Lab 9: Security Policy Development and Implementation

Introduction

Most organizations have a number of information security controls. The ISO 27001 standard specifies a management system that is intended to bring information security under explicit management control. You may find information and guidelines at: http://www.27000.org/iso-27001.htm

In this lab we will get to use previously acquired knowledge from the labs, in order to create a high-level technical policy and implement it in a practical situation (Packet Tracer).

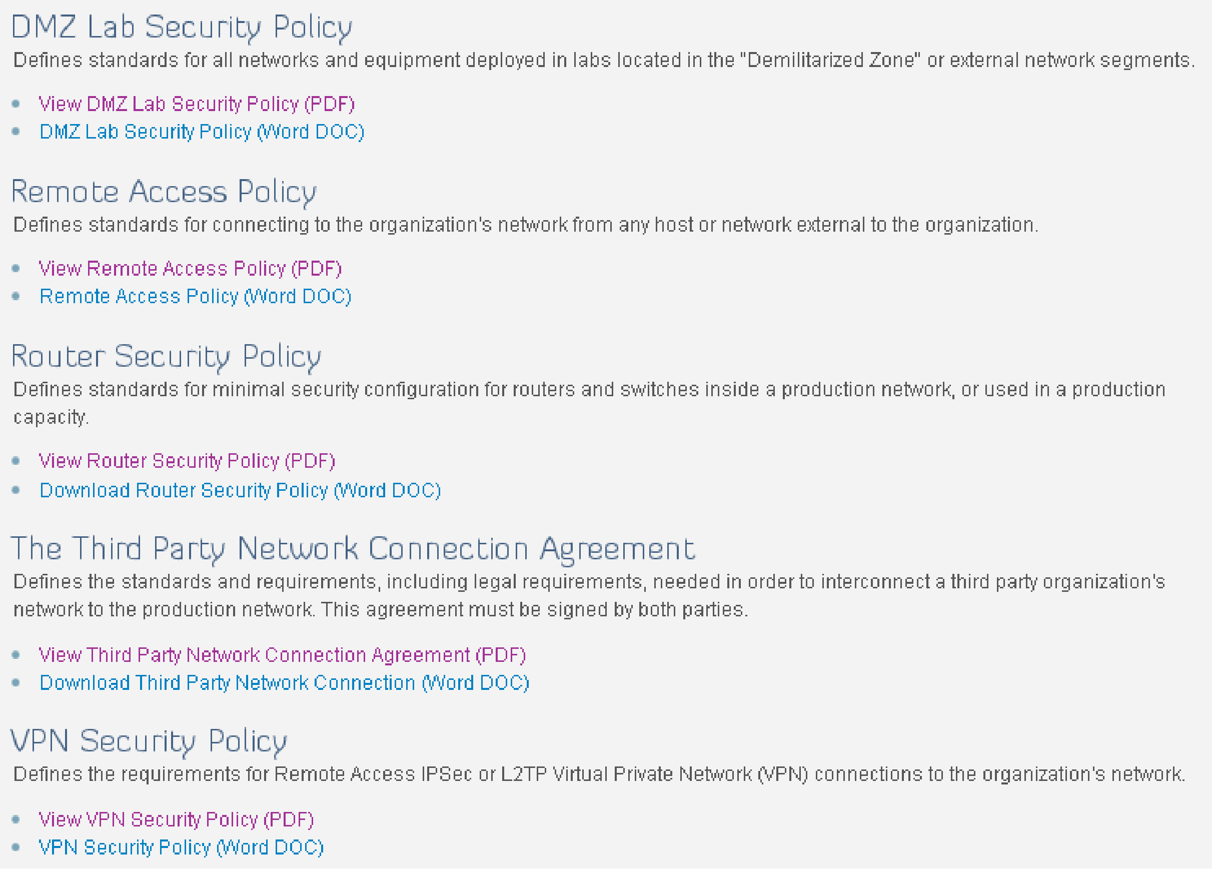
Objectives

- Review Network Security Policies
- Review the objectives for previous CCNA Security labs.
- Create a Network Security Guidelines document (high-level technical policy) for router and switch security.
- Implement the security guidelines in a virtual topology (Packet Tracer).

Task 1: Review Network Security Policies

Start by looking at current available policy templates.
The SANS Institute provides many different types of templates for various information security areas. You may find Network Security specific templates at:
http://www.sans.org/security-resources/policies/network.php

Review some of those policies. The policies may cover areas such as remote access, firewalls/dmz, layer-two/access layer security, passwords and so on. You could mix and match between the templates to create something for your own company. For now, I'd just like you to see what such a document may look like at the SANS site.



DMZ Lab Security Policy

Defines standards for all networks and equipment deployed in labs located in the "Demilitarized Zone" or external network segments.

- View DMZ Lab Security Policy (PDF)
- DMZ Lab Security Policy (Word DOC)

Remote Access Policy

Defines standards for connecting to the organization's network from any host or network external to the organization.

- View Remote Access Policy (PDF)
- Remote Access Policy (Word DOC)

Router Security Policy

Defines standards for minimal security configuration for routers and switches inside a production network, or used in a production capacity.

- View Router Security Policy (PDF)
- Download Router Security Policy (Word DOC)

The Third Party Network Connection Agreement

Defines the standards and requirements, including legal requirements, needed in order to interconnect a third party organization's network to the production network. This agreement must be signed by both parties.

- View Third Party Network Connection Agreement (PDF)
- Download Third Party Network Connection (Word DOC)

VPN Security Policy

Defines the requirements for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the organization's network.

- View VPN Security Policy (PDF)
- VPN Security Policy (Word DOC)

Task 2: Create a Network Equipment Security Guidelines document.

This document describes guidelines in a more detailed format with a step-by-step configuration list.

Step 1: Review the objectives for previous CCNA Security labs.

- Open each of the previous labs completed from chapters one through eight and review the objectives listed for each one.
- Copy them to a separate document for use as a starting point. Focus mainly on those objectives that involve security practices and device configuration.

Step 2: Create a Network Device Security Guidelines document (See example, page 5.) for router and switch security.

Create a high-level list of tasks to include for network device security. Incorporate router and switch security. The purpose of this document is to reinforce and supplement the information presented by a network security policy.

The Network Device Security Guidelines document will provide the basis for the equipment configuration in the remaining parts of this lab.

Task 3: Implementation in Packet Tracer

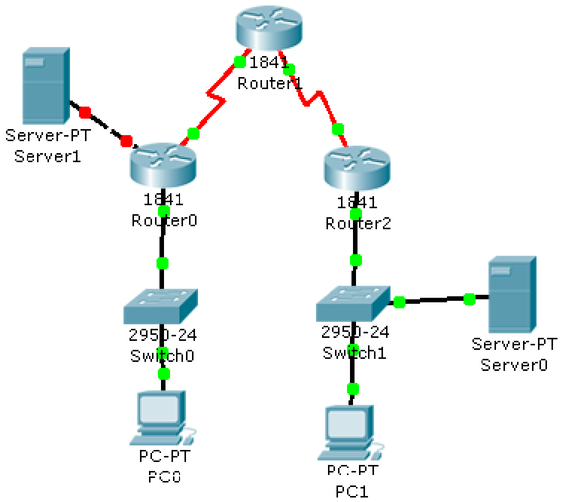
Step 1

- Build a small topology consisting of three routers, two switches, two desktop computers and a server or two to handle services as you may choose based on your Security Policy. (ie. AAA-Radius/NTP/Syslog). You're free to design the network as you please.

- Perform the tasks described in your guidelines document.

- Test that everything is working.

Step 2: Show your document *"Network Device Security Guidelines"* and the implementation (Packet Tracer/ .pkt file) to your instructor.



PT topology example

Example: **<Network Security Policy document>**

1.0 Purpose

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of <Company Name>.

2.0 Scope

All routers and switches connected to <Company Name> production networks are affected.

3.0 Policy

Router Administrative Access

Approved <Company Name> employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of MyExampleNetwork

Every router must meet the following configuration standards:

1. No local user accounts are configured on the router. Routers must use RADIUS for all user authentication.

2. The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization.

3. Each router must have the following statement posted in clear view:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device."

4. Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH is the preferred management protocol.

VPN Security Measures

1. VPN gateways will be set up and managed by <Company Name> network operational groups.

2. All computers connected to <Company Name> internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard (provide URL to this software); this includes personal computers.

3. VPN users will be automatically disconnected from <Company Name>'s network after thirty minutes of inactivity.

Example: <**Network Device Security Guidelines document>**

Unless otherwise indicated, these policy guidelines apply to all primary network devices such as switches and routers.

Router Administrative Access

The following steps must be taken to secure and harden routers.
1. Configure the enable secret, console, and vty passwords.
2. Encrypt all passwords, which should be a minimum of 10 characters. Passwords should include a combination of uppercase, lowercase, numbers, and special characters.
3. Configure a login banner warning unauthorized users of the penalties of access to this device.
4. Configure an administrative user with privilege level 15 and a secret password.
5. Configure an SSH server and disable Telnet access.
6. Configure a centralized synchronized time source using NTP.
7. Configure syslog support on edge routers.
8. Enable HTTP secure server for web-based access.
9. Configure centralized authentication for each site using AAA and RADIUS.
10. Disable unneeded services.
11. Configure static routing between edge routers and the ISP.

Router Firewalls and Intrusion Prevention

Configure a firewall on edge routers using Context-Based Access Control (CBAC) or SDM Zone-Based
Firewall tools. The firewall must allow external SSH connections, VPN traffic, and NTP.
Configure a Cisco IOS Intrusion Prevention System (IPS) on the edge router's internal and external interfaces.

Switch Security Measures

The following steps should be taken to secure and harden switches.
1. Configure the enable secret, console, and vty passwords.
2. Encrypt all passwords, which should be a minimum of 10 characters. Passwords should include a combination of uppercase, lowercase, numbers, and special characters.
3. Configure a login banner warming unauthorized users of the penalties of accessing this device.
4. Configure an administrative user with privilege level 15 and a secret password.
5. Configure NTP to access a centralized synchronized time source.
6. Configure an SSH server and disable Telnet access.
7. Disable the HTTP server.
8. Configure centralized authentication using AAA and RADIUS.
9. Configure forced trunking mode on trunk ports.
10. Change the native VLAN for trunk ports to an unused VLAN.
11. Enable storm control for broadcasts.