<<Cisco ASA、PIX与FWSM >

图书基本信息

书名：<<Cisco ASA、PIX与FWSM防火墙手册>>

13位ISBN编号：9787115218612

10位ISBN编号：7115218617

出版时间：2010-4

出版时间：人民邮电出版社

作者：赫本

页数：627

前言

当今的网络要求能将数据、语音、视频会议、无线通信及更多方面的内容安全传输到诸如雇员、供应商、合作伙伴和客户之类的广泛用户。
保护网络的安全已经成为一项极为重要的任务，应能保证“无处不在的连接”不会受到网络上未验证访问、滥用或攻击风险的影响而正常地运行。
当各种数量庞大的安全技术应用到安全网络和终端问题上时，具有长期可靠性的防火墙仍然是所有安全部署的核心部分。
防火墙继续承担主要的网守任务，确保所有从第2层到第7层的网络流量经合法验证、授权后传输到网络。
有关网络安全和防火墙的许多书籍主要关注的是概念和理论。
然而本书的内容远远超出了这些主题，它涵盖了每个网络和安全管理员在配置和管理包括PIX和ASA安全设备以及Catalyst防火墙服务模块在内的Cisco市场领先防火墙产品时，需要了解的大量细节信息。
正如书名提示的那样，本书是一个实用的用户手册，提供对初始配置，更重要的是对Cisco防火墙日常管理的深入解释。
本书对如何成功配置防火墙包括建立访问控制策略、验证终端用户、调节高可用性部署、通过大量管理界面监控防火墙健康在内的所有方面，提供了日常的实践指导。
本书的作者，CCIE David Hucaby在充当肯塔基大学（University of Kentucky）管理Cisco防火墙的首席网络工程师之余，还花费了相当多的时间直接与负责这些产品的Cisco工程小组协作，确保本书涵盖了深入、实用、最新的可用信息。
将本书放在手边——你会发现经常需要参考它！

<<Cisco ASA、PIX与FWSM >

内容概要

在网络威胁泛滥的今天，利用防火墙技术保护网络的安全已经成为一项极为重要的任务。本书主要内容包括防火墙概述和配置基础、防火墙管理和用户管理、通过防火墙的控制访问、检测流量、使用故障切换增强防火墙的可用性、防火墙负载均衡、防火墙日志、验证防火墙运行、ASA模块等内容，附录部分还对通用协议和端口号、安全设备日志消息进行了介绍。

本书适合网络管理员、防火墙安全工程师(或顾问)、对防火墙相关技术感兴趣的初学者阅读。

作者简介

David Hucaby，CCIE NO.4594，肯塔基大学杰出的网络工程师，致力于以Cisco Catalyst、ASA、FWSM和VPN产品线为基础的网络维护，曾是ASA 8.0操作系统beta版的审查者之一，拥有肯塔基大学的电气工程学士和硕士学位，曾出版过3本思科教材：《CCNP BCMSN Official Exam Certificatior Guide》、《Cisco Field Manual：Router Configuration》和《Cisco Field Manual：Catalyst Switch Configuration》。现与妻子Marci和两个女儿一起居住在肯塔基。
技术支持Greg Abelar，从1996年11月至今，一直受雇于Cisco。
他是Cisco技术支持安全团队的创始人之一，协助聘用并培训了众多工程师。
他在Cisco安全架构和安全技术营销工程团队中担任多个职务。
他是Cisco发起的CCIE安全笔试的主要奠基人和项目管理者，曾出版过Cisco教材《Securing Yom Business with Cisco ASA and PIX Firewalls》，与他人合作出版过《Security Threat Mitigation and Response：Understanding Cisco Security MARS》，并为多本Cisco出版的安全类教材担任技术编辑。

<<Cisco ASA、PIX与FWSM >

书籍目录

章节摘录

插图：当开始考虑安全策略并着手配置防火墙时，必须牢记几件事情。
这一小节讲解了保护网络的经验法则，而不是长篇累牍地介绍安全策略和如何防范漏洞和攻击。
如果遵循这些建议，就能够配置防火墙使其提供最佳的防护。
·定期收集并查看防火墙日志在配置防火墙之后，可以根据正确的安全策略通过简单测试来查看防火墙是否阻止或允许对安全资源进行访问。
然而，如果不查看允许或拒绝的流量记录，就没有简易的方法来观察拒绝服务或蠕虫攻击。
防火墙会产生大量的日志信息。
这些数据通过可以胜任的系统日志服务器来收集。
也应该定期查看系统日志数据，从中可以发现新的恶意活动或暴露出忘记关闭的敏感端口的使用。
保存防火墙日志最重要的原因是对网络活动的审计跟踪。
如果遭受了攻击或者网络资源的恶意使用，可以依据系统日志记录来作为证据。
·制定精确的入站ACL必须严格控制流量从公共网络或者不安全的方面进入到受保护网络。
例如，如果要对公司Web或者E-mail服务器提供公共访问，一定要确定只允许开放那些特定协议和端口。
否则，如果让入站访问过于宽泛或开放，就会增加有些人设法利用意想不到的协议或服务的机会。
此外，最佳做法建议任何入站访问必须止于中立区（DMZ，demilitarized zone）防火墙接口上的主机，而不是内部网络中的主机。
至于出站流量控制，内部（受保护的）用户通常是已知的和受信任的。
可以开放出站访问，但最佳做法建议配置出站访问列表，以防止内部网络的主机参与针对DMZ或外部网络的蠕虫或攻击。
也可以使用出站访问列表来实施公司政策，来限制或禁止某些行为或控制非授权服务的访问。
防火墙也可以对出站用户进行访问验证，并与外部服务器联动控制网页内容。
·在不同方面保护DMZ如果向公共网络提供公司资源，通常最好放在DMZ中。
这是一个在防火墙接口上的小型网络，具有中级安全级别。
外部或者公共网络的用户可利用指定协议和端口来访问DMZ上的服务器。
谨慎配置DMZ接口上的安全策略。
确保外部用户只能允许访问必需的指定协议，然后保证DMZ接口的设备仅能通过传输数据的协议访问内部（可靠的）主机。
例如，假设有一个公共Web服务器使用HTTP提供信息服务。
这个Web服务器需要向内部网络的其他数据中心服务器发送SQL请求来填充其网页。
对于DMZ，应该配置防火墙允许外部只能使用TCP端口80（HTTP）来访问Web服务器。
此外，应该允许DMZ服务器向内部数据中心只能发送SOL数据包，而不是别的。
如果在DMZ服务器和内部区域之间开放访问（任何协议或端口号），DMZ区就会成为一个“跳板”，使外部的恶意用户能够危害DMZ服务器，并使用它来危害内部区域的其他主机。

媒体关注与评论

“ 许多网络安全和防火墙方面的图书仅仅满足于用大量的篇幅去讨论相关的概念和原理，但是本书却超越了这样的界限。
它对网络和安全管理员在配置和管理Cisco的市场领先的防火墙产品时，所要知道的一切知识进行了全面详细的讲解。
” ——Jason Nolet，工程副总裁，安全技术团队，Cisco

编辑推荐

《Cisco ASA、PIX与FWSM防火墙手册(第2版)》是一本实施当前流行的Cisco防火墙安全解决方案常见特性的指南。
涵盖了最新的防火墙版本，能够帮助你轻松快速地配置、集成和管理全系列Cisco防火墙产品，这包括ASA、PIX和Catalyst防火墙服务模块（FWSM）。
《Cisco ASA、PIX与FWSM防火墙手册(第2版)》按照特性族进行组织。
能够帮助你快速有效地掌握诸如文件管理、连通性的建立、控制访问、防火墙管理、利用failover特性增强可用性，负载平衡、记录日志和验证操作等主题。
书中有些段落用带阴影的标签标注。
供快速参考所用。
每一个特性的信息都以一种简捷的格式列出，这包括背景、配置和实例组件。
无论你是在寻找最新的ASA、PIX和FWSM设备的介绍。
还是在寻找Cisco防火墙部署的完整参考，《Cisco ASA、PIX与FWSM防火墙手册(第2版)》都能够帮助你实现对网络资源的最大保护。
·学习不同的防火墙模型、用户界面、特性集以及配置方法：·理解Cisco防火墙如何检测流量；·配置防火墙接口、路由、IP寻址服务和IP组播支持；·维护安全context、flash和配置文件，管理用户，使用SNMP监视防火墙；·对防火墙用户进行认证、授权，并维护审计记录；·通过部署透明模式和路由模式的防火墙、地址转换以及流量回避（shun）对穿越防火墙的访问进行控制；·以模块化的策略框架定义可识别并作用于不同流量类型的安全策略；·利用防火墙的failover特性提高防火墙的可用性；·理解防火墙负载平衡的工作原理；·生成防火墙行为日志，并学习如何分析日志内容；·对防火墙的操作和连通性进行验证并对“穿越”防火墙的数据进行研究；·配置安全服务模块，如内容安全控制（CSC）模块和高级检测处理器（AIP）模块。
《Cisco ASA、PIX与FWSM防火墙手册(第2版)》属于Cisco Press网络技术图书中的安全类别。
Cisco Press出版的安全图书可以帮助网络专业人员保护关键的数据和资源，阻止和缓解网络攻击。
以及构建端到端的自防御体系。

版权说明