Defending The Perimeter Against Cyber Attacks

Chapter 1: Setting Your Security Objectives

- The CIA Security Model
- Attacks and Countermeasures
- AAA
- Defense In Depth
- Perimeter Security
- What Is a Security Policy
- What's in a Security Policy
- Policy Decisions and Risk
- Risk Management
- Risk Assessment and Mitigation

Chapter 2: Firewalls: Accessing External Services

- Firewalls and Policy Statements
- Firewalls
- Protocol/Application Types
- TCP/UDP Ports
- Simple Use of Ports
- Firewall Technology
- Stateless Packet Filters
- Stateless Packet Filters: Pros and Cons
- Stateful Packet Filters
- Stateful Packet Filters: Pros and Cons
- Circuit-Level Gateways
- Operation of a Circuit-Level Gateway
- Circuit-Level Gateways: Pros and Cons
- Application Proxies
- Operation of an Application Proxy
- Application Proxies: Transparent vs. Non-Transparent
- Application Proxies: Pros and Cons
- Hands-On Exercise 2.1: Installing the Sophos UTM Firewall
- Hardening Your Operating System
- Application Content
- Scripting
- Content Checking
- Content Checking: Malicious Code
- Integrating Content Checking With Your Firewall
- Encrypted Web Traffic and Your Firewall
- Tunnel Data Using an External Server
- Hands-On Exercise 2.2: Content Filtering

Chapter 3: Firewalls: Supporting External Services

- Firewall Architecture
- External Access Through a Proxy
- Database Access
- DNS
- DNS Resolver Operations
- DNS Through Your Firewall
- Dual DNS Architecture
- DNS Proxy
- Hands-On Exercise 3.1: Supporting DNS Through a Firewall
- Mail Servers
- SMTP Proxy
- SMTP Security Server
- Content Scanning
- Encrypted Mail
- Web Servers
- Hands-On Exercise 3.2: Supporting SMTP Mail Through a Firewall
- Border Router Security
- Source Routing
- IP Broadcasts
- Router Protection
- Stateless Packet Filtering on Routers
- Interface-Based ACLs
- Outgoing HTTP Filter Rule Example
- Cisco Access Control Lists
- Hands-On Exercise 3.3: Protecting the DMZ With Cisco ACLs

Chapter 4: Intrusion Detection and Prevention

- Intrusion Detection Systems (IDS)
- Active vs. Passive Detection
- IDS Components
- Types of IDS
- NIDS
- NIDS Appliances
- Stealth Monitoring
- IDS Alerts
- Snort IDS
- Hands-On Exercise 4.1: Using Snort IDS
- IDS Accuracy
- IDS Tuning
- Reducing False Positives in Snort
- Dealing With False Positives
- Handling Alerts
- Attack Mitigation
- Intrusion Prevention Systems

- IDS vs. IPS
- Hands-On Exercise 4.2: Using Intrusion Prevention

- Denial-of-Service Attacks
- DNS Server
- Wireless Networks
- Specific Protocol Attacks
- SYN Floods
- Hands-On Exercise 7.1: Cisco IOS SYN Flood Defense
- Defending Against DoS Attacks
- Hands-On Exercise 7.2: Sophos UTM 9 DoS Defense
- Perimeter Architectures
- Basic (DMZ) Firewall Architecture
- Placing IDS Sensors
- Other Perimeter Weaknesses

Chapter 5: Supporting Remote User Access

- Virtual Private Networks (VPNs)
- VPN Security Requirements
- VPN Security
- Introduction to Encryption
- Keyed Encryption
- Symmetric (Secret Key) Cryptography
- Example Symmetric Encryption Algorithms
- Symmetric Encryption Key Management
- Asymmetric Encryption
- Asymmetric Encryption: Properties and Uses
- Using Public Key Cryptography for Key Exchange
- Using Public Key Cryptography for Authentication
- Public Key Management
- Hashing
- Hash Function Weaknesses
- Digital Signatures
- Hashed Message Authentication Codes
- Tunneling
- Layer 2 Tunneling Protocol (L2TP
- IPsec
- ISAKMP/IKE for L2TP/IPsec
- Hands-On Exercise 5.1: Remote User VPN Using L2TP Over IPsec
- Remote Access VPN Alternatives
- L2TP Protected by IPsec
- SSL Authentication and Encryption
- SSL Portal
- SSL VPNs

Chapter 6: Site-to-Site VPNs

- IP Security
- IPsec Formats and Modes
- ESP Tunnel Mode
- ESP Transport Mode
- IPsec Policy
- Encryption and Hashing Algorithms for IPsec
- IPsec Security Associations
- IPsec Policies
- SA Granularity
- Hands-On Exercise 6.1: IPsec Site-to-Site VPN
- VPN Architecture
- Star, Hub-and-Spoke, Meshed
- Star VPN Topology
- Star VPN Topology Implementation
- Hub-and-Spoke VPN Topology
- Hub-and-Spoke VPN Topology Implementation
- Partially Meshed VPN Topology
- Partially Meshed VPN Topology Implementation
- Fully Meshed VPN Topology
- Fully Meshed VPN Topology Implementation
- Internet Access and Split Tunneling
- IPsec Tunnel Limitations
- IPsec Tunnel Mode Advantages
- IPsec Transport Mode
- L2TP/IPsec for Site-to-Site VPNs
- GRE/IPsec
- Configuring Filters With Access Lists
- Hands-On Exercise 6.2: Cisco GRE IPsec VPN