Implementing Cisco IOS Network Security (210-260), Skill Labs

Course Specifications

Course Number: ACI76-038SL_rev1.0
Lab Length: Approximately 15 hours

Implement Security on Cisco Routers Using the CLI (210-260)

Introduction
Objective

The Implement Security on Cisco Routers Using the CLI lab provides you with the instructions and Cisco hardware to develop your hands-on skills in the following topics:

- Using the CLI to Implement Security Features Using the AutoSecure Feature
- Verify the Security Features Implemented with AutoSecure

Implement IOS Features to Mitigate Threats in a Network (210-260)

Introduction
Objective

The Implement IOS Features to Mitigate Threats in a Network lab provides you with the instructions and Cisco hardware to develop your hands-on skills in the following topics:

- Implementing ACLs Using the CLI to Mitigate Address Spoofing
- Implementing ACLs Using the CLI to Mitigate Against ICMP Reconnaissance Attacks
- Using TCP Intercept to Help Prevent DoS Attacks
- Configuring and Verifying VACLs

Spanning Tree and Other Layer 2 Best Practices (210-260)

Introduction
Objective

The Spanning Tree and Other Layer 2 Best Practices module provides you with the instructions and Cisco hardware to develop your hands-on skills in the following topics:

- Configure spanning tree portfast and rapid spanning tree.
- Lock down switchports.

Implement Zone-Based Policy Firewall Using the Command-Line Interface (210-260)

Introduction
Objective

By completing this lab, you will be able to:

Security Zone Configuration

- Create and configure security zones for network segmentation.
- Assign router interfaces to appropriate security zones.
- Understand the self zone and its special properties.
- Configure zone membership for different network segments.

Traffic Classification with Class Maps

- Create class maps to identify specific traffic types.
- Use match statements for protocol and ACL-based classification.
- Configure match-any and match-all logical operations.
- Build hierarchical class maps for complex traffic patterns.

Policy Creation and Application

- Configure policy maps with appropriate security actions.
- Apply inspect, pass, drop, and log actions to traffic classes.
- Create zone pairs defining directional traffic flow.
- Apply service policies to zone pairs.

Zone-Based Policy Firewall Verification and Troubleshooting

- Use show commands to verify zone configuration.
- Monitor active sessions and connection states.
- Troubleshoot policy misconfigurations.
- Analyze dropped packets and policy violations.

Cisco CCNA Security 210-260 Objective Mapping

Task Area	Exam Objective Reference
Zone Configuration	2.2 Configure and verify Cisco IOS zone-based firewalls
Class Maps	2.2.a Configure class maps
Policy Maps	2.2.b Configure policy maps
Zone Pairs	2.2.c Configure service policies
Verification	2.2.d Verify zone-based firewall operation

Overview

This hands-on lab provides comprehensive practice in implementing zone-based policy firewall (ZBPF) on Cisco IOS routers—a critical skill for network security professionals and Cisco CCNA Security 210-260 certification candidates. ZBPF represents a significant evolution from the classic firewall context-based access control [CBAC], offering a more intuitive and flexible approach to securing network perimeters. Unlike traditional access control lists (ACLs) that filter traffic based on interfaces, ZBPF groups interfaces into security zones and applies policies to traffic moving between these zones, providing a more scalable and manageable security architecture.

Through guided exercises using GNS3 you'll develop proficiency in creating security zones that logically group network interfaces, configuring class maps to identify specific traffic types for inspection, building policy maps that define security actions (inspect, drop, pass), and establishing zone pairs that control traffic flow between zones. You'll learn how ZBPF's stateful inspection engine tracks connection states, understand the critical difference between inter-zone and intra-zone traffic, and master the verification commands essential for troubleshooting firewall policies. These configurations represent real-world scenarios where organizations need granular control over traffic flows while maintaining stateful security inspection.

Understanding ZBPF implementation is essential for modern network security as it provides a structured approach to implementing defense-in-depth strategies. ZBPF's zone concept aligns with how security professionals think about network segmentation—grouping similar trust levels together and controlling traffic between different trust zones. Organizations rely on ZBPF to enforce security policies that are both powerful and maintainable, allowing them to protect critical resources while enabling necessary business communications. The modular nature of ZBPF configurations makes it easier to adapt to changing security requirements without complete policy rewrites.

	Key Term	Description
1	ZBPF	Zone-based policy firewall—zone-centric security architecture
2	Security Zone	Logical grouping of interfaces with similar security requirements
3	Class Map	Configuration element that identifies and classifies traffic
4	Policy Map	Defines security actions for classified traffic
5	Zone Pair	Directional relationship between two security zones
6	Self Zone	Special zone representing the router itself
7	Stateful Inspection	Tracking connection states for intelligent filtering
8	Inter-zone Traffic	Traffic flowing between different security zones
9	Intra-zone Traffic	Traffic within the same security zone
10	Service Policy	Policy map applied to a zone pair
11	Inspect Action	Stateful inspection allowing return traffic
12	Class-Default	Catch-all class for unmatched traffic

Implement the Cisco Adaptive Security Appliance (210-260)

Introduction
Objective

By completing this lab, you will be able to:

ASA Basic Configuration and Security Levels

- Configure ASA hostname, domain, and management settings.
- Set up interfaces with appropriate security levels.

- Understand traffic flow based on security levels.
- Configure inter-interface communication policies.

Access Control Lists and Object Groups

- Create network and service object groups.
- Implement ACLs using object group references.
- Understand ACL processing with NAT.
- Configure time-based access control.

NAT Configuration on ASA

- Configure Auto NAT (Object NAT).
- Implement Manual NAT for complex scenarios.
- Set up static NAT for server publishing.
- Understand NAT precedence and processing order.

Advanced Security Features

- Enable and configure stateful packet inspection.
- Implement application layer inspection.
- Configure threat detection and botnet filtering.
- Verify security policies using packet-tracer.

Overview

This hands-on lab provides comprehensive practice in implementing the Cisco Adaptive Security Appliance (ASA)—a critical skill for network security professionals and Cisco CCNA Security 210-260 certification candidates. The Cisco ASA is a purpose-built security appliance that combines firewall, antivirus, intrusion prevention, and virtual private network (VPN) capabilities, providing comprehensive security and networking services for organizations of all sizes. Unlike traditional routers with security features added, the ASA is designed from the ground up for security, offering superior performance and advanced threat protection.

Through guided exercises using an ASA simulator, you'll develop proficiency in configuring ASA security levels to control traffic flow between network zones, implementing access control lists with object groups for scalable policy management, configuring various Network Address Translation (NAT) types specific to ASA architecture, and enabling advanced security features like stateful packet inspection and application layer inspection. You'll learn how the ASA's security level concept simplifies security policy implementation, understand the relationship between NAT and ACLs in ASA packet processing, and master the verification commands essential for troubleshooting ASA configurations. These configurations represent real-world scenarios where organizations deploy ASAs to protect their networks from external threats while enabling secure connectivity.

Understanding Cisco ASA implementation is essential for modern network security as it serves as the cornerstone of many enterprise security architectures. The ASA's unique approach to security through interface security levels, combined with its stateful inspection engine and application awareness, provides defense-in-depth that traditional firewalls cannot match. Organizations rely on ASAs to

segment their networks into security zones (inside, outside, DMZ), control traffic between these zones based on business requirements, and provide secure remote access through integrated VPN capabilities. The skills developed in this lab form the foundation for advanced ASA features including high availability, clustering, and integration with next-generation security services.

	Key Term	Description
1	ASA	Adaptive Security Appliance—Cisco's dedicated firewall platform
2	Security Level	Numeric value (0–100) defining interface trust level
3	Nameif	Logical name assigned to ASA interface
4	Stateful Inspection	Tracking connection states for intelligent packet filtering
5	Object Group	Collection of similar items for simplified policy management
6	Auto NAT	NAT configured within network object definition
7	Manual NAT	Flexible NAT configured in global configuration
8	ACL	Access control list for traffic filtering
9	MPF	Modular Policy Framework for advanced policies
10	Application Inspection	Deep packet inspection of application protocols
11	Connection Table	Database of active connections through ASA
12	Packet-Tracer	ASA tool for simulating and debugging packet flow

Implement Network Address Translation and Port Address Translation (210-260)

Introduction
Objective

By completing this lab, you will be able to:

Static Network Address Translation Configuration

- Configure one-to-one address mappings for servers.
- Understand bidirectional translation for inbound access.
- Verify static translations using show commands.
- Troubleshoot static NAT connectivity issues.

Dynamic Network Address Translation Implementation

- Create and configure public address pools.
- Define access lists to identify NAT candidates.
- Understand pool exhaustion and timeout behavior.
- Monitor dynamic translation allocation.

Port Address Translation (Network Address Translation Overload) Configuration

- Configure many-to-one translation using ports.
- Implement PAT using interface address.
- Configure PAT with address pools.
- Verify port allocation and translation.

Port Forwarding Setup

- Configure static PAT for service publishing.
- Map multiple services through single public IP.
- Understand port redirection concepts.
- Test inbound connectivity to internal servers.

Cisco CCNA Security 210-260 Objective Mapping

Task Area	Exam Objective Reference
NAT Configuration	2.4 Configure and verify network address translation
Static NAT	2.4.a Configure static NAT
Dynamic NAT	2.4.b Configure dynamic NAT
PAT Configuration	2.4.c Configure PAT/NAT overload
Port Forwarding	2.4.d Configure port forwarding

Overview

This hands-on lab provides comprehensive practice in implementing network address translation (NAT) and port address translation (PAT) on Cisco routers—critical skills for network security professionals and Cisco CCNA Security 210-260 certification candidates. NAT and PAT are fundamental technologies that enable private IP addresses to communicate with public networks while conserving the limited IPv4 address space and providing an additional layer of security by hiding internal network structure. These technologies are essential in virtually every enterprise network, allowing thousands of internal devices to share a single or small pool of public IP addresses.

Through guided exercises using GNS3, you'll develop proficiency in configuring all major NAT types: static NAT for servers requiring consistent public addresses, dynamic NAT for client pools requiring temporary public access, PAT (also called NAT overload) for maximum address conservation, and port forwarding for publishing internal services. You'll learn to identify inside and outside interfaces, create address pools, define access lists for NAT selection, and use verification commands to troubleshoot translation issues. These configurations represent real-world scenarios where organizations must balance public IP address conservation with the need to provide internal users with Internet access and publish services to external clients.

Understanding NAT and PAT implementation is essential for modern network security as these technologies provide the first line of defense by obscuring internal network topology from external threats. Beyond security benefits, NAT/PAT enables organizations to use private RFC 1918 addresses internally while maintaining full Internet connectivity, significantly extending the lifespan of IPv4 addressing. The ability to configure various NAT types allows network engineers to meet diverse requirements from simple client Internet access to complex server publishing scenarios, all while maintaining security and conserving valuable public IP addresses.

	Key Term	Description
1	NAT	Network address translation—technology for IP address remapping
2	PAT	Port address translation—NAT using port numbers for uniqueness
3	NAT Overload	Cisco term for PAT, many-to-one translation
4	Inside Local	Private IP address of internal host
5	Inside Global	Public IP address representing internal host externally
6	Outside Local	How internal network sees external host address
7	Outside Global	Actual IP address of external host
8	NAT Pool	Range of public IP addresses for dynamic NAT
9	Static NAT	Permanent one-to-one address mapping
10	Dynamic NAT	Temporary mapping from address pool
11	Port Forwarding	Redirecting specific ports to internal hosts
12	Translation Table	Database of active NAT mappings

Configure Cisco IOS IPS Using the CLI (210-260)

Introduction
Objective

By completing this lab, you will be able to:

IPS Infrastructure Configuration

- Create and configure IPS storage directories on router flash .
- Initialize IPS configuration with proper file locations.
- Understand memory constraints and signature management.
- Configure public crypto keys for signature updates.

Signature and Category Management

- Retire and unretire signature categories appropriately.
- Understand hierarchical signature organization.
- Select appropriate signatures for network environment.
- Manage memory usage through selective signature loading.

Event Notification Configuration

- Configure SDEE for structured event reporting.
- Implement syslog for real-time event streaming.
- Understand differences between notification methods.
- Set up proper event buffering and storage.

IPS Implementation and Monitoring

- Apply IPS rules to specific interfaces and directions.
- Verify IPS operation using show commands.
- Interpret IPS statistics and event logs.
- Troubleshoot common IPS configuration issues.

Cisco CCNA Security 210-260 Objective Mapping

Task Area	Exam Objective Reference
IPS Configuration	2.3 Configure and verify network infrastructure security
Signature Management	2.3.a Describe IPS/IDS fundamentals
Event Notification	2.3.b Configure and verify IOS IPS
Interface Application	2.3.c Monitor IPS events and alerts
Troubleshooting	2.3.d Troubleshoot IPS implementation

Overview

This hands-on lab provides comprehensive practice in implementing Cisco IOS intrusion prevention system (IPS) using command line interface (CLI)—a critical skill for network security professionals and Cisco CCNA Security 210-260 certification candidates. IOS IPS transforms a Cisco router into an inline intrusion prevention sensor, monitoring network traffic in real-time and taking immediate action to block malicious activities before they can compromise network security. Unlike traditional firewalls that focus on ports and protocols, IPS examines packet payloads and traffic patterns to detect and prevent sophisticated attacks.

Through guided exercises using the simulator, you'll develop proficiency in configuring IPS signature files, managing signature categories to optimize router memory usage, implementing Security Device Event Exchange (SDEE) and syslog for event notification, and applying IPS rules to specific interfaces. You'll learn the critical difference between retiring and unretiring signatures, understand how IPS processes traffic inline versus promiscuously, and master the verification commands essential for monitoring IPS effectiveness. These configurations represent real-world scenarios where organizations need advanced threat protection at network boundaries without dedicated IPS appliances.

Understanding IOS IPS implementation is essential for modern network security as it provides defense-in-depth by adding application-layer inspection to existing router infrastructure. Organizations leverage IOS IPS to detect and prevent zero-day attacks, buffer overflows, SQL injection attempts, and other sophisticated threats that traditional access control lists (ACLs) cannot address. The ability to configure IPS on existing routers provides cost-effective security enhancement, particularly for branch offices and small to medium businesses that cannot justify dedicated IPS appliances.

	Key Term	Description
1	IPS	Intrusion prevention system—inline security device that blocks detected threats
2	IDS	Intrusion detection system—passive monitoring system that alerts on threats
3	Signature	Pattern or rule that identifies specific attack or malicious behavior
4	Signature Category	Logical grouping of related signatures for management purposes
5	SDEE	Security Device Event Exchange—XML-based IPS event notification protocol
6	Syslog	Standard logging protocol for sending event messages to central server
7	Inline Mode	IPS deployment where traffic passes through the sensor
8	Promiscuous Mode	IDS deployment using port mirroring without blocking capability
9	Retire/Unretire	Disable/enable signatures for active inspection
10	False Positive	Legitimate traffic incorrectly identified as malicious
11	Signature Update	Process of downloading latest threat signatures from Cisco
12	Event Action	Response taken when signature matches (drop, reset, alert)

Implement an IOS IPSec Site-to-Site VPN with Pre-Shared Key Authentication (210-260)

Introduction
Objective

By completing this lab, you will be able to:

IKE Phase 1 Configuration and Security Associations

- Configure IKEv2 policies defining encryption, hashing, and DH groups.
- Implement pre-shared key authentication between VPN peers.
- Understand IKE security association establishment and lifetime.
- Verify Phase 1 connectivity and troubleshoot negotiation issues.

IPSec Phase 2 Transform Sets and Encryption

- Create transform sets specifying ESP encryption and authentication.
- Understand the relationship between Phase 1 and Phase 2 security.
- Configure IPSec security association parameters and lifetime.
- Select appropriate encryption and hashing algorithms for data protection.

Crypto Maps and Traffic Selection

- Create crypto maps binding all IPSec parameters together.
- Configure access control lists identifying interesting traffic.
- Apply crypto maps to appropriate router interfaces.
- Understand the relationship between routing and VPN traffic flow.

VPN Verification and Troubleshooting

- Use show commands to verify VPN establishment and operation.
- Interpret IPSec security association database information.
- Troubleshoot common VPN connectivity issues.
- Monitor VPN performance and packet statistics.

Cisco CCNA Security 210-260 Objective Mapping

Task Area	Exam Objective Reference
ISAKMP Configuration	3.4 Configure and verify site-to-site IPsec VPN
Transform Sets	3.4.a Describe IPsec protocols and delivery modes
Crypto Maps	3.4.b Configure site-to-site VPN with pre-shared keys
Access Lists	3.4.c Verify VPN operations
Troubleshooting	3.4.d Troubleshoot site-to-site VPN connectivity

Overview

This hands-on lab provides comprehensive practice in implementing Internet Protocol Security (IPSec) site-to-site Virtual Private Networks (VPNs) using pre-shared key authentication on Cisco IOS routers—a critical skill for network security professionals and Cisco CCNA Security 210-260 certification candidates. IPSec site-to-site VPNs enable secure communication between geographically separated networks over untrusted public networks, providing confidentiality, integrity, and authentication for corporate data transmission.

Through guided exercises using GNS3, you'll develop proficiency in configuring both phases of IPSec VPN establishment: Internet Key Exchange (IKE) Phase 1 for secure key negotiation and IPSec Phase 2 for actual data encryption. You'll learn to implement pre-shared key authentication, configure transform sets defining encryption and hashing algorithms, create crypto maps binding all VPN parameters, and identify interesting traffic that triggers VPN establishment. These configurations represent real-world scenarios where organizations need secure connectivity between branch offices, data centers, or partner networks.

Understanding IPSec site-to-site VPN implementation is essential for modern network security as it provides the foundation for secure wide area network (WAN) communications. Organizations rely on IPSec VPNs to extend their private networks across public infrastructure while maintaining data confidentiality and integrity. The pre-shared key authentication method, while simpler than certificate-based authentication, provides robust security when properly implemented with strong keys and is widely deployed in enterprise environments where scalability requirements are moderate.

	Key Term	Description
1	IPSec	Internet protocol security—framework providing encryption and authentication for IP packets
2	ISAKMP	Internet security association and key management protocol—negotiates security associations
3	IKE Phase 1	Initial key exchange phase establishing secure channel for VPN negotiation
4	IKE Phase 2	IPSec phase negotiating security associations for actual data transfer
5	Pre-Shared Key	Symmetric key manually configured on both VPN peers for authentication
6	Transform Set	Collection of encryption and authentication algorithms for IPSec
7	Crypto Map	Configuration element binding IPSec parameters to router interface
8	Security Association	Agreed security parameters between IPSec peers for data protection
9	ESP	Encapsulating Security Payload—IPSec protocol providing encryption and

	Key Term	Description
		authentication
10	DH Group	Diffie-Hellman group defining key exchange strength
11	Interesting Traffic	Data matching ACL that triggers VPN tunnel establishment
12	Perfect Forward Secrecy	Feature ensuring unique keys for each IPSec security association

Implement SSL VPN using ASA Device Manager (210-260)

Introduction
Objective

The Implement SSL VPN using ASA device manager module provides you with the instructions and Cisco hardware to develop your hands-on skills in the following topics:

- Implement a Clientless SSL VPN using the Cisco ASA Device Manager
- Implement AnyConnect using the Cisco ASA Device Manager

Configuring Secure OSPF with Authentication (210-260)

Introduction
Objective

The Configuring Secure OSPF with Authentication module provides you with the instructions and Cisco hardware to develop your hands-on skills in examining OSPF security threats and configuring OSPF to mitigate these threats.

In this module, you will perform the following exercises:

- Examine the Initial OSPF Configuration
- Examine and Understand OSPF Security Vulnerabilities
- Configure OSPF with Authentication

Control Plane Policing (210-260)

Introduction
Objective

The Control Plane Policing module provides you with the instructions and Cisco hardware to develop your hands-on skills in the following topics:

- Configure control plane policing.
- Verify and test the control plane policing configuration.

Configure and Verify Switch Security Features (210-260)

Introduction
Objective

The Configure and Verify Switch Security Features module provides you with the instructions and Cisco hardware to develop your hands on skills in configuring various switch security technologies as outlined in the following list of exercises:

- ARP inspection DHCP snooping and IP source guard
- Configuring Private VLANs

Policy Based NAT on a Cisco ASA (210-260)

Introduction
Objective

By completing this lab, you will be able to:

ASA Interface Configuration and Security Levels

- Configure ASA interfaces with appropriate names and security levels.
- Understand the relationship between security levels and traffic flow.
- Implement interface IP addressing for inside, outside, and DMZ zones.
- Verify interface configuration and connectivity.

Object Groups and Access Control Implementation

- Create network objects for subnet and host definitions.
- Configure service objects for protocol and port specifications.
- Implement object groups for simplified policy management.
- Apply access control lists using object group references.

Policy-Based NAT Configuration

- Differentiate between Auto NAT and Manual NAT capabilities.
- Configure Object NAT for source address translation.
- Implement Manual NAT for policy-based translation decisions.
- Create NAT

NAT Verification and Troubleshooting

- Use packet-tracer command to simulate and verify NAT behavior.
- Analyze NAT translation tables and precedence rules.
- Troubleshoot common NAT configuration issues.
- Monitor active NAT translations and connection states.

Cisco CCNA Security 210-260 Objective Mapping

Task Area	Exam Objective Reference
ASA Configuration	2.6 Configure and verify Cisco ASA interface security levels
Object Groups	2.7 Configure and verify Cisco ASA default modular policy framework
NAT Configuration	2.8 Configure and verify Cisco ASA NAT types
ACL Implementation	2.5 Configure and verify Cisco ASA access management
Troubleshooting	2.9 Configure and verify Cisco ASA security features

Overview

This hands-on lab provides comprehensive practice in implementing policy-based Network Address Translation (NAT) on Cisco Adaptive Security Appliance (ASA) firewalls—a critical skill for network security professionals and Cisco CCNA Security 210-260 certification candidates. Policy-based NAT, also known as conditional NAT, enables administrators to make translation decisions based on both source and destination addresses, providing granular control over address translation in complex network environments.

Through guided exercises using GNS3, you'll develop proficiency in configuring various NAT types including Auto NAT (Object NAT) and Manual NAT (Twice NAT), implementing NAT policies based on destination criteria, and troubleshooting NAT configurations using ASA verification commands. You'll learn how policy-based NAT differs from traditional NAT implementations and when to apply each type for optimal network security and connectivity.

Understanding policy-based NAT is essential for modern network security as it enables sophisticated traffic management scenarios such as translating internal hosts differently based on their destination, implementing NAT exemption for VPN traffic, and providing conditional access to demilitarized zone (DMZ) resources. These skills are fundamental for securing enterprise networks while maintaining necessary connectivity between different security zones.

	Key Term	Description
1	Policy-Based NAT	NAT translation decisions based on both source and destination addresses
2	Object NAT (Auto NAT)	NAT configured within network object definition, limited to source translation
3	Manual NAT (Twice NAT)	NAT configured in global config, allows source and destination translation
4	NAT Precedence	Order of NAT rule processing: Manual NAT, Auto NAT, After-Auto Manual NAT
5	Security Levels	Numeric values (0–100) determining trust levels and traffic flow between interfaces
6	Object Groups	Logical groupings of network objects, services, or protocols for policy application
7	Access Control Lists	Rules defining permitted or denied traffic based on source, destination, and service
8	Dynamic PAT	Many-to-one translation using IP address and port number modification
9	Static NAT	One-to-one permanent mapping between real and translated addresses
10	NAT Exemption	Configuration preventing NAT for specific traffic, typically for VPN connections
11	Translation Table (xlate)	ASA table containing active NAT translations and connection information
12	Packet-Tracer Command	ASA diagnostic tool simulating packet flow through security policies and NAT

Configuring Secure Network Management Features and Services (210-260)

Introduction
Objective

The Configuring Secure Network Management Services module provides you with the instructions and Cisco hardware to develop your hands-on skills in configuring services including Simple Network Management Protocol and Secure Copy Protocol. This module contains the following topics:

- Configure and verify secure access to SNMPv2c and SNMPv3 using an access list.
- Use SCP for a secure file transfer.

Configuring 802.1x Port-Based Authentication (210-260)

Introduction
Objective

The Configuring 802.1x Port-Based Authentication module provides you with the instructions and Cisco hardware to develop your hands-on skills in configuring port-based authentication. This module contains the following topics:

- Enable and configure 802.1x port-based authentication on a port on the switch.
- Configure a switch to act as a 802.1x port-based authentication supplicant.
- Observe the negotiation process of these two devices.