Introduction

The networking world is evolving at an ever-increasing pace. The rapid displacement of legacy, purpose-built networks based on time-division multiplexing (TDM), Frame Relay, and Asynchronous Transfer Mode (ATM) technologies to ubiquitous Internet Protocol (IP) packet-based networks capable of supporting converged network services is well under way. Service providers can no longer afford to deploy multiple networks, each built to support a single application or service such as voice, business-class data, or Internet traffic. The cost of deploying and operating multiple networks in this business model is not financially sustainable. In addition, customer demand for integrated services and applications, as well as new services and applications, means service delivery velocity is a critical requirement of modern network architectures. Leading wireline and wireless service providers worldwide are already migrating legacy network services onto IP core networks to take advantage of the bandwidth efficiencies and scalability offered by IP networks, and their ability to enable rapid expansion into new service markets.

Building and operating IP network infrastructures to meet the same carrier-class requirements that customers demand, while carrying multiple, diverse services that have different bandwidth, jitter, and latency requirements, is a challenging task. Single-purpose networks were designed and built to support specific, tightly controlled operational characteristics. Carrying Internet traffic, voice traffic, cellular traffic, and private (VPN) business traffic over a common IP backbone has significant implications for both network design and network security. The loss of integrity through a network attack, for example, in any one of the traffic services can potentially disrupt the entire "common network," causing an impact to the entire revenue base. Further, enterprises are increasingly dependent upon IP networking for business operations.

Fundamentally, all networks have essentially two kinds of packets: *data packets*, which belong to customers and carry customer traffic, and *control and management packets*, which belong to the network and are used to create and operate the network. One of the strengths of the IP protocol is that all packets traverse a "common pipe" (or are "in-band"). Networking professionals coming from the legacy TDM/ATM network world may be unfamiliar with the concept of a common pipe for data and control plane traffic, as these legacy systems separate data channels from "out-of-band" control channels. Misunderstanding and trepidation often exist about how data packets and control packets can be segmented and secured in a common network.

Even though IP networks carry all packets in-band, it is possible and, now more than ever, critical to distinguish between the various types of packets being transported. Separating traffic into data, control, management, and services planes (referred to as traffic planes) and properly segmenting and protecting these traffic planes are required tasks to secure today's highly converged IP networks. This book is the first to cover IP network traffic plane separation and security in a formal and thorough manner.

Goals and Methods

The goal of this book is to familiarize you with concepts, benefits, and implementation details for segmenting and securing IP network traffic planes. This includes a review of the many threats facing IP networks and the many techniques available to mitigate the risks. Defense in depth and breadth strategies are also reviewed to highlight the interactions between various IP traffic plane security techniques. Detailed analyses at the operational level of IP networks from the perspective of each of the data, control, management, and services planes form the basis for the security principles and configuration examples described herein. Case studies further illustrate how optimizing the selection of IP traffic plane protection measures using defense in depth and breadth principles provides an effective security strategy.

Who Should Read This Book?

This book was written for network engineers, and network operations and security staff of organizations who deploy and/or maintain IP and IP/MPLS networks. The primary audience includes those engineers who are engaged in day-to-day design, engineering, and operations of IP networks. Subscribers of a service based on IP or IP/MPLS will benefit from this book as well. The secondary audience includes those with less network-centric backgrounds who wish to understand the issues and requirements of IP network traffic plane separation and security. This book also provides great insight into the technical interworkings and operations of IP routers that both senior and less-experienced network professionals can benefit from.

How This Book Is Organized

For those readers who are new to IP network security concepts, especially the concepts of separation and protection of IP traffic planes, this book should be read cover to cover. If you are already familiar with IP networks, protocols, network design, and operations, you may refer to specific sections of interest. This book is divided into four general parts, which are described next.

Part I, "IP Network and Traffic Plane Security Fundamentals," provides a basic overview of the IP protocol, the operations of IP networks, and the operations of routers and routing hardware and software. It is in this section that the concepts of IP traffic segmentation and security are introduced. At the end of this section, casual readers will understand, at a high level, what IP traffic plane separation and protection entails. This section includes the following chapters:

- **Chapter 1, "Internet Protocol Operations Fundamentals":** Discusses the fundamentals of the IP protocol, and looks at the operational aspects of IP networks from the perspective of the routing and switching hardware and software. It is in this context that the concept of IP network traffic planes is introduced.
- **Chapter 2, "Threat Models for IP Networks":** Lays out threat models for routing and switching environments within each IP network traffic plane. By reviewing threats in this manner, you learn why IP traffic planes must be protected and from what types of attacks.
- **Chapter 3, "IP Network Traffic Plane Security Concepts":** Provides a broad overview of each IP traffic plane, and how defense in depth and breadth strategies are used to provide robust network security.

Part II, "Security Techniques for Protecting IP Traffic Planes," provides the in-depth, working details that serious networking professional can use to actually implement IP traffic plane separation and protection strategies. For less-experienced network professionals, this section provides great insight into the technical operations of IP routers. This section includes the following chapters:

- **Chapter 4, "IP Data Plane Security":** Focuses on the data plane and associated security mechanisms. The data plane is the logical entity containing all user traffic generated by hosts, clients, servers, and applications that use the network as transport only.
- **Chapter 5, "IP Control Plane Security":** Focuses on the control plane and associated security mechanisms. The control plane is the logical entity associated with routing protocol processes and functions used to create and maintain the necessary intelligence about the operational state of the network, including forwarding topologies.
- **Chapter 6, "IP Management Plane Security":** Focuses on the management plane and associated security mechanisms. The management plane is the logical entity that describes the traffic used to access, manage, and monitor all of the network elements for provisioning, maintenance, and monitoring functions.
- **Chapter 7, "IP Services Plane Security":** Focuses on the services plane and associated security mechanisms. The services plane is the logical entity that includes user traffic that receives dedicated network-based services requiring special handling beyond traditional forwarding to apply or enforce the intended policies for various service types.

Part III, "Case Studies," provides case studies for two different network types: the enterprise network, and the service provider network. These case studies are used to further illustrate how the individual components discussed in detail in Part II are integrated into a comprehensive IP network traffic plane separation and protection plan. This section includes the following chapters:

- **Chapter 8, "Enterprise Network Case Studies":** Uses two basic enterprise network situations—the Internet-based IPsec VPN design, and the MPLS VPN design—to illustrate the application of IP network traffic plane separation and protection concepts for enterprises. These cases studies focus on the Internet edge router and customer edge (CE) router, respectively, to present the IP traffic plane security concepts.
- **Chapter 9, "Service Provider Network Case Studies":** Uses the same topologies from the two case studies of Chapter 8, but presents them from the service provider network perspective. In this chapter, two provider edge router configurations are studied—one for the Internet-based IPsec VPN design case, and one for the MPLS VPN case—to illustrate the application of IP network traffic plane separation and protection concepts for service providers.

Part IV, "Appendixes," supplements many of the discussions in the body of the book by providing handy references that should be useful not only during the course of reading the book, but also in day-to-day work. The following appendixes are provided:

- **Appendix A, "Answers to Chapter Review Questions":** Provides answers to the chapter review questions.
- **Appendix B, "IP Protocol Headers":** Covers the header format for several common IP network protocols, and describes the security implications and abuse potential for each header field.
- **Appendix C, "Cisco IOS to IOS XR Security Transition":** Provides a one-for-one mapping between common IOS 12.0S security-related configuration commands and their respective IOS XR counterparts.
- **Appendix D, "Security Incident Handling":** Provides a short overview of security incident handling techniques, and a list of common security incident handling organizations.