策略 策略模型 Internet网 网络管理 (19)

计算机科学2000Vol.27№.5

81-83

策略及策略模型的研究与应用*)

The Research and Application of Policy and Policy Model

蒋 韬 李信满 刘积仁

(东北大学软件中心 沈阳110006)

TP3P3

Abstract With the application of Internet and complexity of network, network management based on policy is more and more important. This paper mainly depicts the concept and key problem of policy, and presents a framework of policy model implement. In the end, this paper presents views on the developing of policy research.

Keywords Policy, Policy model, Conflict detecting, Security, QoS

1 策略概述

随着Internet应用的日益广泛和网络的日益复杂,基于策略的网络管理越来越显得重要,所以对策略本身的研究也有很重要的意义.IETF已在多个工作组中对此问题展开了研究,并已出台了一些草案,以供大家讨论。

所谓策略就是描述一组策略规则集合的被命名的对象,是所需求的高层商业规范与提供服务的低层配置之间的一种连接。对它的研究包括:策略的存储、分配、决策、冲突检测、冲突消解、维护和管理。从网络的角度来看,策略是经营和管理网络元素的能力,以便它们能够提供网络客户所需的服务。

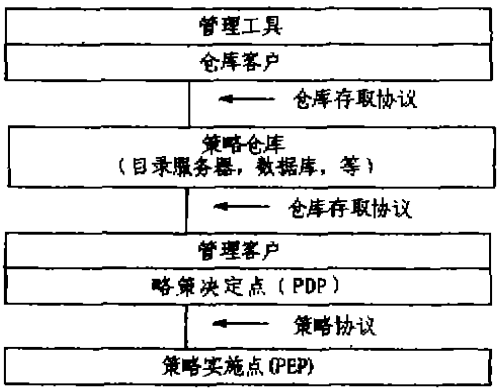

图1 策略的基本结构

如图1所示,这是策略的一般结构。其中三个基本实体是:仓库(Repository)、策略决定点(PDP)、策略实施点(PEP),现以某虚拟企业的网络安全系统为例说明这个问题。

从上图可以看出,策略的基本功能是:决策、执行、审查。策略从使用上可分为授权策略和强制策略。授权策略是指允许或不允许管理员对管理对象进行某种操作。强制策略则规定了管理员所必须做或不应该完成的功能。策略从触发方式可分为静态策略和动态策略。所谓静态策略是根据预定义的参数以预定的方式执行的一组固定的动作。这种方式在应用上有一定的局限;而动态策略是在需要时才执行的策略。尽管策略执行的条件是预定义的,但并不是通过设定时间或参数来触发,而是当满足一定条件时才触发。

2 策略研究需要解决的关键问题

2.1 模型

网络上的多个设备都需要执行不同的策略,如何维护这些策略的一致性就显得越来越重要,这就需要开发一种具有伸缩性的策略框架来处理不同设备和设备类型之间的策略的互操作问题。策略框架由定义策略所需的不同部件组成。制定策略框架的目的是为了使多个设备以及不同类型的设备能够在一起互操作,以便执行网络管理员的策略。因此,策略框架的结构必须具有伸缩性、互操作性和重用性。伸缩性是指可由一组简单策略任意构造出可重用的复杂策略。互操作性是指策略框架必须提供一种描述其本质信息的能力,以满足不同厂商所提供的策略管理系统之间和策略管理系统所控制的设备之间的通讯。重用性是指一个策略的部件可以被其它策略重用。

*)本文受到国家863计划资助。蒋韬 博士生,研究方向为计算机网络。刘积仁 教授,博士导师,研究方向为分布式多媒体技术,计算机网络。

策略框架核心信息模型(CIM,Common Information Model)是一种面向对象的策略模型。将策略显式地表示为对象有很多优点:首先,便于查找、修改和管理策略,例如,可以定义一个授权策略以限制只允许某些管理员修改一组策略或定义"元策略";其次,便于定义具有某特定策略属性的类。在为一个特定应用定义策略时,该策略的实例即被创建,并保存有为特定实例而定义的策略属性。策略类就象一个模板一样,当一个策略实例被创建时就拥有了特定的策略属性类。同时,由于对象的继承性也便于策略向其子域的传播。以下就是策略部件的层次划分:

·复杂策略类　由一个或多个简单策略所组成,例如可以重用现成的安全策略、DHCP 策略和 QoS 策略。

·简单策略类　由一个或多个策略规则组成。即每一个简单策略都是由一组策略条件和一组策略行为组成。

·策略规则类　描述了一组条件以及满足条件时所触发的一组行动。

·策略条件类　由策略条件表组成。每个策略条件表由一个或多个策略条件语句组成。每个策略条件语句又包括两部分:策略条件分类和策略条件值。策略条件语句定义了策略条件分类和策略条件值之间的关系。策略条件分类是针对某一特定领域的预定义值。策略条件值则是所取的实际值(在策略条件分类预定义的值中选取)。

·策略行为类　由一个或多个策略行为组成。每个策略行为又描述为一个策略行为表。每个策略行为表又由一个或多个策略行为语句组成,每个策略行为语句包括两部分:策略行为种类和策略行为值。策略行为语句定义了策略行为种类和策略行为值的关系。策略行为分类是针对某一特定领域的预定义值。策略行为值则是所取的实际值(在策略行为分类预定义的值中选取)。

2.2　策略的一致性检查与冲突检测

策略的一致性检查是对当前活动的策略进行检查,以确定其一致性或可能不一致的地方。策略冲突的检测对策略框架来讲是至关重要的。策略冲突分为两类:Intra-Policy 冲突和 Inter-Policy 冲突。

Intra-Policy 冲突一般发生在有两个或多个条件被同时满足,但至少有一个策略的行为不能被执行。表现在:①一个或多个策略规则满足同一需求;②每个冲突策略的规则的每个条件满足同一需求;③一个策略的一个或多个行为与别的策略的一个或多个行为相冲突。

Inter-Policy 冲突是指两个或多个策略应用在网络时所引起的网络设备的配置或应用机制的冲突。例如,原本不冲突的两个策略应用在同一网络设备上时,有可能将相同的信息流分配给不同的端口,从而造成冲突。

冲突的消解有多种办法。其中最简单的办法是修改冲突策略的条件,以达到消解冲突的目的。如果仍然不能消解冲突,则可按照下面的方法处理:①"匹配优先"原则,即满足匹配的第一条策略;②"优先权"原则,即满足优先权高的策略;③"仲裁"原则,即增加附加条件以确定使用哪一条规则。

2.3　策略本身的安全性要求

策略本身可能存在两方面的安全隐患。一是未经授权地阅读并修改策略规则和目录仓库中的相关对象,其解决办法是采用 LDAP 中的存取控制机制。二是策略决定点与目录仓库之间的通讯安全问题,其解决办法是通过 SSL/TLS 鉴别或 IPSec 规范来保障通讯安全。

2.4　策略的生存周期

策略也存在生存周期,包括休眠态、静止态、激活态和删除态,其触发条件及状态转换如图2所示。

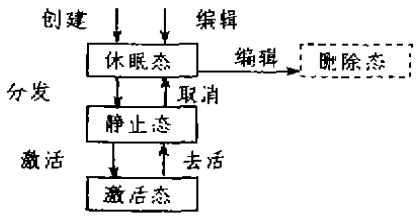

图2　策略的生存周期

3　策略及其策略描述语言的应用

3.1　在网络安全中的应用

在安全策略描述语言(Security Policy Specification Language, SPSL)中,策略被定义为一组通讯条件和相应行为的绑定。同时,SPSL 提供对两种安全模型的支持:在基于结点的模型中,安全策略将网络结点与安全设备绑定;在基于域的模型中,安全策略与安全域绑定在一起。SPSL 使用了对象变化,尽管它不是面向对象或基于类型的语言。SPSL 包括以下类型:

·基本数据:包括用于策略规范的基本或原子数据元素。

·管理代理:包括与管理实体相关的信息。

·网络实体:描述了与策略规范相关的网络元素。

·审查(Policies):对策略的执行情况进行审查。

此外,SPSL 必须满足这样一些基本要求:①支持 IPSec/ISAKMP 和通用的通讯安全策略规范;②支持基于结点的和域的安全模型;③支持多个分布式策略执行点;④支持认证和授权机制;⑤支持语言的灵活性和扩展性。

图3给出了基于 IPSec 规范的策略类结构图。

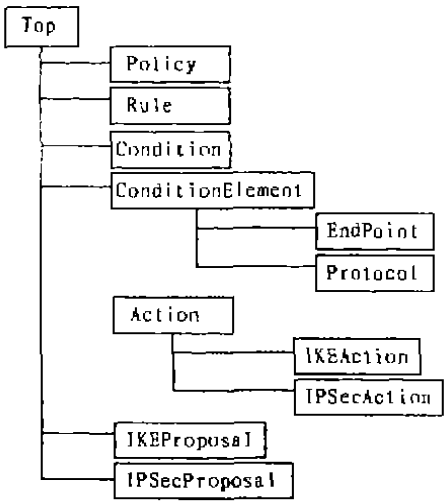

图3 基于 IPSec 的策略类结构

3.2 在 QoS(服务质量)中的应用

QoS 策略类必须满足下列要求:①灵活的,与供应商独立的策略描述;②提供策略发现机制;③提供一个机制来满足策略交换与信息查询;④提供策略谈判;⑤提供动态策略升级;⑥提供失败策略的错误通知。

图4给出了满足 QoS 要求的策略类结构图。

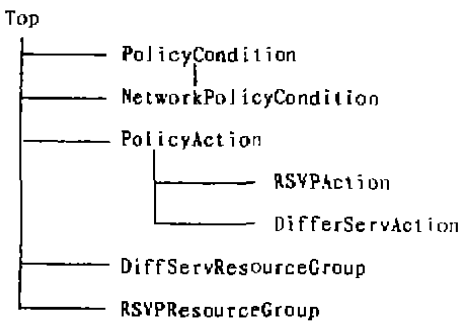

图4 基于 QoS 的策略类结构

4 策略的实现框架

一个完善的策略管理与应用框架(如图5所示)包括以下几个部分:

DEN(Directory Enabled Network):DEN 是一种高级的目录系统,它把网络中的各种目录链接在一起,构造出一个单一"虚拟"目录。DEN 定义了网络元素和网络业务,并将它们和网络应用以及用户的相互关系标准化,从而简化了不同种设备的集成方案。由于网络中的所有信息都包含在一个 DEN 目录中,因此它可以提高策略管理水平。

DEN 允许网络管理者在虚拟目录中定义网络的工作特性,例如可以对某一个具体的应用或用户规定带宽优先级,还可以定义有关策略信息的检索和存储的方式。策略服务器可以从虚拟中心目录中采集信息,并与规定带宽的具体策略相匹配,从而提高 QoS。

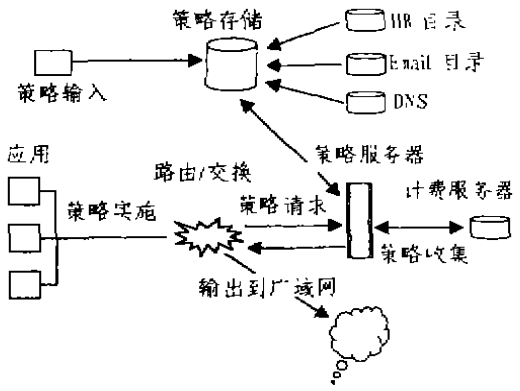

图5 策略的实现框架

策略服务器:它担负与策略发生设备的通信以及对策略要求的接受、解释、检验和接受任务。一个完整的策略管理模式应当包括策略机制、网络资源分配协议以及企业内部策略。策略服务器是策略管理系统的核心设备,它采集相关信息,参照网络目录确定服务等级,根据网络资源和网络管理者的策略设置做出决策,并将这一决策结果传给最近的接入结点。策略服务器与当前网络的其它设备同时工作,它通过软件监视网络运行,实现 QoS 的优化配置,对网络路由和交换作动态配置。

管理:策略决定网络资源如何分配给用户或数据流这样的实体。用户与服务提供商有各自的策略范畴,企业与服务提供商也有共用的策略。一个服务提供商的例子是用于创建网络中不同服务级别的内部机制,而共用策略的例子是用户对内部网管理,而由服务提供商确认,但由用户证实。用户策略用来在网络中实施诸如应用、协议或群组传输优先权和带宽等商业策略规则。

结束语 总之,对策略本身及其应用的研究已经越来越受到重视,不仅 IETF 已对此展开了研究,并公布了相关草案,许多公司也推出了相关产品。例如 IBM 公司推出了 AppDrvN,就是基于策略管理的应用软件,Cisco 公司也推出了支持策略路由的路由器。当然,策略研究方面尚有许多亟待解决的问题,比如说策略的形式化描述、标准的制定以及应用。

参 考 文 献

1 Draft-ietf-ipsec-policy-schema-00.txt
2 Draft-ietf-ipsec-policy-model-00.txt
3 Draft-rajan-policy-qosschema-01.txt
4 Draft-ietf-policy-core-schema-03.txt
5 Draft-ietf-policy-framework-pfdl-00.txt