货运营销与生产管理信息系统网络安全管理的研究与设计

北方交通大学自动化所　许红升
铁道部电子中心　许向东　张骏

本文针对FMOS网络安全管理需求，提出采用WebST和NetST软件产品实现FMOS网络层和应用层的安全管理，建立了FMOS网络安全管理模型，提出了在该模型下实现应用层安全管理的策略。

引言

货运营销与生产管理信息系统（Freight Marketing and Operation System，简称FMOS）涉及铁道部、铁路局、分局及主要货运站的货运生产管理信息的处理，同时向全国范围十万多家货主提供信息服务，以便使这些客户及时、准确地获得有关铁路货物运输的服务信息，如装车审批信息、货物发运情况和货物到达通知等等。

由于FMOS面向的一些大货主都是国内的骨干企业，其分支机构遍布全国乃至世界，未来企业内/企业外、国内/国外电子商务将成为这些企业的基本经营方式。因此，我们采用了Intranet技术建设FMOS网络平台。根据FMOS网络实现的功能，我们将FMOS网络逻辑上分为三个子网：生产子网、服务子网和公共子网。

生产子网由分布在铁道部、铁路局和分局的各局域网中的内部DNS服务器、内部Email服务器、内部Web服务器和客户机等组成。它是铁路货运生产管理信息的运行基础，实现各级货运部门之间、铁路货运员工之间的信息传递，以及信息快速获取和信息发布的功能。

服务子网由分布在铁道部、铁路局和分局的各局域网中的DB服务器和Web服务器组成，是FMOS网络中最主要的信息和服务资源。DB服务器存储有关铁路货物运输的各种信息，由铁道部、铁路局和分局的各级货源数据库组成。服务子网不直接对外服务，只接受公共子网中应用代理的服务，铁路用户和货主都必须通过应用代理才能对服务子网中的服务器进行访问。

公共子网由分布在铁道部、铁路局和分局的各局域网中的外部DNS服务器、外部Email服务器、公共Web服务器、Agent服务器和客户机等组成。公共子网为生产子网内的铁路用户提供对外访问的连接和管理服务，以及提供货主对生产子网的访问代理服务。该子网是货主和铁路用户唯一都能到达的网络区域。

本文针对FMOS网络的安全管理问题进行了深入的研究，并提出了解决的方法。

FMOS网络安全需求分析

FMOS网络在有效地实现了网络资源共享的同时，还必须确保网络上信息资源和服务资源的安全性。网络安全问题关系到铁路和货主自身的利益，对铁路货运部门而言，没有完善的网络安全解决方案，就没有信息技术的投资回报。对货主而言，没有完善的网络安全解决方案，就没有互联网络上的竞争保护。因此，网络安全是FMOS网络设计中的一个重要问题。

基于Intranet的FMOS网络，其安全管理的主要任务是保证合法的铁路用户和货主对网络资源的合法访问，同时防止非法用户（网络黑客）对FMOS网络的攻击。

从FMOS网络的逻辑结构和应用对象两个方面考虑，FMOS网络安全管理问题涉及网络层的安全防护、应用层的安全防护和安全检测三个方面。

(1)网络层的安全防护。主要目的是保证FMOS网络的可用性和合法使用，保护网络中的网络设备、主机操作系统、以及各TCP/IP服务的正常运行，根据IP地址控制铁路用户和货主对网络的访问。网络层在ISO的体系层次中处于较低的层次，因而其安全防护也是较低级的。网络层的安全防护是面向IP空间的，我们采用包过滤、应用代理等防火墙技术作为安全防护手段，实现初级的安全防护。

(2)应用层的安全防护。主要目的是保证信息访问的合法性，确保合法用户根据授权合法地访问数据。应用层在ISO的体系层次中处于较高的层次，因而其安全防护也

是较高级的。应用层的安全防护是面向用户和应用程序的，我们采用身份认证和授权管理系统作为安全防护手段，实现高级的安全防护。

(3)安全检测。辅助性的安全管理措施。通过安全检测／监控手段，可以及时发现FMOS网络存在的安全漏洞或恶意攻击，从而，实现动态和实时的网络安全控制。

因此，一个完整的FMOS网络安全解决方案必须从上述三个方面加以设计和实现。

FMOS网络安全模型

根据上述对FMOS网络安全需求的分析，我们提出采用清华得实网络安全技术公司的网络安全产品NetST和WebST来设计和实现FMOS网络的安全管理。

NetST是一套网络层的防火墙和计费系统，运行在Linux操作系统平台，具有包过滤、应用代理相结合的防火墙功能。同时，能够提供针对IP的流量计费功能，实现网络间的边界安全、流量管理控制和网络服务的实时监控。

WebST是一套应用层的网络安全管理系统，基于Client/Server模式。其基本特征是为Intranet提供统一的安全管理平台，作为网络的授权和访问控制中心，提供了身份认证、授权管理、以及对Web服务器的细粒度访问控制等功能，实现由用户到应用的安全管理。

WebST产品由WebST安全服务器、WebSEAL服务器、NetSEAL服务器、公共密钥管理服务器（PKMS）和安全客户端软件NetSEAT组成。WebST安全服务器实现基于DCE/Kerberos技术的身份认证；WebSEAL服务器和NetSEAL服务器是应用代理级服务器，是在WebST安全服务器进行身份认证之后，实施访问控制。PKMS公共密钥管理服务器是WebSEAL的安全代理，是由SSL安全通道到WebST安全通道的安全网关。NetSEAT安全客户端软件是运行在客户端的瘦型的DCE客户端软件，用来进行身份认证和建立安全通信通道。

由上可知，NetST较好地解决了网络层的安全问题，WebST较好地解决了应用层的安全问题。NetST防火墙能够解决网络的边界安全和系统安全，能防止外部攻击；WebST能解决网络的整体安全和数据安全，能防止内部攻击，并实现安全管理。将NetST和WebST相结合，能够实现Intranet的整体安全，为用户构建一个完善的安全防护体系。因此，我们将NetST和WebST产品相互结合，设计了FMOS网络安全模型，如图1所示。

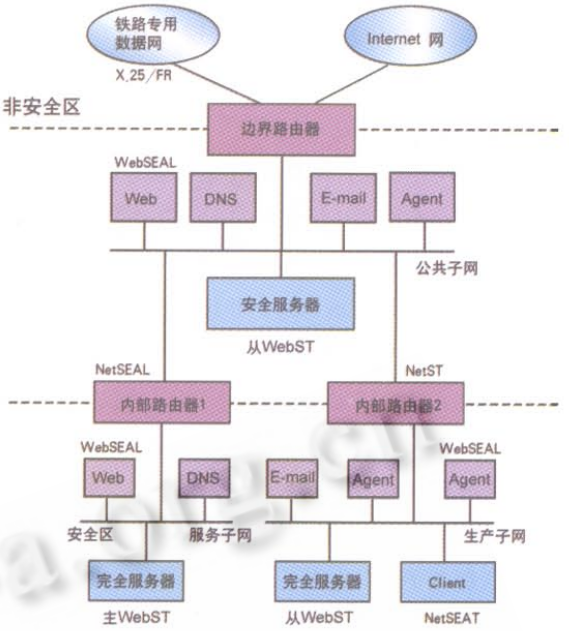

图 1 FMOS安全网络模型

图中，FMOS网络安全模型由边界路由器和内部路由器分隔为三个区域：非安全区、停火区和安全区。边界路由器和内部路由器实现了FMOS网络层的安全防护。

边界路由器采用包过滤技术对由外部网络进入FMOS网络的IP数据包进行过滤，使得外部IP数据包只能到达FMOS网络的公共子网部分。

内部路由器实现逻辑子网之间的访问控制管理。其中，内部路由器1作为应用网关代理服务，采用NetSEAL服务器软件实现，完成铁路用户和货主对服务子网中的DB服务器和Web服务器的访问代理服务。内部路由器2采用NetST防火墙软件，实现包过滤和网络地址转换功能。在FMOS网络中，保证只有公共子网的IP数据包才能进入生产子网，而生产子网的IP数据包只能到达公共子网，不能到达外部网，使得生产子网和外部网之间不能直接通信。

对于应用层的安全防护，由于服务子网、生产子网和公共子网提供给铁路用户和货主的应用服务各不相同，我们分别在各子网中配置了一个WebST安全服务器，并将其设置成主/从工作方式，实现用户身份认证和授权管理。

此外，对FMOS网络中的Web服务器，我们采用WebSEAL服务器软件实现集中式统一管理，使分布的Web空间在逻辑上成为一个整体。在客户机端运行NetSEAT安全软件，与WebSEAL服务器软件构成Client/Server模式的安全防护体系。

FMOS 网络安全管理策略

针对上述FMOS网络安全模型，我们提出以下策略实现应用层安全管理。

(1)用户身份认证。在WebST安全服务器中，我们建立了一个用户数据库（USER_DB），存储每个铁路用户和货主的登录帐号ID、密码Kc、以及用户组信息。当一个用户C登录到FMOS网络，并且请求访问应用服务器时，安全服务器根据USER_DB中存储的用户密码Kc生成一个加密密钥，应用Kerberos/DCE协议，对用户C进行双向身份验证。即在登录过程中，用户C和应用服务器双方相互确认对方的身份。

(2)Web服务器的统一管理。从FMOS网络的逻辑结构可知，服务子网、生产子网和公共子网中均包含Web服务器，这些Web服务器在图1所示的安全模型中，由WebSEAL服务器软件实施安全管理。为了方便地对这些Web服务器进行统一管理，我们运用WebST的Smart Junctions机制，将网络中的所有Web服务器组成一个Web群，实施统一的访问控制管理，如图2所示。

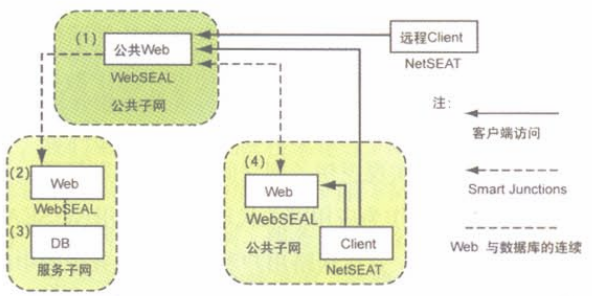

图 2 统一Web应用服务体系

图中，Web_1通过Smart Junctions机制连接Web_2和Web_4，使授权货主能够访问公共数据信息Web_2和数据库信息DB_3以及Web_4。通过Smart Junctions连接机制，铁路用户可以直接访问Web_4，也可以通过Web_4、Web_1访问公共数据信息Web_2。这样生产子网内的Web服务器和服务子网内的DB服务器能够被授权货主访问，同时又隐藏在生产子网和服务子网中，避免遭受外界的攻击。

在该Web群中，Web_1服务器还可以连接到远程的Web服务器，使得在分局、铁路局和铁道部之间可以安全地共享信息和通信。

(3)货主安全访问控制策略。目前，有10万多家货主对FMOS网络中铁道部、铁路局和分局的各局域网中的应用服务器，例如Web等进行访问。这些货主随着运输市场的变化，在不断地增加或消失，即货主本身具有自生自灭的特点。如何在FMOS网络中对货主实施一致的访问控制策略，是确保货主安全访问和管理FMOS网络资源的有效手段。

在FMOS网络安全模型中，我们配置了WebST安全服务器，WebST安全服务器提供了授权访问控制机制。在该机制中，WebST提供了两种访问控制粒度：粗粒度控制和细粒度控制。粗粒度控制是基于网络连接的访问控制，细粒度控制是基于具体应用对象的访问控制。

对于FMOS中的货主而言，首先，我们定义粗粒度的访问控制，用来管理和控制哪些货主可以访问哪些服务器的哪些应用。其次，定义细粒度访问控制，用来管理和控制哪些货主可以访问Web服务器上的哪些页面。细粒度访问控制利用访问控制表（ACL）实现，ACL规定了货主对资源对象的访问权限。从数学上来看，ACL是一个表，其行表示资源对象，其列表示货主，行和列的交叉表示货主对某项资源的访问权限。

(4)安全检测方法。WebST和NetST实现了FMOS网络的应用层和网络层的安全管理。但对于一个完善的网络安全体系来说，还必须提供对网络进行动态、实时的安全检测和监控管理，及时发现网络存在的安全漏洞或恶意的攻击。

在FMOS网络安全模型中，铁路用户和货主对Web服务器的所有访问均通过WebST安全服务器的访问控制机制管理。由于WebST提供细粒度的访问控制管理，通过WebST安全服务器，我们可以获得铁路用户和货主对Web服务器访问的详细情况。这些情况以一定的格式存储在WebST日志文件中。

WebST提供了三种格式的日志文件：DCE标准格式、WebST专用格式和HTTP标准格式。日志文件记录了铁路用户和货主在一次浏览中，是如何访问各个页面的，包括请求系统的主机名或IP地址、时间和日期、路径和被请求文档的文档名、请求成功信息或失败代码、以及传输的字节数。同时，日志文件也记录了某些用户或黑客执行的各种非法操作。通过周期地读取日志文件，同时对其内容进行分析处理，我们便实现了对FMOS网络的动态和实时的安全监测管理。■