



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.



White Paper

Providing Unparalleled Security for Internal Networks

Check Point InterSpect



Intelligent Security

Check Point protects every part of your network—perimeter, internal, Web—to keep your information resources safe, accessible, and easy to manage.

Contents

Executive Summary	3
Internal Networks: an Under-Guarded Resource	3
Internal Networks Present Unique Security Challenges	4
What Is Needed to Secure Internal Networks?	4
Existing Solutions Are Not Optimized for Internal Networks	5
- Patches	5
- Antivirus	5
- Switch- and Router-based Security Solutions	5
- Firewalls	5
- Intrusion Detection and Prevention Systems	6
Check Point InterSpect:	
Meeting the Security Challenges of Internal Networks	6
- Intelligent Worm Defender	7
- Network Zone Segmentation	8
- Quarantine Capabilities	8
- Comprehensive Microsoft and LAN Protocol Protection	9
- Preemptive Attack Protection	9
- Centralized Management	9
- Endpoint Security Integration	10
- High Performance	11
- Choice of Platforms	11
Conclusion	11

Executive Summary

IT security administrators have long focused on securing the network perimeter. While focus on the perimeter is important, organizations have realized the need to secure their internal networks in order to stem the sharp increase of worms and other attacks specifically introduced inside the network via mobile and wireless devices. However, while many of the same principles used to construct and operate perimeter security solutions also apply to internal networks, internal security can be more complex, require higher performance, and have unique requirements. As a result, existing perimeter security solutions (e.g., patches, antivirus software, switch and router-based solutions, legacy firewalls, and intrusion detection and prevention systems) are inadequate for securing internal systems.

This white paper details the security requirements for internal networks and discusses why existing perimeter security solutions are unable to fulfill these requirements. The paper also describes how Check Point InterSpect™ uses proven and new technologies, methodologies, and approaches to address the security challenges unique to internal networks.

Check Point InterSpect provides the following capabilities:

- Intelligent Worm Defender that restricts the spread of worms and attacks inside the network
- Network zone segmentation capabilities that isolate attacks and prevent them from spreading through the network
- Quarantine of suspicious computers
- Comprehensive LAN protocol protection to guard against attacks while maintaining application connectivity
- Preemptive attack protection that stays a step ahead of exploits and intruders
- Integrated management that is scalable, easy to use and manage
- Endpoint security integration assures that only compliant users can access network resources

Internal Networks: an Under-Guarded Resource

Historically, IT security organizations have focused security resources on the network perimeter. Yet, even organizations with strong perimeter security can fall victim to attack when legitimate, authenticated users introduce attacks from inside the network through mobile and wireless devices. Once inside firewall boundaries, these attacks easily evade the limited internal controls, such as antivirus scanners. For example, the Blaster worm, which commonly propagated among network users after being introduced by an internal source, caused more than \$500 million (USD) in economic damages (source: Computer Economics, Inc.). Organizations must therefore augment their existing perimeter security solutions by implementing controls directly within the internal “back-end” environment.

Internal Networks Present Unique Security Challenges

At the perimeter, organizations control access and prevent attacks by creating demilitarized zones that incorporate firewalls, authentication, intrusion detection, and antivirus solutions. Security solutions for internal networks require similar functionality, but must also address additional requirements.

Internal networks are characterized by greater scale and complexity than external networks. While securing network perimeters, administrators typically work with a network environment that includes multiple systems and hundreds of megabytes of traffic. On the other hand, internal networks may include thousands of systems and gigabytes of traffic, creating heightened potential for security risk.

The application environment for an external network may include dozens of applications and related protocols. These standard, well-defined applications adhere strictly to protocols and run in a client-to-server configuration. In contrast, internal networks may include a much wider range of applications and underlying protocols. Many internal applications are homegrown, adhere loosely to protocols, and are not “hardened” for security.

Finally, the management environment for external networks involves a limited number of user classifications. As a result, administrators usually configure firewalls to block unknown traffic. The internal management environment includes a far greater number of user roles and groups, resulting in a much more complicated set of policies and controls. Because traffic must flow freely on an internal network, administrators of internal networks cannot block traffic categorically. In order to maintain internal network business continuity, administrators must allow all traffic except attack or clearly inappropriate traffic.

Any solution that attempts to provide internal security must account for the above differences.

What Is Needed to Secure Internal Networks?

To meet the requirements of internal networks, a security solution must

- Protect against common and troublesome attacks, such as worms and blended threats, which legitimate users might unleash on the network (these attacks often occur at the application layer)
- Segment the network into separate security zones to limit any attacks that do occur to a single sub-network, and to prevent users within the organization from accessing data to which they are not authorized
- Quarantine suspicious or unpatched computers to isolate attacks and compromised devices
- Enable mission-critical application communications to continue while eliminating attack traffic from network and application layers
- Provide proactive defenses against both known and undiscovered vulnerabilities and attacks
- Offer centralized management capabilities necessary for easy and scalable management of both perimeter and internal security solutions
- Be easy to deploy as part of a larger corporate security environment

- Offer endpoint security integration to allow enforcement of security policies throughout the core of the network to the desktop, preventing the spread of attacks from infected devices
- Provide excellent performance to support the higher throughput requirements of an internal network

Existing Solutions Are Not Optimized for Internal Networks

Many conventional security products and approaches can be applied to internal security, including patches, antivirus software, switch and router based solutions, firewalls, and intrusion detection and prevention solutions. However, these solutions are not well-tuned to fully address the unique requirements of internal networks.

Patches

One common method used to secure internal systems is to install application patches. While the timely installation of a patch can eliminate specific vulnerabilities, patches will never offer a complete, fail-proof security solution for internal networks. To start with, patches are not always available. And over the past two years, the time between the initial identification of the vulnerability and the development of an attack that exploits that vulnerability has shrunk dramatically. Therefore, vendors may not be able to provide patches quickly enough to deflect well-aimed attacks.

Even when patches are available, managing and installing patches is becoming a huge burden. Patch quality is often poor, requiring organizations to test each patch to ensure that it doesn't cause problems on the network. Because current patch-management processes remain ad hoc and manual, installing patches on all systems in a large network is time and resource intensive. To further complicate matters, industry trends indicate that software vendors are releasing an increasing number of security and software fixes. The trend is likely to continue, and the patch management process will only become a more daunting challenge as the number of patches continues to grow.

Finally, not all vulnerabilities involve design or coding errors; they may result from configuration errors, such as a poorly constructed security policy. Patching is irrelevant in these cases.

Antivirus Software

Antivirus software is a ubiquitous and important security measure that protects desktop and server machines against many known viruses. However, virus software is notoriously bad at providing protection against worms. Because antivirus software is signature-based, it is purely reactive and unable to protect against new, previously unknown threats. For these reasons, antivirus software can be thought of as an "anti-nuisance" tool because it prevents the nuisance of being infected by a previously known virus. However, antivirus software has severe limitations when trying to proactively defend vulnerabilities before the vulnerability is exploited by a new attack.

Switch- and Router-based Security Solutions

Some switch- and router-based security solutions apply security functions to any traffic that passes through the switch and router. When they detect an attack, these solutions completely shut down access to affected ports. This is an unacceptable response for an internal network. Moreover, these solutions detect

attacks only at the network protocol layer and are unable to furnish application-level protection. Security policy for switches and routers can also be extremely difficult to configure for an internal network since administrators must explicitly allow certain traffic types—often a time-consuming process.

Firewalls

Enterprise firewalls have emerged as the staple of perimeter security architecture because they defeat most attacks when used to enforce a properly defined security policy. But while firewalls provide effective perimeter security, vendor implementations vary widely when it comes to providing the ability to inspect application protocols and preemptively prevent attacks. Additionally, firewalls are usually designed to block all traffic that is not specifically permitted. Because internal network environments consists of numerous applications and protocols, many of which are homegrown, configuring “allowed” internal traffic using perimeter firewalls can be a difficult task. Perimeter firewalls also lack internal quarantine capabilities, which are important to internal network security.

Intrusion Detection and Prevention Systems

Intrusion Detection Systems (IDS) are designed to detect application-level attacks by examining data for patterns and anomalies that indicate an attack. IDS solutions then announce suspicious or anomalous traffic and wait for manual intervention. IDS are traditionally used to fine-tune a security policy and defenses after a security incident has occurred, but do not offer proactive protection.

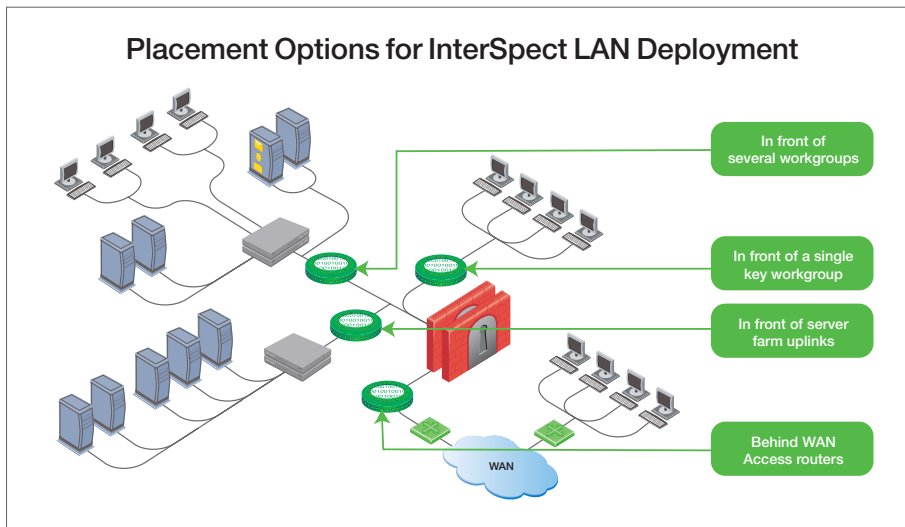
Intrusion Protection Systems (IPS) are primarily complementary technology to perimeter firewalls. IPS use an evolved form of intrusion detection technology to reactively block threats to a network based on similar signatures. Most IPS do not offer any integration with endpoint security solutions. IPS are also heavily signature-based, and like all signature-based solutions, have difficulty proactively thwarting previously unknown threats.

CheckPoint InterSpect: Meeting the Specific Security Challenges of Internal Networks

Check Point, known for its leading security management architecture and intelligent security solutions, has addressed the unique challenges of securing internal networks with InterSpect, the first and only complete Internal Security Gateway. InterSpect combines technologies designed specifically for LANs, and other proven technologies, to offer multiple layers of attack protection within the core (internal) network through the following features:

- *Intelligent Worm Defender* blocks the spread of worms and attacks inside the network
- *Network zone segmentation* limits attacks to administrator-defined security zones and minimizes unrestricted employee access
- *Quarantine capabilities* contain attacks to compromised devices and isolate unpatched servers
- *Comprehensive Microsoft and LAN protocol protection* supports protocols and applications used inside the network to maintain application connectivity
- *Preemptive attack protection* enables the gateway to proactively guard against known and unknown threats, and to safeguard vulnerabilities before they are exploited by an attack

- *Centralized management* environment that manages internal and perimeter security devices and that is scalable, easy to use and manage
- *Endpoint security integration* for in-depth defense throughout the core of the network to the desktop, and to enforce endpoint security policies
- *High performance* that does not impact network throughput



Intelligent Worm Defender

Worms are one of the most ubiquitous threats to internal networks today. InterSpect Intelligent Worm Defender blocks the spread of worms and attacks through the use of Check Point INSPECT™, the industry's most intelligent and adaptive inspection technology. The patented Check Point INSPECT engine uses Stateful Inspection and Application Intelligence™ to enforce the security policy on the InterSpect gateway. InterSpect examines all application layers, and brings cumulative data from the network configuration, security rules, and communication and application states to evaluate connection attempts. By incorporating an understanding of how LAN and Windows-based applications are used on the network, InterSpect ensures that network traffic conforms to protocol standards and expected usage. InterSpect also ensures secure use of Microsoft applications in situations where other solutions force a trade-off between connectivity and security. For example, the Blaster Worm exploited the MS-RPC protocol; InterSpect can block malicious RPC connections while allowing non-dangerous RPC connections to proceed.

Because the InterSpect gateway watches traffic as it flows through the network, it can also catch fast-moving worms that other technologies are unable to detect or contain. For example, virus protection software can protect a system only when malicious files attempt to write themselves to disk. Because SQL Slammer fits into a single packet that is never written to disk, antivirus software is useless in the face of this type of attack. IDS solutions that do recognize SQL Slammer are unable to react quickly enough to defend against it because they require manual intervention.

Network Zone Segmentation

Internal networks can contain thousands of individual systems. InterSpect can be deployed at various points in the infrastructure to segment the network into multiple security zones, defined by physical or virtual segments, and to control access and communications between these zones. InterSpect allows all necessary traffic to flow throughout the network, yet prevents unauthorized (intentional or unintentional) use between segments.

To meet the widest range of network topology requirements, InterSpect supports VLAN-based virtualization leveraging previous investments in VLAN segmentation. This allows for greater deployment flexibility closer to the core of the network. Virtual zones allow InterSpect to protect a very large number of geographically separated zones, applying a unique security policy to each protected zone, allowing a single appliance to protect potentially thousands of segments. By allowing configuration of both physical and virtual zone segments, organizations can enforce a zone-based security policy, thus enabling true organizational or departmental security zones.

Quarantine of Suspicious Computers

InterSpect's quarantine capabilities can isolate suspicious systems to contain attacks. The quarantine capabilities can be configured to automatically isolate computers when they fall victim to an attack, thus preventing the spread of infection to other systems. Network administrators can use the quarantine capability to isolate servers and mitigate risks before and during the patching process. The following examples illustrate these two quarantine scenarios:

Scenario 1—InterSpect Quarantines Suspicious Computers

1. InterSpect segments the network into separate security zones
2. InterSpect identifies a suspicious or infected computer in one of the security zones
3. InterSpect isolates the suspicious or infected computer from the network so it cannot infect computers in other zones

Scenario 2—InterSpect Quarantines Unpatched Computers

1. InterSpect segments the network into security zones
2. Administrator identifies a group of unpatched servers
3. Administrator sets up a quarantine of the unpatched servers
4. Administrator patches the quarantined servers, while InterSpect ensures that the rest of the network is protected

When a system is quarantined, InterSpect's unique notification capabilities can provide notification messages to quarantined users. This feature reduces the total cost of ownership for the InterSpect gateway by reducing time spent troubleshooting connectivity issues during user calls to technical support. Another way that InterSpect reduces management complexity is by allowing a quarantine to be unidirectional, meaning that a quarantined machine cannot perform outbound communications but can still receive inbound communications. This unidirectional quarantine capability prevents a suspicious computer from infecting others yet allows it to be cleansed or receive patches remotely.

Comprehensive Microsoft and LAN Protocol Protection

Internal networks use more and different protocols than perimeter networks. Internal network security products require a deep understanding of Microsoft and LAN protocols if they are to block attack traffic while allowing all other traffic to flow normally. InterSpect utilizes Check Point's Application Intelligence and Stateful Inspection to provide the industry's deepest, most comprehensive support for Microsoft and other LAN protocols. Supported protocols include Microsoft RPC, CIFS, MS SQL, DCOM, DCE RPC, HTTP, and many others.

Preemptive Attack Protection

Successful attacks take advantage of either known or previously unknown vulnerabilities. Most security solutions on the market today guard only against known vulnerabilities. Check Point, however, takes a proactive approach to security with products that utilize a deep understanding of how protocols can be used and misused to guard against both known and unknown threats.

Check Point InterSpect incorporates Stateful Inspection and Application Intelligence to actively protect internal networks from known and unknown attacks. Because new types of threats are continually emerging, Check Point also monitors industry vulnerability forums and works with application software vendors to identify vulnerabilities and develop appropriate safeguards before the vulnerabilities are exploited, and often before the vulnerability is even discovered. Check Point provides customers with the resulting updates to the pre-configured defenses via the SmartDefense™ Subscription Service.

Check Point's track record speaks for itself. Check Point has delivered safeguards and defenses for new or potential vulnerabilities in HTTP 1.1, SIP, CIFS, and DCE RPC before these vulnerabilities became public, and in many cases before the vulnerabilities were discovered.

Centralized Management

InterSpect can be centrally managed based on the Check Point Security Management Architecture (SMART) including both SmartCenters and Provider-1®/SiteManager-1™, simplifying administration and boosting productivity.

Seamless management is integrated into InterSpect's non-disruptive deployment paradigm to allow for easy deployment and management in almost any existing network environment. Some of the capabilities that allow InterSpect to be deployed in a non-disruptive manner include

- Multiple in-line deployment modes (bridge, switch, or router), which are discussed below in more detail.
- Monitor-only capability to allow the product to be deployed in-line but without blocking traffic. This attribute allows a system administrator to "test" the product in-line, determine what malicious or undesirable content would be caught, but not perform the actual blocking. With the monitor-only capability activated, logs and reports are generated and the system administrator can then fine-tune defenses as appropriate. When the administrator feels comfortable with a defense, he or she can switch from monitor-only to fully active mode. The monitor-only capability is set on a defense-by-defense basis (i.e., some defenses can be in monitor-only mode while others are in fully active mode).
- Exception lists to allow certain traffic or communications to always be allowed, or conversely to always be blocked.



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

To enable organizations to best deploy the gateway into their networks, InterSpect can be deployed in one of three modes: bridge mode, switch mode, and router mode.

Bridge mode protects the internal network by dividing it into protected zones. InterSpect can run in bridge mode over a trunk link between two switches carrying multiple VLANs over a single physical link. Each zone bridges one or more Ethernet segments to the backbone and is invisible to the IP network. Virtual zones are identified by their unique VLAN ID and packets belonging to a zone are processed by InterSpect accordingly. With bridge mode, organizations benefit from simple and fast segmentation, non-disruptive deployment, and application-layer protection for legacy firewalls.

Switch mode, which is InterSpect's default configuration, allows InterSpect to replace a network switch. In switch mode, InterSpect acts as a multi-port switch that links all ports together to make a single zone. Organizations need not configure any zones or perform any other configuration. Switch mode can be used for transparent deployment of worm defenses and quarantine capabilities for every network segment when full segmentation is not required.

Router mode allows organizations to use InterSpect to replace a router. They simply configure every active port with the same IP address as the router being replaced. Router mode provides sophisticated network zone segmentation for multiple security zones including virtual zones defined by VLAN ID. This can alleviate physical wiring and minimize network gear requirements.

Endpoint Security Integration

InterSpect provides robust security to the core network, but to reach in-depth defense beyond both the perimeter and the core network, security must also be provided to the desktop or endpoint. Rouge devices, such as laptops that travel in and out of the protected network, present a direct threat to the entire internal network. In such cases, an infected device can potentially connect directly to the LAN, completely independent of the perimeter security already in place, and

very quickly allow an attack to spread across the entire network. With Integrity deployed, Check Point's proactive endpoint security solution, an additional layer of security is provided. Even more, through Cooperative Enforcement™, InterSpect works in conjunction with Check Point Integrity™ to secure all desktops and laptops that connect to the network. Even further, Cooperative Enforcement technology enables Integrity to integrate with hundreds of network gateway products—from VPNs to switches to wireless access points.

Only InterSpect and Integrity offer Total Access Protection by providing enhanced security not only at the LAN, but also down to the wired or wireless desktops and laptops that connect to the network.

High Performance

Because of their greater traffic, internal networks require much higher performance from a security gateway than do external networks. InterSpect offers excellent performance when used with internal networks. The InterSpect INSPECT Engine imposes negligible processing overhead on the gateway because it runs inside the system kernel; it requires no context switching, and achieves low-latency operation. InterSpect also includes SecureXL™, an open interface that enables administrators to offload intensive security operations to third-party hardware or optimized software. As a result, InterSpect can deliver gigabit performance levels that will not impact the throughput of internal networks.

Choice of Platforms

In addition to the line of Check Point InterSpect appliances, Check Point and Crossbeam Systems have partnered to offer InterSpect on Crossbeam X-Series security switches. The result is cost-effective, bulletproof segmentation and quarantining that delivers up to 8-Gbps performance with 99.999% availability. The InterSpect-on-X solution provides a single hardware device that seamlessly integrates at core, distribution or access layers. Its high port density allows many separate network segments to be protected and it can operate in bridge or switch mode. InterSpect-on-X offers the highest scaling and highest availability solutions for internal network protection.

Conclusion

Unlike point security products designed for perimeter defense, Check Point InterSpect uses proven security technologies to address the unique challenges involved in protecting internal networks. The Intelligent Worm Defender protects against the most common and costly internal attacks. Quarantine and network zone segmentation offer multiple layers of attack protection and security segmentation. Comprehensive LAN protocol protection guards against application-layer attacks while allowing normal LAN communications to continue uninterrupted. Proactive attack prevention keeps the solution one step ahead of intruders. Cooperative Enforcement between InterSpect and Integrity provides for more granular and more secure layered internal security environment. Along with these features, InterSpect provides the high throughput internal networks require and management capabilities that address the singular concerns of internal networks, while also providing for a centralized management environment for all network security systems. Taken together, these features provide the most comprehensive protection available to internal networks today, while reducing the total cost of ownership of internal security deployment.

About Check Point Software Technologies

Check Point Software Technologies (www.checkpoint.com) is the worldwide leader in securing the Internet. It is the market leader of both the worldwide VPN and firewall markets. Through its Next Generation product line, the company delivers a broad range of intelligent Perimeter, Internal and Web security solutions that protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company's ZoneAlarm product line is one of the most trusted brands in Internet security, creating award-winning endpoint security solutions that protect millions of PCs from hackers, spyware and data theft. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from over 350 leading companies. Check Point solutions are sold, integrated and serviced by a network of more than 2,200 Check Point partners in 88 countries.

CHECK POINT OFFICES

Worldwide Headquarters

3A Jabotinsky Street, 24th Floor
Ramat Gan 52520, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256
e-mail: info@Checkpoint.com

U.S. Headquarters

800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391 ; 650-628-2000
Fax: 650-654-4233
URL: <http://www.checkpoint.com>

©2004-2005 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Express, the Check Point logo, ClusterXL, Cooperative Enforcement, ConnectControl, Connectra, CoSa, Cooperative Security Alliance, Eventia Analyzer, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, IMSecure, INSPECT, INSPECT XL, Integrity, InterSpect, IQ Engine, Open Security Extension, OPSEC, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureKnowledge, SecurePlatform, SecuRemote, SecureServer, SecureUpdate, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, Smarter Security, SmartDashboard, SmartDefense, SmartL.SM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, TrueVector, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 VSX, VPN-1 XL, Web Intelligence, ZoneAlarm, ZoneAlarm Pro, Zone Labs, and the Zone Labs logo, are trade-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. The products described in this document are protected by U.S. Patent No. 5,606,668, 5,835,726 and 6,496,935 and may be protected by other U.S. Patents, foreign patents, or pending applications.

February 8, 2005 P/N: 501695



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.