Check Point™
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

PROTECT

SmartDefense

PRODUCT FEATURES:

- Blocks network and application attacks by type and class
- Online security updates—Maintain optimal defenses
- Complete integration with FireWall-1
- Real-time logs with attack details and forensics

PRODUCT BENEFITS:

- Comprehensive network and application security
- Easy configuration of attack defenses
- Ensures attack defenses are up-to date and consistent across the security environment

CONNECT PROTECT MANAGE ACCELERATE

YOUR CHALLENGE

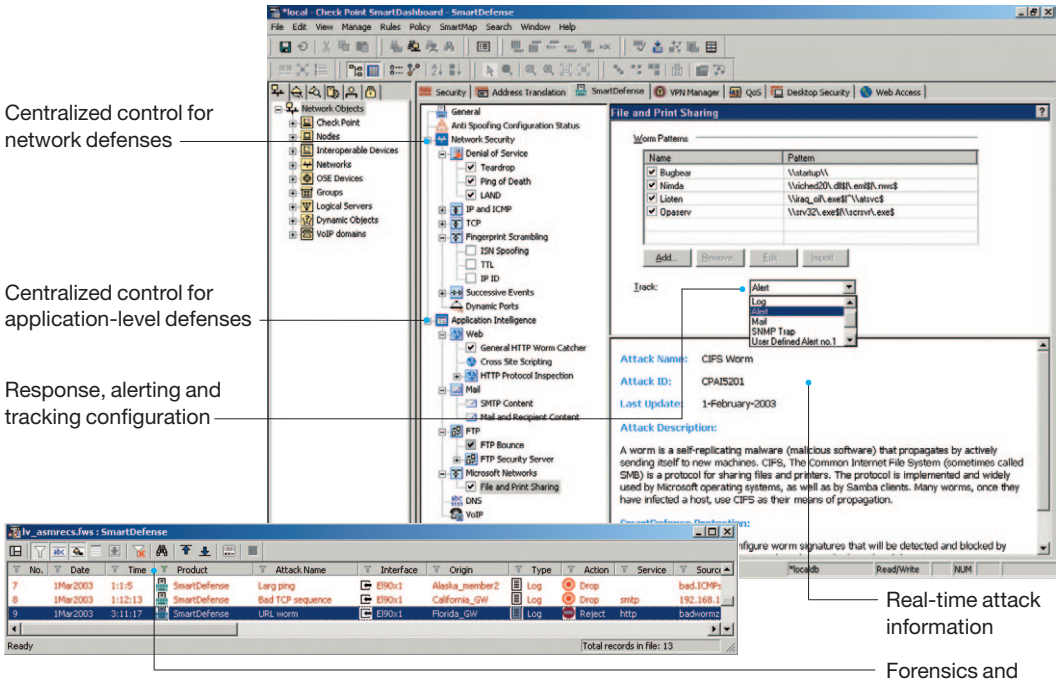
Organizations of all sizes, across all industries, face a serious threat of attacks against both networks and critical applications. Network-level attacks attempt to target network components or the firewall directly, while application-level attacks attempt to exploit vulnerabilities in applications running on the network. The growing number and severity of these threats requires a renewed vigilance on the part of the security manager to actively and intelligently block Internet attacks.

A robust and reliable security solution must have the intelligence not only to block all attacks at both the network and application level, but also to provide the security manager with a detailed understanding of the attacks. Useful forensic information combined with real-time security updates delivers better perimeter security and protects the organization from emerging Internet threats.

OUR SOLUTION

SmartDefense™ is a product offering that enables customers to configure, enforce and update network and application attack defenses. Included with FireWall-1®, SmartDefense actively protects organizations from network and application attacks using Check Point's patented Stateful Inspection and innovative Application Intelligence technologies.

SmartDefense not only protects against a range of known attacks, varying from different types of HTTP and Microsoft Networking worms to Distributed Denial-of-Service attacks, but it also incorporates intelligent security technologies that protect against entire categories of emerging, or unknown, attacks. In addition, SmartDefense integrates with the Check Point SMART Management and reporting infrastructure to provide a single, centralized console for real-time information on attacks as well as attack detection, blocking, logging, auditing and alerting.



SmartDefense actively protects organizations from all known and unknown network and application attacks using Application Intelligence and Stateful Inspection technology.

Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

CENTRALIZED CONTROL AGAINST ATTACKS

SmartDefense provides security managers with a single, centralized point of control against attacks. Attack types include mass-distributed and emerging attacks, like Code Red or Nimda, as well as Denial of Service (DOS), Internet worms, illegal and malformed Internet traffic, and fragmentation attacks. Alerting, tracking and auditing are all configured centrally, providing a complete solution for responding to attacks.

ONLINE UPDATES

Because keeping security current is a key element of remaining secure, SmartDefense works in conjunction with an ongoing subscription service delivered by Check Point to ensure that the latest information on new and emerging attacks is available to SmartDefense users. These online updates expand the capabilities of SmartDefense, delivering a level of response and flexibility that ASIC-based firewalls are not designed to provide.

Subscribing customers get one-click, automatic SmartDefense updates from within SmartDashboard™. When Check Point publishes updates, the SmartCenter™ management server retrieves new signature patterns, protocol definitions and attack mitigation solutions from Check Point and distributes them to enforcement modules.

DEDICATED PROTECTION CATEGORIES

In addition to the strict access control and attack protections offered by FireWall-1, SmartDefense offers a dedicated means to configure defenses and safeguards at both the network and application level.

- Anti-Spoofing
- Denial-of-Service
- IP
- ICMP
- TCP
- Fingerprint Scrambling
- Successive Events
- Dynamic Port Allocation
- Web Applications
- E-Mail
- FTP
- Microsoft Protocols
- DNS
- VoIP

REAL-TIME ATTACK INFORMATION

The SmartDefense user interface includes background details on attacks and hyperlinks to even more information on the nature and characteristics of attacks.

Valuable attack forensics are provided through Check Point's rich log data and distributed logging infrastructure. SmartDefense integrates with the Check Point log infrastructure by adding attack log entries and relevant views in SmartView Tracker™, SmartView Monitor™, and SmartView Reporter™. This data provides security managers with knowledge about the nature of the attacks and potential responses, enhancing their understanding of and control over attacks.

STORM CENTER INTEGRATION

The SmartDefense Storm Center Module is included in the standard FireWall-1 product installation. It enables a two-way information flow between the network Storm Centers, and the organizations requiring network security information.

Check Point SmartDefense integrates with the SANS DShield.org Storm Center in two ways

- The SmartDefense Storm Center Module can retrieve a Block List of known attacker addresses for addition to the Security Policy.
- Administrators send anonymous logs to the Storm Center in order to help other organizations combat the same threats that were directed at their networks.

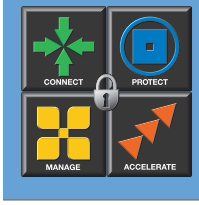
SYSTEM REQUIREMENTS

SmartDefense shares the same system and configuration requirements as the related FireWall-1 enforcement module. SmartDefense can be active on the following enforcement points:

- FireWall-1
- VPN-1® Pro™
- VPN-1/FireWall-1 VSX
- VPN-1/FireWall-1 SmallOffice[1]
- VPN-1/FireWall-1 SecureServer[2].

SmartDefense can be managed using SmartCenter, SmartCenter Pro™, SiteManager-1™, or Provider-1®.

[1] Does not support the SMTP Security Server.
[2] Does not support Security Servers.



P/N 500557