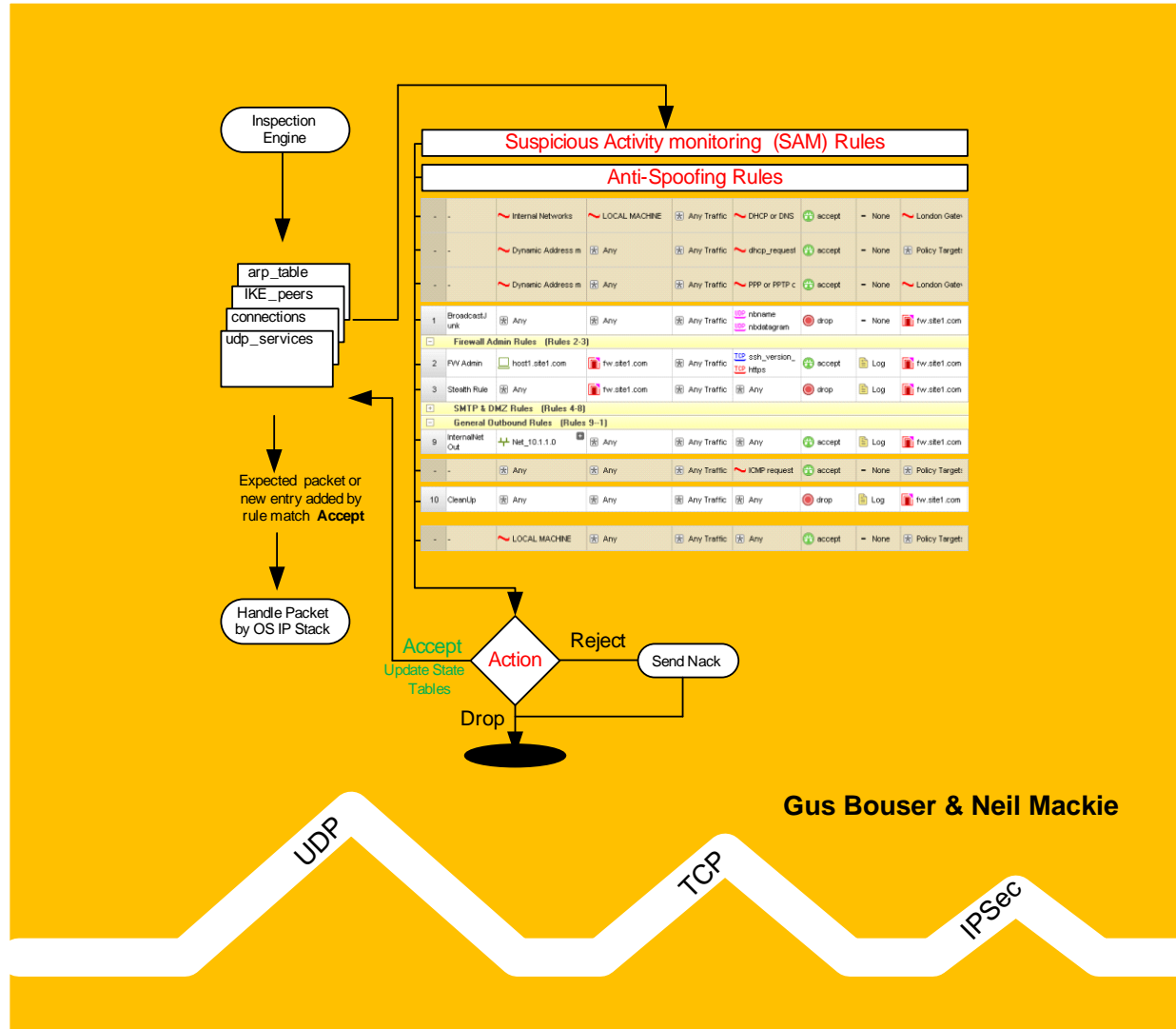


# Check Point R75 Management Essentials - Part 1

Training course materials  
Preparation for CCSA Certification



Copyright © Lezha Publications. All rights reserved.

Lezha Publications acknowledge all registered trademarks. All references to trademarks are purely editorial. These training course materials have no affiliation with or endorsement from any company whose trademark may have been referenced.

All rights reserved. This product and related documentation are protected by copyright and distribution under licensing restricting their use. No part of this work may be reproduced in any form or by any means – graphic, electronic, or mechanical – including but not limited to photocopying, recording, taping or storage in an information retrieval system, without the prior written permission of the copyright owner.

The information in this book is distributed on an 'As Is' basis, without warranty or liability. While every precaution has been taken in the preparation of this book, neither the printer, or copyright owner shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by information contained in this book or by the computer software or hardware products described herein.

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

## Prerequisites

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

## Approximate time for completing each section

<b>Section 1</b>	Securing Networks	20 Minutes
<b>Section 2</b>	Basic Network Packet Analysis	10 Minutes
	Total time	35 Minutes

## Contents

<b>1</b>	<b>Securing Networks</b>	<b>3</b>
1.1	All Firewalls are Not Equal	3
1.1.1	Primary Organization Network	3
1.1.2	Hosted Services Network	4
1.1.3	Remote Office Networks	5
1.2	Basic Protocols	5
1.2.1	IP Protocol	5
1.2.2	TCP Protocol	6
1.2.3	UDP Protocol	7
1.2.4	ICMP Protocol	8
1.3	Protection Using Simple Packet Filters	8
1.3.1	Packet Filter Protection	8
1.4	Protection Using Application Proxies	8
1.4.1	Application Proxy Protection	9
1.5	Protection Using Hybrids – Stateful Inspection	9
1.5.1	Stateful Inspection Protection	9
1.5.2	Building State Tables	10
1.5.3	Check Point Filtering Modules	12
1.5.4	Check Point State Tables	12
<b>2</b>	<b>Basic Network Packet Analysis</b>	<b>14</b>
2.1	Sniffing Packets	14
2.1.1	tcpdump	14
2.1.2	Wireshark	14

## 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

<b>Section 1</b>	Check Point Components	20 Minutes
<b>Section 2</b>	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](http://www.checkpoint.com)***

## Contents

<b>1</b>	<b>Check Point Components</b>	<b>3</b>
1.1	Product Overview	3
1.1.1	Securing the Global Organization	3
1.1.2	Perimeter	4
1.1.3	Remote Access	4
1.2	Check Point VPN-1 UTM/Power Components	5
1.2.1	Component Overview	5
1.2.2	SmartCenter	5
1.2.3	VPN-1 Power/UTM Modules/Blades	6
1.2.4	GUI Clients	6
<b>2</b>	<b>Product Combinations</b>	<b>7</b>
2.1	Modules/blades	7
2.1.1	Check Point Power-1	7
2.1.2	Check Point UTM-1	7
2.1.3	Check Point UTM-1 Edge	7
2.1.4	Check Point Software Gateways	7
2.1.5	Check Point Software SmartCenter & Gateway Bundles	7
2.2	R70 onwards Products – Blades	8
2.2.1	Check Point Gateway Appliances – Power-1	8
2.2.2	Check Point Gateways – IP Appliances	8
2.2.3	Check Point Gateways – UTM-1 Appliances	8
2.2.4	Check Point Gateways – UTM-1 Edge	8
2.2.5	Check Point Software – Security Gateways Bundles	8
2.2.6	Check Point Gateways – Security Management Bundles	8
2.2.7	Check Point Gateways – EndPoint Security	8
2.2.8	Check Point Gateways – Abra	8

### 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

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

## Contents

<b>1</b>	<b>Check the Status the Virtual Machine for fw-Site1 &amp; mgmt-Site1</b>	<b>3</b>
1.1	Check the VM settings for fw-Site1	3
1.1.1	Virtual Machine fw-Site1	3
1.1.2	Machine mgmt-Site1	3
<b>2</b>	<b>Installing the SecurePlatform Base Build</b>	<b>4</b>
2.1	Install SecurePlatform (SPLAT)	4
2.1.1	Set Keyboard Layout	5
2.1.2	Set an Administration IP Address	5
2.1.3	Set the Port for Web GUI Access	6
2.1.4	Format the Hard Disk & Reboot	6
<b>3</b>	<b>Installing Firewall Blades on SecurePlatform</b>	<b>7</b>
3.1	Configure the Base OS Parameters & Check Point Products	7
3.1.1	Initial Login	7
3.1.2	Run 'sysconfig'	7
3.1.3	Set the Hostname	8
3.1.4	Set the Domain	8
3.1.5	Set Network parameters for Interface eth3	8
3.1.6	Set Network Parameters for Interface eth2	9
3.1.7	Set the Date and Time	10
3.1.8	Import Check Point Products Configuration	11
3.1.9	Check Point Product Install	11
3.1.10	Select Installation Type	12
3.1.11	Select Check Point Products – Security Gateway	12
3.1.12	Select Check Point Products – Basic Configuration	12
3.1.13	Set the Activation Key for SIC	13
3.1.14	Gateway Reboot	13
<b>4</b>	<b>SecurePlatform with VPN-1 Installed - Basics</b>	<b>14</b>
4.1	SecurePlatform Access Level & Shells	14
4.1.1	Initial Debugging – fw unloadlocal	14
4.1.2	CPSHELL Command List	15
4.1.3	Setting the 'idle' Timeout	16
4.1.4	Expert Mode	16
4.2	Understanding 'cpstop' Security Risks	17
4.2.1	Testing 'cpstop'	17

4.2.2	Basic tcpdump – Packets on an Interface	18
4.2.3	Using 'cpstop –fwflag –default'	19
4.2.4	Using 'cpstop –fwflag –proc'	19
4.2.5	Using 'fwstop'	20
4.3	Basic Network Scan – Using Superscan	20
4.3.1	Superscan - InitialPolicy	20
4.3.2	Superscan - Defaultfilter	22
4.3.3	Superscan – 'fw unloadlocal' No Policy installed	22
4.4	Firewall installation Summary	23



## 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

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

## Contents

<b>1</b>	<b>Management Server Virtual Machine</b>	<b>3</b>
1.1	Virtual Machine Setup mgmt-Site1	3
1.1.1	Set the CDRom Boot Device	3
<b>2</b>	<b>Installing the Check Point SmartCenter and SmartConsole</b>	<b>4</b>
2.1	Install SecurePlatform (SPLAT) for the SmartCenter	4
2.1.1	Set Keyboard Layout	4
2.1.2	Set an Administration IP Address	5
2.1.3	Set the Port for Web GUI Access	5
2.1.4	Format the Hard Disk & Reboot	5
2.2	Configure the Base OS & Check Point SmartCenter	6
2.2.1	Initial Login	6
2.2.2	Run 'sysconfig'	6
2.2.3	Set the Hostname	6
2.2.4	Set the Domain	7
2.2.5	Network Parameters	7
2.2.6	Set the Date and Time	7
2.2.7	Import Check Point Products Configuration	8
2.2.8	Check Point Product Install	8
2.2.9	Select Installation Type	9
2.2.10	Select Check Point Products – Security Gateway	9
2.2.11	SmartCenter License	10
2.2.12	SmartCenter Administrator	10
2.2.13	SmartCenter GUI Clients	11
2.2.14	SmartCenter CA & Fingerprint	11
2.2.15	SmartCenter Reboot & Check Network Connectivity	12
2.2.16	Set the 'expert' Password	13
2.2.17	'cpconfig' and 'sysconfig' on the SmartCenter	13
<b>3</b>	<b>SmartConsole Clients</b>	<b>14</b>
3.1	Installing the SmartConsole Clients on Host1	14
3.1.1	Location and Clients to Install	14
3.1.2	Getting the SmartConsole from SPLAT	16

## 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

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

## Contents

<b>1</b>	<b>Check Point Configuration .....</b>	<b>3</b>
1.1	Check Point Configuration - cpconfig .....	3
1.1.1	'cpconfig' on a SPLAT SmartCenter.....	3
1.1.2	Adding Administrators.....	3
1.1.3	Checking the GUI Client List.....	4
1.1.4	Displaying the SmartCenter Fingerprint .....	4
1.1.5	Moving the Fingerprint File to a Workstation.....	4
1.2	Time, SmartCenter and Firewall.....	6
1.2.1	Install NTP Server on Host1.....	6
1.2.2	Set Time Synchronization for SmartCenter and Firewall.....	6
<b>2</b>	<b>Basic SmartDashboard – Connecting to the SmartCenter .....</b>	<b>8</b>
2.1	The SmartConsole Clients.....	8
2.2	Initial Login to the SmartCenter .....	8
2.2.1	The SmartCenter Fingerprint .....	9
2.2.2	Check Point Software Blades.....	9
2.3	The SmartDashboard Layout .....	10
2.3.1	Turning Display Areas On/Off .....	10
2.3.2	The Objects List .....	10
2.3.3	SmartDashboard Security Policy Tabs.....	11
2.4	Editing the SmartCenter Object.....	11
2.4.1	Objects Tree.....	11
2.4.2	Comment & Color.....	12
2.4.3	Topology .....	12
2.4.4	Log and Masters .....	12
<b>3</b>	<b>Basic Rule Parameters .....</b>	<b>14</b>
3.1	Introduction to Rules .....	14
3.1.1	Adding a Rule.....	14
3.1.2	Rule Elements.....	14
3.1.3	Rule number and Name .....	14
3.1.4	Setting Source/Destination.....	14
3.1.5	Setting the VPN Column .....	15
3.1.6	Setting the Service.....	15
3.1.7	Setting the Type of Action.....	15
3.1.8	Setting the Type of Logging .....	16

3.1.9	Gateway Installation – Install On.....	16
3.1.10	Comment Field.....	17
3.2	Starting the Other SmartConsole Clients .....	17

## 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

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

## Contents

<b>1 Object Types</b>	<b>3</b>
1.1 Object Types	3
1.1.1 Creating Objects	3
1.2 Network Objects	4
1.2.1 Check Point	4
1.2.2 Nodes	5
1.2.3 Network	5
1.2.4 Groups	5
1.2.5 Dynamic	5
1.2.6 Security Zones	6
1.2.7 Others	6
1.2.8 VoIP Domains	6
1.3 Services, Resources, OPSEC, Users & VPN Communities	7
1.3.1 Services	7
1.3.2 Resources	7
1.3.3 Servers & OPSEC Applications	7
1.3.4 Users and Administrators	8
1.3.5 VPN Communities	8
<b>2 Creating the Firewall Object</b>	<b>9</b>
2.1 Check Point Gateway Object	9
2.1.1 Create a New Check Point Gateway	9
2.1.2 Set the Hostname and IP address 172.21.1.1	9
2.1.3 Set the Color to Red	10
2.1.4 Select Check Point Software Blades	10
2.1.5 Set Secure Internal Communications	10
2.1.6 Changes to the Firewall Tab Option List	11
2.1.7 HTTPS Inspection	11
2.1.8 SecurePlatform	12
2.1.9 Setting Logs And Masters	12
2.1.10 Capacity Optimization	13
<b>3 Breaking SmartCenter and Firewall Communications</b>	<b>15</b>
3.1 Breaking and Resetting SIC	15
3.1.1 Reset SIC on the Firewall	15
3.1.2 Test Trust for the Firewall Object in the SmartCenter	16
3.1.3 Reset SIC in the Firewall Object	17
<b>4 Creating General Network Objects</b>	<b>18</b>
4.1 Creating the Network Type Objects	18
4.1.1 Create the Internal Network	18
4.1.2 Network Object – Broadcast Address	18
4.1.3 Create the DMZ Network	18
4.1.4 Create the External Network	19
4.1.5 Create the Remote Site2 Network	20
4.2 Creating Node Type Objects	20
4.2.1 Create the Internal Server adsrv01	20
4.2.2 Create the Internal Workstation host1	21
4.2.3 Create the DMZ SMTP Server Host	21
4.2.4 Create the DMZ Web/FTP Server Host	21
4.2.5 Create the Class Room Web Server Host	22
4.3 Creating External FTP servers for ftp.hp.com	23
4.3.1 Using nslookup	23
4.3.2 Creating the FTP Servers – Cloning Objects	24
4.3.3 Creating a Group Object	24
4.3.4 Create the Classroom Router – Gateway Object	25
4.4 Summary of Objects Created	26
<b>5 Dealing with Anti-spoofing</b>	<b>27</b>
5.1.1 Setting the Topology – Get Interfaces	27
5.1.2 Setting Topology – Get Interfaces with Topology (Anti-spoofing)	27
5.1.3 Making Topology Changes	28

## 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

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

## Contents

<b>1</b>	<b>Dealing With Policy Packages</b>	<b>3</b>
1.1	Policy Packages	3
1.1.1	Simplified or Traditional Policy	3
1.1.2	Creating a New Policy Package	3
<b>2</b>	<b>Adding rules</b>	<b>5</b>
2.1	Adding rules	5
2.1.1	Stealth Rule	5
2.1.2	Internal Network Out bound Rule	5
2.1.3	Cleanup Rule	5
2.1.4	Broadcast Junk Rule	5
2.1.5	SMTP Inbound Rule	6
2.1.6	SMTP Outbound Rule	6
2.1.7	Web Inbound Rule	6
2.1.8	Firewall Secure Shell Access Rule	7
2.1.9	Negating Objects in a Rule	7
2.2	Reviewing the rules	7
2.2.1	Rule Review - Firewall at Risk from the SMTP Server	8
2.2.2	Internal Network at Risk from the SMTP Server	8
2.2.3	Adding Rule Section Titles	9
2.2.4	Rule Summary	10
<b>3</b>	<b>Policy Installs</b>	<b>11</b>
3.1	Installing the Policy	11
3.1.1	Verifying the Security Policy	11
3.1.2	Correcting the Policy after Verification Failures	11
3.1.3	Setting the Policy Targets	12
3.1.4	Installing the Policy	13
3.1.5	Checking the Firewall Status	15
3.1.6	Testing the Rules	15
3.1.7	Firewall Existing Connections - Behavior	16
<b>4</b>	<b>Explicit and Implicit Rules</b>	<b>17</b>
4.1	Implicit Rules	17
4.1.1	Viewing Implied Rules	17
4.1.2	Turning Implied Rules Off	19
4.1.3	Configuring DNS as an Implied Rule – (Don't)	21

4.1.4	Accept ICMP requests	21
4.2	Rule Base Filtering Order	22
4.3	Breaking SmartCenter to Firewall Connectivity with Implied rules	23
4.3.1	Break SmartCenter to Firewall Connectivity	23
4.3.2	SmartCenter Connectivity Recovery - cpstop/cpstart	24
4.3.3	SmartCenter Connectivity Recovery – SIC Reset	26
4.3.4	SmartCenter Connectivity Recovery – 'fw unloadlocal'	28
4.3.5	SmartCenter Connectivity Recovery – 'fw fetch mgmt' (Use this)	29
4.4	SmartCenter and Firewall Services	30
4.4.1	Check Point 'FW' Services	30
4.4.2	Check Point 'CP' Services	30
4.4.3	SmartCenter to Firewall Explicit Rule – (For Safety)	31
<b>5</b>	<b>Saved Versus the Installed Policy</b>	<b>32</b>
5.1	Saved Policy	32
5.2	Installed Policy	32



## 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

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

## Contents

<b>1</b>	<b>Generate Traffic Using a Network Scanner .....</b>	<b>3</b>
1.1	Scan 172.21.1.254 .....	3
1.1.1	Set the IP Address Range to Scan – 172.21.1.254.....	3
1.1.2	Check the Type and Ports to Scan.....	3
1.1.3	Run the Scan .....	3
1.1.4	Check Log Events Generated .....	4
<b>2</b>	<b>SmartView Tracker .....</b>	<b>5</b>
2.1	Log Tabs, Log, Active, Audit.....	5
2.1.1	Network & Endpoint .....	5
2.1.2	Active .....	7
2.1.3	Management .....	8
2.1.4	Predefined Filters .....	9
2.2	Rotating, Archiving and Exporting Logs .....	9
2.2.1	Rotating Log Files .....	9
2.2.2	Archiving Log Files.....	9
2.2.3	Exporting Log Files .....	10
2.2.4	Fetching Log Files from the Firewall .....	10
2.3	Searching and Custom Filters .....	12
2.3.1	Filter Options.....	13
2.3.2	Doing Simple Searches.....	14
2.3.3	Custom Filters.....	15
2.3.4	View Query Properties .....	16
2.4	Custom Commands.....	17
2.4.1	Adding a Secure Shell Custom Command.....	17
2.5	Log Parameters in the SmartDashboard .....	18
2.5.1	Log Type.....	18
2.5.2	Firewall Object .....	18
2.5.3	SmartCenter.....	18
2.5.4	Policy Global Properties.....	19
2.6	Logging to an Alternative Directory .....	20

## 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

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

## Contents

<b>1 SmartView Monitor</b> .....	<b>3</b>
1.1 Gateway Status.....	3
1.1.1 Filtered views.....	3
1.1.2 Gateway Properties.....	3
1.1.3 Other Objects.....	4
1.2 SmartCenter Object.....	4
1.2.1 System Information.....	4
1.2.2 Licences.....	4
1.2.3 Certificate Authority.....	5
1.2.4 Status and Connected Clients.....	5
1.2.5 Disconnecting SmartConsole Clients.....	5
1.3 Firewall Object.....	5
1.3.1 System Information.....	5
1.4 Threshold Settings.....	6
1.4.1 Global, None, Custom.....	6
1.4.2 System Alert Daemon.....	6
<b>2 SmartView Monitor Traffic Statistics</b> .....	<b>8</b>
2.1 Traffic Statistics.....	8
2.1.1 Enable SmartMonitor on the Firewall.....	8
2.1.2 Generate Some Traffic.....	9
2.1.3 Traffic & System Counters.....	9
<b>3 Suspicious Activity Monitoring (SAM)</b> .....	<b>11</b>
3.1 Suspicious Activity Monitoring and Filter Location.....	11
3.2 Using SmartView Tracker – Active Log.....	11
3.2.1 Create a Suspicious Connection.....	11
3.2.2 View Connection in the SmartView Tracker – Active Tab.....	11
3.2.3 Select Tools – Block Intruder.....	11
3.2.4 Kill Connection for three Minutes.....	11
3.2.5 Test Connection Rejects and Alerts.....	12
3.2.6 Clear all SAM Connections – ‘fw sam –f All –D’.....	12
3.2.7 Test Connections Work.....	12
3.3 Using SmartView Monitor - Tools.....	12
3.3.1 Create a Suspicious Connection.....	12
3.3.2 View Connection in SmartView Tracker – Active Tab.....	13

3.3.3 Select Tools and Block Intruder.....	13
3.3.4 View all SAM rules using SmartView Monitor.....	13
3.3.5 Delete the SAM Rule.....	13
3.3.6 Create a New SAM Rule Using SmartView Monitor.....	13
3.3.7 Test the New SAM Rule.....	14

## 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 are 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

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

## Contents

<b>1</b>	<b>Check Point User Center</b>	<b>3</b>
1.1	Logging into the User Center	3
1.1.1	Viewing Account Information	3
1.1.2	Viewing Product information	3
1.1.3	Products and Licenses	4
1.1.4	Contracts File	4
1.2	Creating Licenses	4
1.2.1	Central or Local licenses	4
1.2.2	SmartCenter IP Address	5
1.2.3	Changing Licensed IP Address	5
1.2.4	Full Version Upgrades Require New Licenses	5
1.3	R75 Blade licenses	5
1.3.1	Management Blades	6
1.3.2	Network Security Blades	6
<b>2</b>	<b>SmartUpdate – Managing Licenses</b>	<b>7</b>
2.1	Using SmartUpdate	7
2.1.1	Licenses and Contracts	7
2.1.2	Product and Package Information	8
2.1.3	Generating cpinfo data	9
2.1.4	Adding Licenses & Contracts	10
2.1.5	Attaching and Detaching Licenses	11

## 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

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

## Contents

<b>1 Policy Revision Control.....</b>	<b>3</b>
1.1 Database Revision Control.....	3
1.1.1 Creating Revisions.....	3
1.1.2 Where are Revisions Stored.....	4
1.1.3 Viewing Revisions.....	5
1.1.4 Rolling Back Revisions.....	6
<b>2 Rule Display.....</b>	<b>9</b>
2.1 Rule Display and Policy Interaction.....	9
2.1.1 Hiding Rules.....	9
2.1.2 Disabling Rules.....	10
2.2 Rule Filters.....	11
2.2.1 Object Location – Where Used.....	11
2.2.2 Finding Objects in Rules.....	12
<b>3 Dealing with Services.....</b>	<b>14</b>
3.1 Predefined Services and the Inspection Engine.....	14
3.1.1 TCP.....	14
3.1.2 UDP.....	16
3.1.3 ICMP.....	17
3.1.4 RPC.....	17
3.1.5 DCE RPC.....	18
3.1.6 Other.....	18
3.1.7 Basic Filtering & IPS Interaction.....	19
3.2 Creating Services.....	20
3.2.1 Creating a TCP Service and Naming Convention.....	20
3.2.2 Advanced Properties - Session Timeout and Filtering.....	20
3.2.3 Two Service Objects Using the Same Port Number.....	21
3.2.4 Applying the New Service to a Rule.....	21
3.3 Abusing a Standard Service – Tunneling over DNS (TCP).....	22
3.3.1 IPS Filtering for DNS TCP – Default is Off.....	22
3.3.2 Turn on DNS TCP in the Policy Global Properties.....	22
3.3.3 Edit the Telnet Server Port on www.server.com & host1.site1.com.....	22
3.3.4 Test the Security Policy – Oops.....	23
<b>4 Adding More Rules.....</b>	<b>25</b>
4.1 Current Rules check.....	25
4.2 DNS rule.....	25
4.2.1 Create the DNS Server Objects – Type Host.....	25
4.2.2 Add the DNS Rule.....	25
4.2.3 Add the Internal DNS Servers.....	26
4.2.4 Modify the DNS Rule.....	26
4.3 Outgoing Rule for HP FTP Servers.....	26
4.3.1 Add the FTP Outgoing Rule.....	26
4.4 Restricting the Outgoing Rule.....	27
4.4.1 Modify the Outgoing Rule.....	27
4.4.2 Modify the FTP Outgoing Rule.....	27
4.4.3 Delete the Disabled Outgoing Rule.....	27
4.5 Current Security Policy Rules Check.....	27
4.5.1 Verify and Install the policy.....	28
<b>5 Simple Systems Analysis for Rule Evaluation.....</b>	<b>29</b>
5.1 How to Evaluate – ‘From A to B allow FTP’ when B is your Server.....	29
5.2 How to Solve the Problem of Abusing Ports.....	31



## 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

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

## Contents

<b>1</b>	<b>Creating Administrator Accounts.....</b>	<b>3</b>
1.1	Administrator Accounts.....	3
1.1.1	cpconfig.....	3
1.1.2	SmartDashboard – Administrators .....	4
1.1.3	Administrator Profile.....	4
1.1.4	Admin - Groups.....	5
1.1.5	Administrator Authentication Schemes .....	5
1.1.6	Using Certificates.....	5
1.1.7	Testing Administrator Account .....	7
1.2	Using a RADIUS Server .....	7
1.2.1	Create a RADIUS Server Object.....	7
1.2.2	Create another administrator Use - RADIUS Authentication.....	8
<b>2</b>	<b>Creating Firewall Rule Authentication Accounts.....</b>	<b>10</b>
2.1	Users for Firewall Rule Authentication .....	10
2.1.1	Supported Authentication Schemes.....	10
2.1.2	Firewall - Enabled Authentication Schemes.....	10
2.1.3	Access Role and Legacy Users Access.....	11
2.1.4	Creating User Groups .....	11
2.1.5	Creating User Templates .....	12
2.1.6	Creating User Accounts .....	14
<b>3</b>	<b>Authentication Processes.....</b>	<b>17</b>
3.1	User Administration Database & Daemons .....	17
3.1.1	fwauth.NDB.....	17
3.1.2	fwauthd.conf.....	17
3.1.3	Exporting & Importing the User Database.....	18
3.2	External User Profiles.....	18
3.2.1	Match all Users .....	18
3.2.2	Match by Domain .....	19
3.3	Authentication and Security Rules.....	19
3.3.1	User Authentication.....	20
3.3.2	Session Authentication.....	20
3.3.3	Client Authentication .....	20

## 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

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

## Contents

<b>1</b>	<b>User Authentication</b>	<b>3</b>
1.1	User Authentication Daemons & Process	3
1.1.1	Authentication Daemons and Supported Services	3
1.1.2	User Authentication – Policy Global Properties	3
1.1.3	Welcome Message	4
1.2	Authentication Using Telnet	4
1.2.1	Add a telnet Authentication rule	4
1.2.2	Check Rule Properties – Intersect with User Database	5
1.2.3	Installing the Policy and Testing Authentication	5
1.3	Authentication Using http	6
1.3.1	Add an http Authentication rule	6
1.3.2	Check Rule Properties – Allowed http Servers	6
1.3.3	Adding predefined servers	7
1.3.4	Installing the policy and Testing Authentication	7
1.4	Authentication Using FTP	8
1.4.1	Add an Authentication rule	8
1.4.2	Format of User/Password for Authenticating Using FTP	8
1.4.3	Installing the Policy and Testing Authentication	8
1.5	Basic Authentication – Summary	9
1.5.1	Multiple Rules or a Single Rule	9
1.5.2	Removing the Check Point Prompt	9
<b>2</b>	<b>Using Authentication from Internal Networks – Rule clashes</b>	<b>10</b>
2.1	Authentication Behavior – Source IP Address	10
2.1.1	Changing the Behavior – GuiDBedit	10
2.2	Using http for Authentication from Internal Networks	12
2.2.1	Adding the Internal Out http Authentication Rule	12
2.2.2	Reason for Authentication Not Being Enforced	13
2.2.3	Correctly Implementing the Authentication Rules	14
<b>3</b>	<b>User Login Details – tcpdump</b>	<b>15</b>
3.1	Stealing User Login Information	15
3.1.1	Packet trace using tcpdump	15
3.1.2	Packet trace using tcpdump and Wireshark	16

## 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

<b>Section 1</b>	Session Authentication	35 Minutes
	Total time	35 Minutes

### Prerequisites

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

## Contents

<b>1</b>	<b>Session Authentication</b>	<b>3</b>
1.1	Session Authentication Daemon & Process	3
1.1.1	Authentication Daemon & Supported Services	3
1.2	Installing the Session Agent	3
1.2.1	Agent Install	3
1.2.2	Agent Behavior – Every Connection or Per Session	4
1.2.3	Problems with Agent Access – Port 261	5
1.3	Authentication Using FTP	6
1.3.1	Add an Authentication rule	6
1.3.2	Installing the Policy and Testing Authentication	6
1.3.3	Session Agent Using SSL Encryption	8
1.3.4	Using ‘Every request’ Authentication	9

## 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

### Prerequisites

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

### Approximate time for completing each section

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

## Contents

<b>1 Client Authentication</b>	<b>3</b>
1.1 Client Authentication Daemons & Process	3
1.1.1 Authentication Daemons & Supported Services	3
1.1.2 Client Authentication – Policy Global Properties	3
1.1.3 Welcome Message	4
1.1.4 Client Authentication and the Perimeter Router/Firewall	4
1.2 Client Authentication Details	4
1.2.1 Client Authentication – aclientd, Port 259	4
1.2.2 Client Authentication – ahclientd, Port 900	5
1.2.3 Controlling the Number of Sessions and Time Period	5
1.2.4 Client Authentication Sign On Methods	6
1.3 Authentication Using FTP – Manual Authentication	6
1.3.1 Add an Authentication rule	6
1.3.2 Installing the Policy and Testing FTP Access	7
1.4 Authentication Using Secure Shell	8
1.4.1 Add an Authentication rule	8
1.4.2 Installing the Policy and Testing Secure Shell Access	8
1.5 Authentication Using a Different Port Number	9
1.5.1 Edit the fwauthd.conf File	9
1.5.2 Test the Authentication Using a Different Port Number	10
1.5.3 Add a Rule to Allow Port 2590 Access to the Firewall	10
1.5.4 Port 259 and 900 Versus a Different Port	11
1.6 Client Authentication Using https	12
1.6.1 Edit the fwauthd.conf File on the firewall	12
<b>2 External User Database – LDAP</b>	<b>13</b>
2.1 LDAP Server – Using Active Directory	13
2.1.1 Check the Details of the AD Server	13
2.1.2 Listing the DN for all Users	13
2.1.3 Create an AD Account for Check Point Firewall Service Access	13
2.1.4 Create an LDAP Account Unit	15
2.1.5 Turn on SmartDirectory for Security Gateways	18
2.1.6 Create an LDAP User Group	18
2.1.7 Fetching the LDAP Account Unit Tree of Data	19
2.1.8 Add a Client Authentication Rule for the LDAP Group	20

2.1.9 Test the LDAP Authentication	21
2.1.10 Check Point LDAP Account, Domain Admin or Not	22
2.1.11 Change Privilege Level – Remove Domain Admin	23
2.1.12 Enable LDAP SSL Encryption	24



## 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

### Prerequisites

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

### Approximate time for completing each section

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

## Contents

<b>1</b>	<b>Current Rules Check</b>	<b>3</b>
1.1	Current Rules	3
1.2	Disable the Legacy Authentication Rules	3
<b>2</b>	<b>Current Objects Check</b>	<b>5</b>
2.1	Current Objects	5
2.1.1	Network Objects	5
2.1.2	Services	6
2.1.3	Servers and OPSEC Applications	6
2.1.4	Users and Administrators	6
<b>3</b>	<b>Identity Awareness</b>	<b>7</b>
3.1	Identity Awareness	7
3.1.1	User Databases	7
3.1.2	AD Query	7
3.1.3	Captive Portal	7
3.1.4	Identity Agent	7
3.2	Enabling Identity Awareness	7
3.2.1	Blade License	7
3.2.2	Check the AD User Account	7
3.2.3	Enabling Identity Awareness on the Gateway Object	8
3.3	Using Identity Awareness with AD Query	10
3.3.1	Check the AD Server Users	10
3.3.2	Security Rules using Active Directory Query	11
3.3.3	Standalone Workstation	12
3.3.4	Domain Member Workstation	12
3.4	Using Identity Awareness with Captive Portal	15
3.4.1	Configuring the Captive Portal	15
3.4.2	Security Rule using Captive Portal	16
3.5	Extending the Rule for Captive Portal	18
3.5.1	Add Telnet and FTP to the Access Role Rule	18
3.6	Using Identity Awareness with Identity Agents	18
3.6.1	Type of Agents	18
3.6.2	Deployment of Agents	19
3.6.3	Security Rule using Identity Agent	20

## 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

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

## Contents

<b>1 Rules Check</b> .....	<b>3</b>
1.1 Current Rules .....	3
1.1.1 Create a New Policy using Save As.....	3
1.1.2 Clean up the Current Rules.....	3
1.2 Rule Summary before starting Network Address Translation .....	3
<b>2 Network Address Translation</b> .....	<b>5</b>
2.1 Basic Network Address Translation.....	5
2.1.1 RFC 1918.....	5
2.1.2 Problems with NAT .....	5
2.2 NAT Properties.....	6
2.2.1 Policy Global Properties - NAT.....	6
2.2.2 Client Side NAT.....	6
<b>2.2.3</b> Server Side NAT .....	<b>7</b>
2.2.4 Objects and the NAT Tab.....	8
2.3 Hide/Dynamic NAT.....	9
2.3.1 Hide NAT - Automatic Rules .....	9
2.3.2 Hide NAT - Manual Rules .....	9
2.4 Static NAT.....	10
2.4.1 Static NAT – Automatic Rules.....	10
2.4.2 Static NAT – Manual Rules.....	11
2.4.3 Problems with Static NAT – Manual Rules.....	11
2.4.4 Why does the Firewall need Proxy ARPs.....	12
2.4.5 Creating Proxy ARPs .....	12
<b>3 Using Network Address Translation - Basic</b> .....	<b>13</b>
3.1 Testing a connection without NAT.....	13
3.1.1 Create a Connection to 172.21.1.254 .....	13
3.1.2 Check the Source Address using 'netstat -a' on 172.21.1.254.....	13
3.2 Implementing Hide/Dynamic NAT .....	14
3.2.1 Hide NAT - Automatic Rules .....	14
3.2.2 Hide NAT - Automatic Rule Testing .....	14
3.2.3 Hide NAT - Manual Rules .....	15
3.2.4 Hide NAT - Manual Rules Testing.....	16
3.3 Implementing Static NAT.....	16
3.3.1 Static NAT – Automatic Rules.....	17
3.3.2 State Table ARP Entries – 'fw tab -t arp_table' or 'fw ctl arp' .....	18
3.3.3 Static NAT – Automatic Rule Testing.....	19
3.3.4 Static NAT – Automatic Rules, Policy Rule Matching.....	20
3.3.5 Static NAT – Manual Rules .....	20
<b>4 Using Network Address Translation - Advanced</b> .....	<b>23</b>
4.1 Implementing Static NAT and Port Mapping.....	23
4.1.1 Static NAT – Automatic Rule Problem Using Different Ports .....	23
4.1.2 Static NAT – Manual Rules with Port Mapping .....	24
4.2 Hiding a Server on the External Network from the Internet .....	25
4.2.1 Taking advantage of ARPs .....	25
4.3 Static NAT without Proxy ARPs, Routed Networks .....	25

## 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

<b>Section 1</b>	IPS and Firewalls	10 Minutes
<b>Section 2</b>	IPS Features	40 Minutes
	Total time	50 Minutes

## Contents

<b>1</b>	<b>IPS and Firewalls</b>	<b>3</b>
1.1	Basic Intrusion Prevention System (IPS)	3
1.1.1	IPS Blade – Requires a License	3
1.1.2	Profile Management	4
1.1.3	Profile Assignment	7
1.1.4	Protections	9
<b>2</b>	<b>IPS Blade Features</b>	<b>10</b>
2.1	Network Security	10
2.1.1	Streaming Engine Settings	10
2.1.2	Anti-Spoofing Configuration Status	11
2.1.3	Denial of Service	11
2.1.4	IP and ICMP	12
2.1.5	TCP	14
2.1.6	Fingerprint Scrambling	14
2.1.7	DShield Storm Center	14
2.1.8	Port Scan	14
2.1.9	NTP	14
2.2	Application Intelligence	15
2.2.1	Mail	15
2.2.2	FTP	16
2.2.3	Microsoft Networks	16
2.2.4	Peer to Peer	16
2.2.5	Instant Messengers	16
2.2.6	DNS	17
2.2.7	VOIP	17
2.2.8	VPN Protocols	17
2.2.9	Remote Control Applications	18
2.2.10	The Others	18
2.3	Web Intelligence	19
2.3.1	Malicious Code	19
2.3.2	Application Layer	20
2.3.3	Information Disclosure	20
2.3.4	HTTP Protocol Inspection	20

## 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

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

## Contents

<b>1</b>	<b>Security Policy Rules Check</b> .....	<b>3</b>
1.1	Create New Policy with Basic Rules.....	3
<b>2</b>	<b>Content Security Servers</b> .....	<b>5</b>
2.1	Content Security Servers.....	5
2.1.1	Servers and Processes, HTTP, FTP, SMTP .....	5
2.1.2	Resouces (filters) .....	6
2.1.3	Example Rules .....	7
<b>3</b>	<b>HTTP Content Security Server</b> .....	<b>8</b>
3.1	HTTP Resources.....	8
3.1.1	Creating an HTTP Resource – Query Word Filter.....	8
3.1.2	Creating an HTTP Resource – Strip Java .....	10
3.1.3	Creating an HTTP Resource – Block an IP Address.....	11
3.1.4	Using URI Resources in Rules.....	12
3.1.5	Testing the Resources .....	12
3.1.6	URI Match – Example file.....	13
<b>4</b>	<b>FTP Content Security Server</b> .....	<b>14</b>
4.1	FTP Resources .....	14
4.1.1	Creating an FTP Resource .....	14
4.1.2	Filter Options.....	14
4.1.3	Apply the Resources to a Rule.....	15
4.1.4	Testing the Resource .....	16
<b>5</b>	<b>SMTP Content Security Server</b> .....	<b>17</b>
5.1	SMTP Resources .....	17
5.1.1	Creating an SMTP Resource .....	17
5.1.2	Apply the Resource to a Rule .....	18
<b>6</b>	<b>CVP and UFP Servers</b> .....	<b>19</b>
6.1	CVP.....	19
6.1.1	Creating a CVP Server.....	19
6.2	UFP.....	21
6.2.1	Creating a UFP Server.....	21
6.3	Using OPSEC Groups.....	22
6.3.1	Creating a Group.....	22
6.3.2	Load Balancing or Chaining .....	23



## 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

### Prerequisites

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

### Approximate time for completing each section

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

## Contents

<b>1</b>	<b>Managing Multiple Firewalls</b>	<b>3</b>
1.1	Creating the Virtual Machine	3
1.1.1	Virtual Machine – Type Linux, Red Hat	3
1.2	Installing SecurePlatform	3
1.2.1	Installing SPLAT	3
1.3	Managing Multiple Firewalls	6
1.3.1	SmartCenter License	6
1.3.2	Firewall Module License	6
<b>2</b>	<b>Creating fw.site2.com</b>	<b>7</b>
2.1	Creating fw.site2.com	7
2.1.1	Turn on Logging for Implied Rules	7
2.1.2	Creating the Firewall Object – fw.site2.com	7
2.1.3	Establishing Trust – SIC Communication	8
2.1.4	Topology	8
2.1.5	Writing Rules	9
2.1.6	Installing the Policy	10
2.1.7	Testing the Policy & Generating Log Traffic	11
2.1.8	Log Origin	12
2.2	Managing Multiple Firewalls	13
2.2.1	Single Policy or Multiple Policies	13
2.2.2	Creating Multiple Policies	14

## 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

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

## Contents

<b>1</b>	<b>Backing up the SmartCenter .....</b>	<b>3</b>
1.1	SmartCenter Configuration - 'upgrade_export' & 'upgrade_import' .....	3
1.1.1	Using upgrade_export.....	3
1.1.2	'upgrade_export' and Policy Revisions .....	5
1.2	Rebuilding a SmartCenter – 'upgrade_import'.....	6
1.2.1	Building a Virtual Machine for the SecurePlatform SmartCenter.....	6
1.2.2	Creating a base Install .....	7
1.2.3	Copying the upgrade_export file cpexport.tgz to the SecurePlatform ..	9
1.2.4	Completing the Install – Run 'sysconfig'.....	9
1.2.5	Testing the Install.....	13
1.3	Reset the Environment back to using the Original SmartCenter .....	14
<b>2</b>	<b>Backing up the Firewall on SecurePlatform .....</b>	<b>15</b>
2.1	Creating Backups – 'backup' .....	15
2.1.1	Create a backup of the Firewall.....	15
2.1.2	'backup' is just an 'alias' .....	16
2.1.3	Setting Automated Backups using the WebGUI.....	16
2.1.4	Local backup Directory.....	17
2.2	Recovering a Backup file using 'restore'.....	19
2.2.1	Using Restore to recover a Firewall .....	19
2.3	Snapshot Images – 'snapshot' .....	20
2.3.1	Creating a snapshot.....	20
2.3.2	The snapshot Directory.....	21
2.4	Restoring snapshot Images – 'revert' .....	21
2.4.1	Restore a snapshot Using 'revert' .....	21
<b>3</b>	<b>SPLAT Maintenance Mode .....</b>	<b>22</b>
3.1	Maintenance Mode – Single User Mode .....	22
3.1.1	Boot into Maintenance Mode – Single User .....	22