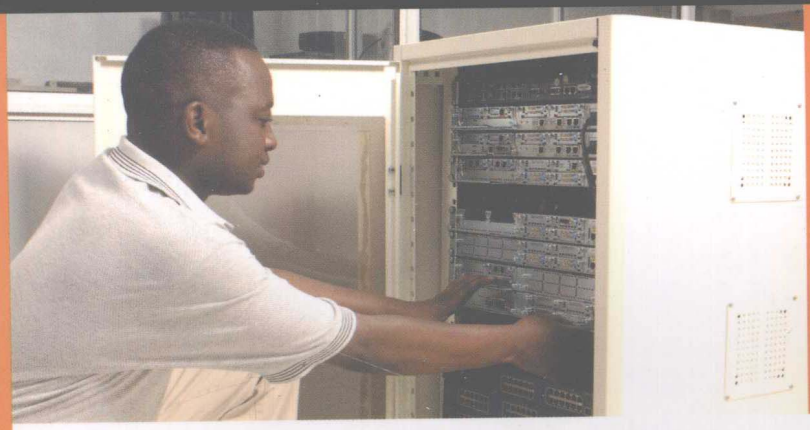
CISCO

ciscopress.com



SECURITY

路由器安全策略

Router Security Strategies

Securing IP Network Traffic Planes

Segment and protect traffic in the data, control, management, and services planes

〔美〕 Gregg Schudel，CCIE #9591
David J. Smith，CCIE #1986 著

姚维 李斌 沈金河 译

人民邮电出版社
POSTS & TELECOM PRESS

路由器安全策略

Router Security Strategies

Securing IP Network Traffic Planes

〔美〕 **Gregg Schudel**，CCIE #9591
David J. Smith，CCIE #1986 著

姚维 李斌 沈金河 译

人民邮电出版社

北京

图书在版编目（CIP）数据

路由器安全策略／（美）舒德尔（Schudel，G.），（美）史密斯（Smith，D. J. ）著．姚维，李斌，沈金河译．—北京：人民邮电出版社，2008.9
ISBN 978-7-115-18591-4

Ⅰ．路… Ⅱ．①舒…②史…③姚…④李…⑤沈… Ⅲ．计算机网络—路由选择—安全技术 Ⅳ．TN915.05

中国版本图书馆 CIP 数据核字（2008）第 115520 号

版 权 声 明

路由器安全策略

◆ 著 [美] Gregg Schudel, CCIE#9591
David J. Smith, CCIE#1986
译 姚 维 李 斌 沈金河
责任编辑 付 飞

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号
邮编 100061 电子函件 315@ptpress.com.cn
网址 http://www.ptpress.com.cn
北京顺义振华印刷厂印刷

◆ 开本：787×1092 1/16
印张：29
字数：728 千字 2008 年 9 月第 1 版
印数：1－4 000 册 2008 年 9 月北京第 1 次印刷

著作权合同登记号 图字：01-2008-3327 号
ISBN 978-7-115-18591-4/TP

定价：69.00 元

读者服务热线：(010)67132705 印装质量热线：(010)67129223
反盗版热线：(010)67171154

内容提要

本书的目标在于使读者熟悉对IP网络流量平面进行分隔和安全保护所需的概念、效益以及实施细节。全书分 4 个部分。第 1 部分提供了 IP 协议、IP 网络运行及路由器和路由硬件以及软件运行的基本概述。第 2 部分提供了深入、详细的内容以供网络专家实现 IP 流量平面分隔和保护策略，还针对经验不足的网络技术人员提供了详细的 IP 路由器运行描述。第 3 部分提供了针对两种不同网络类型——企业网络和服务提供商网络的案例研究。这些案例研究用于进一步说明在第 2 部分中介绍的策略如何集成为一个完整的 IP 网络流量平面分隔和保护规划。第 4 部分则对本书正文部分所讨论的内容进行了补充，提供了一些不仅在阅读本书过程中有用，而且在日常工作中也很有帮助的参考内容。

本书适合组织机构中负责部署和维护 IP 及 IP/MPLS 网络的网络工程师，以及网络运营和网络安全性人员阅读。

关于作者

Gregg Schudel, CCIE No. 9591 (Security)于2000年作为咨询系统工程师加入Cisco Systems，其职责是为美国的网络服务提供商组织提供支持。Gregg 关注针对长途交换电信运营商、网络服务提供商及移动服务提供商的IP核心网络和服务安全性体系结构和技术。

此外，Gregg还是Corporate and Field资源小组的成员，该小组的工作重点在于推动 Cisco 服务提供商安全性策略。在加入Cisco Systems之前，Gregg在BBN Technologies公司工作了多年，他负责支持与 DARPA 及联邦政府其他机构共同进行的涉及到安全性方面的网络安全性研究和开发。

Gregg 拥有乔治华盛顿大学的工程学硕士学位和获得佛罗里达理工学院的工程学学士学位。

David J.Smith，CCIE No.1986（Routing and Switching）于1995年作为咨询工程师加入Cisco Systems，其职责是为美国的网络服务提供商组织提供支持。David从1999年开始关注服务提供商IP核心和边缘网络技术，包括IP路由、MPLS技术、QoS、架构安全性及网络遥测。在1995～1999年，David负责为企业用户在设计园区 WAN 和全球 WAN 方面提供支持。在加入Cisco Systems之前，David在Bellcore公司工作，负责开发系统软件以及开通ATM交换机试验局。

David在卡内基·梅隆大学获得信息网络硕士学位，在里海大学获得计算机工程学士学位。

关于技术审稿人

Marcelo I.Silva，M.S.是 Cisco Systems 服务提供者技术组（Service Provider Technology Group，SPTG）的技术营销工程师，他是一位在技术领域具有 19 年学术和高技术经验的老手。在加入 Cisco Systems 之前，Marcelo 是一位独立的系统咨询顾问，并且是巴尔的摩马里兰大学的全职讲师。Marcelo 从 2000 年开始他在 Cisco Systems 的职业生涯，在此期间，他与美国的一些大型服务提供商一起设计 IP/MPLS 核心和边缘网络。目前，Marcelo 在 Cisco Systems 的主要职责是作为技术营销工程师（Technical Marketing Engineer，TME），为全球服务提供商在部署 Cisco Systems 的高端路由器 Cisoc 12000 系列（GSR）和 Cisco CRS-1 电信运营商路由系统方面提供咨询和建议。Marcelo 在马里兰大学获得信息系统硕士学位，现和他的妻子 Adriana 和儿子 Gabriel 居住在比利时的滑铁卢市。

Vaughn Suazo，CCIE#5109（Routing and Switching，Security），是 Cisco Systems 针对有线新兴服务提供商（Wireline Emerging Provider）的咨询系统工程师。Vaughn 是一位在服务器技术、LAN/WAN 网络连接及网络安全性方面具有 19 年经验的老手。他在 Cisco Systems 的职业生涯开始于 1999 年，负责与思科的服务提供商客户一起致力于诸如核心网和边缘 IP 网络架构、MPLS 应用、网络安全性和 IP 服务等技术领域的研究。目前，Vaughn 在 Cisco Systems 的主要职责是作为针对服务提供商提供支持的咨询系统工程师（Consulting Systems Engineer，CSE），他的专长在于服务提供商网络安全性及数据中心技术和解决方案。目前 Vaughn 和他的妻子 Terri 和两个儿子现居住在俄克拉何马州的俄克拉何马市，在其业余时间以高尔夫作为娱乐。

献　辞

献给我最好的朋友和美丽的妻子 Carol，感谢她给我的爱和鼓励，也感谢她允许我放弃与家人共享的宝贵时间来专心编写本书。此外还要感谢我的两个孩子 Alex 和 Gary 对我表现出的耐心和理解，以及他们带给我的活力和激情。

感谢我的合作者 David Smith 接受编著本书这一挑战，并感谢他为本书贡献的知识和经验。

——Gregg

我要将本书献给我可爱的妻子 Vickie，以及我出色的孩子 Harry、Devon 和 Edward，他们使我的梦想成真。感谢他们在我编写本书期间对我的支持和鼓励。我还要感谢我的母亲和父亲，他们含辛茹苦地把我和我的兄弟抚养大并让我们有成才的机会。最后，我要感谢我的合作者 Gregg Schudel 给我参与编写本书的机会，这是我一生中不可多得的机会，我将为此永怀感激。

——David

致　谢

本书得益于在IP网络安全性方面与我们进行分享的所有Cisco Systems的工程师，在这些人当中，有几位是我特别需要感谢的。感谢Barry Greene一直以来对我的鼓励、无尽的指导，以及对SP安全性方面的专注。若没有他的付出，本书中的许多IP流量平面安全性概念将不会诞生。此外，我要感谢Michael Behringer，感谢他一直鼓励并对我的许多技术问题提供了宝贵的建议。我还要感谢Roland Dobbins、Ryan McDowell、Jason Bos、Rajiv Raghunarayan、Darrel Lewis、Paul Quinn、Sean Donelan和Dave Lapin，他们自始至终为我的许多问题提供了详细的咨询建议。

我们要感谢本书出色的技术审校者Marcelo Silva和Vaughn Suazo为本书提供全面的意见和反馈。我们还要感谢John Stuppi和Ilker Temkir很有价值的评审意见，以及Russell Smoak的指导。感谢Dan Hamilton、Don Heidrich、Chris Metz、Vaughn Suazo和Andrew Whitaker对我们最初的计划所给出的宝贵建议。还要特别感谢Cisco Systems副总裁和首席安全官John Stewart，他从自己宝贵的日程中抽出时间来为本书撰写了前言，也感谢他在安全性和网络运营等领域的卓越领导。

感谢我们的经理Jerry Marsh和Jim Steinhardt，他们在本书编写过程中给予了我们极大的支持。

最后，特别感谢Cisco出版公司和本书的制作团队，他们是Brett Bartow（执行编辑）、Eric Stewart（开发编辑）、San Dee Phillips（高级项目编辑）、Jennifer Gallant（项目编辑）和Bill McManus（文字编辑）。还要感谢Andrew Cupp（开发编辑）提供的编辑支持。感谢你们和我们一起付出的努力使得本书得以出版。

序

在过去 20 年来，网络从 archane（ARPAnet）发展到任何地方（无线热点），并且已经被应用于卫生保健系统、航空、商业、视频通信、电话、存储和交互式运动等诸多领域。

网络来源于数据中心，然后到达服务提供商，到达我们的邻居，到达我们的家里。对我而言，说网络安全是一个“重要的主题”无论如何都不过分，因为主机安全无法和它相提并论——网络安全需要花费很大的开销，而主机安全则花费甚少。为什么会是这种情况，为什么会发生这种情况呢？

在此，我并不想正面回答这个问题，之所以承认网络安全至关重要，是因为网络现在是必不可少的。因此，本书包括了那些针对网络设备的现有威胁和攻击的知识，对这些威胁和攻击提供最佳防范的必要的网络设备配置技术，以及这些技术如何提高网络恢复能力的现实例子，以供读者学习。

Gregg 和 David 编写的这本图书将其篇幅划分为数据、管理和业务平面安全，解释了每种流量平面的概念、相关的安全威胁及对策。对所有 4 种流量平面提供保护对于网络设备的保护是必需的，对于保护由这些网络设备组成的网络则更是必需的。对所有这 4 种彼此不同的流量平面进行不遗余力的保护是惟一正确的做法。

如果读者在阅读本书之后什么都没有做，那么询问自己，在对数据进行保护的同时，是否已经对自己日益依赖的数据、业务及功能不断丰富的网络进行了保护？经验告诉我们当中的每一个人，深入防御和广泛防御都属于强有力的安全技术。您的网络是由多种设备、多个层次组成的，并且其触角几乎无处不在——网络自身已经在保护您的网络中扮演了关键角色。要确保它是成功的，毕竟……我们都连接在一起。

Cisco Systems 副总裁，首席安全官

John Stewart

前　言

网络世界正在飞速地发生着变革。以前基于时分复用（TDM）技术、帧中继以及异步传输模式（ATM）技术构建的旧式网络正在被无所不在的、基于网际协议（IP）包的网络所替代，后者可以支持融合的网络服务。由于财力和人力所限，服务提供商无法同时部署只支持单一应用或服务，例如语音、业务数据或互联网流量的多个网络。以这种业务模式来部署和运营多个网络的成本在财务上是难以为继的。此外，客户对集成业务和应用，以及新业务和应用的需求，意味着服务的快速提供成为了现代网络架构中的关键需求。目前全球的有线和无线服务提供商正在将它们原有的网络业务移植到 IP 核心网络，以充分利用 IP 网络所提供的带宽效率和可伸缩性，以及 IP 网络可支持快速扩展新兴业务的能力。

构建和运营可以满足客户需求，同时又可以支持多种不同业务（这些业务对带宽、抖动及延时具有各自不同的需求）的电信运营商级 IP 网络架构是一个富有挑战性的任务。以前单一用途的网络在设计和构建时只支持特定的、单一的运营模式。在一个公共的 IP 骨干网络上承载互联网流量、语音流量、移动电话流量及 VPN 业务数据流对于网络设计和网络安全性提出了更高的要求。例如，在任意一种流量业务中遭遇的网络攻击都有可能使整个“公共网络”瘫痪，这种牵一发而动全身的特点导致部分业务会对整个网络营收产生影响。此外，企业也日益依赖 IP 网络来满足自己的业务运营要求。

从基本上而言，任何网络都具有两种类型的包：数据包（data packet）、控制和管理包（control and management packet）。数据包属于客户所有并负责承载客户流量，控制和管理包属于网络本身，并且用于网络运营。IP 协议的一个优点是：所有这些包通过一个“公共管道”（或称为“带内”方式）来传输。那些出身于原有 TDM/ATM 网络领域的网络专家可能不熟悉这一同时承载数据流和控制流的公共管道，

因为这些原有的系统是将数据通道和控制通道（“带外”通道）分开的。他们常常会对如何在同一个网络中对数据包和控制包进行分隔并提供安全保护产生误解。

此外，即使 IP 网络能够以带内方式传递所有的包，对这些不同类型的包进行区分仍然显得很重要。将流量分为数据、控制、管理及业务平面（称为流量平面）并且对这些流量平面进行相应的分隔和保护，这对于当前高度融合的 IP 网络提供安全保护是一个必须完成的任务。本书是第一本全面、正式地对 IP 网络流量平面分隔和安全保护专门进行介绍的图书。

目标和方法

本书的目标在于使读者熟悉对 IP 网络流量平面进行分隔和安全保护所需的概念、效益以及实施细节。其中包括对 IP 网络所面临的诸多威胁，以及可用于减轻这些威胁的许多技术的概述。此外，本书还介绍了深入而且广泛的防御策略来强调各种 IP 流量平面安全性技术之间的交互。本书还从数据、控制、管理和业务平面的角度，从 IP 网络运营这一级别进行了细致的分析，这些内容构成了随后所描述示例的安全性原则和配置基础。此外，本书中的案例研究进一步说明了如何根据既有深度又有广度的原则，对 IP 流量平面保护方法的选择进行优化以提供有效的安全性。

本书的读者对象

本书的读者对象是组织机构中负责部署和维护 IP 及 IP/MPLS 网络的网络工程师，以及网络运营和网络安全性人员。主要读者群是那些涉及 IP 网络日常设计、工程施工和运营的工程师，此外，那些使用基于 IP 或 IP/MPLS 网络业务的用户也可以从本书中受益。其次，本书的读者还包括那些网络背景不是很强，但是希望对 IP 网络流量平面分隔和安全性等方面的问题和需求进行了解的人。本书还对 IP 路由器的运行以及网络连接技术提供了详细介绍，无论是高级网络专家还是经验不足的新手都可以从中受益。

本书的组织结构

对于那些尚不熟悉 IP 网络安全性概念，尤其是不了解 IP 流量平面分隔和保护概念的读者，应当逐页阅读本书。如果读者已经了解了 IP 网络、协议、网络设计和运行，则可以阅读自己感兴趣的章节。本书分为 4 个部分，描述如下。

第 1 部分讲述了 IP 协议、IP 网络运行及路由器和路由硬件以及软件运行的基本概念。本部分介绍了 IP 流量分隔和安全性的概念。在本部分的结尾，读者将可以从更高的层面来理解 IP 流量平面分隔和保护涉及到的内容。本部分包括以下章节。

- 第 1 章讨论了 IP 协议的基础，并从路由和交换硬件及软件的角度介绍了 IP 网络的基本方面。然后以此作为上下文背景来介绍 IP 网络流量平面的概念。
- 第 2 章指出了在每种 IP 网络流量平面中针对路由和交换环境的威胁模型。通过以这种方式来评估这些威胁，读者可以了解到为什么需要对 IP 流量平面进行保护，以及需要防范何种类型的攻击。

- 第 3 章概述了每种 IP 流量平面，并介绍了如何使用既有深度又有广度的策略来用于防范，以提供强大的网络安全。

第 2 部分讲述了深入、详细的内容以供网络专家实现 IP 流量平面分隔和保护策略。对于经验不足的网络人员，本部分还提供了详细的 IP 路由器运行描述。本部分包括以下章节。

- 第 4 章集中介绍数据平面和相关的安全性机制。数据平面是这样一个逻辑实体，它包含了主机、客户端、服务器及那些只使用网络作为传输方式的应用所生成的所有用户数据流。
- 第 5 章集中介绍控制平面和相关的安全性机制。控制平面是这样一个逻辑实体，它与那些路由协议进程和功能相关联，这些路由协议进程和功能用于创建和维护与网络运行状态，包括转发拓扑有关的必要智能。
- 第 6 章集中介绍管理平面和相关的安全性机制。管理平面是这样一个逻辑实体，它描述了所有用于访问、管理和监视针对所有提供、维护和监视功能的那些网元的数据流。
- 第 7 章集中介绍了业务平面和相关的安全性机制。业务平面是这样一个逻辑实体，它包括了那些接收基于网络的具体业务的用户数据流，这些用户数据流不仅仅需要传统的转发处理，还需要进一步的特殊处理来针对不同的业务类型施加或应用预期的策略。

第 3 部分对两种不同网络类型（企业网络和服务提供商网络）进行了案例研究。这些案例研究用于进一步说明在第 2 部分详细讨论的组成部分如何集成为一个完整的 IP 网络流量平面分隔和保护规划。本部分包括以下章节：

- 第 8 章“企业网络案例研究”：使用两个基本的企业网络环境——基于互联网的 IPsec VPN 设计以及 MPLS VPN 设计——来说明如何应用针对企业的 IP 网络流量平面分隔和保护概念。这些案例研究分别着眼于互联网边缘路由器和客户端边缘（CE）路由器来介绍 IP 流量平面安全性概念。
- 第 9 章“服务提供商网络案例研究”：使用与第 8 章所用案例研究相同的拓扑结构，但却是从服务提供商网络的角度来加以描述。在本章中，研究了两个位于服务提供商网络的边缘路由器配置——一个针对基于互联网的 IPsec VPN 设计案例，一个针对 MPLS VPN 案例——从而说明如何应用针对服务提供商的 IP 网络流量平面分隔和保护概念。

第 4 部分附录则对本书正文部分所讨论的内容进行了补充，这部分提供了一些不仅在阅读本书过程中有用，而且在日常工作中也很有帮助的参考内容。附录部分包括以下章节。

- 附录 A“复习题答案”：提供了每章复习题的答案。
- 附录 B“IP 协议报头”：介绍了针对一些常用 IP 网络协议的报头格式，并且说明了针对每种报头字段的安全性含义以及可能的非正常使用情况。
- 附录 C“Cisco IOS 到 XOS XR 安全性过渡”：提供了在常用的 IOS 12.0S 安全性相关配置命令和各自对应的 IOS XR 配置命令之间的一对一映射。
- 附录 D“安全事故处理”：概述了安全事故处理技术，并提供了一个常用的安全事故处理组织列表。

本书中使用的图标

命令语法约定

本书中用于介绍命令语法的约定和 IOS 命令参考中使用的约定相同。命令参考手册中使用的约定说明如下：

- **黑体**表示按照字面所示所输入的命令和关键字。在实际的配置示例和输出（不是通常的命令语法）中，黑体表示了用户手工输入的命令（例如 **show** 命令）。
- *斜体*表示用户为某个实际值所提供的参数。
- 竖线（|）负责分隔可选的、互斥的元素。
- 方括号（[ ]）表示可选元素。
- 花括号（{ }）表示一个必需的选项。
- 方括号中的花括号（[{ }]）表示某个可选元素中的一个必需的选项。

目　录

第 1 部分

第 1 章　互联网协议操作基础……3

1.1　IP 网络概念……3
1.1.1　企业网络……5
1.1.2　服务提供商网络……6
1.2　IP 协议操作……8
1.3　IP 流量概念……13
1.3.1　过境 IP 包……14
1.3.2　接收—邻接 IP 包……15
1.3.3　异常 IP 和非 IP 包……15
1.4　IP 流量平面……17
1.4.1　数据平面……18
1.4.2　控制平面……19
1.4.3　管理平面……21
1.4.4　服务平面……22
1.5　IP 路由器包处理概念……24
1.5.1　进程交换……26
1.5.2　快速交换……29
1.5.3　思科特快转发……33
1.6　常见的 IP 路由器体系结构类型……37
1.6.1　集中式的基于 CPU 的体系结构……37
1.6.2　集中式的基于 ASIC 的体系结构……39
1.6.3　分布式的基于 CPU 的体系结构……40
1.6.4　分布式的基于 ASIC 的体系结构……42
1.7　小结……46
1.8　复习题……46
1.9　延伸阅读……46

第 2 章　IP 网络的威胁方式……49

2.1　对于 IP 网络基础设施的威胁……49
2.1.1　资源消耗攻击……50
2.1.2　欺骗攻击……57
2.1.3　传输协议攻击……58
2.1.4　路由协议威胁……62
2.1.5　其他 IP 控制平面威胁……63
2.1.6　未经授权的接入攻击……65
2.1.7　软件漏洞……65
2.1.8　恶意网络监测……66
2.2　针对第 2 层网络基础设施的威胁……67
2.2.1　CAM 表溢出攻击……68
2.2.2　MAC 欺骗攻击……68
2.2.3　VLAN 的跳跃攻击（VLAN Hopping Attacks）……69
2.2.4　专用 VLAN 攻击……71
2.2.5　STP 攻击……72
2.2.6　VTP 攻击……72
2.3　针对 IP VPN 网络基础设施的威胁……72
2.3.1　MPLS VPN 威胁模式……73
2.3.2　针对用户边缘的威胁……74
2.3.3　针对运营商边缘的威胁……75
2.3.4　针对运营商核心的威胁……77
2.3.5　针对跨运营商边缘的威胁……78
2.3.6　IPSec VPN 的威胁模式……82
2.4　小结……84
2.5　复习题……84
2.6　延伸阅读……85

第 3 章　IP 网络流量平面安全概念……89

3.1　全方位防御的原则……89

3.1.1 理解全方位的防御概念……90
3.1.2 IP 网络流量平面：全方位的防御……94
3.1.3 网络接口类型……96
3.2 网络边缘安全概念……101
3.2.1 互联网边缘……101
3.2.2 MPLS VPN 边缘……103
3.3 网络核心安全概念……105
3.3.1 IP 核心……105
3.3.2 MPLS VPN 核心……106
3.4 小结……107
3.5 复习题……107
3.6 延伸阅读……108

第 2 部分

第 4 章 IP 数据平面安全性……113

4.1 接口 ACL 技术……113
4.2 单播 RPF 技术……120
4.2.1 严格 uRPF……120
4.2.2 松散 uRPF……123
4.2.3 VRF 模式 uRPF……125
4.2.4 可行性 uRPF……127
4.3 灵活的数据包匹配……128
4.4 QoS 技术……130
4.4.1 排队……130
4.4.2 IP QoS 数据包着色（标记）……131
4.4.3 速率限制……132
4.5 IP 选项技术……133
4.5.1 禁用 IP 源路由……134
4.5.2 IP 选项选择性丢弃……134
4.5.3 用于过滤 IP 选项的 ACL 支持……135
4.5.4 控制平面管辖……136
4.6 ICMP 数据平面减缓技术……136
4.7 禁用 IP 直接广播……138
4.8 IP 健康检查……139
4.9 使用 QPPB 的 BGP 策略增强……140
4.10 IP 路由技术……143
4.10.1 IP 网络核心基础结构隐藏……143
4.10.2 IP 网络边缘外部链接保护……144
4.10.3 远程触发黑洞过滤……148
4.11 IP 传输和应用层技术……153
4.11.1 TCP 截取……153
4.11.2 网络地址转换……154
4.11.3 IOS 防火墙……156
4.11.4 IOS 入侵预防系统……157
4.11.5 通信清洗……158
4.11.6 深度数据包检查……158
4.12 第 2 层以太网安全技术……159
4.12.1 端口安全性……159
4.12.2 基于 MAC 地址的通信阻塞……160
4.12.3 禁用自动主干……160
4.12.4 VLAN ACL……161
4.12.5 IP 来源守卫……162
4.12.6 专用 VLAN……162
4.12.7 通信风暴控制……163
4.12.8 未知单播流阻塞……163
4.13 小结……163
4.14 复习题……164
4.15 延伸阅读……164

第 5 章 IP 控制平面安全性……169

5.1 禁用未使用的控制平面服务……169
5.2 ICMP 技术……170
5.3 选择性数据包丢弃……171
5.3.1 SPD 状态检查……172
5.3.2 SPD 输入队列检查……174
5.3.3 SP 监视和优化……175
5.4 IP 接收 ACL……177
5.5 控制平面管辖……185
5.5.1 CoPP 配置指导原则……187
5.5.2 特定于平台的 CoPP 实现细节……199
5.6 邻居身份验证……206

5.6.1 MD5 身份验证……207
5.6.2 一般化的 TTL 安全机制…210
5.7 特定于协议的 ACL 过滤器……212
5.8 BGP 安全技术……214
5.8.1 BGP 前缀过滤器……214
5.8.2 IP 前缀限制……216
5.8.3 AS 路径限制……216
5.8.4 BGP 正常重启……217
5.9 第二层以太网控制平面安全…218
5.9.1 VTP 身份验证……218
5.9.2 DHCP 偷窥……219
5.9.3 动态 ARP 检查……221
5.9.4 粘性 ARP……223
5.9.5 跨越树协议……223
5.10 小结……224
5.11 复习题……225
5.12 延伸阅读……225

第 6 章 IP 管理平面安全性……229

6.1 管理接口……230
6.2 密码安全……232
6.3 SNMP 安全……234
6.4 远程终端访问安全……236
6.5 禁用未使用的管理平面服务…238
6.6 禁用空闲的用户会话……241
6.7 系统标志……242
6.8 安全的 IOS 文件系统……244
6.9 基于角色的 CLI 访问……245
6.10 管理平面保护……248
6.11 身份验证、授权和计账……250
6.12 自动安全……252
6.13 网络遥测和安全……253
6.14 针对 MPLS VPN 的 VPN 管理……256
6.15 小结……261
6.16 复习题……261
6.17 延伸阅读……262

第 7 章 IP 服务平面安全性……265

7.1 服务平面概述……265
7.2 服务质量……267
7.2.1 QoS 机制……268
7.2.2 保护 QoS 服务……275
7.3 MPLS VPN 服务……277
7.3.1 MPLS VPN 概述……277
7.3.2 客户边缘安全性……278
7.3.3 提供商边缘安全性……279
7.3.4 提供商核心安全性……282
7.3.5 提供商之间边缘安全性……284
7.4 IPsec VPN 服务……287
7.4.1 IPsec VPN 概述……287
7.4.2 保护 IPsec VPN 服务……294
7.4.3 其他 IPsec 安全相关特性……300
7.5 其他服务……301
7.5.1 SSL VPN 服务……301
7.5.2 VoIP 服务……302
7.5.3 视频服务……303
7.6 小结……304
7.7 复习题……304
7.8 延伸阅读……305

第 3 部分

第 8 章 企业网络案例研究……311

8.1 案例研究 1：IPSec VPN 和互联网访问……312
8.1.1 网络拓扑结构和要求……312
8.1.2 路由器配置……315
8.2 案例研究 2：MPLS VPN……328
8.2.1 网络拓扑结构和要求……328
8.2.2 路由器配置……330
8.3 小结……340
8.4 延伸阅读……340

第 9 章 服务提供商网络案例研究……343

9.1 案例研究 1：IPSec VPN 和互联网接入……344
9.1.1 网络拓扑和需求……345

9.1.2 路由器配置……347
9.2 案例研究 2：MPLS VPN……359
9.2.1 网络拓扑和需求……359
9.2.2 路由器配置……361
9.3 小结……374
9.4 延伸阅读……374

第 4 部分

附录 A 复习题答案……379

附录 B IP 协议报头……387

B.1 IP 版本 4 头……388
B.2 TCP 头……392
B.3 UDP 头……396
B.4 ICMP 头……398
B.4.1 ICMP 回应请求/回应回复查询消息头……400
B.4.2 传输中的 ICMP 生存时间超过消息头……402
B.4.3 ICMP 目的地不可到达、分段需要和设置不分段错误消息头……404
B.4.4 其他 ICMP 目的不可到达错误消息头……407
B.5 以太网/802.1 Q 头……409
B.5.1 IEEE 802.3 以太网帧头格式……409
B.5.2 IEEE 802.1 Q VLAN 头格式……411
B.6 MPLS 协议头……412
B.7 延伸阅读……415

附录 C Cisco IOS 到 XOS XR 安全性过渡……417

C.1 数据平面安全性命令……418
C.2 控制平面安全性命令……420
C.3 管理平面安全性命令……428
C.4 服务平面安全性命令……435
C.5 延伸阅读……436

附录 D 安全事故处理……439

D.1 事故响应的 6 个阶段……439
D.1.1 准备……440
D.1.2 确定……441
D.1.3 分类……442
D.1.4 跟踪……442
D.1.5 反应……442
D.1.6 事后评估分析……442
D.2 Cisco 产品安全……443
D.2.1 Cisco 安全弱点策略……443
D.2.2 Cisco 计算机和网络安全……443
D.2.3 Cisco 安全……444
D.2.4 IPS 签名包更新和归档……444
D.2.5 Cisco 安全中心……444
D.2.6 Cisco IntelliShield 警报管理器服务……444
D.2.7 Cisco 软件中心……444
D.3 行业安全组合……444
D.4 域网络操作员组织……445
D.5 延伸阅读……446