

SmartDefense

PRODUCT FEATURES:

- Complete integration with FireWall-1
- Blocks attacks by type and class
- Online security updates
- Real-time logs with attack details and forensics

PRODUCT BENEFITS:

- Enhanced network security
- Detects and defends against all network attacks
- Ensures attack defenses are up-to-date and consistent across the security environment
- Enhances understanding and control over attacks

YOUR CHALLENGE

Organizations are facing increasing risks from Internet attacks. 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 to not only block all attacks, but provide the security manager with a detailed understanding of the attacks. Useful forensic information combined with real-time security updates delivers better firewall security and protects the organization from emerging Internet threats.

OUR SOLUTION

Check Point Software's SmartDefense™ introduces a new category of Internet security products: Active Defense solutions. Included with FireWall-1®, SmartDefense actively protects organizations from all known and unknown network attacks using intelligent security technology. It blocks attacks by type and class using Check Point's patented Stateful Inspection technology and provides a single, centralized console for real-time information on attacks as well as attack detection, blocking, logging, auditing and alerting.

Real-time attack information

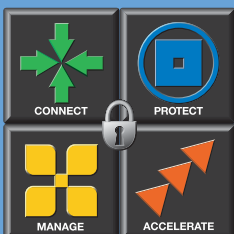
Centralized control for all network attacks

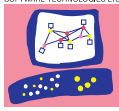
Response, alerting and tracking configuration

No.	Date	Time	Product	Inter.	Attack Name	Origin
24	16-Jan-2002	18:35:13	SmartDefense	EIS...	Under SYN attack - Switching to active protection	10.27.10.2
25	16-Jan-2002	18:40:13	SmartDefense	EIS...	SYN attack abated - Switching to passive protec...	10.27.10.2

Forensics and active response

SmartDefense actively protects organizations from all known and unknown network attacks using intelligent security technology.





CENTRALIZED CONTROL AGAINST ATTACKS

SmartDefense provides security managers with a single, centralized point of control against attacks. It defeats a broad range of attack types, including denial of service (DoS), IP attacks, network probing, and web and application vulnerabilities. In addition, alerting, tracking and auditing are all configured centrally, providing a complete network defense.

NETWORK ATTACKS DEFEATED

Denial of Service DoS Attacks

- SYN Flood
- LANd

IP Attacks

- IP Spoofing
- IP Fragmentation
- Illegal and Malformed Packets

Web and Application Vulnerabilities

- DNS Attacks
- Protocol Non-compliance
- Application-specific Vulnerabilities
- Trojan Horses
- Back Door and Remote Administration
- Mobile code (JavaScript, Active-X)
- Hidden File Extension

Network Probing

- Port Scanning
- Service Scanning

HTTP Worms*

- Code Red
- htr Overflow
- Nimda

*Additional worms added as they emerge

ONLINE UPDATES

Check Point provides an optional SmartDefense update service to ensure that the latest information on new and emerging attacks is available to SmartDefense customers. These online updates expand the capabilities of SmartDefense, delivering a level of response and flexibility that hardware- and ASIC-based firewalls are not designed to provide.

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. This data provides security managers with knowledge about the nature of the attacks and potential responses, enhancing their understanding and control over network attacks.

SYSTEM REQUIREMENTS

SmartDefense is integrated with FireWall-1 FP2 and later.

See FireWall-1 system requirements for more information

