维普资讯 http://www.cqvip.com

基于SOAP的分布式防火墙策略发布研究

陈 军[1,2] 王海洋[1] 曹鲁慧[1,2]

(山东大学计算机科学与技术学院 济南250061)[1] (山东大学网络中心 济南250100)[2]

摘 要 文章提出了一种基于SOAP的分布式防火墙策略发布方法。介绍了集中式管理中分布式防火墙的体系结构,使用XML描述策略,通过SOAP将策略发布到防火墙上,用SOAP数字签名和加密保证信息传输的安全性。具有平台无关性、语言无关性、易扩展性、能穿越防火墙等优点。这种方法也可用于分布式防火墙管理信息的传输。

关键词 SOAP,分布式防火墙,策略发布

Research in Policy Issue of Distributed Firewalls Based SOAP

CHEN Jun[1,2] WANG Hai-Yang[1] CAO Lu-Hui[1,2]

(School of Computer Science and Technology, Shandong University, Jinan 250061)[1]

(Network Center of Shandong University, Jinan 250100)[2]

Abstract This paper introduces a issue method of distributed firewalls policy based SOAP. It adopts the centralized management, uses XML to describe policies, issues policies on firewalls through SOAP and adopts SOAP signature and encrygraph to protect the data flowing on network. It also gives the centralized architecture of distributed firewalls. The advantages of the method are the independence of platform, the independence of language, the extensibility, the ability of passing through firewall and so on. This method is apt to transmit management data of distributed firewalls.

Keywords SOAP, Distributed firewalls, Policy distributing

1 引言

防火墙是保护Internet网络安全的一个有效手段。传统的防火墙布署在网络的边界,阻挡来自外部的攻击或未授权的访问,它不能解决内部攻击的问题,DFW(Distributed Firewalls,分布式防火墙)弥补了这一不足,可以提供对网络内部细颗粒度的保护,并且不依赖网络的拓扑结构。DFW的实现有两种类型:一种是文[1~3]提到的EFW(Embedded Firewall,嵌入式防火墙),它采用集中式管理,在计算机的网卡上执行,具有性能高、不依赖操作系统、防篡改、支持VPG(Virtual private groups,虚拟私有组)等优点,功能受网卡处理能力的限制,主要集中在IP包过滤上。另一种是文[4]提到的在操作系统内核或用户级实现的方法,能处理应用级策略,功能扩展能力强。本文讨论第二种实现类型的问题。DFW的防御是静态的,需要与DIDS(Distributed Intrusion Detection System,分布式入侵检测系统)相结合来实现动态防御,根据DIDS的告警消息修改策略,阻断正在发生的网络攻击[5]。DFW管理还应能与网络管理、资源管理等集成在一起形成一个综合的网络管理系统。

DFW的关键技术在安全管理信息的描述及其分布式传输上。文[6]提出了一个DFW通讯协议,该协议运行在BGP-4(Border Gateway Protocol version 4,边界网关协议版本4)上,需要路由器的支持,不适合内网的环境。文[7]用KeyNote描述策略,用IPsec隧道进行传送。这种情况下防火墙不能对IPSEC报文做处理,削弱了防火墙对内部网络的安全防护能力[8]。XML技术出现后,XML具有的简单性、灵活性、开放性、平台无关性、可扩充性和自描述等特性,使其特别适合异构平台间的信息交换和表示,也适合描述DFW的安全管理信息,文[9]采用构建在BEEP(Blocks Extensible Exchange Protocol,块可扩展交换协议)安全通信框架上的XML-RPC传输信息。该方法具有平台无关性、语言无关性等优点,安全信息可以穿越防火墙。我们对DFW的策略描述和发布进行了研究,提出了一种满足分布式要求的防火墙的体系结构,在此基础上给出了一个基于SOAP(Simple Object Access Protocol 简单对象访问协议)的策略发布方法,BEEP在TCP/IP层连接、验证和封装消息,和HTTP在同一层上,SOAP是在BEEP的上层实现的,同样具有文[9]方法的优点,可以集中管理分层的DFW。SOAP可以捆绑在HTTP、SMTP等协议之上,与BEEP相比具有更大的灵活性。

2 基本概念和原理

定义1 网络防火墙是一种加强网络间访问控制的网络安全互联设备,本身自带多个网口,可以同时连接多个子网,它对两个或多个网络之间传输的数据包和链接方式按照预定的安全策略进行审查,决定网络之间的通信是否被允许,从而达到保护网络内部的信息不受外部非授权用户的访问和过滤不良信息的目的。部署在内网和外网之间的称边界防火墙,部署在网络内部的称内网防火墙。

定义2 主机防火墙是一种软件,它运行在服务器主机上,对进出服务器的数据包进行规则匹配、过滤或转发,作用

陈 军 工程师,在读硕士研究生,主要研究方向为网络与分布式技术。王海洋 教授,博士导师,主要研究方向为软件与数据工程。曹鲁慧 在读硕士研究生,主要研究方向为网络应用。

维普资讯 http://www.cqvip.com

域是该服务器，即仅对服务器本身进行安全保护。它一般是作为操作系统内核模块工作的。

定义3 策略是一组防火墙规则的集合。在支持异构平台的DFW环境下，描述策略的语言应是平台无关的。在策略发布到防火墙执行时，由解析器将其翻译成具体防火墙可以识别的规则代码。

定义4 存储各防火墙策略信息的机器称为策略管理服务器，它还存储着防火墙的其他配置信息、状态信息，可通过它对防火墙进行远程管理：变更策略、配置，查询状态，获取日志等。

定义5 DFW的管理方式分为集中式和分布式，集中式通过一台策略管理服务器管理所有的防火墙，适合防火墙数量不特别多的情况。防火墙数量庞大时要使用分布式管理。

定义6 策略发布方式分为主动式和被动式，主动式：策略改变时，由策略管理服务器实时发送到相应的防火墙（客户机）上。被动式：由客户机定时向策略管理服务器查询，发现策略改变时下载新策略到本地。

定义7 DFW是一个多层次的安全防护体系，由网络防火墙、主机防火墙、安全策略管理、安全策略发布机制等组成。作用域是整个网络。可以根据需要，对内网中的一个或多个子网、网络上的一个或多个服务器主机进行有针对性的、精细的防护。DFW应是平台无关的，即DFW可由多个厂家的产品混合组成。DFW可以有多个层次，即如果将策略管理服务器看成树根，各防火墙看成树上的节点，这样形成的多叉树的深度≥2。典型的分布式防火墙如图1所示。

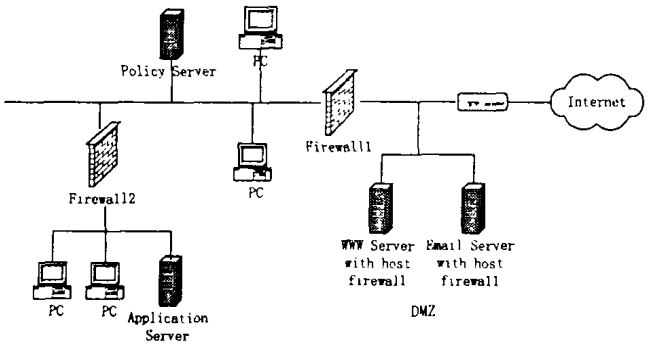

图1 分布式防火墙网络结构

DFW的工作原理 策略制定或修改后，策略管理服务器通过事先规定的发布机制，将策略完整、准确、安全地传送到目的防火墙上，目的防火墙上的解析器将策略翻译成本地防火墙可以执行的规则，在防火墙上实施。策略翻译也可以在策略管理服务器上完成。

SOAP的信息交换原理 SOAP是基于XML的简单的、可扩展的通信协议，是一个传送信息的格式，具有平台无关性和语言无关性特点，能在应用间通过HTTP交换信息，防火墙一般是允许HTTP通过的，因此用SOAP可以穿过防火墙[10]，IPsec和BEEP是通过隧道方式穿越防火墙的。

3 基于SOAP的DFW策略发布方案

我们这里只对实际中使用最多的集中式管理阐述策略的发布方法。当防火墙数量很多，比如几十台时，可以分组管理。采用策略主动发布方式。

3.1 系统的体系结构

服务器端的体系结构 服务器端的体系结构如图2所示，是一个典型的三层结构。httpd提供分布式防火墙管理的Web界面，管理员通过浏览器完成管理工作。管理工作包括：①组的管理，添加、修改、删除、显示组。②防火墙管理：添加、修改、删除、显示防火墙。③防火墙的配置管理，包括策略管理：在防火墙中添加、修改、删除、显示策略。④发布策略及发布失败处理。⑤性能监测及日志察看。⑦用户管理及登录认证。这些功能由engine完成。API为数据库接口。数据库用于存放engine使用的相关管理信息。

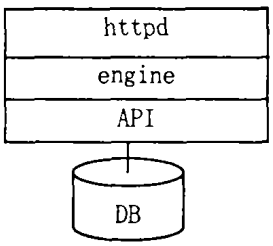

图2 服务器端的体系结构

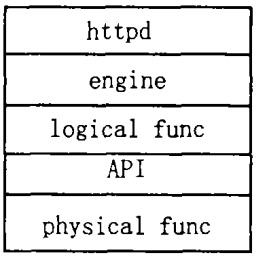

图3 防火墙的体系结构

客户端的体系结构 防火墙的体系结构如图3所示。httpd提供防火墙管理的Web界面。engine层接收配置、状态查询等管理命令，包括接收新的策略，回送状态查询结果。逻辑功能层为防火墙功能的逻辑实现，包括调用解析器将策略转成内部可识别的代码交给下层执行。API为逻辑/物理功能层的接口层。物理功能层为防火墙功能的真正实现。这种体系结构的优点有三个：①各厂家的产品可以使用相同的语言描述策略，提供一致的界面，减轻管理员的管理难度。②防火墙无论是独立使用还是在分布式环境中使用，用户看到的是同样的界面。③防火墙的逻辑实现和物理实现分开，API层以上的代码可以重用，降低产品开发的工作量。

这样的服务器、客户端体系结构在用统一的语言描述信息时，可以使DFW管理系统开发与具体的防火墙系统开发分开，易于与DIDS集成实现网络动态防护，易于与网络管理系统集成。

3.2 策略的组织、存放

服务器端使用关系数据库保存管理信息，用XML描述的策略也存入该数据库中。因为XML是半结构化的，要建立XML元素到数据库表的对应关系才能方便存取。

在客户端（防火墙上）将接收到的用XML描述的策略以文本文件形式存放。防火墙重启时执行该文件中的策略。

3.3 用SOAP发布策略

在服务器端，防火墙的策略改变后，产生发布策略的消息，engine使用HTTP1.1向对应防火墙发出以SOAP envelop封装的策略。基本内容为：

```
POST /receiverfwr HTTP/1.1
Host: firwallname
Content-Type: application/soap+xml; charset=utf-8
Content-Length: nnn
<?xml version="1.0"?>
```

维普资讯 http://www.cqvip.com

```
〈soap:Envelope xmlns:soap="http://www.w3.org/2001/12/soap-
      envelope"
soap:  encodingStyle  =  "  http://www.w3.org/2001/12/soap-
       encoding"〉
       〈soap:Body xmlns:m="http://firewallname/receivefwr"〉
         〈m:SendFwRule〉
          〈m:Rule〉
              〈m:Input〉……〈/m:Input〉
              〈m:Output〉……〈/m:Output〉
              〈m:Forward〉……〈/m:Forward〉
          〈/m:Rule〉
         〈/m:SendFwRule〉
       〈/soap:Body〉
〈/soap:Envelope〉
```

防火墙中的 engine 接收完成后向服务器发送回应，调用解析器将策略翻译成本地可以识别的规则传递到下层执行。回应内容为：

```
HTTP/1.1 200 OK
Content-Type: application/soap; charset=utf-8
Content-Length: nnn
〈?xml version="1.0"?〉
〈soap:Envelope xmlns:soap="http://www.w3.org/2001/12/soap-
      envelope"
soap:  encodingStyle  =  "  http://www.w3.org/2001/12/soap-
       encoding"〉
       〈soap:Body xmlns:m="http://firewallname/receivefwr "〉
         〈m:SendFwRuleResponse〉
          〈m:Result〉OK〈/m:Result〉
         〈/m:SendFwRuleResponse〉
       〈/soap:Body〉
〈/soap:Envelope〉
```

3.4 分布中的安全问题

防火墙策略是保护网络安全的重要信息，在网络上传送时要保证信息的安全，这里主要包括信息的保密性、信息的完整性和身份认证。在点对点的环境下，可以用安全套接字层(SSL)和传输层安全性(Transport Layer Security，TLS)一起提供传输级别的安全性，包括认证、数据完整性和数据机密性。在端对端的环境下，可以通过 XML 数字签名、XML 加密和 SOAP 安全性扩展来解决传输安全问题[11~14]，也可以利用 WS-Security 技术[15]。这里使用前一种方法。

认证 认证是对通讯对方身份的验证，确保对方就是他声称的那个人，避免身份的假冒。发送方在 SOAP 头元素中增加〈SOAP-SEC:Authorization〉元素，用对方的公钥加密得到的证书，将其进行 BASE64编码后放到〈AttributeCert〉子元素中。接收方将〈AttributeCert〉中的内容解码，用自己的私钥解密后验证证书。

信息完整性 信息的完整性指信息在网络传递过程中内容不能被破坏或被修改。W3C 制定了 SOAP 数字签名安全扩展标准，它基于 XML-SIG 实现。SOAP 数字签名规范允许对整个 SOAP 消息或其中一部分进行签名，如果消息带有附件，也可以对附件进行签名。SOAPEnvelop 中〈SOAP-SEC:Signature〉元素标识一个签名头实体，它必须包含一个〈ds:Signature〉元素。发送方将对策略的签名信息、签名值、密钥信息等放入〈ds:Signature〉中。接收方利用这些信息验证策略内容和发送方身份。

信息保密性 信息保密性指信息在网络传递过程中一些私有的、重要的内容不能被别人获取，防止数据泄漏。SOAP 报文加密以 XML-Encryption 为标准，加密对象可以是整个 SOAP 报文或其中的一部分。发送方将加密数据位置、密钥信息放到头实体〈SOAP-SEC:Encryption〉的子元素〈xenc:DecryptionInfo〉中，加密了的策略放到 SOAP 信封体的〈xenc:EncryptedData〉子元素中。接收方从〈xenc:EncryptedData〉的属性 DecryptionInfoURI 中得到解密信息的位置，然后取得相关信息对策略解密。

3.5 发布失败处理

发送失败的情况有三种：发送不成功、防火墙没返回 OK 响应、没收到响应。发送失败的信息需要及时显示给管理员，待排除故障后由管理员重发。

3.6 解决方法的技术可行性

现在已有很多商业的或免费的 XML、SOAP 开发工具或软件包如 Microsoft Visual Studio .NET、JbuilderX、Apache SOAP 等。目前防火墙产品中都普遍包含了认证、加密等功能，都有图形界面(基于浏览器或 Window)的远程管理功能，有实力的厂家已经做到了对自己产品的分布式管理。所以在防火墙中增加对 XML、SOAP 的支持技术上是可行的。对于主机防火墙来说实现该方法需要集成一个嵌入式的 Web 服务器，要做到端到端的信息传递安全，还有一定的困难。

结束语 本文描述了集中式管理 DFW 的体系结构，给出了一种基于 SOAP 的 DFW 策略发布方法。用 XML 作策略描述语言，用 SOAP 数字签名和加密保证信息传输的安全性，具有平台无关性、语言无关性、易扩展、灵活、能穿越防火墙等优点。这种方法也可用于分布式防火墙管理信息的传输，能方便与入侵监测系统和网络管理系统集成。这种方法采用了策略主动发布方式，在多层 DFW 环境中，位于中间层的防火墙需要开放80端口以允许传向底层防火墙的策略通过，这可能会使部分内网的计算机遭到内部伪造 IP 地址针对80端口的攻击。如何在主机防火墙上支持 XML、SOAP 协议，做到端到端(点对点)的信息安全传输还有待进一步研究。目前 SOAP 加密尚不存在标准规范，文中 SOAP 加密基于其初步草案。

参 考 文 献

1 Payne C, Markham T. Architecture and Applications for a Distributed Embedded Firewall. In: Proc. 17th Annual Computer Security Applications Conf. 2001. ACSAC 2001. 329～336

2 Meredith L M. A Summary of the Autonomic Distributed Firewalls (ADF) project. In: Proc. DARPA Information Survivability Conf. and Exposition, 2003,2:260～265

3 Markham T, Payne C. Security at the network edge: a distributed firewall architecture DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01,2001,11:279～286

4 Ioannidis S, Keromytis A D. Implementing a Distributed Firewall. In:7th ACM Conf. on Computer and Communications Security, Athens, GREECE,ACM, Nov. 2000

5 杨海松，李津生. 分布开放式的入侵检测与响应架构——IDRA. 计算机学报,2003,26(9):1177～1182

6 Smith R N, Bhattacharya S. A Protocol and Simulation for Distributed Communicating Firewalls. In: Proc. Computer Software and Applications Conf. COMPSAC '99. The Twenty-Third Annual Intl. 1999. 74～79

7 Bellovin S M. Distributed Firewalls. http://www.research.att.com/～smb/papers/distfw.html, 1999

8 姚立红，谢立. IPSEC 与防火墙协同工作设计与实现. 小型微型计算机系统,2004,25(12):183～186

9 王伟，曹元大. 分布式防火墙下的分布式通信技术. 计算机工程,2003,29(22):148～150

10 http://www.w3schools.com/soap/

11 SOAP Security Extensions. http://www.trl.ibm.com/projects/xml/soap/wp/wp.html

12 SOAP Security Extensions: Digital Signature http://www.w3.org/TR/SOAP-dsig/

13 XML Encryption Syntax and Processing http://www.w3.org/TR/xmlenc-core/

14 Steve Graham. 用 Java 构建 Web 服务. 机械工业出版社,2003

15 Web Services Security http://www-106.ibm.com/developerworks/library/ws-secure