

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 MgmtSite1 & fwsite1 must be running

Approximate time for completing each section

Section 1	Dealing with Policy Packages	10 minutes
Section 2	Rule Basics	30 minutes
Section 3	Adding Rules	30 minutes
Section 4	Policy installs	10 minutes
Section 5	Explicit and Implicit Rules	15 minutes
Section 6	Saved Versus the Installed Policy	15 minutes
	Total time	1 Hr 50 Min

Contents

1	Dealing With Policy Packages	3
1.1	Policy Packages.....	3
1.1.1	Simplified or Traditional Policy	3
1.1.2	Creating a New Policy Package.....	3
2	Rule Basics	5
2.1	Rules	5
2.1.1	Rule Number	5
2.1.2	Name	5
2.1.3	Source and Destination	5
2.1.4	VPN.....	5
2.1.5	Service.....	6
2.1.6	Action	6
2.1.7	Track.....	6
2.1.8	Install On.....	6
2.1.9	Time.....	6
2.1.10	Comment	7
3	Adding rules.....	8
3.1	Adding rules	8
3.1.1	Stealth Rule	8
3.1.2	Internal Network Out bound Rule.....	8
3.1.3	Cleanup Rule	8
3.1.4	Broadcast Junk Rule	8
3.1.5	SMTP Inbound Rule	9
3.1.6	SMTP Outbound Rule	9
3.1.7	Web Inbound Rule.....	9
3.1.8	Firewall Secure Shell Access Rule	9
3.1.9	Negating Objects in a Rule.....	10
3.2	Reviewing the rules.....	10
3.2.1	Firewall at Risk from the SMTP Server.....	11
3.2.2	Internal Network at Risk from the SMTP Server.....	11
3.2.3	Adding Rule Section Titles	12
3.2.4	Rule Summary.....	13
4	Policy Installs.....	14
4.1	Installing the Policy	14

4.1.1	Verifying the Security Policy.....	14
4.1.2	Correcting the Policy after Verification Failures.....	14
4.1.3	Setting the Policy Targets	15
4.1.4	Installing the Policy.....	16
4.1.5	Checking the Firewall Status.....	17
4.1.6	Testing the Rules	17
4.1.7	Firewall Existing Connections - Behavior	17
5	Explicit and Implicit Rules.....	19
5.1	Implicit Rules.....	19
5.1.1	Viewing Implied Rules.....	19
5.1.2	Turning Implied Rules Off	21
5.1.3	Configuring DNS as an Implied Rule – (Don't)	22
5.1.4	Accept ICMP requests.....	22
5.2	Rule Base Filtering Order	22
5.3	Breaking SmartCenter Connectivity with Implied rules	22
5.3.1	Break SmartCenter to Firewall Connectivity	23
5.3.2	SmartCenter Connectivity Recovery - cpstop/cpstart.....	24
5.3.3	SmartCenter Connectivity Recovery – SIC Reset	25
5.3.4	SmartCenter Connectivity Recovery – ‘fw unloadlocal’	27
5.3.5	SmartCenter Connectivity Recovery – ‘fw fetch mgmt’ (Use this).....	28
5.4	SmartCenter and Firewall Services	28
5.4.1	Check Point ‘FW’ Services.....	29
5.4.2	Check Point ‘CP’ Services	29
5.4.3	SmartCenter to Firewall Explicit Rule – (For Safety)	29
6	Saved Versus the Installed Policy	31
6.1	Saved Policy	31
6.2	Installed Policy	31