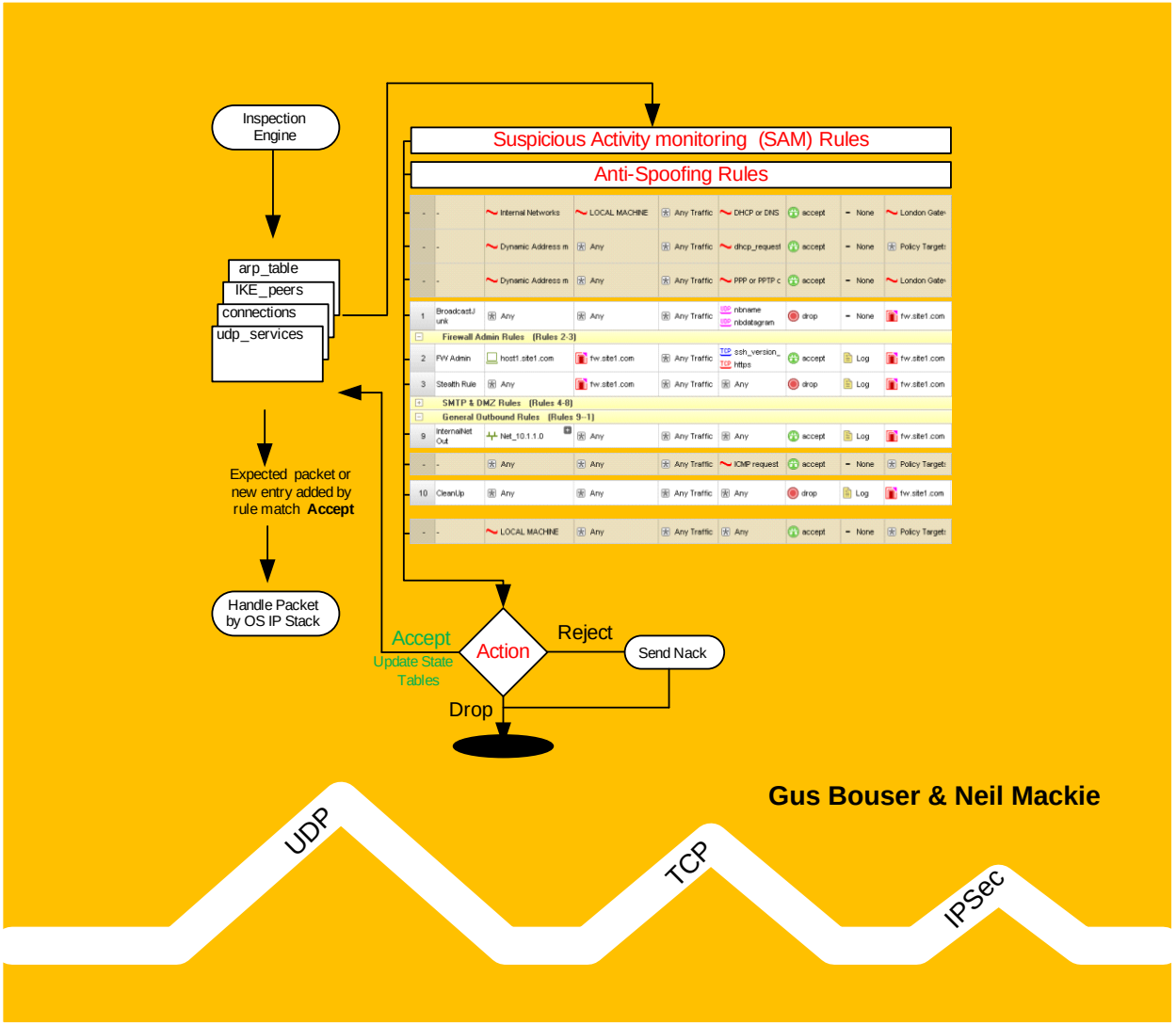
Check Point R75
Management Essentials - Part 1

Training course materials
Preparation for CCSA Certification



Printed and distributed under license from Lezha Publications by ITSec Solutions Ltd.

1 - Networks and Firewalls

Objectives

- Know how packet filtering works
- Know how application proxies work
- Know how Stateful Inspection works
- Know how to apply basic filters in tcpdump
- Know how to create a pcap file for analysis by WireShark

Approximate time for completing each section

Section 1	Securing Networks	20 Minutes
Section 2	Basic Network Packet Analysis	10 Minutes
	Total time	35 Minutes

Prerequisites

- Basic understanding of TCP/IP
- Knowledge of MS-Windows
- Have VMWare Workstation or a Hypervisor Installed
- Have the Virtual Machines ready for use

Contents

2 - Check Point Components

Objectives

- Understand Check Point products Secure the Global network
- Understand the function of the SmartCenter
- Understand the function of the VPN-1 Power/UTM Module
- Understand the Interaction between GUI Clients, SmartCenter & Firewalls
- Understand the product options for NGX R75 and Blades
- Understand the Blade options using Containers

Prerequisites

- Complete Module 1

Approximate time for completing each section

Section 1	Check Point Components	20 Minutes
Section 2	Product Combinations	10 Minutes
	Total time	30 Minutes

The contents of this module should not be relied on when purchasing products. It is only meant as a simple overview.

The product combinations and offers continually change and a qualified reseller with access to the latest information and datasheets should be consulted before any purchase decisions are made.

Make sure you always get the latest product data sheets from www.checkpoint.com

Contents

3 - Installing the Firewall – SecurePlatform

Objectives

- Check the Virtual Machine template for the Firewall
- Install a SecurePlatform Firewall
- Configure the Firewall Interfaces
- Understand the difference between CPShell & Expert Shell/Mode
- Understand the use of ‘fw unloadlocal’
- Understand the InitialPolicy & Defaultfilter Security policies
- Understand the security risks of using ‘cpstop’ & ‘fwstop’
- Understand debugging connectivity issues for a new firewall

Prerequisites

- VMWare Workstation or Server
- The virtual machine ClassRouter needs to be started, IP address 172.21.1.254
- The virtual machine Host1 needs to be started, IP address 10.1.1.100
- SecurePlatform ISO image available on the local disk

Approximate time for completing each section

Section 1	Creating and configuring the Virtual Machine	20 Minutes
Section 2	Installing the SecurePlatform Base Build	15 Minutes
Section 3	Installing VPN-1 on SecurePlatform	30 Minutes
Section 4	SecurePlatform with VPN-1 Installed - Basics	45 Minutes
	Total time	1Hr 50 Min

Contents

4 - Installing the Check Point SmartCenter

Objectives

- Check the status of the Virtual Machine mgmt-Site1
- Install the SmartCenter
- Know the difference between a Primary and Secondary SmartCenter
- Install the SmartConsole clients
- Understand the importance of a rebuild strategy for the SmartCenter
- Know why the SmartCenter needs to be protected
- Know where log files are stored
- Know the use and limitation of the initial administrator
- Know the purpose of the remote GUI clients list
- Set the FQDN for the Certificate Authority
- Know the purpose and use of the SmartCenter fingerprint

Prerequisites

- VMWare Workstation or Server
- The virtual machine mgmt-Site1 base machine should exist with no OS installed
- Check Point SPLAT & Windows ISO available on the local disk

Approximate time for completing each section

Section 1	Management Server Virtual Machine	10 Minutes
Section 2	Installing the Check Point SmartCenter	45 Minutes
Section 3	Installing the SmartConsole Clients	10 Minutes
	Total time	65 Minutes

Contents

5 - Connecting to the SmartCenter

Objectives

- Understand the options in ‘cpconfig’ on a SmartCenter
- Know the main configuration file for storing the SmartCenter objects – Objects_5_0.C
- Know what is required to connect to the SmartCenter
- Know why some objects are automatically created
- Understand the use of Logs Servers & Masters
- Know how to select products installed on a Check Point Object
- Understand the elements of a rule, SRC/DST/VPN/Service/Action/Track/Install On/Time/Comment

Prerequisites

- Complete Module 4
- Virtual Machine mgmt-Site1 must be running
- Virtual Machine Host1 must be running

Approximate time for completing each section

Section 1	Check Point Configuration	10 Minutes
Section 2	Basic SmartDashboard – Connecting to the SmartCenter	15 Minutes
Section 3	Basic Rule Parameters	15 Minutes
	Total time	40 Minutes

Contents

6 - Creating Network Objects

Objectives

- Understand the type of objects that can be used in a Security Policy
- Create the Firewall object and change some parameters
- Establish trust between the SmartCenter and Firewall
- Understand how to set Anti-spoofing
- Know how to set the maximum concurrent connections through the Firewall
- Know how to break and reset Secure Internal communications (SIC) between a SmartCenter and Firewall
- Create the basic objects required for the classroom environment

Prerequisites

- Complete Module 5
- Virtual machines Host1, mgmt-Site1 & fw-Site1 must be running

Approximate time for completing each section

Section 1	Object Types	15 Minutes
Section 2	Creating the Firewall Object	15 Minutes
Section 3	Breaking SmartCenter & Firewall SIC	15 Minutes
Section 3	Creating General Network Objects	25 Minutes
	Total time	70 Minutes

Contents

7 - Creating Rules and Installing the Security Policy

Objectives

- Create a Policy Package
- Add Rules to a Security Policy
- Understand how rules interact with each other
- Know how to install security policies
- Understand how to check the policy currently installed on a firewall
- Understand the difference between Implicit and Explicit rules
- Understand the risk of using implied rules for allowing DNS
- Understand how to break and reset SIC trust between a SmartCenter and Firewall
- Understand that Security Policies can be pulled from the SmartCenter as well as being pushed to a firewall
- Be aware of the services Check Point products use

Prerequisites

- Complete Module 6
- Virtual machines Host1, Mgmt-Site1 & fw-Site1 must be running

Approximate time for completing each section

Section 1	Dealing with Policy Packages	10 Minutes
Section 2	Adding Rules	40 Minutes
Section 3	Policy installs	20 Minutes
Section 4	Explicit and Implicit Rules	30 Minutes
Section 5	Saved Versus the Installed Policy	10 Minutes
	Total time	110 Minutes

Contents

8 - SmartView Tracker

Objectives

- Create log events using a scanner
- Know the different tabs in the SmartView Tracker, Log, Active, Management
- Use filters to display different log details
- Understand the events in the Active view
- Understand the events in the Management view
- Know how to rotate log files
- Know how to export log files to third party products
- Fetch log files from remote firewall modules
- Create simple filtered searches
- Know how to create custom commands in SmartView Tracker

Prerequisites

- Complete Module 7
- Virtual Machines mgmt-Site1, fw-Site1, host1 & ClassRouter must be running

Approximate time for completing each section

Section 1	Generate Traffic Using a Network Scanner	10 Minutes
Section 2	SmartView Tracker	40 Minutes
	Total time	50 Minutes

Contents

9 - SmartView Monitor

Objectives

- Know the type of information monitored
- Know how to set alert types for specific events
- Know the licensing requirement for SmartView Monitor
- Use SmartTracker Active Log to block connections
- User SmartView Monitor to view blocked connections
- Use SmartView Monitor to block connections

Prerequisites

- Complete Module 8
- Virtual Machines mgmt-Site1, fw-Site1, Host1 & ClassRouter must be running

Approximate time for completing each section

Section 1	SmartView Monitor General Status	10 Minutes
Section 2	SmartView Monitor Traffic Statistics	20 Minutes
Section 3	Suspicious Activity Monitoring (SAM)	20 Minutes
	Total time	50 Minutes

Contents

10 - SmartUpdate

Objectives

- Know how to access the Check Point User Center
- Know how to manage licenses
- Understand the purpose of the Contracts file
- Know how to attach and detach licenses
- Know the functions that a free in SmartUpdate

Prerequisites

- Complete Module 9
- Virtual machines mgmt-Site1, fw-Site1, Host1 and ClassRouter should be running

Approximate time for completing each section

Section 1	Check Point User Center	10 Minutes
Section 2	SmartUpdate Managing Licenses	15 Minutes
	Total time	25 Minutes

Contents

11 - Working with the Security Policy

Objectives

- Know how to use Revision Control.
- Use the features of the SmartDashboard to Disable, hide and search for objects in the rulebase.
- Understand pre-defined services and the timeouts associated with them.
- Understand how to create new services (ports) and the risks associated with them.
- Understand how to abuse and tunnel services over standard ports.
- Adjust the security policy to increase the security checking of the policy.
- Understand that even a simple addition to the security policy rules can require careful risk analysis.

Prerequisites

- Complete Module 10
- Virtual machines mgmt-Site1, fw-Site1 Host1 & ClassRouter must be running

Approximate time for completing each section

Section 1	Policy Revision Control	20 Minutes
Section 2	Rule display	15 Minutes
Section 3	Dealing with Services	30 Minutes
Section 4	Adding More Rules	30 Minutes
Section 5	Simple Systems Analysis for Rule Evaluation	10 Minutes
	Total time	105 Minutes

Contents

12 - Setting up User Account Authentication

Objectives

- Know how to add new SmartCenter administrator accounts
- Know the authentication schemes that Check Point can use, OS Password, Internal Password, RADIUS, TACACS, SecurID
- Create User Accounts, Groups and Templates
- Know the authentication database and Daemons used for Authentication
- Know how to export the user database
- Know the three types of authentication used, User, Session & Client

Prerequisites

- Complete Module 11
- Virtual Machines mgmt-Site1, fw-Site1, Host1 & ClassRouter must be running

Approximate time for completing each section

Section 1	Creating Administrator Accounts	30 Minutes
Section 2	Creating Firewall Rule Authentication Accounts	20 Minutes
Section 3	Authentication Processes	20 Minutes
	Total time	70 Minutes

Contents

13 - Using User Authentication

Objectives

- Know the Services that can be used with User Authentication
- Know the daemons associated with User Authentication
- Complete User Authentication using telnet
- Complete User Authentication using FTP
- Complete User authentication using HTTP
- Understand the problem with User Auth & Accept rule clashes
- Use ‘tcpdump’ to sniff Usernames/Passwords

Prerequisites

- Complete Module 12
- Virtual machines mgmt-Site1, fw-Site1, Host1, asdrv01 & ClassRouter must be running

Approximate time for completing each section

Section 1	User Authentication	35 Minutes
Section 2	Using Authentication from internal Networks – Rule clashes	30 Minutes
Section 3	User Login Details - tcpdump	15 Minutes
	Total time	80 Minutes

Contents

14 - Using Session Authentication

Objectives

- Understand how Session Authentication works
- Install and use the Session Agent
- Understand the limitation of Session authentication

Approximate time for completing each section

Section 1	Session Authentication	35 Minutes
	Total time	35 Minutes

Prerequisites

- Complete Module 13
- Virtual machines mgmt-Site1, fw-Site1 Host1 & ClassRouter must be running

Contents

15 - Using Client Authentication

Objectives

- Know the daemons that Client Authentication uses
- Know the port numbers used by Client Authentication daemons
- Know the different sign-on methods for Client Authentication
- Use client authentication with FTP

Approximate time for completing each section

Section 1	Client Authentication	60 Minutes
Section 2	External User Database - LDAP	40 Minutes
	Total time	100 Minutes

Prerequisites

- Complete Module 14
- Virtual machines mgmt-Site1, fw-Site1, Host1, adsrv01, & ClassRouter must be running

Contents

16- Identity Awareness

Objectives

- Understand how Identity Awareness works
- Understand the use of AD Query
- Understand the use of Captive Portal
- Understand the use of Identity Agents

Approximate time for completing each section

Section 1	Current Rules Check	5 Minutes
Section 2	Current Objects Check	10 Minutes
Section 3	Identity Awareness	45 Minutes
	Total time	60 Minutes

Prerequisites

- Complete Module 15
- Virtual machines mgmt-Site1, fw-Site1, Host1, adsrv01 & ClassRouter must be running.

Contents

17 - Network Address Translation

Objectives

- Know the networks defined in RFC1918
- Understand that NAT may cause Client/Server connection problems
- Understand the NAT setting in Global Properties
- Know how to use Hide/Dynamic NAT
- Know how to use Static NAT
- Know which NAT method to apply for a given situation
- Understand the important of ARPs in relation to Static NAT
- Use NAT in a Security Policy

Prerequisites

- Complete Module 16
- Virtual machines mgmt-Site1, fw-Site1, ClassRouter & Host1 must be running

Approximate time for completing each section

Section 1	Rules Check	10 Minutes
Section 2	Network Address Translation	30 Minutes
Section 3	Using Network Address Translation - Basic	35 Minutes
Section 4	Using Network Address Translation - Advanced	30 Minutes
	Total time	1 Hr 45 Min

Contents

18 – Intrusion Prevention System (IPS)

Objectives

- Know how to create IPS Profiles
- Understand the typical network features IPS protects against
- Understand where Application Intelligence fits into the Security Policy
- Know how to use the features of Web Intelligence to protect web servers and http traffic
- Change settings in IPS, apply them a Security Policy and test the features

Prerequisites

- Complete Module 17
- Virtual machines mgmt-Site1, fw-Site1, ClassRouter & Host1 must be running

Approximate time for completing each section

Section 1	IPS and Firewalls	10 Minutes
Section 2	IPS Features	40 Minutes
	Total time	50 Minutes

Contents

19 - Content Security Servers

Objectives

- Understand how Content Security server work at the application level and not the kernel level
- Create Resources that can be used with the Content Security Servers
- Make use of the HTTP Content Security Server
- Make use of the FTP Content Security Server
- Understand how CVP Servers integrate with the Content Security Servers
- Understand how UFP Servers integrate with the Content Security Servers

Prerequisites

- Complete Module 18
- Virtual machines mgmt-Site1, fw-Site1, Host1 & ClassRouter must be running

Approximate time for completing each section

Section 1	Content Security Servers	10 Minutes
Section 2	HTTP Content Security	30 Minutes
Section 3	FTP content Security	35 Minutes
Section 4	CVP and UFP Servers	30 Minutes
	Total time	1 Hr 45 Min

Contents

20 - Managing Multiple Firewalls

Objectives

- Create a second SecurePlatform firewall
- Establish trust and take control of the firewall
- Install a Basic Security Policy
- Understand the use of Single or Multiple Security Policies when managing multiple firewalls
- Create log data and filter traffic based on the Firewall Origin

Approximate time for completing each section

Section 1	Managing Multiple Firewalls	15 Minutes
Section 2	Creating fw.site2.com	80 Minutes
	Total time	1Hr 35 Min

Prerequisites

- Complete Module 19
- Virtual machines mgmt-Site1, fw-Site1, Host1 & ClassRouter must be running
- Virtual machine fw-Site2

Contents

21 - Backups and Recovery Procedures

Objectives

- Understand how to use ‘upgrade_export’ to backup a SmartCenter
- Understand how to use ‘upgrade_import’ to clone a SmartCenter
- Understand how to migrate a SmartCenter from a Windows platform to Check Points SecurePlatform
- Know how to create backups of the Firewall
- Know how to restore from backups
- Know how to create snapshot images
- Know how to restore from a snapshot image

Prerequisites

- Complete Module 20
- Virtual machines mgmt-Site1, fw-Site1, Host1 & ClassRouter must be running

Approximate time for completing each section

Section 1	Backing up the SmartCenter	60 Minutes
Section 2	Backing up the Firewall on SPLAT	45 Minutes
Section 3	SPLAT Maintenance Mode	15 Minutes
	Total time	2 Hrs

Contents

