

# Check Point InterSpect

## The Internal Security Gateway™

### PRODUCT FEATURES:

- Intelligent Worm Defender
- Network Zone Segmentation
- Quarantine of Suspicious Computers
- LAN Protocol Protection
- Pre-emptive Attack Protection

### PRODUCT BENEFITS:

- Blocks the spread of worms and attacks inside the network
- Segments the network into organizational security zones
- Isolates attacks and compromised devices
- Provides the deepest and most comprehensive support for Microsoft and other LAN Protocols
- Provides proactive defenses against vulnerabilities before they are exploited

### YOUR CHALLENGE

To date, IT security organizations have focused on the network perimeter. However, many of today's attacks are introduced from inside the network. Laptops, PDAs and other devices travel into and out of the network daily, making it possible for legitimate users to infect the network or unwittingly grant attackers access to the network via a Trojan horse or other spyware.

For example, many worms have propagated inside the network after being introduced by an internal source. Once a single network device has been infected, the entire network can be compromised very quickly. Fast-spreading worms, often called "flash" or "blitz" worms, can spread worldwide in a matter of minutes!

With such costly threats becoming increasingly common, organizations have come to realize that they must provide better defenses against worms, unauthorized access threats and other attacks within their internal network.

### OUR SOLUTION

Check Point InterSpect™ is an internal security gateway that blocks the spread of worms and attacks inside the network and provides network zone segmentation. Based on Check Point's proven security technologies: INSPECT™, Stateful Inspection and Application Intelligence™, and SMART (Security Management Architecture), InterSpect is built specifically for internal network security. InterSpect provides:

- Intelligent Worm Defender™
  - Blocks the spread of worms and attacks inside the network
- Network Zone Segmentation
  - Segments the internal network into organizational security zones
- Quarantine of Suspicious Computers
  - Isolates attacks and compromised devices
- LAN Protocol Protection
  - Provides the deepest and most comprehensive support for Microsoft and other LAN protocols
- Pre-emptive Attack Protection
  - Provides proactive defenses against vulnerabilities and attacks before they are exploited



*InterSpect is designed for flexible and non-disruptive deployment into existing network environments and includes a management interface tailored specifically for internal security.*



Intelligent Security

## FEATURES

### Intelligent Worm Defender

The Intelligent Worm Defender provides the most powerful internal network worm protection by applying Check Point Stateful Inspection and Application Intelligence technologies. These technologies are based on INSPECT, which provides the most comprehensive and adaptive protection available. InterSpec is installed between protected network zones and prevents the spread of worms inside the network by inspecting the traffic from connected devices and blocking dangerous traffic.

### Network Zone Segmentation

InterSpec segments the network into multiple administrator-defined security zones to prevent unauthorized access between zones. This prevents users or compromised computers on the network from accessing information and systems they are not authorized to view. Network zone segmentation also contains attacks within a sub-segment of the network.

### Quarantine

InterSpec can identify suspicious or infected computers on the network and quarantine them, preventing the rest of the network from being compromised. InterSpec also allows the quarantine of computers during security patch deployment. This helps ease the risk of infection while network administrators identify, install and test patches.

InterSpec also has a unique user notification capability for quarantine. When a user's computer is quarantined, typically because the computer has been identified as infected, the user is notified via a customized dynamic web page. This notification helps to minimize the time spent troubleshooting the issue at the help desk, and also allows the network administrator to be made aware of the issue, reducing user downtime.

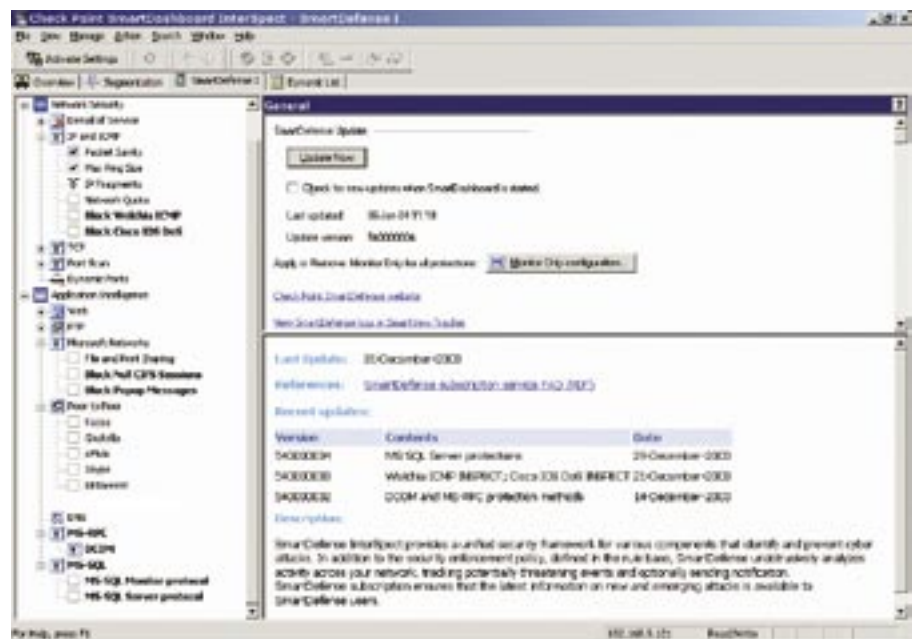
### LAN Protocol Protection

InterSpec provides the deepest and most comprehensive protection for Microsoft protocols such as MS RPC, CIFS, MS SQL, and DCOM, as well as other LAN protocols such as Sun RPC, DCE RPC, and HTTP. InterSpec uses INSPECT technology to provide the industry's most adaptive security inspection capability. By taking advantage of INSPECT updates, available via SmartDefense™ subscription, InterSpec users can keep their internal security infrastructure up-to-date as new attacks and threats emerge.

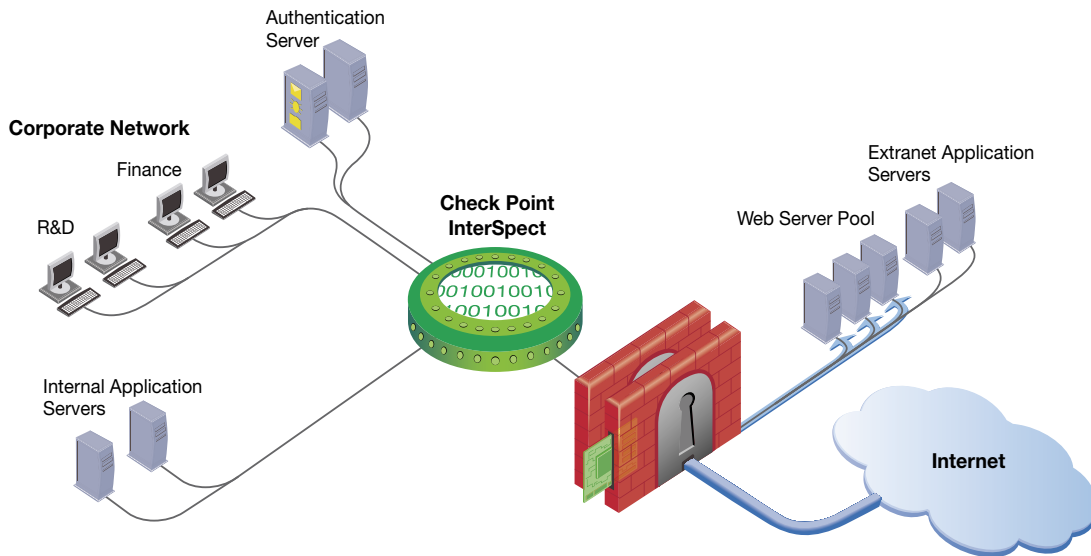
### Pre-emptive Attack Protection

InterSpec provides proactive and dynamic protection for known and unknown attacks, enabling organizations to defend against vulnerabilities before they are exploited.

InterSpec includes a version of SmartDefense customized for internal network security that allows administrators to configure, enforce, and update all network and application attack defenses using Stateful Inspection and Application Intelligence, which are based on INSPECT, the industry's most intelligent and adaptive security inspection technology.



*InterSpec includes SmartDefense for internal networks, providing pre-emptive protection for known and unknown attacks inside the network.*



*InterSpec is the only solution specifically designed for internal security.*

### Management Tailored for Internal Security

Managing InterSpec is made easy by using a management interface designed specifically for internal security. Based on SMART, this interface provides a powerful, easy-to-use interface to address the configuration and policy management issues unique to internal security.

Typically, network-level firewalls are configured to drop all traffic unless explicitly allowed. This can be quite complex to configure for internal deployments. But with Check Point, security segmentation is as simple as

installing InterSpec into your network and defining your network security zones. InterSpec immediately begins inspecting traffic and dropping malicious content while allowing all common LAN traffic. Administrators can then explicitly disallow specific traffic patterns as well as configure internal security zones with an easy-to-use interface.



*InterSpec's management interface is specialized for internal security, providing a simple, powerful interface for configuring network zone segmentation and exception policies.*

### PERFORMANCE

InterSpec is an appliance that has been designed to meet the performance demands of internal security. InterSpec is based on SecurePlatform, Check Point's hardened security operating system. To ensure the highest level of performance, InterSpec also includes Check Point's patented SecureXL™ security acceleration technology.

## DEPLOYMENT MODES

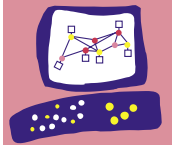
To support various deployments, InterSpect can work in three in-line operating modes (bridge, switch, and router mode). Monitor-only capability can be used with all modes.

Description	Primary Deployment Scenarios
<b>Bridge mode</b> InterSpect bridges one or more segments to the backbone and is invisible to the IP network	Transparent deployment of segmentation, worm defense and quarantine
<b>Switch mode</b> InterSpect acts as a multi-port bridge in which all ports are bridged together to make one zone	Transparent deployment of worm defense and quarantine when full segmentation is not required
<b>Router mode</b> InterSpect acts as a router, every active port is configured with a different IP address	Sophisticated network zone segmentation for multiple security zones
<b>Monitor-only capability</b> InterSpect inspects traffic without enforcing safeguards and defenses (Can be used with Bridge, Switch, or Router Modes)	Pilot deployments to understand InterSpect's effect on legacy applications prior to active, in-line deployment

## SPECIFICATIONS

	InterSpect 210	InterSpect 410	InterSpect 610	InterSpect 610F
Target	One workgroup protection	Multiple workgroup protection	Gigabit network protection	Gigabit network protection
Operating Environment	Check Point SecurePlatform	Check Point SecurePlatform	Check Point SecurePlatform	Check Point SecurePlatform
Throughput	200 Mbps	500 Mbps	1000 Mbps	1000 Mbps
Fiber interfaces	N/A	Add-on available	Add-on available	Included
Expansions Slots	N/A	1	1	1
Inspection Ports	2	3-10	3-10	3-10
Management Port	1	1	1	1
Max ports	3	10	10	10
Interface speed	10/100 Mbps	10/100/1000 Mbps	10/100/1000 Mbps	10/100/1000 Mbps
VLAN Support	8 VLANs	128 VLANs	Unlimited VLANs	Unlimited VLANs
Redundant Power	No	Optional	Included	Included
SmartDefense Subscription	Included for 1st year	Included for 1st year	Included for 1st year	Included for 1st year
Width	16.7"/42.5 cm	17.61"/44.7 cm	17.61"/44.7 cm	17.61"/44.7 cm
Height	1.68"/4.2 cm (1U)	1.68"/4.2 cm (1U)	1.68"/4.2 cm (1U)	1.68"/4.2 cm (1U)
Depth	21.9"/55.5 cm	27"/68.3 cm	27"/68.3 cm	27"/68.3 cm
Weight	27 lbs/12.25 kg	35 lbs/15.9 kg	35 lbs/15.9 kg	35 lbs/15.9 kg
Power	100-220 Volts 50/60 Hz	100-220 Volts 50/60 Hz	100-220 Volts 50/60 Hz	100-220 Volts 50/60 Hz

Check Point  
SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

© 2004 Check Point Software Technologies Ltd. All rights reserved. Check Point, the Check Point logo, Application Intelligence, Check Point Express, Cluster XL, ConnectControl, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FireWall-1 VSX, FireWall-1 XL, FloodGate-1, INSPECT, INSPECT XL, InterSpect, IQ Engine, Meta IP, MultiGate, Open Security Extension, OPSEC, Provider-1, Safe@Office, SecureKnowledge, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartView Tracker, UAM, User-to-Address Mapping, UserAuthority, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecureRemote, VPN-1 SecureServer, and VPN-1 VSX are trademarks, service marks, or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

P/N 501210