Implementing Cisco IOS Network Security

Practice Labs™

Implementing Cisco IOS Network Security

Powered by Practice Labs

Lab Outline

The 210-260 IINS Practice Lab will provide you with the necessary platform to gain hands on skills using real Cisco Routers, Switches and Firewalls. By completing the lab tasks you will improve your practical skills in securing routers and switches and their associated networks, implementing the Cisco ASA firewall and creating SSL and IPSec based VPNs.

These same tasks will help you understand the objectives and competencies required by the Implementing Cisco IOS Network Security 210-260 exam.

Outcomes

After completing this Practice Lab, students will be able to:

- Configure and verify switch security features
- Configure security and the management plane on cisco routers using the CLI
- Setup IOS security features
- Configure VLANs, Trunking and Spanning Tree
- Be familiar with layer 2 best practices
- Implement Zone Based Policy Firewall using the CLI
- Configure a Cisco Adaptive Security Appliance
- Implement Network Address Translation
- Configure port address translation and 801x authentication
- Configure Cisco IOS IPS using the CLI
- Implement a IOS IPSec Site-to-Site VPN
- Implement SSL VPN using ASA Device Manager
- Configure secure OSPF
- Implement control plane policing
- Configure policy based NAT on a Cisco ASA

Course Code
IINS 210-260

Skill Level
Intermediate

Released
Jan 2017

Duration
17 hours

Prerequisites

It is recommended that you have gained the following certification before attempting the 210-260 exam:

- Cisco Networking Devices Part 1 (ICND1)

No prior hands-on experience is required to use or complete this Practice Lab, however it would be beneficial to be familiar with:

- Windows operating systems
- Cisco IOS networking and concepts

Who is it For?

The 210-260 certificate is aimed at those wanting to enter a career in network security.

Additional Info

This Practice Lab focuses on the practical aspects of the IINS 210-260 exam objectives. It is therefore advised to refer to your own course materials to gain a deeper understanding of any theoretical aspects of the exam objectives.

Support 9am-5pm(GMT) : +44 (0) 203 588750
E-mail: sales@practice-labs.com

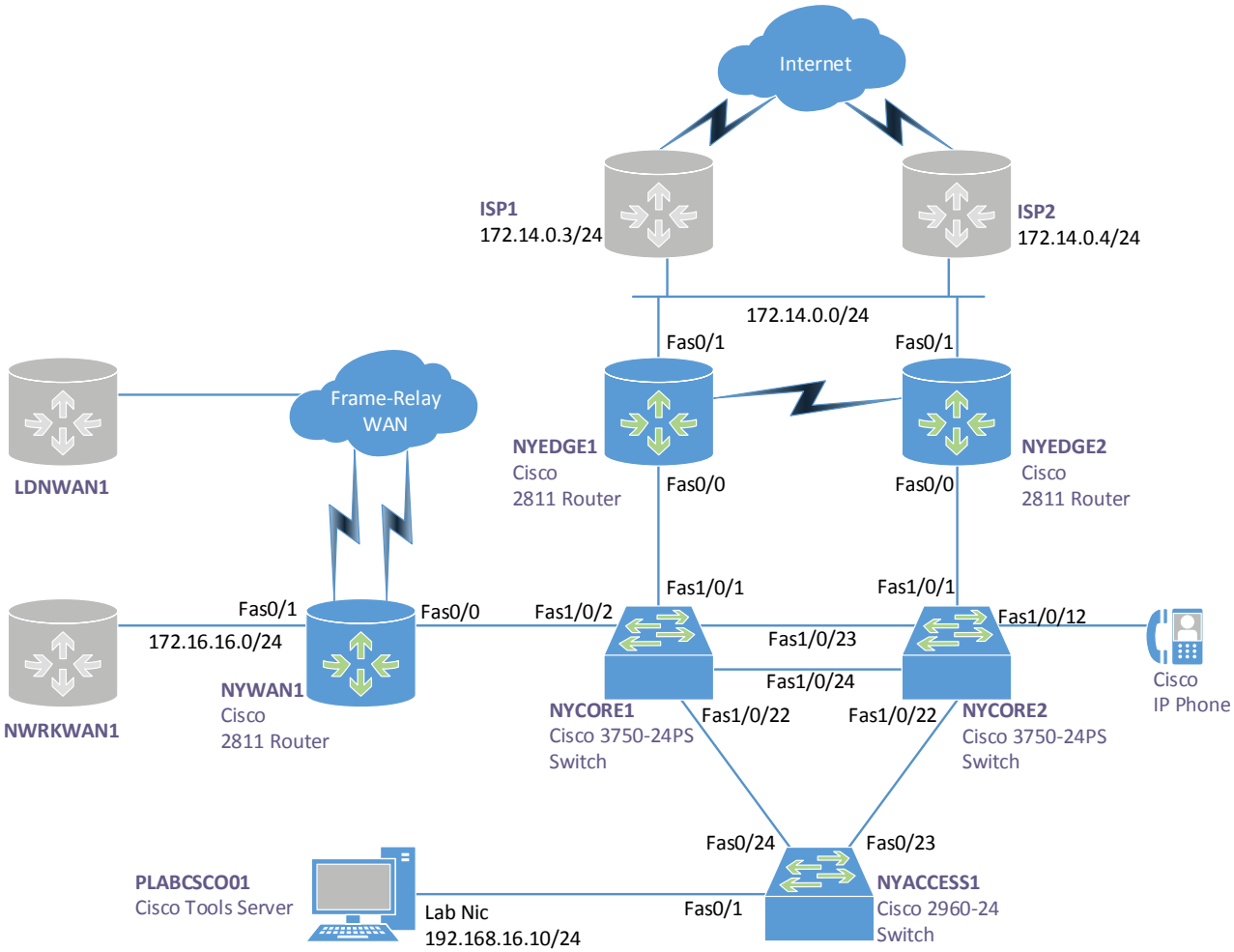
Company No. 05939037 VAT No. 900079851

Implementing Cisco IOS Network Security

Powered by Practice Labs

Lab Topologies

You will also have access to the following topologies:



Implementing Cisco IOS Network Security

Powered by Practice Labs

Modules and Exercises

Implement Security on Cisco Routers using the CLI

- Introduction
- Exercise 1 - Using the CLI AutoSecure feature
- Exercise 2 - Verifying security features implemented by
- AutoSecure
- Summary

Securing the Management Plane on Cisco Routers using the CLI

- Introduction
- Exercise 1 - Securing remote access using SSH and HTTPS
- Exercise 2 - Configuring custom privilege levels and views
- Exercise 3 - Cisco IOS and key network services
- Summary

Implement IOS Features to Mitigate Threats in a Network

- Introduction
- Exercise 1 - Implementing ACLs using the CLI to mitigate address spoofing
- Exercise 2 - Implementing ACLs using CCP to mitigate against ICMP reconnaissance attacks
- Exercise 3 - Using TCP intercept to help prevent DOS attacks
- Exercise 4 - Configure and verify VACLs
- Summary

Implement VLANs and Trunking

- Introduction
- Exercise 1 - Configuring VLANs and Trunks
- Exercise 2 - Configuring interVLAN routing
- Exercise 3 - Securing layer 2
- Exercise 4 - Configuring port security
- Summary

Spanning Tree and other Layer 2 Best Practices

- Introduction
- Exercise 1 - Spanning tree portfast and rapid spanning tree
- Exercise 2 - Locking down switchports
- Exercise 3 - ARP inspection DHCP snooping and IP source guard
- Summary

Implement Zone Based Policy Firewall using the CLI

- Introduction
- Exercise 1 - Configuring zone to zone policy using the CLI
- Exercise 2 - Testing the zone to zone policy
- Exercise 3 - Configuring the self zone using the CLI
- Summary

Implement the Cisco Adaptive Security Appliance

- Introduction
- Exercise 1 - Configuring Core ASA Features
- Exercise 2 - Configuring NAT
- Exercise 3 - Configuring a Security Policy
- Exercise 4 - Modular Policy Framework
- Summary

Implement Network Address Translation and Port Address Translation

- Introduction
- Exercise 1 - Translating inside source addresses
- Exercise 2 - Overloading inside source addresses
- Summary

Configure Cisco IOS IPS using the CLI

- Introduction
- Exercise 1 - Configure Cisco IOS IPS using the CLI
- Exercise 2 - Verify the IPS
- Summary

Implement an IOS IPSec Site-to-Site VPN with Pre-Shared Key Authentication

- Introduction
- Exercise 1 - Implement an IOS IPSec site-to-site VPN using the CLI
- Summary

Implement SSL VPN using ASA Device Manager

- Introduction
- Exercise 1 - Implement a Clientless SSL VPN using the Cisco ASA Device Manager
- Exercise 2 - Implement AnyConnect using the Cisco ASA
- Device Manager
- Summary

Company No. 05939037 VAT No. 900079851

Implementing Cisco IOS Network Security

Powered by Practice Labs

Configuring Secure OSPF with Authentication

- Introduction
- Exercise 1 - Examine the Initial OSPF Configuration
- Exercise 2 - Examine and Understand OSPF Security Vulnerabilities
- Exercise 3 - Configure OSPF with Authentication
- Summary

Control Plane Policing

- Introduction
- Exercise 1 - Configuring CoPP
- Exercise 2 - Verify and Test the CoPP Configuration
- Summary

Configure and Verify Switch Security Features

- Introduction
- Exercise 1 - ARP Inspection, DHCP Snooping and IP Source Guard
- Exercise 2 - Private VLANs (PVLANs)
  Summary

Policy Based NAT on a Cisco ASA

- Introduction
- Exercise 1 - Configuring Policy Based NAT with Source and Destination IP Addresses
- Exercise 2 - Configuring Policy Based NAT using Destination Ports
- Summary

Configuring Secure Network Management Features and Services

- Introduction
- Exercise 1 - Configuring SNMP
- Exercise 2 - Use SCP for a Secure File Transfer
  Summary

Configuring 801x Port Based Authentication

- Introduction
- Exercise 1 - Enable and Configure Port Based
- Authentication for a Single Client
- Summary

Company No. 05939037 VAT No. 900079851