Check Point Security Administration NGX I

- Course Objectives

Course Layout

- Prerequisites
- Check Point Certified Security Administrator (CCSA)

Exam-Number Note: 156-215.1

- Revision Differences

Recommended Setup for labs

What's New in VPN-1 NGX

- Security-Management Cost Reduction
- Network and Application Security
- VPN Management
- For More Information

VPN-1 NGX Overview

- Objectives
- Key Terms

VPN-1 NGX Architecture

- SmartConsole and SmartDashboard
- SmartCenter Server
- Security Gateway

How VPN-1 NGX Works

- The INSPECT Engine

Distributed Deployments

- SVN Foundation
- Secure Internal Communications (SIC)

SmartConsole Components

- SmartDashboard
- SmartView Tracker
- SmartView Monitor
- Eventia Reporter

Lab 1: NGX Stand-Alone Installation

Review

- Review Questions
- Review Answers

The Security Policy

- Objectives
- Key Terms

Security Policy Defined

- What Is a Security Policy?
- Security Policy Considerations

Rule Base Defined

Lab 2: Launching SmartDashboard

Lab 3: Defining Basic Objects

Detecting IP Spoofing

- Configuring Anti-Spoofing

Multicasting

- Configuring Multicast Access Control
- Interface Properties Multicast Restrictions
- IGMP
- Multicast Routing Protocols
- Multicast Traffic

Creating the Rule Base

- Basic Rule Base Concepts
- The Default Rule

- Basic Rules
- Implicit/Explicit Rules
- Control Connections

Completing the Rule Base
- Understanding Rule Base Order

Lab 4: Configuring Anti-Spoofing Measures
Lab 5: Defining Basic Rules
Security Policy Command-Line Options
- cpstart
- cpstop
- fw Commands

Advanced Rule Base Functions
- Object Cloning

Lab 6: Creating Objects Using Object Cloning
Rule Base Management
Database Revision Control and Policy Package Management
- Database Revision Control
- Policy Package Management

Lab 7: Using Database Revision Control
Review
- Review Questions
- Review Answers

Monitoring Traffic and Connections
- Objectives
- Key Terms

SmartView Tracker
- SmartView Tracker Login
- Log Types
- SmartView Tracker Views
- Log-File Management
- Administrator Auditing
- Global Logging and Alerting
- Time Settings

Blocking Connections
- Terminating Active Connections

Lab 8: Blocking Intruder Connections
SmartView Monitor
- SmartView Monitor Login
- Key Features
- Monitoring Suspicious Activity Rules
- Monitoring Alerts
- Monitoring Gateways
- Monitoring Traffic or Counters
- Monitoring Tunnels
- Monitoring Remote Users

Lab 9: Setting Up Suspicious Activity Rule in SmartView Monitor
Lab 10: Checking Status in SmartView Monitor
Eventia Reporter
Report Types
- Eventia Reporter Standard Reports
- Eventia Reporter Express Reports
- Predefined Reports

Eventia Reporter Considerations
- Log-Consolidation Process
- Stand-Alone vs. Distributed Deployments

- Log Availability vs. Log Storage/Processing
- Log-Consolidation Considerations
- Report-Generation Considerations

Eventia Reporter Database Management
- Database Tuning
- Database-Configuration Modifications
- Database-Size Maintenance
- Backing Up

Eventia Reporter Licensing
Review
- Review Questions
- Review Answers

SmartDefense
- Objectives
- Key Terms

Active Defense
- Components of SmartDefense
- SmartDefense Capabilities

SmartDefense in Action
- Anti-Spoofing Configuration Status
- Denial-of-Service Attacks
- IP and ICMP
- TCP
- Successive Events
- Web Intelligence
- Centralized Control Against Attacks
- Online Updates

SmartDefense Storm Center
- Storm Center Integration
- Planning Considerations

Lab 11: Configuring SmartDefense
Review
- Review Questions
- Review Answers

Network Address Translation
- Objectives
- Key Terms

Understanding Network Address Translation
- IP Addressing
- Dynamic (Hide) NAT
- Static NAT

Configuring NAT
- Global Properties
- Dynamic NAT Object Configuration
- Static NAT Object Configuration

Manual NAT
- When to Use Manual NAT
- Configuring Manual NAT
- Special Considerations

Lab 12: Configuring Hide NAT
Lab 13: Configuring Static NAT
Review
- Review Questions
- Review Answers

Encryption and VPNs
- Objectives
- Key Terms

How Encryption Works
- Privacy
- Symmetric Encryption (Shared Key)
- Asymmetric Encryption
- Diffie-Hellman
- Message Integrity
- Two Phases of Encrypted Communication

IKE Encryption Scheme
- Encryption Algorithms
- Tunneling-Mode Encryption

Lab 14: Encryption Demonstration

Review
- Summary
- Review Questions
- Review Answers

Authentication
- Objectives
- Key Terms

Understanding Authentication
- User Authentication
- Session Authentication
- Client Authentication
- Authentication Types
- Authentication Schemes

User Authentication

Client Authentication
- How Client Authentication Works
- Sign-On Methods

Lab 15: Defining User Templates

Lab 16: Setting Authentication Parameters (Optional)

Lab 17: Defining Users

Lab 18: Configuring User Authentication

Lab 19: Configuring Client Authentication

Review
- Review Questions
- Review Answers

LDAP User Management with SmartDirectory
- Objectives
- Key Terms

LDAP Servers
- Introduction to Account Management
- LDAP Features
- Multiple LDAP Servers

Integrating LDAP with VPN-1 NGX
- Exporting Users
- Using an Existing LDAP Server

Managing LDAP Users
- Organizational Units
- Before Starting Account Management
- Deleting an Object Tree