

17 - SmartDefense

Objectives

- Know how to create SmartDefense Profiles
- Understand the typical network features SmartDefense 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 SmartDefense, apply them a Security Policy and test the features

Prerequisites

- Complete Module 16
- Virtual machines MgmtSite1, fwsite1 & classrouter must be running

Approximate time for completing each section

Section 1	SmartDefense and Firewalls	10 minutes
Section 2	SmartDefense Features	40 minutes
	Total time	50 Min

Contents

1 SmartDefense and Firewalls	3
1.1 Basic SmartDefense	3
1.1.1 SmartDefense Updates – Requires a License.....	3
1.1.2 Profile Management	3
1.1.3 Profile Assignment.....	4
1.1.4 Protection Overview	5
2 SmartDefense Features.....	6
2.1 Network Security.....	6
2.1.1 Denial of Service	6
2.1.2 IP and ICMP	7
2.1.3 TCP.....	8
2.1.4 Fingerprint Scrambling	8
2.1.5 Successive Events	9
2.1.6 DShield Storm Center	9
2.1.7 Port Scan.....	10
2.1.8 Dynamic Ports	10
2.2 Application Intelligence	11
2.2.1 Mail	11
2.2.2 FTP	11
2.2.3 Microsoft Networks.....	11
2.2.4 Peer to Peer.....	11
2.2.5 Instant Messengers	11
2.2.6 DNS	12
2.2.7 VOIP	12
2.2.8 VPN Protocols	12
2.2.9 Others	12
2.3 Web Intelligence.....	13
2.3.1 Malicious Code	13
2.3.2 Application Layer.....	14
2.3.3 Information Disclosure.....	14
2.3.4 HTTP Protocol Inspection	14