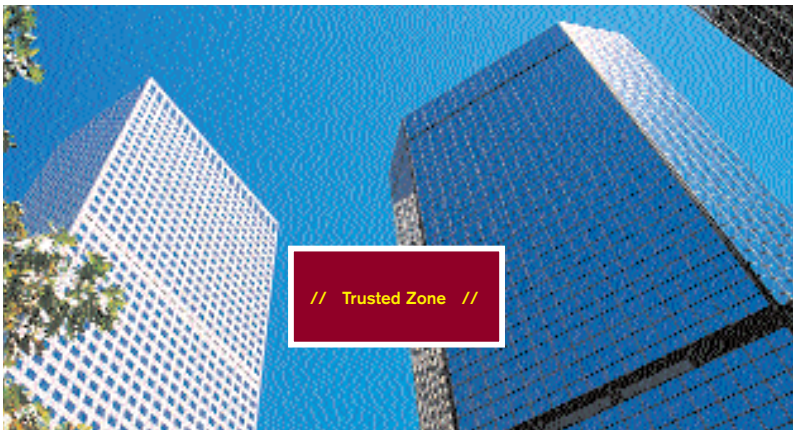
Zone Labs Integrity

Integrity for
Cisco VPN 3000
Concentrator
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 Cisco Systems have partnered to deliver maximum remote access security. Zone Labs® Integrity's™ stateful distributed firewall assures that remote access remains secure on every connected PC, regardless of location.

Policy Enforcement Delivers Continuous Defense

Integration with Cisco's VPN 3000 Series Concentrators is part of Zone Labs overall Total Access Protection strategy. With Total Access Protection, Zone Labs Integrity extends endpoint protection across the full spectrum of enterprise network endpoints, including employees and guest PCs, remote and internal PCs, and wired and wireless PCs. By providing best-of-breed, policy-enforced security on each endpoint, Total Access Protection dramatically mitigates the risks of worms, spyware, and other threats to business continuity and network integrity.

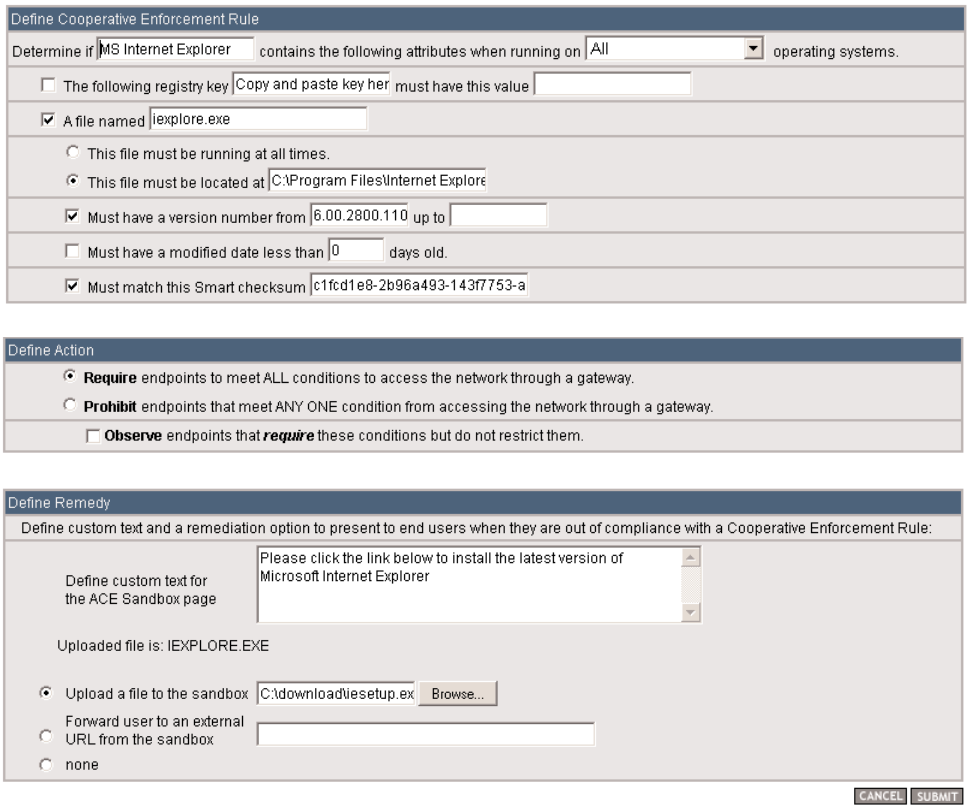
Integrity ensures that only endpoint computers running the Integrity client can access your network both before and during access through the VPN. Cooperative Enforcement™ also prevents the user from obtaining access to the network if the Integrity client is shut down, ensuring that the endpoint is protected by Integrity throughout the network session.

The Integrity solution makes it easy for administrators to implement security policies that are as stringent or lenient as desired. Once configured, the Integrity Server verifies that the Integrity client is running on the endpoint computer with the appropriate policies and cooperates with the Cisco VPN Concentrator to terminate connections that do not meet network security requirements. Integrity can ensure that all endpoint PCs have anti-virus running, all required patches, anti-virus updates, registry keys, files and applications before it grants access.

If any of these conditions is not met, users and administrators are notified that a correction is required. When a user is out of compliance, his/her network access is restricted to the IP address of the Integrity server's "sandbox," which can be configured by the security administrator to provide remediation guidance and downloadable resources. Integrity can also automatically generate a different remediation page for each type of compliance violation. In addition, administrators have the option to provide links to external remediation resources on each page. Together, these capabilities allow administrators to assist non-compliant end users and restore their access to network resources quickly, without resorting to a help desk call.

Comprehensive Anti-Virus Policy Enforcement

As a part of maintaining endpoint security, Integrity has the ability to enforce the use of antivirus software on client machines. The antivirus enforcement features can ensure that the antivirus application is installed and running on the client, as well as enforce versioning of the antivirus application's engine



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

and virus definitions file. Integrity provides Cooperative Enforcement with leading antivirus solutions including McAfee VirusScan, Norton AntiVirus and Trend Micro PC-cillin.

Easy Integration, Rapid Deployment, Immediate Protection

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

The Cisco-Integrity integration offers a "set and forget" type option that is also self-maintaining. Once the Integrity Server and the Cisco VPN Concentrator are each made aware of the other via the entering of network addressing information, and through the automated exchange of certificates, the systems will automatically maintain a synchronized list of users for the purposes of Cooperative Enforcement and policy deployment. This secure process allows authorized Cisco users to be automatically entered into Integrity's database and issued a policy that will secure the endpoint. The endpoints themselves need only a generic client install with the appropriate Cisco profile. All policies and endpoint security settings are automatically deployed and configured upon the initial connection to the remote VPN tunnel. A preconfigured policy can also be delivered with the client installation, providing instantaneous security upon the completion of the installation.

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. Both Cisco and Zone Labs support the industry-standard Extensible Authentication Protocol (EAP) and 802.1x standard, which

enables Integrity to integrate with other Cisco products that support EAP and 802.1x, including Cisco routers, Cisco Catalyst switches, and the Cisco Aironet wireless access points. Integrity also integrates with over 200 network access devices – including many switches and wireless access points – from more than other 22 leading vendors.

Zone Labs offers the industry's most comprehensive and functional Cisco integration. With Integrity and Cisco networking products, you are assured that maximum strength, multi-layered protection is in force on each and every Integrity-protected endpoint PC that accesses your network. The result: trusted end-to-end network security.

Cisco VPN with Cooperative Enforcement in Action

1. A Cisco VPN client contacts the VPN Concentrator.
2. The Cisco VPN Concentrator performs initial authentication of the user.
3. If authentication is successful, the tunnel is placed into a restricted state, allowing only network connectivity to the Integrity Server.
4. The Concentrator sends the Cisco gateway group name and user name to Integrity Server.
5. Integrity Server performs a lookup for the group and user name, and verifies compliance. It then selects the appropriate policy based on this information. The Integrity client is then interrogated for the current policy MD5 checksum.
6. The Integrity client sends the checksum of its policy to Integrity Server. If the policy and the rules within the policy are correct, the connection is removed from restricted mode. If the Integrity client has an incompliant policy, then the correct policy is sent.
7. Once the checksum sent from the Integrity client matches the correct policy, the VPN connection will be removed from its restricted state. If the checksum has not been corrected within six heartbeats, the Integrity Server will inform the VPN gateway to terminate the connection.
8. If any of these conditions is not met, Cooperative Enforcement allows access only to HTML pages that can provide explanations and software updates. These resources enable the user to comply with enterprise security policy quickly and easily. Once the user installs the necessary updates, his or her remote network access is restored.
9. Once connected, the Integrity client cannot be closed without also terminating the VPN connection. If the service is terminated through extraordinary means, the VPN connection will be immediately closed.
10. If the Integrity client misses three heartbeats in a row while connected to the LAN, the connection will be restricted. If the Integrity client misses ten heartbeats in a row the connection will be terminated.

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)

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.

Database Server Hardware

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

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

Cooperative Enforcement

- VPN software 3.5.1 and above
- VPN Client for Windows 3.5.1 and above

	Optimal	Minimal
Processor	Pentium II 450 MHz	Pentium II 233 MHz
RAM	128 MB	32 MB
Disk Space	10 MB	10 MB

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

A Check Point Company

Check Point SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.