Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

White Paper

Check Point Application Intelligence

INTERNAL
WEB
PERIMETER
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

Introduction—application-driven attacks 4

Application Intelligence—defending against today’s threats 4

Network and transport layers: necessary foundation for Application Intelligence 8

Conclusion 9

List of attack prevention safeguards 10

EXECUTIVE SUMMARY

Since the popularization of the Internet in 1994, enterprise firewalls have proven an effective defense against security exploits aimed at the network and transport levels. Firewalls with a defined security policy—especially Check Point patented Stateful Inspection firewalls based on INSPECT™ technology, the most intelligent, adaptive inspection technology—defeat a full 90 percent of these attacks. However, 21st Century hackers do more than look for exposed vulnerabilities in the network and transport layers. Today, these technically talented rogues actively attack the application level. For example, crucial services like HTTP (TCP port 80), HTTPS (TCP port 443), RPC (Remote Procedure Calls), and NFS (Network Files Systems) have become primary targets of sophisticated schemes to manipulate applications.

To help network administrators deal with application-level attacks, Check Point security solutions with Application Intelligence™ technology provide a potent combination of attack safeguards and attack blocking tools. These safeguards and blocking tools protect the network's most valuable asset—actual user data. Specifically, Check Point security gateways offer Application Intelligence protections and SmartDefense™ Services to prevent and block attacks using mechanisms such as Validating Compliance to Standards, Validating Expected Usage of Protocols (Protocol Anomaly Detection), Limiting Application Ability to Carry Malicious Data, and Controlling Application-Layer Operations. These mechanisms aid proper usage of Internet resources such as Voice over Internet Protocol (VoIP), Instant Messaging, Peer-to-Peer (P2P) file sharing, Web site scripting, print-sharing operations, and File Transfer Protocol (FTP) uploading, among others.

In addition, Application Intelligence and SmartDefense Services continue to offer industry-leading protection against network- and transport-level attacks with strategies countering IP Fragmentation, Smurfing, Non-TCP Denial of Service (Non-TCP DOS), and Port Scans. Overall, Check Point gateways provide the most proven and comprehensive answer to quickly evolving hacker attacks aimed at the application, network, and transport levels, offering a truly multi-layer security solution.

INTRODUCTION—APPLICATION-DRIVEN ATTACKS

Firewalls have become the staple of network security architectures, primarily providing access control to network resources, and they have been successfully deployed in the large majority of networks. A major reason for firewall success is that when used to enforce a properly defined security policy, firewalls commonly defeat more than 90 percent of network attacks—a crucial element in providing networks with the reliability required in today's competitive environment. However, while most firewalls provide effective access control, many are not designed to detect and thwart attacks at the application level.

Recognizing this reality, hackers have devised sophisticated attacks designed to circumvent the traditional access control policies enforced by perimeter firewalls. Today’s knowledgeable hackers have advanced well past scanning for open ports on firewalls and are now directly targeting applications.

Some of the most serious threats in today’s Internet environment come from attacks that attempt to exploit known application vulnerabilities. Of particular interest to hackers are services such as HTTP (TCP port 80) and HTTPS (TCP port 443), which are commonly open in many networks. Access control devices cannot easily detect malicious exploits aimed at these services.

By targeting applications directly, hackers attempt to achieve at least one of several nefarious goals, including:

- Denial of Service to legitimate users (DoS attacks)
- Gaining administrator access to servers or clients
- Gaining access to back-end information databases
- Installing Trojan horse software that bypasses security and enables access to applications

Since application-driven attacks are sophisticated in nature, effective defenses must be equally sophisticated and intelligent. In order to address the increasing threat from application-driven attacks, firewalls must provide comprehensive security on multiple levels. These levels of security should protect against both network and application attacks, while providing robust access control to IT resources.

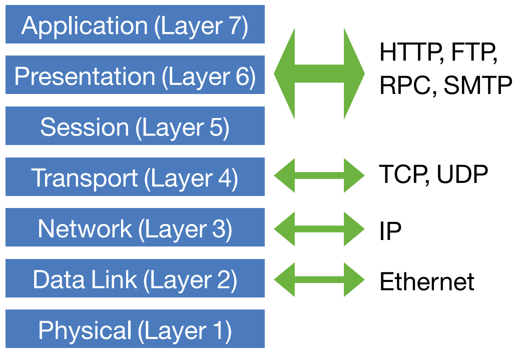
Check Point Application Intelligence™ is a set of advanced capabilities integrated into Check Point products that detect and prevent application-level attacks.

APPLICATION INTELLIGENCE—DEFENDING AGAINST TODAY’S THREATS

Many firewalls, particularly those based on Check Point patented Stateful Inspection technology, have maintained successful defense arsenals against network assaults. As a result, a growing number of attacks attempt to exploit vulnerabilities in network applications rather than target the firewall directly. This important shift in attack methodology requires that firewalls provide not only access control and network-level attack protection, but also understand application behavior to protect against application attacks and hazards. Based on INSPECT™, the industry’s most intelligent, adaptive inspection technology, Check Point Application Intelligence™ provides this expansive view of network security solutions.

APPLICATION LAYER SECURITY

Sample protocols



The OSI reference model is a framework, or guideline, for describing how data is transmitted between devices on a network. NOTE: The Application Layer is not the actual end-user software application, but a set of services that allows the software application to communicate via the network. Distinctions between layers 5, 6, and 7 are not always clear, and some competing models combine these layers, as does this paper.

OSI (Open Systems Interconnection) reference model

The application layer attracts numerous attacks for several reasons. First, it is the layer that contains a hacker's ultimate goal—actual user data. Second, the application layer supports many protocols (HTTP, CIFS, VoIP, SNMP, SMTP, SQL, FTP, DNS, etc.), so it houses numerous potential attack methods. And third, detecting and defending against attacks at the application layer is more difficult than at lower layers because more vulnerabilities arise in this layer.

In order to successfully provide application-layer security, a security solution must address the following four defense strategies.

1. Validate Compliance to Standards

Firewalls must be able to determine whether communications adhere to relevant protocol standards. Violation of standards may be indicative of malicious traffic. Any traffic not adhering to strict protocol or application standards must be closely scrutinized before it is permitted into the network, otherwise business-critical applications may be put at risk. Examples include:

- **Voice over IP (VoIP)**—VoIP traffic is typically supported using H.323, SIP and other protocols. The operation of these protocols can be complex, resulting in numerous communication ports supporting the establishment and maintenance of VoIP calls. Improper enforcement of these protocols can leave VoIP deployment vulnerable to the following hazards:
  - Call redirection—calls intended for the receiver are redirected
  - Stealing calls—the caller pretends to be someone else
  - DoS—preventing legitimate usage of VoIP

Security gateways must ensure that VoIP protocol commands fully conform to appropriate standards and RFCs and that packets are structurally valid and arrive in a valid sequence. In addition, firewalls should examine the contents of packets passing through every allowed port to ensure that they contain proper information.

- **Binary data in HTTP headers**—While the official HTTP standard prohibits binary characters in HTTP headers, the rule is ambiguous and not checked by most firewalls. As a result, many hackers launch attacks by including executable code in HTTP headers. All security gateways should allow for the blocking or flagging of binary characters in HTTP headers and requests.

2. Validate Expected Usage of Protocols (Protocol Anomaly Detection)

Testing for protocol compliance is important, but of equal importance is the capability to determine whether data within protocols adheres to expected usage. In other words, even if a communication stream complies with a protocol standard, the way in which the protocol is being used may be incongruous with what is expected. Examples include:

- **Use of HTTP for peer-to-peer (P2P) communications—**P2P is a communication model in which each party has the same capabilities and either party can initiate a communication session. P2P applications can be divided into two major categories:
  - Instant messaging (IM)—whose main goal is to enable direct online communication between people
  - File sharing networks—whose main goal is to share resources such as storage

  P2P communications often utilize TCP port 80, which is usually designated for HTTP traffic and is thus open for outgoing connections. While many proprietary P2P protocols exist, P2P communications often embed themselves within HTTP traffic. In these situations, firewalls that check only for protocol compliance will allow the P2P session (since the session is using standard HTTP). Because commonly expected usage of HTTP is for Web traffic, P2P communications embedded within HTTP traffic should be blocked or flagged by the firewall.

Many organizations want to block or limit P2P traffic for security, bandwidth, and legal reasons. Security issues arise because P2P communications are designed to allow file transfers, chat, games, voice, and email, while bypassing firewalls, virus checking, logging, and tracking. As a result, hackers can use P2P as an attack vector into networks. Security gateways should block unauthorized P2P traffic, or conversely, selectively allow authorized P2P traffic.

- **Directory traversal—**Directory traversal attacks allow a hacker to access files and directories that should be out of reach and can result in running undesired executable code on the Web server by trying to access unauthorized resources. Most of these attacks are based on the ".." notation within a file system. Firewalls should block requests in which the URL contains a directory request that complies with syntax, but does not comply with expected usage. For example, HTTP://www.server.com/first/second/../../.. should be blocked because it attempts to go deeper than the root directory.
- **Excessive HTTP header length—**The HTTP standard does not limit header length. However, excessive header length falls outside of normal or expected HTTP usage. Headers of excessive length should be blocked or flagged to reduce the chance of buffer overflows and to limit the size of code that can be inserted using the overflow.

3. Limit Applications' Ability to Carry Malicious Data

Even if application-layer communications adhere to protocols, they may still carry data that can potentially harm the system. Therefore, a security gateway must provide mechanisms to limit or control an application's ability to introduce potentially dangerous data or commands into the internal network.
Examples include:

- **Cross-Site Scripting attacks**—Scripts provide a common mechanism for launching attacks against an application. While most scripts are harmless, unsuspecting users can easily and inadvertently execute malicious scripts. These scripts can often be hidden in innocuous looking links or, for instance, disguised as an email card. A common example of malicious scripts appears in Cross-Site Scripting attacks (XSS). Cross-Site Scripting attacks exploit the trust relationship between a user and a Web site by employing specially crafted URLs. The intention of the attack is to steal cookies that contain user identities and credentials or to trick users into supplying their credentials to the attacker. Typically, a Cross-Site Scripting attack is launched by embedding scripts in an HTTP request that the user unwittingly sends to a trusted site. To protect Web servers, the security gateway should provide the capability to detect and block HTTP requests that contain threatening scripting code.
- **Limit or block potentially malicious URLs**—Malicious data can also enter the internal network by embedding itself in URLs. For example, an application such as an email client could automatically execute an HTML-embedded URL. If the URL was malicious, damage to the network or the user's system may occur. Access to potentially malicious URLs should be blocked or limited.
- **Detect and block attack signatures**—Security gateways should perform content filtering on all data streams to detect and block data patterns that are indicative of attacks, worms, etc.

4. Control Application-Layer Operations

Not only can application-layer communications introduce malicious data to a network, the application itself might perform unauthorized operations. A network security solution must have the ability to identify and control such operations by performing "access control" and "legitimate usage" checks. This level of security requires the capability to distinguish, at a granular level, application operations. Examples include:

- **Microsoft Networking Services**—A network security solution can implement security policy using many parameters from CIFS, the Microsoft-based Common Internet File System. CIFS supports, among other capabilities, file- and print-sharing operations. Using these operations as examples, a security gateway should have the capability to differentiate and block file-sharing operations originating from a user or system that does not have appropriate authorization. Conversely, print-sharing operations originating from the same user may be allowed and accepted. Providing a level of security with this granularity requires a thorough understanding of CIFS, as well as the ability to control application-layer protocol components.
- **FTP**—A firewall should place connection restrictions on particular file names and control potentially hazardous FTP commands like PUT, GET, SITE, REST, and MACB. For example, a security policy may require operational restrictions on all files containing the word "payroll."

NETWORK AND TRANSPORT LAYERS: NECESSARY FOUNDATION FOR APPLICATION INTELLIGENCE

Application Intelligence, in its purest form, associates itself with application-level defenses. However, in practice many attacks aimed at network applications actually target the network and transport layers. Hackers target these lower layers as a means to access the application layer, and ultimately the application and data itself. Also, by targeting lower layers, attacks can interrupt or deny service to legitimate users and applications (e.g., DoS attacks). For these reasons, Application Intelligence and other network security solutions must address not only the application layer but also network and transport layers.

NETWORK LAYER SECURITY

Preventing malicious manipulation of network-layer protocols (e.g., IP, ICMP) is a crucial requirement for multi-level security gateways. The most common vehicle for attacks against the network layer is the Internet Protocol (IP), whose set of services resides within this layer. While many network-layer hazards and attacks exist, some examples include:

- **IP Fragmentation**—IP fragmentation can be used to deliver and disguise attacks in order to avoid detection. This technique utilizes the resilience mechanisms inherent in the IP protocol itself (RFC 791 and RFC 815) to intentionally fragment attacks into multiple IP packets so they can circumvent firewalls that do not perform IP fragment reassembly. IP fragmentation can also be used to launch a DoS attack by inundating IP fragment reassembly devices with incomplete fragment sequences.
- **Smurfing (Smurf attack)**—ICMP allows one network node to ping, or send an echo request to, other network nodes to determine their operational status. This capability can be used to perpetrate a "Smurf" DoS attack. The Smurf attack is possible because standard ICMP does not match requests to responses. Therefore, an attacker can send a ping with a spoofed source IP address to an IP broadcast address. The IP broadcast address reaches all IP addresses in a given network. All machines within the pinged network send echo replies to the spoofed, and innocent, IP source. Too many pings and responses can flood the spoofed network and deny access for legitimate traffic. This type of attack can be blocked by dropping replies that don't match requests, as performed by Check Point's Stateful ICMP.

TRANSPORT LAYER SECURITY

As with the network layer, the transport layer and its common protocols (TCP, UDP) provide popular access points for attacks on applications and their data. Examples of transport layer attacks and threats include:

- **Non-TCP DoS**—Non-TCP (e.g., UDP and ICMP) DoS attacks can completely overwhelm mission-critical applications—such as SMTP, HTTP, FTP, etc., which use TCP traffic. Firewalls can protect against these threats by reserving a dedicated portion of the state table for TCP connections. If non-TCP connections attempt to utilize too many resources, TCP connections will be unaffected because they are handled by reserved or dedicated system resources.
- **Port Scan**—A port scan does what the name implies: a hacker scans a range of ports on a target host in hopes of identifying and exploiting weaknesses on running applications. The reconnaissance that a port scan performs is a hazard that can lead to an attack. A security gateway must be able to raise alerts and block or shutdown communications from the source of the scan.

CONCLUSION

Firewalls have established themselves as the staple of network security infrastructures based on their ability to block attacks at the network level. As a result of firewall success, hackers have developed more sophisticated attack methodologies. The new breed of attacks directly targets applications, often attempting to exploit vulnerabilities inherent in the applications themselves or in the underlying communication protocols. Providing security on multiple levels is required to safeguard corporate networks from these threats. Additionally, multi-level security solutions must protect against both network and application-layer attacks, while providing access control to IT resources.

Check Point Application Intelligence, based on INSPECT, is a set of advanced capabilities integrated into Check Point products that detect and prevent application-level attacks. Check Point solutions provide the industry’s most proven and comprehensive answer to the increasing number of attacks directed at critical applications.

Check Point Multi-Layer Security:

Attack Prevention Safeguards and Attacks Blocked

Check Point gateways, including VPN-1, FireWall-1, InterSpect, and Connectra, with SmartDefense, Application Intelligence, and Web Intelligence protection enabled block many attacks and provide numerous attack prevention safeguards. This table lists some of these defenses and organizes them by protocol and OSI model layer.

Note: Check Point continually expands the breadth of defenses provided. This table is a snapshot, not an exhaustive list. Some of the defenses listed under “Attack Prevention Safeguards” are available with SmartDefense updates (through purchase of additional SmartDefense Services). These updates provide additional safeguards to the ones listed in the table. List is current as of April 26, 2005.

Application Layer/Presentation Layer	Session Layer	Transport Layer	Network Layers

APPLICATION LAYER/PRESENTATION LAYER

	Attack Prevention Safeguards	Attacks Blocked
HTTP Client (browser and other client machine components)	• Limit maximum response header length • Prohibit binary characters in HTTP response headers • Validate HTTP response protocol compliance • Block user-defined URLs • URL filtering • Restrict download of user-defined files • Restrict peer-to-peer (P2P) connections • Restrict P2P connections for non-HTTP ports • Block Java code • Strip script tags • Strip applet tags • Strip FTP links • Strip port strings • Strip ActiveX tags	• Code Red worm and mutations • Nimda worm and mutations • HTR Overflow worm and mutations • MDAC Buffer Overflow and mutations • Malicious URLs • User-defined worm and mutations • Cross-Site Scripting attacks
HTTP Server	• Limit maximum URL length • Limit maximum number of response headers allowed • Limit maximum request header length • Limit maximum response header length • Reject HTTP headers that contain specific header names or values • Prohibit binary characters in HTTP response headers • Prohibit binary characters in HTTP requests • Block user-defined URLs • Enforce HTTP security on nonstandard ports (ports other than 80) • Compare transmission to user-approved SOAP scheme/template • Restrict download of user-defined files • ASN.1 buffer overflow • Restrict non-RFC HTTP methods	• Encoding attacks • User-defined worm and mutations • Code Red worm and mutations • Nimda worm and mutations • HTR Overflow worm and mutations • Directory Traversal attacks • MDAC Buffer Overflow and mutations • Malicious URLs • Chunked Transfer Encoding attacks • Cross-Site Scripting attacks • HTTP-based attacks spanning multiple packets • WebDAV attacks • PCT worm and mutations • HTTP header spoofing attacks • IIS Server Buffer Overflow • Santy worm and mutations • Spyware and Adware attacks • LDAP injection attacks

Application Layer/Presentation Layer	Session Layer	Transport Layer	Network Layers

APPLICATION LAYER/PRESENTATION LAYER

	Attack Prevention Safeguards	Attacks Blocked
HTTP Server	• ASN.1 buffer overflow • Restrict non-RFC HTTP methods • Distinguish between different HTTP v1.1 requests over same connection • Restrict unsafe HTTP commands • Fingerprint scrambling (spoofing) to hide server information • SOAP scheme validation • SSL overflow attacks • SSL v3 version enforcement • Restrict header values • Malicious Code Protector (prohibit malicious executable code against Web servers) • SQL Injection • Command Injection • Restrict binary data in forms • Restrict HTTP methods • Block HTTP traffic featuring negative content-length HTTP headers • Block Trojans by identifying attempts to receive script traffic containing HTML tags • Block content disposition in HTTP header • Define specific network objects as Web servers • Perform strict HTTP protocol enforcement • Reject HTTP requests that contain illegal SWAT header • Strip files extensions in Web traffic • Block network access to files with certain extensions (to prevent worm infection) • Block HTML tags from HTTP request header • Block shell commands from HTTP request header • Block HTTP requests containing scripting code using POST command • Block non-ASCII characters in HTTP request/response header	• Code Red worm and mutations • Nimda worm and mutations • HTR Overflow worm and mutations • MDAC Buffer Overflow and mutations • Malicious URLs • User-defined worm and mutations • Cross-Site Scripting attacks
SMTP	• Block multiple “content-type” headers • Block multiple “encoding headers” • Camouflage default banner • Restrict unsafe SMTP commands • Header forwarding verification • Restrict unknown encoding • Restrict mail messages not containing sender/recipient domain name • Restrict MIME attachments of specified type • Strip file attachments with specified names • Strict enforcement of RFC 821 and 822 • Monitor and enforce restrictions on ESMTP commands • Hide internal mail user names and addresses • Perform reverse DNS lookup	• SMTP Mail Flooding • SMTP worm and mutations • Extended Relay attacks • Message/Partial MIME attack • Spam attack (large number of emails) • Command Verification attack • SMTP Payload worm and mutations • Worm Encoding • Firewall Traversal attack • SMTP Error Denial-of-Service (DoS) attack • Mailbox DoS (excessive email size) • Address Spoofing • SMTP Buffer Overflow attacks

Application Layer/Presentation Layer | Session Layer | Transport Layer | Network Layers

APPLICATION LAYER/PRESENTATION LAYER

	Attack Prevention Safeguards	Attacks Blocked
SMTP	• Strict enforcement of MAIL and RCPT syntax • Restrict mail from user-defined sender or domain • Restrict mail to user-defined recipients • Restrict mail to unknown domains • Enforce limits on the number of RCPT commands allowed per transaction • Restrict mail relay usage • Enforce ASN.1 standard • Strip script tags • Strip ActiveX tags • Block malicious filenames • Block the X-LINK2STATE SMTP extended verb	• MyDoom worm and mutations • Bagle worm and mutations • Sober worm and mutations • Zafi worm and mutations • Bagz.C worm and mutations
POP3	• Restrict connection with passwords identical to user name • Enforce maximum character limit for user names (buffer overflow protection) • Enforce maximum password length (buffer overflow protection) • Restrict binary characters in user name (buffer overflow protection) • Restrict binary characters in passwords (buffer overflow protection) • Restrict binary characters in POP3 commands (buffer overflow protection) • Limit number of NOOP commands, freeing POP3 daemon resources (DoS protection)	• POP3 Buffer Overflow attacks
IMAP4	• Restrict connection with passwords identical to user name • Enforce maximum character limit for user names (buffer overflow protection) • Enforce maximum password length (buffer overflow protection) • Restrict binary characters in user name (buffer overflow protection) • Restrict binary characters in passwords (buffer overflow protection) • Restrict binary characters in POP3 commands (buffer overflow protection) • Limit number of NOOP commands, freeing POP3 daemon resources (DoS protection)	• IMAP4 Buffer Overflow attacks
RSH	• Auxiliary port monitoring • Restrict reverse injection	
RTSP	• Auxiliary port monitoring	
IIOP	• Auxiliary port monitoring	
FTP	• Analyze and restrict hazardous FTP commands • Block custom file types • Camouflage default banner • Strip FTP references • Restrict non-RFC FTP methods	• FTP Bounce attack • Passive FTP attacks • Client and Server Bounce attacks • FTP Port Injection attacks • Directory Traversal attack • Firewall Traversal attack • TCP Segmentation attack

Application Layer/Presentation Layer	Session Layer	Transport Layer	Network Layers

APPLICATION LAYER/PRESENTATION LAYER

	Attack Prevention Safeguards	Attacks Blocked
DNS	• Restrict DNS zone transfers • Restrict usage of DNS server as a public server • Provide separate DNS service for private vs. public domains • Enforce DNS over TCP protocol • Restrict domains on “not allowed” list • Provide cache protection • Restrict inbound requests • Restrict mismatched replies • Enforce DNS query format • Enforce DNS response format • Set maximum values for Answer, Authority, and Additional Resource Records allowed in reply for a DNS query over TCP	• Protect against DNS Cache positioning attacks • DNS Query Malformed Packet attacks • DNS Answer Malformed Packet attacks • DNS Query-Length Buffer Overflow • DNS Query Buffer overflow–Unknown Request/Response • Man-in-the-Middle attacks
Microsoft Networking	• CIFS filename filtering (protect against worms utilizing CIFS protocol) • Restrict remote access to registry • Restrict remote null sessions • Restrict popup messages • Enforce ASN.1 standards • Reject invalid headers by type of service • Restrict file extensions in email messages and Web traffic • HTTP filename filtering (protect against worms utilizing HTTP protocol) • Restrict specially crafted packets • Restrict insufficient name validation • Block long CIFS passwords	• Bugbear worm • Nimda worm • Liotan worm • Sasser worm • Opaserv worm • SQUID NTLM Authentication Buffer Overflow attack—HTTP Header Filter attack • MS05-003 Indexing Service • MS05-010 License Logging Service
SSH	• Enforce SSH v2 protocol	• SSH v1 Buffer Overflow attacks
SNMP	• Restrict SNMP get/put commands • Restrict known dangerous communities • Enforce or require SNMPv3 protocol	• SNMP Flooding attacks • Default Community attacks • Brute Force attacks • SNMP Put attacks
MS SQL	• Block remote command execution • Restrict potentially dangerous commands (Information Leakage) • Restrict usage of default system administrator password • Enforce Windows authentication • Perform sanity checks on SQL login packet	• SQL Resolver Buffer Overflow attacks • SQL Slammer worm • Buffer Overflow (various attack variations) • MS SQL networking DoS (various DoS attack variations) • Heap Overflow attacks
Oracle SQL	• Verify dynamic port allocation and initiation	• SQLNet v2 Man-in-the-Middle attacks
SSL	• Enforce SSL V3 protocol	• SSL V2 Buffer Overflow
H.323	• Verify protocol fields and values • Identification and restriction of the PORT command • Enforce existence of mandatory fields • Enforce user registration	• Buffer Overflow attacks • Man-in-the-Middle attacks

APPLICATION LAYER/PRESENTATION LAYER

	Attack Prevention Safeguards	Attacks Blocked
H.323	• Prevent VoIP firewall holes • Disable H.323 audio and video transmissions • Enforce H.323 call duration limits • For H.323, allow only traffic associated with a specific call • For H.323, restrict blank source in calls	
MGCP	• Verify protocol fields and values • Identification and restriction of the PORT command • Enforce existence of mandatory fields • Enforce user registration • Prevent VoIP firewall holes • Enforce MGCP protocol • Verify state of MGCP commands • Restrict unknown and unsafe MGCP commands	• Buffer Overflow attacks • Man-in-the-Middle attacks
SCCP (Cisco Skinny VoIP)	• Enforce SCCP protocol • Secure SCCP dynamic ports • Verify state of SCCP commands • Verify protocol fields and values • Identification and restriction of the PORT command • Enforce existence of mandatory fields • Enforce user registration • Prevent VoIP firewall holes	• Buffer Overflow attacks • Man-in-the-Middle attacks
SIP	• Limit number of invite commands (DoS protection) • Restrict SIP-based instant messaging • Verify protocol fields and values • Identification and restriction of the PORT command • Enforce existence of mandatory fields • Enforce user registration • Prevent VoIP firewall holes • Restrict MSN Messenger file transfers • Restrict MSN Messenger application sharing • Restrict MSN Messenger whiteboard sharing • Restrict MSN Messenger remote assistance	• Buffer Overflow attacks • Man-in-the-Middle attacks
X11	• Restrict reverse injection • Block special clients	
DHCP	• Perform Strict DHCP options enforcement • Restrict BOOTP clients • Restrict non-Ethernet DHCP clients	
Peer-to-Peer	• Restrict IRC protocol on all TCP high ports • Restrict P2P connections • Restrict P2P connections on non-HTTP ports	
SOCKS	• Restrict SOCKS versions other than Version 5 • Restrict unauthenticated SOCKS connections	

Application Layer/Presentation Layer	Session Layer	Transport Layer	Network Layers

APPLICATION LAYER/PRESENTATION LAYER

	Attack Prevention Safeguards	Attacks Blocked
Routing Protocols	• Enforce MD5 routing authentication on various routing protocols (OSPF, BGP, RIP) • Enforce the validity of IGMP packets	
Content Protection	• Block malformed JPEG • Block malformed ANI file • Block malformed GIF	
Instant Messengers	• Restrict invalid MSN Messenger over MSNMS patterns (prevent worm infection) • Restrict file transfer in Instant Messages via MSN/Windows Messenger • Restrict the MSN_Messenger group	• Bropia.E worm • Kelvir.B worm
Remote Control Applications	• Restrict VNC connections on VNC and other ports • Restrict Remote Administrator connection attempts made on Remote Administrator well-known port and on other ports • Enforce authentication scheme on Radmin connections	

Check Point gateways, including VPN-1, FireWall-1, InterSpect, and Connectra, with SmartDefense, Application Intelligence, and Web Intelligence protection enabled block many attacks and provide numerous attack prevention safeguards. This table lists some of these defenses and organizes them by protocol and OSI model layer.

Note: Check Point continually expands the breadth of defenses provided. This table is a snapshot, not an exhaustive list. Some of the defenses listed under “Attack Prevention Safeguards” are available with SmartDefense updates (through purchase of additional SmartDefense Services). These updates provide additional safeguards to the ones listed in the table. List is current as of April 26, 2005.

Application Layer/Presentation Layer	Session Layer	Transport Layer	Network Layers

SESSION LAYER

	Attack Prevention Safeguards	Attacks Blocked
RPC	• Block RPC portmapper exploits	• ToolTalk attacks • snmpXdmid attacks • rstat attacks • mountd attacks • cmsd attacks • cachefsd attacks
DEC-RPC	• Block DCE-RPC portmapper exploits • Allow endpoint mapper communications via EPM port only • Allow only authenticated DCOM	• Blaster • Sasser
SUN-RPC	• Block SUN-RPC interface scanning • Enforce RPC protocol and packet lengths	
HTTP Proxy	• HTTP Proxy enforcement: Enforce HTTP session logic in proxy mode	
VPN	• Validate digital certificates used against Certificate Revocation List • Monitor for preshared secrets vulnerability	• IKE Brute Force attacks • Hub-and-Spoke Topology attacks • IKE UDP DoS attacks • Windows 2000 IKE DoS attacks • VPN IP Spoofing attacks • VPN Man-in-the-Middle attacks • IKE Aggressive Mode attacks
SSL	• Protect against SSL Null Pointer	• Microsoft PCT

Check Point gateways, including VPN-1, FireWall-1, InterSpect, and Connectra, with SmartDefense, Application Intelligence, and Web Intelligence protection enabled block many attacks and provide numerous attack prevention safeguards. This table lists some of these defenses and organizes them by protocol and OSI model layer.

Note: Check Point continually expands the breadth of defenses provided. This table is a snapshot, not an exhaustive list. Some of the defenses listed under "Attack Prevention Safeguards" are available with SmartDefense updates (through purchase of additional SmartDefense Services). These updates provide additional safeguards to the ones listed in the table. List is current as of April 26, 2005.

Application Layer/Presentation Layer	Session Layer	Transport Layer	Network Layers

TRANSPORT LAYER

	Attack Prevention Safeguards	Attacks Blocked
TCP	• Enforce correct usage of TCP flags • Limit per-source sessions • Enforce minimum TCP header length • Block unknown protocols • Restrict FIN packets with no ACK • Enforce that TCP header length is as indicated in the header and not longer than the packet size indicated by the header • Block out-of-state packets • Verify that first connection packet is SYN • Enforce three-way handshake between SYN and SYN-ACK, client can send only RST or SYN • Enforce three-way handshake between SYN and connection establishment, server can send only SYN-ACK or RST • Block SYN on established connection before FIN or RST packet is encountered • Restrict server-to-client packets belonging to old connections • Drop server-to-client packets belonging to old connections if packets contain SYN or RST • Enforce minimum TCP header length • Block TCP fragments • Block SYN fragments • Scramble OS fingerprint • Verify TCP packet sequence number for packets belonging to an existing session • Enforce TCP session sequence verification (protect persistent unauthenticated network sessions) • Network quota–enforce a limit upon the number of connections that are allowed from the same source IP to protect against DoS attacks • Anomaly detection–used ports • Drop ICMP error packets that belong to established TCP connections	• ACK DoS attacks • SYN attacks • Land attacks • Tear Drop attacks • Session Hijacking attacks • Jolt attacks • Bloop attacks • Cpd attacks • Targa attacks • Twinge attacks • Small PMTU attacks • Session Hijacking attacks (TCP sequence number manipulation) • TCP-based attacks spanning multiple packets • XMAS attacks • Port Scan • Witty worm • Cisco IOS DoS
UDP	• Verify UDP length field • Match UDP requests and responses • Non-TCP flooding–limit percentage of non-TCP connections to prevent DoS	• Port Scan

Check Point gateways, including VPN-1, FireWall-1, InterSpect, and Connectra, with SmartDefense, Application Intelligence, and Web Intelligence protection enabled block many attacks and provide numerous attack prevention safeguards. This table lists some of these defenses and organizes them by protocol and OSI model layer.

Note: Check Point continually expands the breadth of defenses provided. This table is a snapshot, not an exhaustive list. Some of the defenses listed under “Attack Prevention Safeguards” are available with SmartDefense updates (through purchase of additional SmartDefense Services). These updates provide additional safeguards to the ones listed in the table. List is current as of April 26, 2005.

Application Layer/Presentation Layer	Session Layer	Transport Layer	Network Layers

NETWORK LAYER

	Attack Prevention Safeguards	Attacks Blocked
IP	• Enforce minimum header length • Restrict IP-UDP fragmentation • Enforce the header length indicated in the IP header is not longer than the packet size indicated by the header • Enforce the packet size indicated in the IP header is not longer than the actual packet size • Scramble OS fingerprint • Control IP options	• IP Address Sweep Scan • IP Timestamp attacks • IP Record Route attacks • IP Source Route attacks • IP Fragment DoS attacks • Loose Source Route attacks • Strict Source Route attacks • IP Spoofing attacks
ICMP	• Block large ICMP packets • Restrict ICMP fragments • Match ICMP requests and responses	• Ping-of-Death attacks • ICMP Flood

ABOUT CHECK POINT SOFTWARE TECHNOLOGIES

Check Point Software Technologies (www.checkpoint.com) is the worldwide leader in securing the Internet. It is the confirmed 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 Zone Labs (www.zonelabs.com) division 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 more than 350 leading companies. Check Point solutions are sold, integrated, and serviced by a network of more than 2,300 Check Point partners in 92 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**

February 22, 2006 P/N 502083

Check Point®
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.