SILLABUS – ACN42AB

Network Security

6. SECURING THE LOCAL AREA NETWORK

6.1. ENDPOINT SECURITY

6.1.1. Introducing Endpoint Security
6.1.2. Endpoint Security with IronPort
6.1.3. Endpoint Security with Network Admission Control

6.2. LAYER 2 SECURITY CONSIDERATIONS

6.2.1. Introducing Layer 2 Security
6.2.2. MAC Address Spoofing Attacks
6.2.3. MAC Address Table Overflow Attacks
6.2.4. STP Manipulation Attacks
6.2.5. LAN Storm Attack
6.2.6. VLAN Attack

6.3. CONFIGURING LAYER 2 SECURITY

6.3.1. Configuring Port Security
6.3.2. Verifying Port Security
6.3.3. Configuring BPDU Guard, BPDU Filter and Root Guard
6.3.4. Configuring Storm Control
6.3.5. Configuring VLAN Trunk Security

6.3.6. Configuring PVLAN Edge
6.3.7. Recommended Practices for Layer 2

6.4. WIRELESS, VoIP AND SAN SECURITY

7. CRYTPTOGRAPHIC SYSTEMS

7.1. CRYPTOGRAPHIC SERVICES

7.1.1. Securing Communications
7.1.2. Cryptography

7.2. BASIC INTEGRITY AND AUTHENITICITY

7.2.1. Cryptographic Hashes
7.2.2. Integrity with MD5 and SHA-1
7.2.3. Authenticity with HMAC
7.2.4. Key Management

7.3. CONFIDENTIALITY

7.3.1. Encryption
7.3.2. Data Encryption Standard
7.3.3. 3DES
7.3.4. Advanced Encryption Standard
7.3.5. Alternate Encryption Algorithms
7.3.6. Diffie-Hellman Key Exchange

7.4. PUBLIC KEY CRYPTOGRAPHY

8. IMPLEMENTING VIRTUAL PRIVATE NETWORK

8.1. VPNs
8.1.1. VPN Overview
8.1.2. VPN Topologies
8.1.3. VPN Solutions

8.2. GRE VPNs

8.2.1. Configuring a Site-to-Site GRE Tunnel

8.3. IPsec VPN COMPONENTS AND OPERATION

8.3.1. Introducing IPsec
8.3.2. IPsec Security Protocols
8.3.3. Internet Key Exchange

8.4. IMPLEMENTING SITE-TO-SITE IPsec VPNs WITH CLI

8.4.1. Configuring a Site-to-Site IPsec VPN
8.4.2. Task 1 – Configure Compatible ACLs
8.4.3. Task 2 – Configure IKE
8.4.4. Task 3 – Configure the Transform Sets
8.4.5. Task 4 – Configure the Crypto ACLs
8.4.6. Task 5 – Apply the Crypto Map
8.4.7. Verify and Troubleshoot the IPsec Configuration

8.5. IMPLEMENTING SITE-TO-SITE IPsec VPNs WITH CCP

8.5.1. Configuring IPsec Using CCP
8.5.2. VPN Wizard – Quick Setup
8.5.3. VPN Wizard – Step by Step Setup
8.5.4. Verifying, Monitoring and Troubleshooting VPNs

8.6. IMPLEMENTING REMOTE-ACCESS VPNs

8.6.1. A shift to Telecommuting
8.6.2. Introducing Remote-Access VPNs
8.6.3. SSL VPNs
8.6.4. Cisco Easy VPN
8.6.5. Configuring a VPN Server with CCP
8.6.6. Connecting with a VPN Client

9. IMPLEMENTING THE CISCO ADAPTIVE SECURITY APPLIANCE (ASA)

9.1. INTRODUCTION TO THE ASA

9.1.1. Overview of the ASA
9.1.2. Basic ASA Configuration

9.2. ASA FIREWALL CONFIGURATION

9.2.1. Introduction to the ASA Firewall Configuration
9.2.2. Configuring Management Settings and Services
9.2.3. Introduction to ASDM
9.2.4. ASDM Wizards
9.2.5. Object Groups
9.2.6. ACLs
9.2.7. NAT Services on an ASA
9.2.8. Access Control on an ASA
9.2.9. Service Policies on an ASA

9.3. ASA VPN CONFIGURATION

9.3.1. ASA Remote-Access VPN Options
9.3.2. Clientless SSL VPN
9.3.3. Configuring Clientless SSL VPN
9.3.4. AnyConnect SSL VPN
9.3.5. Configuring AnyConnect SSL VPN

10. MANAGING A SECURE NETWORK

10.1. PRINCIPLES OF SECURE NETWORK DESIGN

10.1.1. Ensuring a Network is Secure
10.1.2. Threat Identification and Risk Analysis
10.1.3. Risk Management and Risk Avoidance

10.2. SECURITY ARCHITECTURE

10.2.1. Introducing the Cisco SecureX Architecture
10.2.2. Solutions for the Cisco SecureX Architecture
10.2.3. Future Trends for Network Security

10.3. OPERATIONS SECURITY

10.3.1. Introducing Operations Security
10.3.2. Principles of Operations Security

10.4. NETWORK SECURITY TESTING

10.4.1. Introducing Network Security Testing
10.4.2. Network security Testing Tools

10.5. BUSINESS CONTINUITY PLANNING AND DISASTER RECOVERY

10.5.1. Continuity Planning and Disaster Recovery