Check Point Security Administration NGX III

- Course Objectives

Course Layout

- Prerequisites

Recommended Setup for labs

- Recommended Lab Topology
- IP Addresses
- Lab Terms
- Lab Stations
- Default Rule Base

General Troubleshooting Methods

- Objectives
- Key Terms

Troubleshooting Guidelines

- Identifying the Problem
- Collecting Related In formation
- Listing Possible Causes
- Testing Causes Individually and Logically
- Consulting Various Reference Sources

What to Check Before Installing VPN-1 NGX

- IP Forwarding
- Routing
- Connectivity

IP Forwarding and Boot Security

SIC and ICA Issues

- SIC Port Use
- Root Causes
- Logging SIC
- Debugging SIC
- Maintaining SIC
- Using fwm sic_reset

Network Address Translation

- Client-Side Destination NAT
- Debugging NAT

Collecting Data

- Rule Base Issues
- NAT Issues
- Anti-Spoofing Issues
- SmartDashboard Issues
- Logging Issues
- Cluster Issues
- Security Server Issues
- OPSEC Server Issues
- LDAP Issues
- Core Dump and Dr. Watson Issues

Review

- Review Questions
- Review Answers

File Management

- Objectives
- Key Terms

cpinfo

- Overview
- cpinfo File

- InfoView
- Opening SmartDashboard in InfoView

objects_5_0.C and objects.C
- objects_5_0.C
- objects.C
- Object Properties in objects_5_0.C
- DbEdit
- objects_5_0.C Editing
- GuiDBedit

fwauth.NDB

$FWDIR/lib/*.def Files
- Example
- Modifying *.def Files

Log Files
- Active Log Files
- Audit Log Files
- Log Mechanism
- Troubleshooting Logging Issues
- Maintaining Logs and Log-Buffer Queue
- Configuring Object Properties

Debugging Logging
- Analysis Tools
- Debugging Log

Lab 1: Using cpinfo
Lab 2: Analyzing cpinfo in InfoView
Lab 3: Using GuiDBedit
Lab 4: Using fw logswitch and fwm logexport

Review
- Review Questions
- Review Answers

Protocol Analyzers
- Objectives
- Key Terms

tcpdump
- tcpdump Syntax
- tcpdump and Expressions
- Using tcpdump
- Viewing tcpdump Output

snoop
- Using snoop
- Reading snoop Output
- snoop and Security
- snoop Limitations

fw monitor
- Overview
- fw monitor Syntax
- INSPECT Virtual Machine
- Filter Expressions
- fw ctl chain
- Buffering Issues

Ethereal
- Using Ethereal
- Viewing Connection Beginnings
- Viewing Connections Dropped by Kernel
- Using Filters with Ethereal

Lab 5: Comparing Client-Side NAT vs. Server-Side NAT with fw monitor
Review
- Review Questions
- Review Answers

NGX Debugging Tools
- Objectives
- Key Terms

fw ctl debug
- fw ctl kdebug
- Kernel Modules
- fw ctl debug Flags

Debugging fwd/fwm
- fwd Daemon
- fwm Process
- Debugging
- fwd/fwm Debug Switches
- Debugging without Restarting fwd/fwm
- Debugging by Restarting fwd/fwm
- Stopping fwd debug

Debugging cpd
- Use

Lab 6: Using cpd and fwm Debugging
Review
- Review Questions
- Review Answers

fw advanced Commands
- Objectives
- Key Terms

fw Commands
fw tab Command
- fw tab Options
- Table Attributes
- fw tab Examples

fw ctl Commands
- fw ctl install
- fw ctl uninstall
- fw ctl iflist
- fw ctl arp
- fw ctl pstat
- fw ctl conn

Other fw Commands
- fw sam
- fw lichosts
- fw log
- fw repairlog
- fw mergefiles
- fw fetchlogs

fw Advanced Commands
- fw fwd
- fw fwm
- fw fetchlocal
- fw unloadlocal
- fw dbloadlocal
- fw defaultgen

- fw getifs
- fw stat

fwm Commands
- Use
- fwm load
- fwm dbload
- fwm logexport
- fwm dbexport/fwm dbimport
- fwm lock_admin

Lab 7: Using fwctl pstat
Lab 8: Using fw stat, fwm load, and fw unloadlocal
Review
- Review Questions
- Review Answers

Security Servers
- Objectives
- Key Terms

The Folding Process
- Overview
- Folding-Process Example
- Content-Security Rule Order
- Security Server Default Messages
- HTTP 1.0 and 1.1

Troubleshooting Security Server Issues
- Reviewing CPU and Memory
- Editing fwauthd.conf
- Listing Possible Causes
- Identifying Issue Sources
- Analyzing Results

Debugging Security Servers
- TD_ERROR_ALL_ALL Flag
- FTP Security Servers
- HTTP Security Servers
- SMTP Security Servers
- Multiple Security Server Troubleshooting

Review
- Review Questions
- Review Answers

VPN Debugging Tools
- Objectives
- Key Terms

IKE Basics
- Phase 1
- Phase 2
- Encryption Issue

Troubleshooting Overview
VPN Debugging Tools
- VPN Log Files
- vpn debug Command
- vpn Command
- Comparing SAs

Troubleshooting Tables
Lab 9: Running IKE Debugging on a Site-to-Site VPN
Review

Review Questions
Review Answers

Troubleshooting and Debugging SecuRemote/SecureClient
Objectives
Key Terms
Necessary Ports
Ports Used Through the Tunnel
Packet Flow
Packet Flow When Creating a Site
Packet Flow When Connecting/Resolving Gateway IP
Packet Flow When Connecting/IKE Negotiation
Packet Flow When Connecting/Encrypting Data
Link Selection for Remote Access
Overview
Link-Selection Methods in VPN-1 NGX
SecuRemote/SecureClient Debugging Tools
srfw monitor
cpinfo
IKE debug
sr_service Debug
IKE and sr_service Debug
sc log Debug
srfw ctl Debug
Enhanced Debugging Tool
Troubleshooting Table
Lab 10: Observing IKE Negotiation Between a Gateway and SecureClient
Lab 11: Running srfw monitor
Review
Review Question
Review Answer

Advanced VPN
Objectives
Key Terms
Route-Based VPN
Domain-Based VPN
VPN Tunnel Interface
VPN Routing Process
Best Practices
Numbered/Unnumbered VTIs
Configuring Numbered VTIs
Configuring Unnumbered VTIs
Dynamic VPN Routing
Configuring Dynamic VPN Routing Using OSPF
Wire Mode
How Wire Mode Works
Wire Mode in Route-Based VPN
Directional VPN Rule Match
Interface Groups
Tunnel Management
Permanent Tunnels
VPN Tunnel Sharing
Tunnel-Management Configuration
VPN Tunnel Sharing Configuration
Lab 12: Route-Based VPN Using Static Routes

Lab 13: Dynamic VPN Routing Using OSPF
Review
- Review Questions
- Review Answers

ClusterXL
- Objectives
- Key Terms

Configuration Recommendations
- Recommendations for ClusterXL
- Recommendations for State Synchronization

Troubleshooting ClusterXL
- cphaprob
- cphaprob state
- cphaprob -a if
- cphaprob –I list
- cphaprob -d <device> -s problem -t 0 register
- cpstat ha -f all .
- fw ctl debug -m cluster

Kernel Flags
- fwha_enable_if_probing and fwha_monitor_if_link_state
- fwha_restrict_mc_sockets(0 by Default)
- fwha_use_arp_packet_queue(0 by Default)
- fwha_send_gratuitous_arp_var
- fw_gratuitous_arp_timeout
- fw_allow_connection_traffic_drop (1 by Default)
- fwha_allow_simultaneous_ping
- fwconn_merge_all_syncs
- fwtcpstr_reject_synced (On by Default)

Lab 14: Manual Failover Using cphaprob -d device Command
Lab 15: Running cphastart -d
Review
- Review Question
- Review Answer

Appendix A: Using DbEdit