Check Point Security Administration NGX II

- Course Objectives

Course Layout

- Prerequisites
- Check Point Certified Security Expert (CCSE)

Exam-Number Note: 156-315.1

Recommended Setup for Labs

- Recommended Lab Topology
- IP Addresses
- Lab Terms
- Lab Stations

Installing VPN-1 NGX and Upgrading

- Objectives
- Key Terms

Preinstallation Configuration

Distributed Installation

Upgrading To VPN-1 NGX

- Upgrade Guidelines
- Upgrade Order
- Upgrade Export/Import
- Upgrading via SmartUpdate

NGX Backward Compatibility

- Supported Versions

Licensing VPN-1 NGX

- Obtaining Licenses
- Deploying Licenses

Upgrading Licenses to VPN-1 NGX

Licensing and Troubleshooting

- Viewing Licenses in User Center
- Viewing Licenses in SmartView Monitor

SmartCenter Server Pre-Upgrade Overview

- Pre-Upgrade Verification-Tool Syntax

SmartCenter Server Upgrade

- SmartCenter High Availability Upgrade
- SecurePlatform Upgrade
- Advanced Upgrade
- Upgrading on Windows

Security Gateway Upgrade

- Clustered-Deployment Upgrade
- SmartUpdate Upgrade
- Upgrading a Gateway Using SmartUpdate Upgrade
- SecurePlatform R54, R55, and Later Upgrade
- SecurePlatform NG FP2, FP3, or FP3 Edition 2 Upgrade
- Upgrading Gateway on Windows

Lab 1: Upgrading NG with AI R55 to NGX

Lab 2: Upgrading NG with AI Security Gateway via SmartUpdate (Optional)

Lab 3: NGX Distributed Installation

Lab 4: Installing VPN-1 Pro Gateway on SecurePlatform Pro

Review

- Review Questions
- Review Answers

Content Security

- Objectives
- Key Terms

Role of the Security Server
- Security Server Overview
- OPSEC

Understanding Content Security
Content Vectoring Protocol (CVP)
- Inspection

URI Filtering Protocol (UFP)
- How UFP Works

Implementing Content Security
- Security Considerations
- URI Filtering
- Mail — SMTP
- FTP Security Server
- Blocking FTP over HTTP for Specific Groups
- Java and ActiveX Stripping
- CVP Inspection

Resources and the Rule Base
- Proper Rule Placement
- Consequences of Incorrectly Configured Rules

CVP Load Sharing and Chaining
- CVP Chaining

Implementing the TCP Resource
- Configuring TCP Security Servers
- TCP Resource Properties
- UFP Tab
- CVP Tab

Lab 5: URL Screening by File
Review
- Review Questions
- Review Answers

Configuring VPNs
- Objectives
- Key Terms

IKE
- Gateway-to-Gateway Configuration
- Specifying Encryption

VPN Deployments
- Intranet VPNs
- Remote-Access VPNs

VPN Implementation
- Three Critical VPN Components

VPN Setup
- Understanding VPN Deployment

Simplified Intranet Setup
- VPN Community Principles

Integrating VPNs into a Rule Base
Lab 6: Two-Gateway IKE Encryption Configuration (Shared Secret)
Lab 7: Two-Gateway IKE Encryption Configuration (Certificates)
Review
- Review Questions
- Review Answers

Configuring Remote Access
- Objectives
- Key Terms

VPN-1 SecuRemote/SecureClient
- Using SecuRemote
- Configuring SecuRemote
- Rule Base Configuration

Configuring a Remote-Access VPN
- Configuring a Remote Access VPN Community
- Remote-Access Community Properties

Global Properties Settings
- Remote-Access Settings
- Client Authentication

Structure of a SecuRemote Connection
- Topology
- Authentication
- Key Exchange
- Connection
- Routing Considerations

Lab 8: Configuring Remote Access in an IKE VPN

Lab 9: Installing SecuRemote

Advanced Configurations
- Secure Domain Login
- Authentication by IP Address

SecuRemote Client

Lab 10: Using VPN-1 SecuRemote in an IKE VPN

The SecureClient GUI
- Authentication Screen
- SecureClient Settings Screen
- The Taskbar Menu

Enabling/Disabling Desktop PolicIES
- Retrieving Desktop Policies from Policy Servers

Obtaining Site Topology
- userc.C
- Overlapping VPN Domains

SecureClient Icon

Passwords
- Auto Local Logon
- Configuring Auto Local Logon
- Disabling Auto Local Logon

SecureClient Considerations
- Modifying Network Configuration
- Multiple Adapters
- SecureClient Files
- Upgrading SecureClient

SecureClient Diagnostics Tool
- Diagnostic Viewer
- Policy Viewer
- SmartView Tracker

Partial Topology Configuration

Connect Mode
- Connection Profiles

Office Mode
- Overview
- How Office Mode Works
- Office Mode by RADIUS Server
- DHCP Enhancements
- Office Mode per User
- Office Mode per Site

- Office Mode per IP Range
- Routing Considerations

Lab 11: Office Mode

Review

- Review Questions
- Review Answers

Enabling Voice Over IP Traffic

- Objectives
- Key Terms

Voice Over IP Basics

- Supported Protocols

Configuring VPN-1 NGX for H.323 based VoIP Traffic

Enabling VoIP Traffic in an H.323 Environment

- Gatekeeper-Object Configuration
- Configuring Gatekeeper Routing Mode
- Gateway-Object Creation (Optional)
- Configuring Gateway Routing Mode
- Configuring Global Properties
- Configuring the Rule Base for H.323 Traffic

Enabling VoIP Traffic in a SIP Environment

- Defining the VoIP SIP Domain
- Configuring Global Properties
- Configuring the Rule Base for SIP Traffic
- SIP Services

Lab 12: Configuring a Gateway for VoIP Communications

Review

- Review Questions
- Review Answers

Check Point QoS

- Objectives
- Key Terms

Check Point QoS Overview

- Check Point QoS Architecture
- Check Point QoS Deployment Considerations

Check Point QoS Policy

- Check Point QoS Rule Base
- QoS Action Properties
- Bandwidth Allocation and Rules

Differentiated Services

- DiffServ Marks for IPSec Packets
- Interaction between DiffServRules and Other Rules

Low Latency Queuing

- Low Latency Classes
- Low Latency Class Priorities
- When to Use Low Latency Queueing

Advanced Features

- Authenticated QoS
- Citrix MetaFrame Support
- Load Sharing

Monitoring QoS Policy

- SmartView Tracker
- SmartView Monitor
- Eventia Reporter

Optimizing Check Point QoS

Lab 13: Configuring Check Point QoS Policy
Review
- Review Questions
- Review Answers

High Availability and Clustering
- Objectives
- Key Terms

Management High Availability
- Primary vs. Secondary
- Active vs. Standby
- Restriction
- Synchronization

Lab 14: Deploying Management HA
HA and ClusterXL
- Key Elements
- Restrictions

Load Sharing
- Load Sharing Multicast Mode
- Load Sharing Unicast Mode
- How Pivot Mode Works
- HA vs. Load Sharing

State Synchronization
- Synchronization Modes
- Selective Synchronization
- Timing Issues

CPHA Commands
- cphastart
- cphastop
- cphaprob
- fw hastat

Debugging ClusterXL Issues
- fw ctl pstat Sync Output

ClusterXL Configuration Issues
- Modes of ClusterXL Supporting SecureXL
- Crossover-Cable Support between Two Cluster Members

Lab 15: Deploying New Mode HA
Lab 16: Manual Failover (Optional)
Lab 17: Configuring Load Sharing Unicast (Pivot) Mode
Lab 18: Configuring Load Sharing Multicast Mode (Optional)
Review
- Review Questions
- Review Answers