以看出以下几个特点。

- 客户端发出的 IP 数据包，其目标 IP 地址和目标端口为 s:t，这意味着客户端直接和代理服务器发起会话，但会话的内容是让代理服务器代替自己与服务器进行网络会话。
- 服务器收到的 IP 数据包，其源 IP 地址和源端口为 p:q，服务器感觉是与代理服务器进行网络会话，但并不知道是代理服务器自身与其会话，还是代理其他客户端与其会话。

值得注意的是，代理模式下客户端是知道代理服务器存在的，因此网络用户在使用外网提供的网络服务时，要配置代理服务器的 IP 地址与端口。如使用 IE 浏览器时，单击菜单“选项”|“Internet 选项”，在所显示的对话框中单击“连接”|“局域网设置”选项，设置应用代理服务器的 IP 地址和端口。这样 IE 在与外网服务器进行会话时，会启用所设置的代理，从而将与服务器的网络会话封装在与代理服务器的网络会话中进行。

3.5.3 网络防火墙的 IP 层接入

前面提到，网络防火墙的网络访问判决结果要能够影响到网络访问的协议处理流程才能真正生效。同样网络访问截获也需要在网络访问所经过的网络路径上，因此需要将网络防火墙（主要是其中的访问截获和控制实施部分）嵌入到原有的网络协议处理流程中，这就是网络防火墙的网络访问接入。

在实现网络防火墙的网络访问接入时，一个最基本的原则就是接入点一定要在网络访问的必经之处，否则该网络防火墙就有可能被绕过，从而起不到安全控制的作用。对应 3.5.1 节和 3.5.2 节的两种网络服务模式，在网络中分别存在两种比较合适的位置来嵌入网络防火墙的网络数据截获和控制实施模块，即一般模式下的网关 IP 层和代理模式下的应用代理服务器。本节和下节分别详细阐述网络防火墙的这两种接入方式。

网关作为局域网的出入口，局域网内主机和外部网络主机间的任何网络访问，不管是内网主机访问外网，还是外网主机访问内网，其网络访问都要经过网关。因此在网关中嵌入网络防火墙的访问截获和控制实施模块比较合适。

从图 3-3 所示的网络协议处理流程可以看出，网关主要在 IP 协议层实现 IP 数据包的路由和转发，对应网络访问的网络数据报文只能到达 IP 层，不会上传到传输层，更不会上传到应用层。因此在网关上实现网络防火墙接入时，要将防火墙的访问截获和控制实施模块