第 35 卷 第 8 期 计 算 机 工 程 2009 年 4 月
Vol.35 No.8 Computer Engineering April 2009
·安全技术· 文章编号：1000—3428(2009)08—0201—04 文献标识码：A 中图分类号：TP393.08

基于策略的一体化网络安全管理系统

韩锐生，赵 彬，徐开勇
(解放军信息工程大学电子技术学院信息安全研究所，郑州 450004)

摘 要：针对当前网络安全管理的缺陷，在网络安全管理中引入基于策略的管理方法，设计一个网络安全管理系统，实现对网络安全的一体化自动管理，简化网络安全管理的复杂性。介绍安全管理系统设计和策略驱动设备间互操作等技术的实现过程，并给出应用实例。
关键词：策略驱动；统一策略管理；事件关联分析；Ponder 策略框架

Policy-based Integrative Network Security Management System

HAN Rui-sheng, ZHAO Bin, XU Kai-yong
(Information Security Institute, Electronic Technology Academe, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】Limitation of network security management is analyzed. This paper introduces Policy-Based Management(PBM) approach to network security management, designs a network security management system. The presented system can manage the network security management systems integrately and automately, dramatically reduce the complicity of network security management. is greatly useful to the security management of large-scale network. This paper introduces the design of the system, shows the completing work of key technologys such as the process of cooperation of security productions driven by event-triggered policy and gives an example of the system application.
【Key words】policy-driven; uniform policy management; event coordination analysis; Ponder policy framework

1 概述

现有网络安全体系基本采取应对式的、以技术为中心的网络安全对策[1]，根据总体需要的功能增加设备或软件。为应对各种日益严重的网络威胁，大量配置了防火墙、防病毒软件、入侵检测、漏洞扫描、灾难恢复等安全设备。这种安全解决方案对解决网络安全问题起到重要的作用，但也对网络安全管理造成严重的局限性，表现为：(1)非集成化实施。各安全产品功能支离破碎、各自为战，缺乏统一的规划和管理；(2)缺乏集中管理，造成管理复杂。由于安全设备间物理差异，对它们的管理须单独进行配置管理，增加了安全管理员的负担；(3)“信息孤岛”效应明显。种类繁多的网络安全产品通常运行在不同的操作系统上，从不同的侧面单一的、静态的保护着网络的安全，相互之间往往不能兼容和联动操作，缺乏安全信息的共享；(4)缺乏融会贯通的策略管理能力。网络拥有者无法定义并有效实施自己的安全和管理需求，只能被动地盲从新技术和新产品，企业网络不能单靠简单地堆积安全产品，也不能靠产品的缺省配置，而要根据网络的需要，在一个统一的控制界面下，制定相应的安全策略并灵活配置安全组件，以实现在达到“整体”和“动态”安全功能的前提下，使安全集成和性能达到一个良好的集成点。

基于策略的管理(Policy-Based Management, PBM)是网络和健在式管理方面的最新发展，学术界、企业界及标准化组织都认为它是解决大规模分布式的管理问题最有前途的方法，PBM 具有 2 个重要特性：

(1)自动化：预定义的行为可使用预先定义的规则自动执行，不需要管理员的人工干预。减少管理员的负担，并对变化的条件做出快速响应。

(2)抽象性：策略作为系统行为规则的描述，在一定抽象层次上指导系统的行为管理并使其保持一致性。策略的抽象性允许管理员将精力集中在必须的“应该做些什么”上，而不是“怎么才能实现”上；同时，在策略管理系统内使用一种通用的、能应用于网络安全和管理的高级策略语言，就可以实现系统内部的信息共享和协作。

基于策略的一体化网络安全管理就试图利用基于策略的管理方法来改变这种现状。通过该系统，管理者根据安全需求，统一制定安全策略，实现不同类型安全设备间、同类型设备不同产品间的统一配置和安全策略实施；统一的网络安全设备管理实现设备的集成化、集中化管理，各设备间的联动操作由安全事件触发的响应策略自动实施执行。此外，系统引入安全事件关联分析的思想，职责策略指导信息收集代理自动收集各安全设备的安全信息(IDS 告警、防火墙日志等)，应用智能关联技术手段，对网络运行时产生的大量安全信息实施有效分析，以降低漏报率和误报率，并对突发安全事件做出及时有效的响应。

2 策略驱动管理模型

采用策略驱动管理过程摆脱了面向设备的管理模式，提高了安全管理的抽象层次，能屏蔽被管理对象的物理差异，灵活方便地对安全设备进行集中管理；同时，在管理过程中，策略管理和系统执行分离开来，管理员只需对策略进行定义，

基金项目：国家部委基金资助项目
作者简介：韩锐生(1982－)，男，硕士研究生，主研方向：网络信息安全，安全策略系统；赵 彬，博士研究生；徐开勇，研究员
收稿日期：2008-08-04 **E-mail：**hrsgcxqq@sina.com

而不必关心实现该策略的具体细节和相关设备的情况;同时，能根据需求变化的需要而动态改变管理策略，相应地改变系统的行为，无须改动系统的底层实现或中断系统的操作，提高了管理系统的可扩展性和灵活性，增加了系统管理的实时性和自动化程度。

策略驱动的网络安全管理将网络视作一个状态机[2]，而安全管理策略则是控制器和调整网络状态的依据。策略驱动管理模型如图 1 所示。

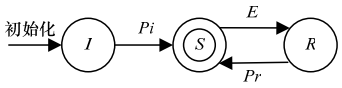

图 1　策略驱动管理模型

其中，状态 *I* 是初始状态；状态 *S* 为终态，也为安全状态；状态 *R* 为危险状态；*Pi* 为管理策略；*E* 为安全事件；*Pr* 为触发的安全响应策略。假如某一时刻处于安全状态，在此状态下，发生了某种安全事件，导致进入一种危险状态，称为安全事件触发。表示为：$A \xrightarrow{E} B$

其中，*A* 为安全状态；*B* 为危险状态；*E* 为安全事件。若某一时刻处于某种危险状态，在此状态下，执行了某种策略，导致进入安全状，称为策略驱动，表示为：$A \xrightarrow{P} B$

其中，*A* 为危险状态，*B* 为安全状态，*P* 为策略或策略集合。

网络状态由初始化的“裸机”状态 *A* 进行相对安全的 *S* 状态，该过程可表示为 $I \xrightarrow{Pi} S$；在安全配置的作用下，各安全产品相互协作，监视网络状况，发现异常情况并形成安全事件，安全事件触发使进行入 *R* 状态，该过程表示为 $S \xrightarrow{E} R$，在相应响应策略的驱动下，实施响应操作，从 *R* 状态转移到 *S* 状态，该过程表示为 $R \xrightarrow{Pr} S$，完成的自动响应、自动恢复。

策略驱动体现了操纵管理过程策略化的观念，在系统中通过响应策略的实施实现了检测与响应的自动化，同时网络的变化、各安全设备的配置变化和各设备间的联动均由策略驱动自动完成。

3　一体化网络安全管理系统设计

要构建一个完备的基于策略的一体化管理系统，不仅要求各异构的安全设备之间共同存在，互相协作，还要有一个集中式的策略管理系统来总体配置、部署和调控这个多层面、分布式的网络设备和安全策略，实现对各种安全设备的集中监控、统一策略管理、安全审计及多种安全功能模块之间的互动，使网络安全管理工作变得简单而有效。

针对上述要求，本文设计实现了一体化网络安全管理系统。系统基于 Ponder 模型[3]，引入基于域管理和安全事件关联分析的思想，实现对被安全设备的集中管理，统一管理配置和各安全设备间的联动协作。系统由管理工具集、策略部署运行设施、安全事件关联模块、被管安全设备集等组成，各模块间关系如图 2 所示。

(1)管理工具集：提供一个图形化的管理员界面，提供资源配置管理、策略管理、网络安全状况显示，允许管理员对安全策略进行定义、存储和运行时管理操作。网络安全状况显示界面，用于显示和查询安全信息和各子的安全状况，并给出网络安全态势图。资源配置管理实现设备的统一配置，集中管理。

(2)策略部署、运行设施：是系统的核心部分，负责系统安全策略的统一定制、分发及自动执行，指导各用户和安全设备的行为，实现管理员的管理意图。该模块包括域服务、策略服务、事件服务及策略实施组件等部分，其核心部分是 3 大支撑服务：域服务，策略服务及事件服务。策略服务用作策略管理的接口，它存储编译好的策略类、创建并分发新的策略对象，策略服务为每个策略对象创建相应的策略控制对象，对策略对象进行运行时管理。域服务用来管理域对象的层次结构并支持运行时主体和目标集的有效性评估，每个域对象包含指向其管理对象的引用及当前应用于域的策略对象的引用；域服务通过 LDAP 目录服务实现。事件服务收集系统事件和系统中被管对象发布的事件，并将它们通知给已预定该事件的策略管理组件，以触发职责策略。

(3)安全事件关联模块：由信息采集代理、安全知识库和关联引擎组成；信息采集代理主要负责收集各安全产品的告警信息和操作日志信息，对所有信息进行标准化、过滤融合等操作；安全知识库包含关联规则库、安全事件库、设备信息库及拓扑信息等，为安全事件关联模块和管理工具集提供及时的和基于历史的数据支持；关联引擎是该模块的核心，以信息采集代理的输出信息为输入，在安全知识库的支持下，利用智能关联算法对网络运行时产生的大量安全信息进行跨边界、跨设备、跨时空的关联分析形成准确的安全事件报告。在安全事件关联模块中主要目的是为减少告警的误报和漏报率，将不同的安全报警信息送入关联模块，进一步进行关联分析，发现新的异常情况和复杂的攻击模式。安全事件关联方法的引入实现了各安全设备间的信息共享，并为实现及时、准确、有效的响应提供了可能。

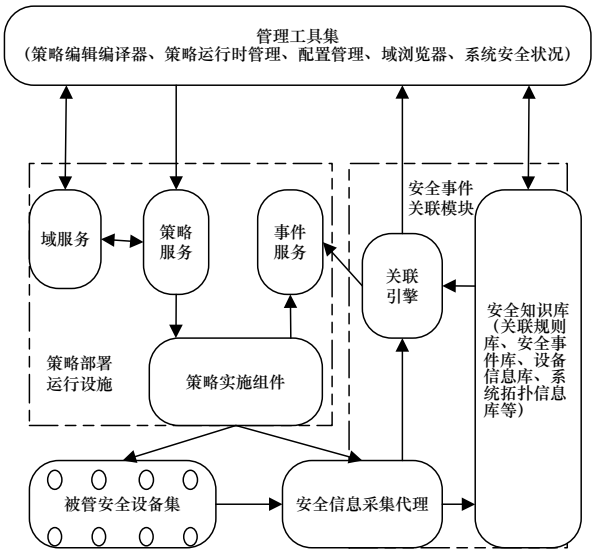

图 2　系统结构

4　系统关键技术的实现

4.1　策略的部署与实施

策略部署是策略管理实现的关键环节，系统中的部署过程无需人工管理策略对象与实施组件间的关联。图 3 显示了策略实例分发过程中涉及的步骤(以序号为顺序)，并展示了系统结构中组件间的相互作用。

除分发策略对象外，PCO 还将策略与策略应用的域对象关联起来。当域发生改变时，域服务能通知 PCO，从而实现对新加入实施组件自动加载策略及自动从实施组件删除不再应用的策略。

管理策略的实施是由事件触发的，是由策略实施代理

PMA 解释执行的。其详细流程见图 4(以序号为顺序执行)。

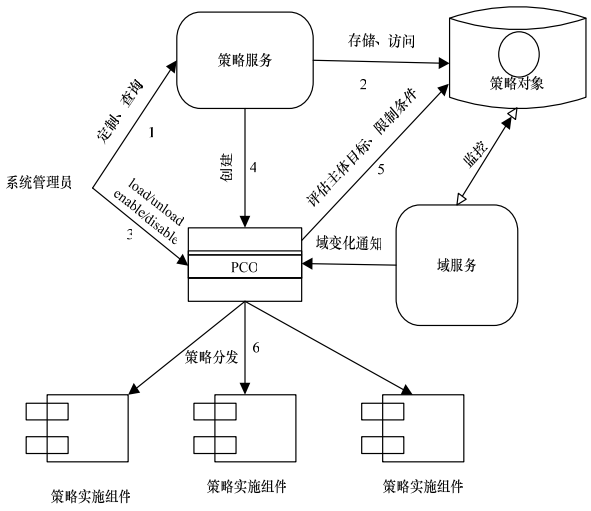

图 3　策略部署流程

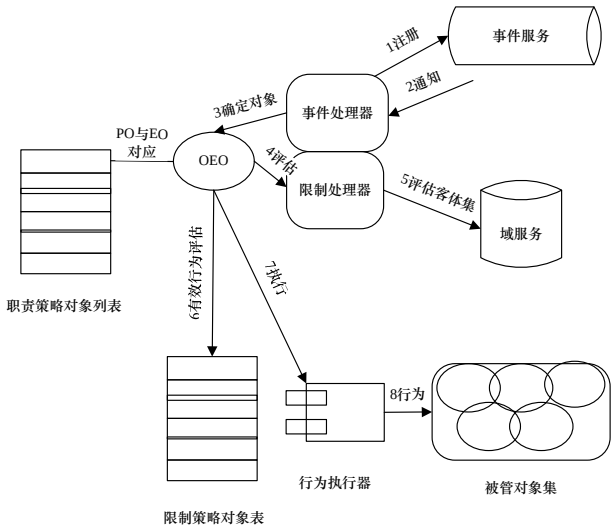

图 4　职责策略实施步骤

4.2　通用事件关联引擎

安全事件关联是指利用安全事件之间、安全事件与网络上下文环境之间的相关性，对安全事件进行有效的分析，从而得到抽象程度更高、可读性更强、更有价值的信息。本文通过综合采用状态机模型、正规表达式匹配、统计分析等技术，实现了满足上述要求的安全事件关联引擎。引擎体系结构如图 5 所示。

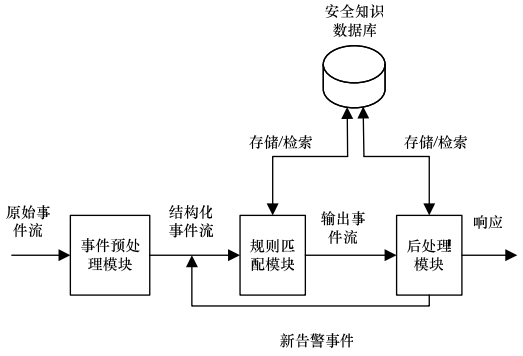

图 5　安全事件关联引擎体系结构

事件关联引擎由 3 个主要模块组成：事件预处理模块，规则匹配模块和后处理模块。事件预处理模块将原始事件流结构化成方便处理的事件对象流。关联模型中要求的各种关联处理都被实现成针对输入事件流的事件查询规则，所有规则匹配都在规则匹配模块中实现。规则模块从事件流中挑选出满足规则的事件信息，作为输出事件流传递给后处理模块中匹配规则对应的后处理模块处理，后处理模块完成事件风险值计算、事件存储、生成新告警、响应等处理，并将新生成的告警重新送回规则匹配模块，以支持嵌套规则。与外部安全知识数据库连接的主要是为了实现事件存储和事件与存储的数据(如策略、历史数据、漏洞信息等)的关联。

本文实现的事件关联引擎能有效实现各种类型的事件关联、过滤、聚合、压缩、滑动时间窗口、滑动事件长度窗口等复杂的事件处理要求，具有高吞吐率、低延迟的特点，满足大数据量的事件流处理的性能要求。规则与 SQL 语句类似，方便动态扩展。

4.3　策略驱动联动响应

安全设备间的联动控制是管理系统的一项关键技术，它能自动协调和管理不同安全设备的行为，达到优势互补，最大化安全设备性能；同时也可以实现主动、自动的响应，如自动应急响应预案、自动阻断攻击源等，最小化网络风险。

笔者利用基于策略驱动的管理思想，实现一个通用的联动控制框架，如图 6 所示。

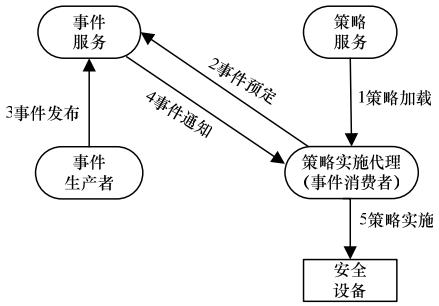

图 6　通用联动控制框架

以“自动阻断攻击源”策略为例来介绍联动框架的具体工作流程，如图 7 所示。该策略要求当安全事件关联分析模块在确认发生了网络攻击时，通过与网络防火墙联动，实时、自动地阻断攻击源。

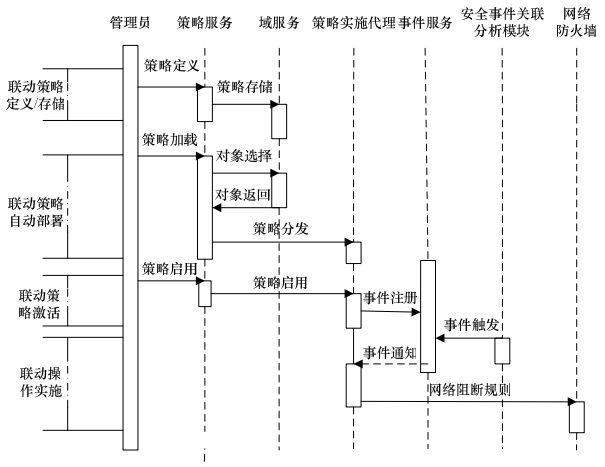

图 7　联动策略交互过程

其中，安全事件关联分析模块是事件生产者，防火墙策

略实施代理是事件消费者，网络防火墙是最终执行网络阻断的安全设备。管理员只需通过策略管理 GUI 定义、加载和启动联动策略，而其余所有操作都由联动控制框架自动完成。

本文实现的基于策略驱动的联动控制框架能实现安全设备间的自动联动控制和管理，大大减少了管理员的工作量，提高管理效率；同时，该框架能最大化各类安全设备的性能，实现优势互补；通过该框架还实现了自动应急响应预案、自动阻断攻击源等主动响应管理，将网络风险降低到最小。

5 系统运行分析

策略部署、运行设施是该系统的核心，它分别与部署在防护模块、检测模块和响应模块的 PMA 进行通信，如图 8 所示。

本文使用 Java RMI 机制实现远程通信和分布式操作。系统安全管理员统一定制安全策略模板，自动分发给各相应模块的 PMA，当中心事件服务收到安全事件后，触发部署在 PMAs 上的策略模板，策略模板指导响应模块进行攻击响应和系统恢复，并对防护模块进行新安全措施的部署，同时对检测模块加强检测规则配置，如果相当一段时间内攻击现象不在发生，策略管理中心可停止策略模板的响应措施，并记录系统当前的安全状态，向系统安全管理员进行报告。

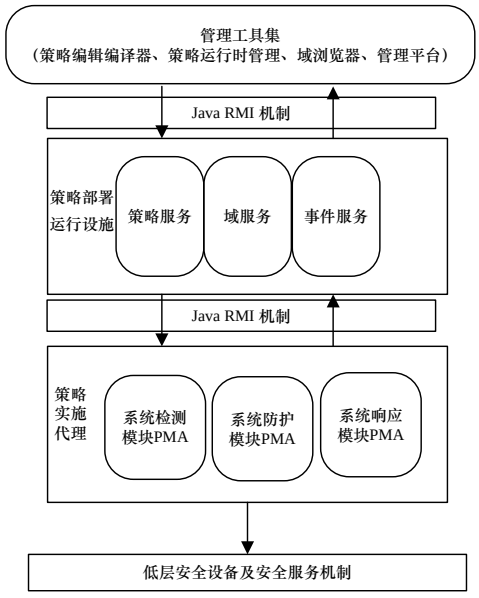

图 8　一体化网络安全管理系统

以简单 Web 服务攻击防御为例来介绍系统的运行细节。当检测模块检测到一个 Web 攻击时，并向策略管理中心告警，告警信息进入安全事件关联引擎，计算告警的严重度与可能性，并重新配置信息收集器以获得更多的攻击特征，从而减少误报率。如果攻击的可能性和严重度很高，则事件服务通过事件通知接口通知响应模块的 PMA 触发相应的响应机制。针对 Web 服务攻击，有效的响应机制应该包括以下几个步骤：(1)向安全管理员报警；(2)关闭攻击源和受害对象的 TCP 连接；(3)重新配置防火墙规则，拒绝所有来自攻击源的连接请求；(4)重新配置检测模块的检测规则，挖掘告警的上下文信息，获得更多的攻击特征。下文给出一个响应预案的例子。

```
Inst oblig /SMPolices/signatureBasedAlertRe {
on      WebAttack(attackSignature, confidence);
subject /PMA/SM;
do      getRisk(attackSignature)->
alert(attackSignature)->generateEvent(AlertRespond,attack
Signatue)->generateEvent(reConfigFW,attackSignature);
when    confidence >MIN_CONFIDENCE;}
Inst oblig /SMPolices/signatureBasedAlert {
on      WebAttack(attackSignature, confidence);
subject         /PMA/SM;
target          t=/PMA/DM;
do    t.reConfigureDM(DecRules)->
t.getContext(attackSignature);
when    confidence <MIN_CONFIDENCE;
}
Inst oblig /SMPolices/signatureBasedAlertFW
{   on          reConfigFW (attackSignature);
subject         /PMA/PM;
target          t=/PMA/FW;
do              t.deny(attackSignature);
}
```

6 结束语

本文针对当前安全管理方面的不足，设计并实现了基于策略驱动的一体化网络安全管理系统，系统引入策略管理的思想和安全事件关联分析方法，统一安全策略管理实现了产品的统一配置和自动管理，提高了系统的可扩展性和灵活性；安全事件关联分析实现了各产品间的信息高度共享，提高了的检测能力，实现了准确快速的安全响应。本系统具有如下特点：

(1)将基于策略的管理思想应用于网络安全管理中，摆脱了传统的面向设备的管理模式，为网络安全管理提供了新颖、有效的方法支持。

(2)设计实现了一体化网络安全管理系统，提供管理策略的统一定义、自动分发、自动实施，安全事件智能关联分析，能有效处理网络运行时产生的大量安全信息(事件)，显著降低检测系统的漏警和误警率，以及策略驱动的安全设备联动，能对突发安全事件做出及时有效的自动响应。

在原型中已实现了对 snort 和 netscreen 的统一管理和联动响应，下一步的研究方向是实现对不同种类的安全产品进行统一安全策略定制，统一分发，自动管理，真正实现系统设计的预期目标。

参考文献

[1] Oltsik J. Network Security: Past, Present & Future[Z]. Information Security Enterprise Strategy Group, 2004.

[2] 张少俊, 李建华, 郑明磊. 基于策略的网络管理[J]. 计算机工程, 2003, 29(16): 127-129.

[3] Damianou N. A Policy Framework for Management of Distributed Systems[D]. London, UK: London University, 2002.

编辑　金胡考