Secure Home and Small Office Network Configuration Guide

Overview

This repository contains comprehensive documentation and configuration examples for implementing secure network infrastructures in home and small office environments. Based on practical experience with Cisco Packet Tracer and networking fundamentals, this guide provides step-by-step instructions for building networks with security best practices.

Project Goals

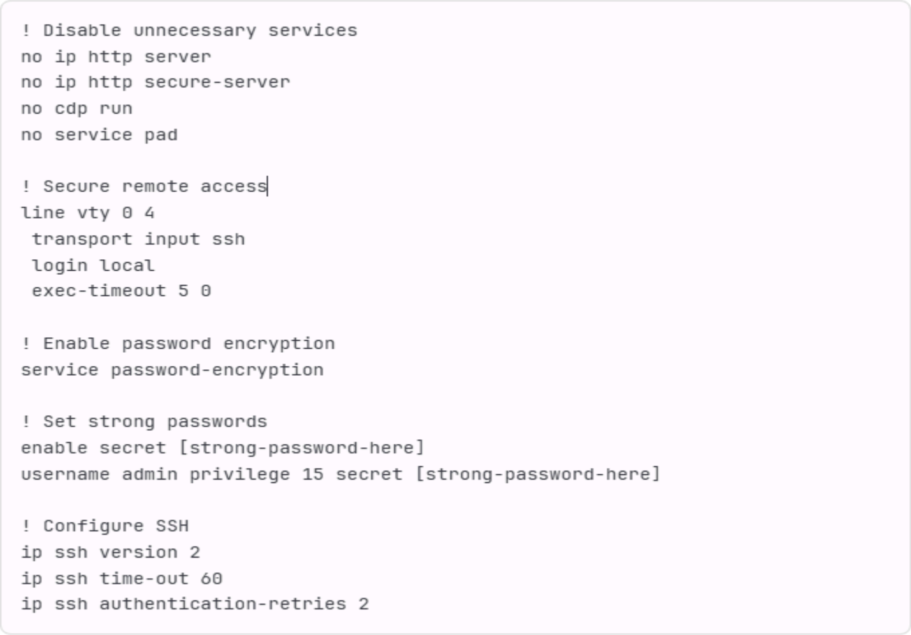
- Demonstrate understanding of network security principles
- Provide practical, implementable security configurations
- Document common vulnerabilities and their mitigations
- Share knowledge gained through Smart IT Technician training

Contents

1. Network Architecture Designs

- **Segmented Home Network**: VLAN implementation for IoT device isolation
- **Small Office Network**: Secure multi-tier network design
- **Guest Network Configuration**: Isolated access for visitors
- **DMZ Implementation**: Securing public-facing services

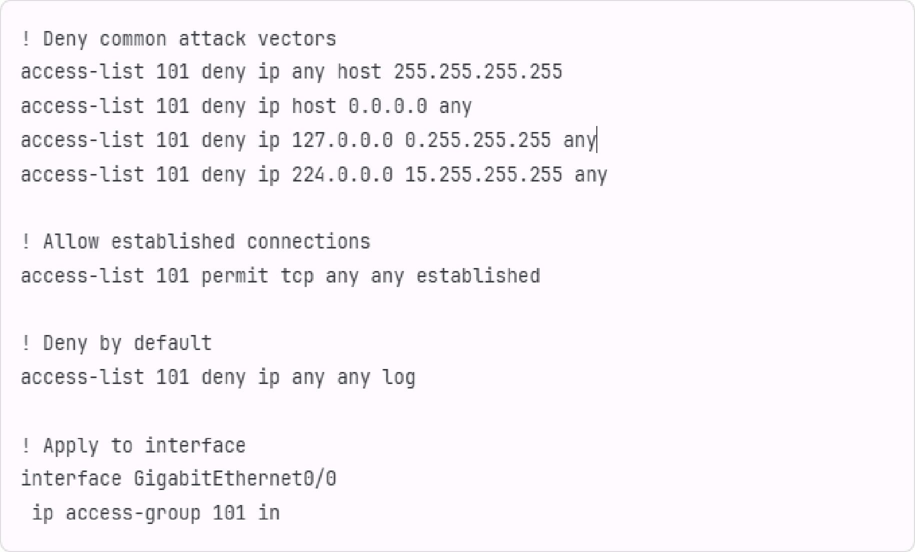
2. Router Security Hardening



```
! Disable unnecessary services
no ip http server
no ip http secure-server
no cdp run
no service pad

! Secure remote access
line vty 0 4
 transport input ssh
 login local
 exec-timeout 5 0

! Enable password encryption
service password-encryption

! Set strong passwords
enable secret [strong-password-here]
username admin privilege 15 secret [strong-password-here]

! Configure SSH
ip ssh version 2
ip ssh time-out 60
ip ssh authentication-retries 2
```

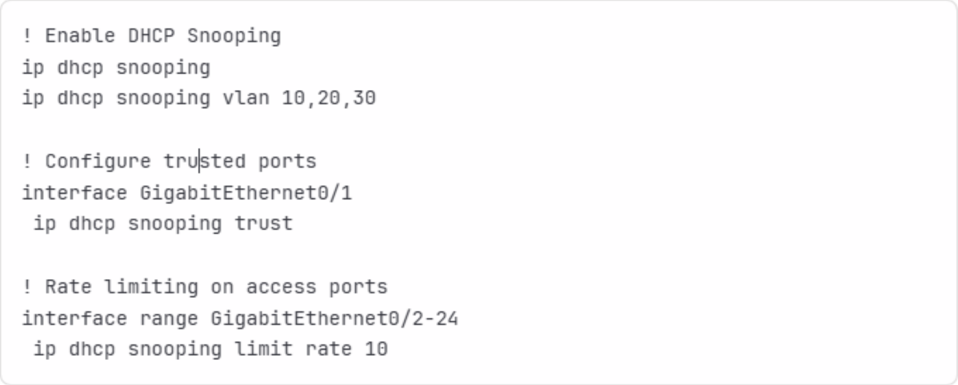
3. Firewall Configuration Examples

Basic ACL for Internet-facing Interface



```
! Deny common attack vectors
access-list 101 deny ip any host 255.255.255.255
access-list 101 deny ip host 0.0.0.0 any
access-list 101 deny ip 127.0.0.0 0.255.255.255 any
access-list 101 deny ip 224.0.0.0 15.255.255.255 any

! Allow established connections
access-list 101 permit tcp any any established

! Deny by default
access-list 101 deny ip any any log

! Apply to interface
interface GigabitEthernet0/0
 ip access-group 101 in
```

4. DHCP Security Configuration



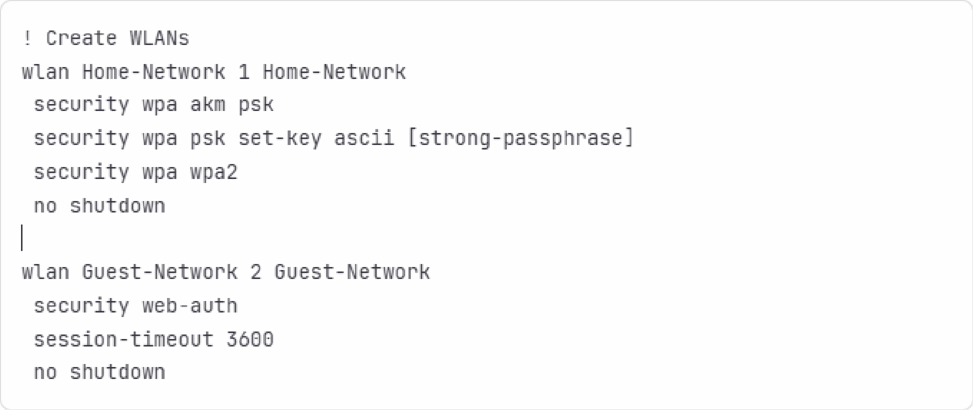
```
! Enable DHCP Snooping
ip dhcp snooping
ip dhcp snooping vlan 10,20,30

! Configure trusted ports
interface GigabitEthernet0/1
 ip dhcp snooping trust

! Rate limiting on access ports
interface range GigabitEthernet0/2-24
 ip dhcp snooping limit rate 10
```

5. Wireless Security Best Practices

Recommended Configuration:

- **Encryption**: WPA3-Personal or WPA2-Enterprise minimum
- **Authentication**: 802.1X with RADIUS where possible
- **SSID**: Disable broadcast for main network (optional)
- **MAC Filtering**: Implement as additional layer (not primary security)
- **Guest Network**: Separate VLAN with limited access

Sample Wireless Controller Configuration:



```
! Create WLANs
wlan Home-Network 1 Home-Network
 security wpa akm psk
 security wpa psk set-key ascii [strong-passphrase]
 security wpa wpa2
 no shutdown

wlan Guest-Network 2 Guest-Network
 security web-auth
 session-timeout 3600
 no shutdown
```

Security Checklist

Network Level

- Change all default passwords immediately
- Disable unused network services and ports
- Implement network segmentation with VLANs
- Configure firewall rules following the principle of least privilege
- Enable logging for security events
- Implement DHCP snooping and IP Source Guard
- Configure port security on access switches
- Disable CDP/LLDP on user-facing ports

Router/Switch Level

- Enable SSH only, disable Telnet
- Configure console and VTY line timeouts
- Implement strong password policies
- Enable password encryption
- Configure NTP for accurate logging timestamps
- Set up SNMP v3 with authentication
- Disable HTTP server, use HTTPS if needed
- Configure banner messages

Wireless Security

- Use WPA3 or WPA2 at minimum
- Implement strong pre-shared keys (20+ characters)
- Separate guest and internal networks
- Disable WPS (WiFi Protected Setup)
- Enable wireless intrusion detection
- Regular firmware updates
- Monitor connected devices

IoT Device Security

- Isolate IoT devices on separate VLAN
- Restrict IoT device internet access where possible
- Change default credentials on all devices
- Disable unnecessary features and services
- Regular firmware updates
- Monitor IoT device traffic patterns

Network Diagrams

Segmented Home Network Architecture

```
                 Internet
                    |
                [Router/Firewall]
                    |
         -----------|-----------
        |           |           |
    [VLAN 10]  |[VLAN 20]   [VLAN 30]
    Trusted      IoT         Guest
    Devices     Devices      Network
```

Small Office Network with DMZ

```
                    Internet
                   |
                  [Firewall]
         --------------|--------------
        |              |              |
    [DMZ VLAN]    [Internal]    [Guest VLAN]
    Web Server     Network       Limited Access
|   Mail Server    Workstations
                   File Server
```

Common Vulnerabilities and Mitigations

1. Default Credentials

Risk: Unauthorized access to network devices **Mitigation**:

- Change all default usernames and passwords
- Use strong, unique passwords (minimum 16 characters)
- Implement password management policy

2. Unencrypted Management Traffic

Risk: Credentials intercepted during remote management **Mitigation**:

- Use SSH instead of Telnet
- Use HTTPS instead of HTTP
- Implement VPN for remote management access

3. Unnecessary Services Running

Risk: Increased attack surface **Mitigation**:

- Audit running services regularly
- Disable CDP, HTTP server, and unused protocols
- Apply principle of least functionality

4. Lack of Network Segmentation

Risk: Lateral movement after compromise **Mitigation**:

- Implement VLANs for different device types
- Use ACLs to control inter-VLAN traffic
- Isolate IoT devices and guest networks

5. Weak Wireless Security

Risk: Unauthorized network access **Mitigation**:

- Use WPA3 or WPA2 with strong passphrases
- Implement 802.1X authentication for enterprise
- Regular security audits of wireless networks

Implementation Guide

Phase 1: Planning

1. Document current network topology
2. Identify security requirements
3. Design segmented network architecture
4. Plan IP addressing scheme with security in mind

Phase 2: Device Hardening

1. Update firmware on all devices
2. Change default credentials
3. Disable unnecessary services
4. Configure secure management access (SSH only)

Phase 3: Network Segmentation

1. Create VLANs for different security zones
2. Configure inter-VLAN routing with ACLs
3. Implement DHCP snooping
4. Configure port security

Phase 4: Security Controls

1. Configure firewall rules
2. Set up logging and monitoring
3. Implement wireless security
4. Test security controls

Phase 5: Documentation and Maintenance

1. Document all configurations
2. Create network diagrams
3. Establish change management procedures
4. Schedule regular security reviews

Configuration Templates

All configuration templates are available in the `/configs` directory:

- `router-hardening.txt` - Secure router baseline configuration
- `switch-security.txt` - Switch security features
- `wireless-secure.txt` - Wireless access point configuration
- `firewall-rules.txt` - Sample ACL configurations
- `vlan-segmentation.txt` - VLAN implementation examples

Learning Resources

Skills Demonstrated

- Network design and architecture
- Cisco IOS CLI configuration
- Security best practices implementation
- IPv4/IPv6 addressing and routing
- VLAN configuration and management
- Access control lists (ACLs)
- Wireless security protocols
- Network monitoring and logging

Related Certifications

This knowledge aligns with:

- CompTIA Network+
- CompTIA Security+
- Cisco CCNA
- Cisco CyberOps Associate