

Zone Labs Integrity

Integrity for Check Point Data Sheet



Maximum Remote Access Protection

Remote PCs accessing the corporate network through a VPN pose special risks to enterprise security. Once compromised, a remote PC and its authenticated VPN tunnel provide the hacker direct access to the corporate network. Adding a basic firewall to each remote PC mitigates this risk. However, to ensure remote PCs are not a corporate liability, comprehensive endpoint protection and network cooperation are required.

To assure end-to-end network security, Zone Labs, Inc. and Check Point Software Technologies deliver OPSEC-certified maximum remote access security. Zone Labs® Integrity's™ stateful distributed firewall assures that remote access remains secure on every connected PC, regardless of location.

Zone Labs Best-of-Breed Security for Check Point VPNs

Integrity enforces security on multiple levels to provide proactive, "always-on," tamper-proof protection that stops known and unknown threats through the following features that enhance Check Point's endpoint security:

- ▶ *Application control:* In addition to blocking network access by unapproved programs, Integrity allows administrators to allow or block network access by a program, or define a set of "classic" firewall rules for the program, providing flexibility in preventing Trojan horses and spyware from compromising enterprise security.
- ▶ *Instant Messaging security:* This optional Integrity module enables the productivity benefits of public Instant Messaging (IM) by mitigating its risks. Zone Labs' IM protection

encrypts messages, filters harmful content, controls service and feature usage, blocks unsolicited communication, and provides usage and event reports.

- ▶ *Cooperative Enforcement™ technology:* With Cooperative Enforcement you can enforce a comprehensive security policy enterprise-wide on internal or remote systems, via wired and wireless network access points. Integrity integrates with over twenty leading vendors of VPNs, switches, routers, and wireless access points. Integrity provides best of breed remote access policy enforcement with Check Point VPN-1. This complete protection far exceeds other security products that only provide policy enforcement for remote access.
- ▶ *Client security options:* Integrity offers Cooperative Enforcement with a disconnected security option that enforces enterprise policy even when the user is not connected to the enterprise network. This option ensures that mobile users are protected at all times. Integrity also offers "Total Client Lockdown", which prevents end users from modifying or disabling enterprise policies or clients, even if they have local administration rights. This protection ensures that endpoint security and policy enforcement can not be circumvented.



Policy Enforcement Delivers Continuous Defense

Integrity ensures that only endpoint computers running the Integrity client policies can access your network. Cooperative Enforcement prevents the user from obtaining access to the network if the Integrity client is shut down, ensuring that the endpoint is protected by Integrity throughout the network session. In addition, Integrity can operate transparently in heterogeneous, multi-vendor environments.

Integrity makes it easy for administrators to implement security policies that are as stringent or lenient as desired. Once configured, the Check Point VPN-1 client verifies that the Integrity client is running on the endpoint computer. Integrity checks remote and internal PCs for compliance with a range of

policy requirements – including running update-to-date anti-virus, required or prohibited programs, registry keys, OS service packs and other conditions, including having essential OS and application patches installed.

Rapid Deployment, Easy Management, Immediate Protection

Integrity is the perfect complement to an existing or new Check Point VPN-1 installation, integrating transparently to provide centrally managed, superior endpoint protection. Integrity provides an extensible client/server architecture that is compatible with existing network IT infrastructures and seamlessly integrates with hardware, software and networks.

Define Cooperative Enforcement Rule

Determine if MS Internet Explorer contains the following attributes when running on All operating systems.

The following registry key Copy and paste key here must have this value

A file named iexplore.exe

- This file must be running at all times.
- This file must be located at C:\Program Files\Internet Explore

Must have a version number from 6.00.2800.110 up to

Must have a modified date less than 0 days old.

Must match this Smart checksum c1fd1e8-2b96a493-143f7753-a

Define Action

- Require** endpoints to meet ALL conditions to access the network through a gateway.
- Prohibit** endpoints that meet ANY ONE condition from accessing the network through a gateway.
- Observe** endpoints that **require** these conditions but do not restrict them.

Define Remedy

Define custom text and a remediation option to present to end users when they are out of compliance with a Cooperative Enforcement Rule:

Define custom text for the ACE Sandbox page: Please click the link below to install the latest version of Microsoft Internet Explorer

Uploaded file is: IEXPLORE.EXE

- Upload a file to the sandbox C:\download\iesetup.ex Browse...
- Forward user to an external URL from the sandbox
- none

CANCEL SUBMIT

Integrity's intuitive interface makes defining policy enforcement rules easy, while still providing powerful security capabilities.

In choosing Integrity for Check Point, you'll also receive the full benefits of Integrity's easy-to-use, central management capabilities. Predefined policy templates, an intuitive Web-based management interface, market-proven firewall and application control let administrators quickly and easily develop, manage and enforce proactive endpoint security.

In addition, Integrity uses a standards-based approach to enforce the most comprehensive endpoint security policies on all PCs that access the network – from inside or outside the corporate perimeter, via a wireless or wired connection. Zone Labs supports the industry-standard Extensible Authentication Protocol (EAP) and 802.1x standard, which enables Integrity to integrate with over 200 network access devices – including many switches and wireless access points – from more than 20 leading vendors.

Zone Labs offers the industry's most comprehensive and functional Check Point integration. With Integrity and VPN-1, you are assured that maximum strength, multi-layered protection is in force on every endpoint PC outside the enterprise that accesses your network. The result: trusted end-to-end network security.

Integrity Server System Requirements

Hardware Specifications

- Intel Pentium III (600MHz) or greater
- Installer requires at least 256 color video

We strongly recommend running Integrity Server and the associated database server on separate host computers.

Physical Memory and Disk Space

Concurrent Connections	RAM	Disk Space
up to 500	512 MB	80 MB
up to 2000	1 GB	80 MB
up to 5000	2 GB	80 MB
up to 20,000	2 GB	80 MB
over 20,000	contact sales rep	contact sales rep

Operating Systems

- Windows 2000 server (SP4) and Advanced Server (SP4)
- Windows Server 2003

Browsers

- Internet Explorer 6 and above
- Netscape Navigator 7 and above

Database Management Systems

- Oracle 9iR2 with Oracle thin JDBC driver version 1.2
- Microsoft SQL Sever 2000 (SP3) with Microsoft SQL Server 2000 Driver for JDBC SP1

JDBC drivers must be downloaded from the vendor Website prior to installing Integrity Server.

We strongly recommend running Integrity Server and the associated database server on separate host computers.

Concurrent Connections	RAM	Disk Space
up to 500	512 MB	1 GB
up to 2000	1 GB	2 GB
up to 5000	1 GB	6 GB
up to 20,000	1 GB	8 GB
over 20,000	contact sales rep	contact sales rep

Database Server Hardware

This table lists required memory and disk space for a database running as a stand-alone server.

Cooperative Enforcement

- Check Point VPN-1 Gateway
- Check Point Firewall-1 NG FP1, 2, 3
- VPN-1® Secure Client™ , version FP3 and above
- Secure Remote

Anti-Virus Solutions (pre-configured)

- McAfee VirusScan 4.5, 7, and 2004 v.8
- Symantec Norton AntiVirus 2002, 2003, and 2004
- Symantec Norton AntiVirus Corporate Edition 7.6 and 8.1
- Trend Micro PC-Cillin 2002 and 2003
- Trend Micro OfficeScan Corporate Edition 5.5

US Headquarters

Zone Labs, Inc.
475 Brannan Street
Suite 300
San Francisco, CA 94107
tel 415.633.4500
fax 415.633.4501

European Headquarters

Zone Labs, GmbH
Frankfurter Str. 181 a
63263 Neu-Isenburg,
Germany
tel +49.6102.36689.0
fax +49.6102.36689.99

www.zonelabs.com

© 2004 Zone Labs. All rights reserved. IMsecure, TrueVector, ZoneAlarm and Zone Labs are registered trademarks of Zone Labs. The Zone Labs logo, Zone Labs Integrity and Cooperative Enforcement are trademarks of Zone Labs L.L.C. Zone Labs Integrity protected under U.S. Patent No. 5,987,611. Reg. U.S. Pat. & TM Off. Check Point is a trademark of Check Point Software Technologies Ltd. All other trademarks are the property of their respective owners. v.06.18.04



A Check Point Company



We Secure the Internet.