



Dear

CHECK POINT CUSTOMER

TABLE OF CONTENTS

- 1 Letter to Our Customers
- 2 OPSEC Alliance
- 3 DHL Protects Critical Information Resources with FireWall-1
- 4 IBM Resells FireWall-1
- 4 ISPs Rely on FireWall-1
- 5 Xylan Embeds FireWall-1 Engine
- 5 Reference Desk
- 6 ConnectControl Module
- 7 Tech Tips
- 8 Calendar

On behalf of Check Point Software Technologies, I would like to welcome you to the inaugural issue of *Check Point Connections*, our new quarterly customer newsletter. As the name implies, this newsletter is intended to keep you, our valued customer, "connected" with Check Point and our products. Each issue will contain product feature highlights, overviews of key products and partnerships recently announced by Check Point, technical tips from our outstanding technical team, and updates on network security issues and references to keep you on top of the latest fast-moving network security market.



The theme of this issue of Check Point Connections is OPSEC, Check Point's Open Platform for Secure Enterprise Connectivity. OPSEC is Check Point's answer to the evolving network security requirements of today's enterprise, one in which Internet, intranet and extranet computing are critical to the lifeblood of the corporation. With the explosion and rapid acceptance of the Internet, the physical corporate boundaries that previously defined and governed corporate networks are irrelevant and obsolete. A new paradigm has evolved, pioneered in part by Check Point, whereby corporate networks are being defined by enterprise-wide security policies. To be effective, these policies must include a broad range of security services that govern access to network information resources and protect the privacy and integrity of network communications, including access control, validation of authorized network users, protection of data privacy, anti-virus scanning, URL filtering, protection against malicious Java and ActiveX applets...the list is virtually endless.

And because enterprise-wide networking means connectivity to anyone, anywhere, internal or external to the corporate network, a security policy must also be enterprise-wide, providing policy-based management for an organization's worldwide offices, remote and mobile users, business partners and customers. This is the OPSEC vision.

Since its initial unveiling in late 1996, OPSEC has been endorsed by more than 80 leaders in network security and the general computer and software industries, including 3Com Corporation, Bay Networks, Hewlett-Packard, IBM, Netscape, Oracle, RSA Data Security, and Security Dynamics. Through OPSEC and our expanding partnerships within the OPSEC Alliance (see article on page 2), Check Point will be able to broaden the range of security functions supported through its integrated management console to meet your evolving requirements.

The essence of the OPSEC architecture is to provide a single platform which integrates and manages all aspects of network security through an open, extensible management framework. Third-party security applications can plug into the OPSEC framework through open, published APIs, industry-standard protocols, as well as INSPECT, Check Point's high-level scripting language. As a result of this architecture, you can easily and seamlessly integrate a customized set of security components to best meet your requirements and later add new security modules as needed. With OPSEC, all facets of network security are defined and driven by a single enterprise-wide security policy.

Yours Truly,

Juniper Ex 1035 p 1

OPSEC ALLIANCE

In support of OPSEC (Open Platform for Secure Enterprise Connectivity), Check Point's emerging industry standard for enterprise security, over 80 industry leaders have joined Check Point's OPSEC Alliance, an open industry-wide initiative. The OPSEC Alliance is dedicated to providing enterprise security solutions and designed to ensure interoperability between best-of-class, leading edge security products at the policy level. It is open to all vendors providing the technology building blocks for enterprise security solutions.

The industry's only open enterprise security platform enabling the integration and management of broad range of enterprise network security technologies through a single, enterprise-wide security policy, the OPSEC Alliance provides Check Point customers a comprehensive set of security components from which to select and easily integrate products already implemented within the corporation.

All OPSEC Alliance partners have use of the "OPSEC Alliance" logo, indicating that their products can plug into the OPSEC framework. Additionally, OPSEC Alliance partners can elect to have their products certified by Check Point, providing a measure of interoperability assurance for customers. Products passing this interoperability testing will receive the "OPSEC Certified" designation and logo from Check Point to clearly designate these certified products.

OPSEC Alliance Partners are divided into three categories: Infrastructure, Framework and Passport. Infrastructure Partners embed or bundle Check Point FireWall-1 with their products delivered to their customer base. Framework Partners are developing or have developed complementary value-added products that can be certified as compatible with Check Point's OPSEC protocols and APIs. Passport Partners are application development vendors that ensure secure computing over the Internet via application compatibility with



OPSEC Alliance Program members to-date include:

INFRASTRUCTURE PARTNERS

AST Research	3Com Corporation
Bay Networks	FTP Software, Inc.
Hewlett-Packard Company	IBM Corporation
Ipsilon Networks, Inc.	NCR
TimeStep Corporation	U.S. Robotics
Sun Microsystems, Inc.	Xylan Corporation

FRAMEWORK PARTNERS

Content Security

ASAP Ltd.	Computer Associates/
Command Software Systems, Inc.	Cheyenne Software
DataFellows	Digitivity, Inc.
Dr. Solomon's Software	EliShim, Inc.
Finjan Software	Integralis, Inc.
McAfee Associates	Security-7 Ltd.
NetPartners Internet Solutions, Inc.	Symantec Corporation

Authentication and Authorization

Axent Technologies, Inc.	ActivCard, Inc.
Blockade Systems Corp.	CryptoCard
Funk Software	MEMCO Software
NeTegrity, Inc.	Secure Computing Corp.
Security Dynamics	Vasco Data Security, Inc.

Encryption

RSA Data Security

Router Security Management

3Com Corporation	Bay Networks, Inc.
------------------	--------------------

Intrusion Detection

AbirNet	Haystack Labs, Inc.
Internet Security Systems	Netect

Event Analysis & Reporting

Accrue Software, Inc.	Bellcore
BGS Systems, Inc.	Kaspia Systems
SecureIT, Inc.	Sequel Technology Corp.
TELEMATE Software, Inc.	

Event Integration

Hewlett-Packard Company	Stonesoft
The Qualix Group, Inc.	

PASSPORT PARTNERS

BackWeb Technologies	BMC Software, Inc.
Campbell Services, Inc.	Citrix; Connected Corp.
e-motion, Inc.	FreeTel Communications
Gradient	Informix Software
InfoData Systems, Inc.	Intel Corporation
Liquid Audio, Inc.	Microsoft Corporation
Netscape Communications Corp.	OnLive! Technologies
Oracle Corporation	OutReach Technologies, Inc.
PointCast, Inc.	PictureTel Corporation
Progressive Networks, Inc.	Starlight Networks
Sybase, Inc.	VDOnet Corporation
VocalTec	Vosaic
Voxware, Inc.	Vxtreme, Inc.
White Pine Software, Inc.	Xing Technology Corp.

To stay current on OPSEC-compliant products and for assistance in building your enterprise security solution, visit the OPSEC Alliance Solutions Center at www.checkpoint.com

DHL PROTECTS CRITICAL INFORMATION RESOURCES WITH FIREWALL-1

In today's competitive international package delivery business, only tracking information moves faster than documents and packages: where a package may take two to three days to reach its destination, tracking data associated with the package must span the globe in minutes in order to meet customer need and demand for this information.

"Tracking information is a critical element in our business because customers want to know where their packages are almost as soon as the courier picks them up," explains Vanessa Lea, Gateway and Internet Services Manager at DHL Systems, Inc. "If we don't have this data available when customers need it, we simply will not be able to compete in the global marketplace."

DHL Systems, a technology service company for the DHL Worldwide Express organization, is charged with providing global network services to the entire enterprise, the world's largest and most experienced international air express network, linking more than 825,000 destinations in more than 225 countries.

DHL Systems realized the potential importance of electronic communications in achieving the company's information needs back in 1988 when they installed their first Internet connection to expedite e-mail communications with customers and suppliers. "As e-mail and Internet usage caught on," says Johan van Reijendam, Senior Network Engineer, "we soon recognized that if we were going to put any value on these services then we would have to protect our investments with a firewall as a precautionary measure."

Accordingly, in 1994, DHL Systems implemented the first DHL firewall, using FireWall-1 from Check Point Software Technologies Ltd., on a Sun SPARC-2 server. "FireWall-1 was selected," Lea says, "because it met our security needs, was straightforward to implement, and features an easy to

use graphical user interface that streamlines maintenance activities."

In 1996, that firewall was upgraded to



FireWall-1 Version 2.1 running on a Sun Solaris platform to meet the increased security requirements associated with the launch of a new application that empowers customers to track their own packages from the DHL Web site (www.dhl.com). "By simply entering a package tracking number, this Web-based application accesses our database hidden from the customer by the firewall and reports back through the firewall with the package status," van Reijendam explains. "We stayed with the Check Point firewall for this new application because of its proven track record in our network as well as the fact that it operates between the second and third OSI (Open Systems Interconnect) layer. As a result, there is no way for data or traffic to circumvent the firewall."

DHL currently has FireWall-1 installed at both of their Web servers, one in Burlingame, California, the other in London, England. "With this configuration," Lea adds, "we can effectively eliminate over-loading that otherwise might occur at either site at any given time. Furthermore, with replicated sites and firewalls distributed on either side of the Atlantic, we have a high degree of both security and disaster protection: should an earthquake ever impact our California facility, for example, London stands ready with its own FireWall-1 to carry on." ♦



IBM OEMS FIREWALL-1

Adding to Check Point Software Technologies' strong list of OEM partners, the company recently announced an agreement with IBM Corporation to OEM the Check Point FireWall-1 enterprise security solution. As part of the agreement, Check Point also announced FireWall-1 for IBM's RS/6000 server family running the AIX operating system.


FireWall-1 for AIX will be available in the third quarter of 1997 from IBM and its authorized resellers, both as a stand-alone software product and as part of an RS/6000 Internet POWERsolution, ready-to-run Web server systems. The product will also be available through Check Point authorized distributors and resellers. ♦

IBM is reselling FireWall-1 as part of its Internet POWERsolutions and as a stand-alone product.



The addition of FireWall-1 for AIX makes Check Point the only network security software vendor to support all major commercial server platforms, including Sun Solaris, HP-UX, Microsoft Windows NT and IBM AIX-based systems.

ISPs RELY ON FIREWALL-1

FireWall-1  The proliferation of intranets and extranets in corporations has brought with it the need to secure these networks from unwanted intruders and unauthorized users. Many companies are choosing to outsource not only the design and management of their intranets and extranets, but also the security component that goes hand-in-hand with these networks. Internet Service Providers worldwide are responding to this demand with comprehensive managed service offerings for their business customers. Check Point FireWall-1 has become the preferred solution among ISPs for the network security component of the majority of managed service offerings available today.

Two of the most recent ISPs to select FireWall-1 for their managed service offerings are MCI and UUNET, who together comprise a majority of the total ISP market. As part of their recent announcement of networkMCI Intranet Builder and networkMCI Intranet Complete, MCI announced that it is using FireWall-1 for the managed firewall component of their networkMCI Intranet Services. MCI will provide both on-site and complete, fully-managed end-to-end solutions to its corporate customers using FireWall-1. Services offered include installation, supervision, technical management and firewall support.

UUNET, the world's largest ISP, is integrating FireWall-1 into its ExtraLink secure virtual private network offering including ExtraLink Remote, which provides integrated remote dial-in capability over the Internet using UUNET's dial-up infrastructure. UUNET is incorporating FireWall-1 SecuRemote, Check Point's client encryption software, to provide secure

- WORLDWIDE ISPS INCLUDE:**
- Concentric Networks
 - Digex
 - CompuServe Network Services
 - EUNet Deutschland (Germany)
 - Genuity
 - Hitachi
 - Netrex
 - NTT PC (Japan)
 - Quza (UK)
 - Telenor Bedrift AS (Norway)
 - UUNET
 - UUNET Pipex (UK)
 - U S West
 - WIITel

CHECK POINT SOFTWARE TECHNOLOGIES LTD.

Xylan SWITCHES SECURELY WITH FIREWALL-1

Xylan Corporation has partnered with Check Point Software Technologies to integrate IP firewalls into the OmniSwitch and PizzaSwitch. Xylan already offers the industry's most sophisticated switching solutions, combining integrated routing, VLANs and LAN/ATM networking in a single chassis. By adding IP firewalls to these powerful products, Xylan now offers customers an integrated secure connectivity solution.

Customers can now integrate IP firewalls into their new or existing OmniSwitches and PizzaSwitches to secure the perimeter of their networks from malicious attacks as well as from access by unauthorized external users. The same firewall capability can also be used to safeguard internal resources from unauthorized access. IP firewalls are ideal for controlling traffic between VLANs, giving only authorized users access across VLAN boundaries. In particular, a firewall can serve as a security barrier in front of servers, mainframes and other sensitive resources.

Enterprise-wide Security. Xylan's firewalls provide an enterprise-wide security solution that organizations can integrate into the OmniSwitches and into the PizzaSwitches in use at their remote offices and campus networks. Instead of dedicating one piece of hardware for wide area connectivity, another for switching and a third for firewalls, an organization can integrate all of these features into a Xylan switch and use it as an integrated security solution wherever it is deployed. It is a simple, yet powerful solution that can be used at remote offices or at the core of a large network.

Most importantly, the firewall capabilities built into the OmniSwitch and PizzaSwitch can be managed from the

same, central Check Point enterprise management console that customers use to manage their FireWall-1 installations on UNIX or Windows NT servers, or the other router and switch platforms in which the FireWall-1 engine is embedded.



Firewalls Between VLANs. Switching alone creates flat networks that do not allow networks to scale to hundreds or thousands of users. VLANs allow large, switched networks to scale and fit their organization's needs by carving broadcast domains out of the network. Xylan has created the most advanced VLAN architecture in the internet-working industry, giving administrators a wide variety of criteria on which to base their virtual LANs.

Inter-VLAN communications requires the routing function to take place somewhere within the network. Xylan has integrated the routing function to the OmniSwitch and PizzaSwitch for inter-VLAN communication. Administrators can use firewalls to control access to VLANs that contain sensitive resources and information. By adding firewall capabilities into the OmniSwitch and PizzaSwitch, administrators can secure resources within their networks and protect their network from unwelcomed users. Administrators can define the access levels of users by the applications used and by VLAN membership. ♦

—Antoine Gaessler, Director of Channels Marketing
Check Point Software Technologies, Inc.

Reference DESK

GENERAL SECURITY RESOURCES:

- [Great Circle Associates](http://www.greatcircle.com)
<http://www.greatcircle.com>
- [Computer Emergency Response Team \(CERT\)](http://www.cert.org)
<http://www.cert.org>
- [Computer Incident Advisory Capability \(CIAC\)](http://ciac.llnl.gov)
<http://ciac.llnl.gov>
- [National Institute of Standards and Technology](http://www.nist.gov)

JAVA SECURITY RESOURCES:

- [JavaSoft FAQ on Security](http://www.javasoft.com/sfaq/index.html)
<http://www.javasoft.com/sfaq/index.html>
- [Official Directory for Java](http://www.gamelan.com)
<http://www.gamelan.com>

ACTIVE X SECURITY RESOURCES:

- [The Unofficial Active X Guide](http://www.shorrock.u-net.com/netindex.html)
<http://www.shorrock.u-net.com/netindex.html>



Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts



Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research



With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips



Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.