

Inhalt CCNA Security 1.0

1 Modern Network Security Threats

- 1.1 Fundamental Principles of a Secure Network
- 1.2 Viruses, Worms, and Trojan Horses
- 1.3 Attack Methodologies

2 Securing Network Devices

- 2.1 Securing Device Access
- 2.2 Assigning Administrative Roles
- 2.3 Monitoring and Managing Devices
- 2.4 Using Automated Security Features

3 Authentication, Authorization, and Accounting

- 3.1 Purpose of AAA
- 3.2 Local AAA Authentication
- 3.3 Server-Based AAA
- 3.4 Server-Based AAA Authentication
- 3.5 Server-Based AAA Authorization and Accounting

4 Implementing Firewall Technologies

- 4.1 Access Control Lists
- 4.2 Firewall Technologies
- 4.3 Context-Based Access Control
- 4.4 Zone-Based Policy Firewall

5 Implementing Intrusion Prevention

- 5.1 IPS Technologies
- 5.2 IPS Signatures
- 5.3 Implementing IPS
- 5.4 Verify and Monitor IPS

6 Securing the Local Area Network

- 6.1 Endpoint Security
- 6.2 Layer 2 Security Considerations
- 6.3 Configuring Layer 2 Security
- 6.4 Wireless, VoIP, and SAN Security

7 Cryptographic Systems

- 7.1 Cryptographic Services
- 7.2 Basic Integrity and Authenticity
- 7.3 Confidentiality
- 7.4 Public Key Cryptography

8 Implementing Virtual Private Networks

- 8.1 VPNs
- 8.2 GRE VPNs
- 8.3 IPsec VPN Components and Operation
- 8.4 Implementing Site-to-Site IPsec VPNs with CLI
- 8.5 Implementing Site-to-Site IPsec VPNs with SDM
- 8.6 Implementing Remote-Access VPNs

9 Managing a Secure Network

- 9.1 Principles of Secure Network Design
- 9.2 Cisco Self-Defending Network
- 9.3 Operations Security
- 9.4 Network Security Testing
- 9.5 Business Continuity Planning and Disaster Recovery
- 9.6 System Development Life Cycle
- 9.7 Developing a Comprehensive Security Policy