

Zone Labs Integrity

Enterprise Endpoint
Security

// Trusted Zone //

Architectural Overview

A White Paper Presented
by Zone Labs

“Fixed fortifications are monuments to man's stupidity.”

-General George S. Patton

The Wall is Already Breached

Patton's statement came at a time when fast moving, mechanized armies had made obsolete the large, stationary defenses that had served to protect people against invaders for thousands of years. Stout walls could no longer guarantee security. Rather, defense had to become a key component of overall strategy, and responsibility for defense had to be pushed down to the lowest levels of command.

There is a remarkable correlation between Patton's famous words and today's computer network landscape. Corporations have traditionally protected their local and wide area networks (LANs and WANs) by building virtual fortifications of firewalls and routers to shield themselves from the outside world of the Internet. However, faced with the overwhelming demand to provide data and applications to individuals outside the network perimeter, corporations are routinely forced to breach their own defenses in order to support outside access through services such as dial-up and virtual private networking (VPN). While perimeter firewalls may guard against a “frontal assault” on the corporate network, each and every client machine provides a potential back door through which a company's network and data can be compromised.

In addition to these external threats, even ostensibly secure machines residing behind a firewall within the corporate

LAN can be points of network vulnerability. These endpoints within the corporate network are susceptible to a variety of threats that often go undetected by perimeter firewalls, such as email-borne attacks, Trojan horses, and Web browser vulnerabilities. In effect, the battleground has shifted from the network gateway to the software running on every networked PC.

The reality of network computing today is that companies are motivated by the obvious benefits of anytime, anywhere access to data for their employees and partners, while hackers are bent on compromising corporate networks for profit or malice. Enterprise IT groups are tasked with the challenge of protecting electronic assets without hampering the legitimate sharing of information. Hackers, for their part, will attack the network at the points they perceive as the weakest: the client machines residing at the network endpoints.

In short, security is about the data, and organizations must ensure the privacy and integrity of their data no matter where it resides or travels.

Extending Security to the Endpoints

Given the potential vulnerability of the enterprise network at its endpoints, the ideal solution is to extend the network security umbrella so that it encompasses those endpoints. While this is a very reasonable concept in abstract, it begs the question: what does it mean to extend enterprise security to network endpoints?

To answer, endpoint security for the enterprise is comprised of at least three major components:

1. Client software to implement and enforce security policies.
2. Centralized development and deployment of security policies.
3. Compatibility with existing infrastructure.

Zone Labs Integrity

// Trusted Zone //

Enterprise Endpoint
Security

Architectural
Overview

Page
3

Zone Labs Integrity™ provides all of these components in a single comprehensive package. Integrity is a security system comprised of client and server components that enables IT organizations to secure and manage endpoint devices over public or private networks. Integrity provides comprehensive capabilities for policy creation and management, server software that works hand-in-hand with network access devices such as VPN servers and IEEE 802.1X-based switches, routers and wireless access points to enforce policy, and award-winning client technology to implement policy and protect network endpoints.

Protecting the Network Through the Desktop

While Integrity's management features are crucial to maintainable endpoint security in the enterprise, the immutable fact is that the entire system is only as valuable as the strength of the software protecting each endpoint. The endpoint security software must have a proven record protecting against the wide variety of threats that put in constant jeopardy the integrity of PCs and the networks to which they are connected. Viruses, Trojan horses, and spyware can enter your computer through a variety of means, including email attachments, networking vulnerabilities, and removable storage media. Once these programs become resident, there's little they cannot do: destroy valuable applications and data, infiltrate other network resources, steal corporate or personal data, or even recruit your machine as a zombie to perpetrate attacks on other networks. In light of all this, client resident security software must be capable of protecting your PC from a variety of different threats. In particular, unsolicited attempts to access the computer over a network must be blocked to prevent intrusion and application-level control must be exerted to prevent unauthorized applications from accessing the network. Email attachment protection, which prevents potentially dangerous attachments from reach-

ing your email reader, is another important piece of the endpoint security puzzle.

Zone Labs' TrueVector® technology has the ability to protect against all varieties of security threat, known and unknown. The Integrity client protects the desktop using an exclusive combination of security technologies:

- A stateful desktop firewall that blocks unsolicited Internet traffic while allowing valid traffic initiated by the client. The effect of the firewall is to put the computer in "stealth" mode, making it invisible to other machines on the Internet.
- Application control, which manages the rights of local applications to access the network. Unlike the firewall, which blocks external intrusion attempts, application control prevents malicious applications from transmitting information over the network.
- Instant messaging security, which encrypts IM traffic and blocks inbound intrusions regardless of public IM client (i.e. AOL Messenger, MSN Messenger, Yahoo! Messenger and third-party clients such as Trillian)
- MailSafe email protection, which guards against potentially harmful email attachments and hijacking of end user address books in order to propagate viruses.

A desktop firewall works by blocking unsolicited attempts to access the computer through the network. While most firewalls demand a relatively high level of technical expertise of the user, the Integrity client's firewall functions "out of the box," without a system administrator having to understand and configure technical details such as IP addresses, ports, or protocols. The firewall is referred to as "stateful" because it monitors outgoing traffic, creating internal states that determine the kinds of incoming traffic that will be accepted in response.

While a desktop firewall is an important component of endpoint security, a firewall alone falls far short of offering complete protection for a desktop. In particular, a firewall works at a very low level with respect to network traffic, monitoring indi-

Zone Labs Integrity

Enterprise Endpoint
Security

Architectural
Overview

Page
4

// Trusted Zone //

vidual data packets as they enter and leave the machine.

The Integrity client's firewall transcends this traditional limitation by working in conjunction with the TrueVector engine to provide application-level security control. This works on the assumption that all applications are untrusted until the user (or a security policy defined by an administrator) explicitly grants trust to the application. This "guilty until proven innocent" logic prevents malicious applications from gaining access to network resources and provides security against even unknown types of threats.

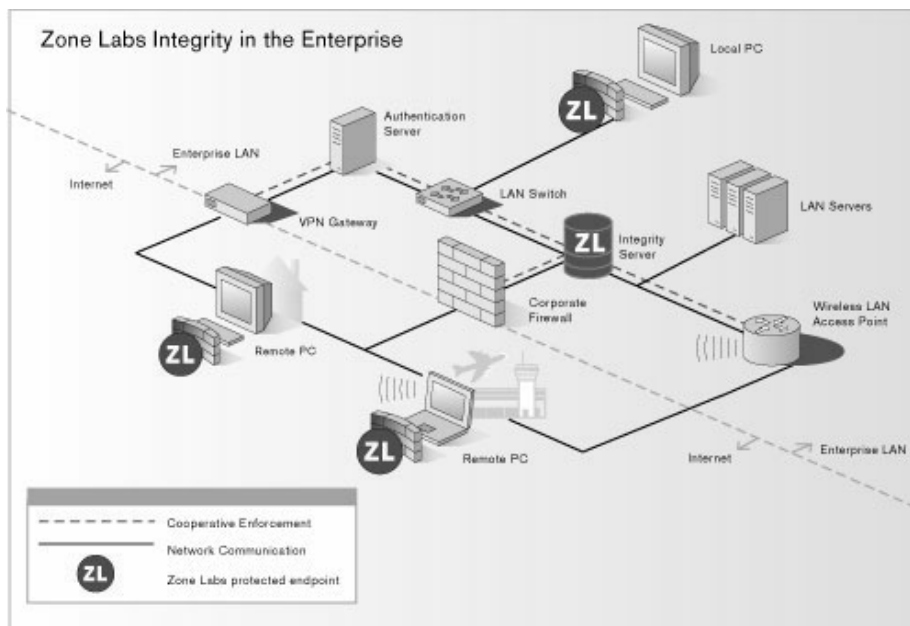
Integrity and TrueVector further extend application-level security to ports, protocols, application components and trusted application "hijacking." For example, firewall rules may be tuned to permit access only to those ports and protocols absolutely necessary (e.g. only HTTP and HTTPS ports for web browser applications). Component control ensures that all components (e.g., DLLs, OCXs, etc.) used by a trusted application are authorized and authenticated. This comprehensive approach stops hackers from replacing or injecting a component into a trusted Internet-accessing application, exploiting it to compromise security.

Similarly, Integrity allows only approved and authenticated applications to control other approved applications that access the Internet. This guards against threats whereby an untrusted, attacking application may hijack a trusted application. For example, when an untrusted application launches Internet Explorer and tries to pass private information in the URL, Integrity blocks it.

Integrity offers built-in port, protocol and component control policies.

These policies may be adapted to specific environments. Administrators may also build and manage custom policies.

Integrity protects Instant Messaging services and traffic including AOL Instant Messenger (AIM), MSN Messenger, and Yahoo Messenger. Integrity Server centrally manages policy which dictates the Integrity client behavior. Integrity brings advanced security to instant messaging by adding the ability to parse the messaging protocol and affect the messenger behavior with policy rule sets. Since Integrity integrates at the protocol level with third party clients such as Trillian, AOL, MSN or Yahoo are also protected. Through the use of protocol analysis, Integrity can determine the content of the instant messaging traffic. Thereby disallowing IM completely or identifying specific functions to disallow, like file sharing or video, while allowing other functions like chat. Instant Messaging for Integrity can also encrypt the IM traffic.



Zone Labs Integrity

// Trusted Zone //

Enterprise Endpoint
Security

Architectural
Overview

Page
5

Since Integrity is not attempting to secure instant messaging based upon the client or port controls, the security behavior is strong and consistent. Port based security controls are easily circumvented by the IM clients, and in fact IM clients are designed to do so to enable easy access through perimeter firewalls. Integrity's protocol based security ensures that security policy will be adhered to at all times. Please note, Instant Messaging Security for Integrity is an optional module that is enabled with its own license key.

In addition, MailSafe email protection takes advantage of the TrueVector engine's ability to parse many different types of Internet protocols by also parsing incoming email messages that originate from servers using the POP or IMAP protocols. MailSafe finds and quarantines more than 47 types of potentially harmful attachments, preventing email-borne viruses from automatically contaminating the machine and potentially spreading to other computers—even before an antivirus remedy is available.

Integrity Architecture

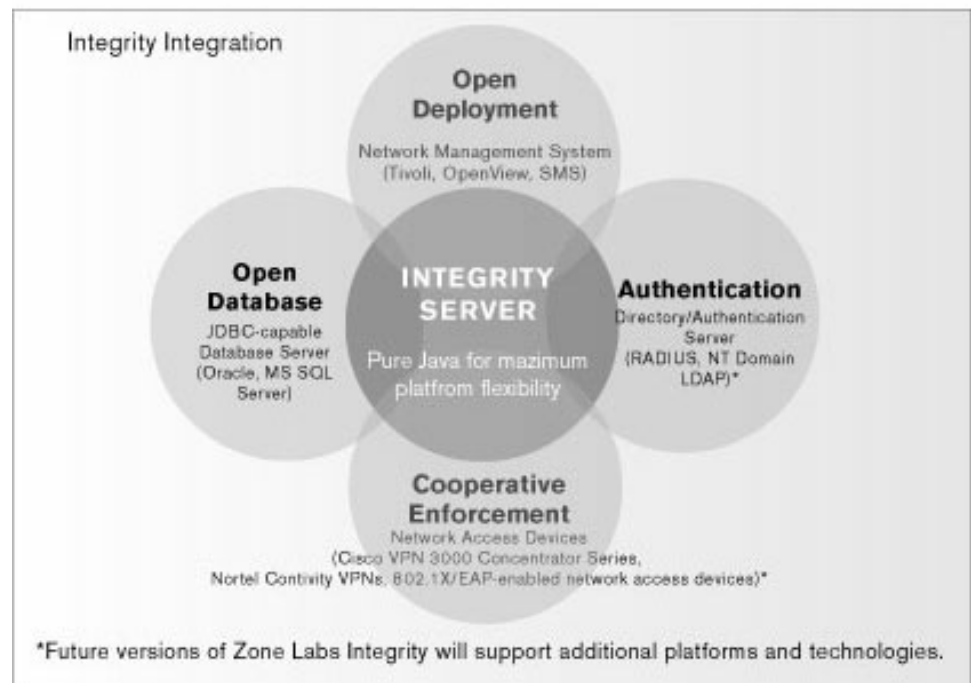
The Integrity system is designed to be “dropped in” to a wide variety of networking environments. The previous diagram illustrates the Integrity system security architecture.

The Integrity Server resides within the corporate LAN. It is responsible for both ensuring implementation of the security policy on each client and working closely with network access devices (the VPN, firewall, 802.1X-enabled switches, routers and

wireless access points in this case) to enforce policy. Each client machine in the diagram is running the Integrity client software, which implements endpoint security for each client based on the policy provided by the Integrity Server. Policies are created and managed on the Integrity Server using an intuitive Web-based interface that allows policies to be developed on a per-group or per-user basis.

Extensible Platform Architecture

The Integrity platform is also designed for maximum extensibility, with a particular focus on scalability. The architecture provides generic interfaces between the Integrity Server and the Integrity client, gateway devices, databases, and directory/



Zone Labs

Integrity

// Trusted Zone //

Enterprise Endpoint
Security

Architectural
Overview

Page
6

authentication server subsystems. These generic interfaces enable Zone Labs to quickly incorporate additional products and technologies as called for by the market. This not only enables the Integrity solution to reach an ever-more-broad range of enterprises, it provides assurance to existing Integrity enterprises that Integrity is architecturally prepared to grow and change with an organization. In fact, for larger deployments, Integrity scales to support thousands of concurrent users per server, and nearly any number of client users at Global 2500 companies with multiple servers.

Policy Enforcement Models

While Integrity works in practically any network environment, the Integrity system can be configured in one of two ways with respect to integration with gateway devices. Stand-alone enforcement is used in a scenario where the gateway device does not natively communicate with the Integrity Server. Cooperative Enforcement™ is used with network access devices having built-in support for managing client connections cooperatively with the Integrity Server.

It is important to note, however, that machines running the Integrity client are always protected, regardless of whether they are currently connected to an Integrity Server. Administrators may configure the client such that the connection status with the Integrity Server dictates what policy is being enforced, but at no time does the connection status with the Integrity Server affect the core protection provided by the client.

Stand-alone Policy Enforcement

In a stand-alone enforcement scenario, the Integrity client and Integrity Server work together to provide centrally-managed endpoint security. The system workflow of this model is as follows:

1. The Integrity client starts up as the machine

starts up and begins enforcing appropriate "disconnected" policy.

2. The Integrity client opens a secure TCP connection with Integrity Server and passes login information.
3. The Integrity client begins enforcing last known "connected" enterprise policy.
4. Integrity Server uses login information to retrieve appropriate policy for user from the database.
5. Integrity Server uses login information to determine whether Integrity client is running the appropriate policy. If not, the new policy is pushed to the Integrity client.
6. The Integrity client accepts policy and begins enforcing new enterprise policy.
7. The Integrity client sends heartbeat (described later in this document) messages to Integrity Server at regular intervals. Integrity Server uses this information to provide real-time monitoring of all clients, and logs instances of out-of-compliance heartbeats.
8. Integrity Server periodically requests uploads of security event information logs from the Integrity client in order to populate the database.
9. If policy for a currently logged on user is updated on Integrity Server, Integrity Server will push new policy to Integrity client in real time.

This system works well in any environment and ensures that clients are always running the appropriate security policy.

Cooperative Enforcement™

Cooperative Enforcement builds on stand-alone enforcement by allowing access to network resources only to those client machines that can provide assurance that they are in compliance with security policy. In particular, Integrity can cooperate with other security products to ensure that clients are running up-to-date firewall and antivirus software before they are granted network access. Clients not in compliance with policy are redirected to and sequestered in a network "sandbox" that

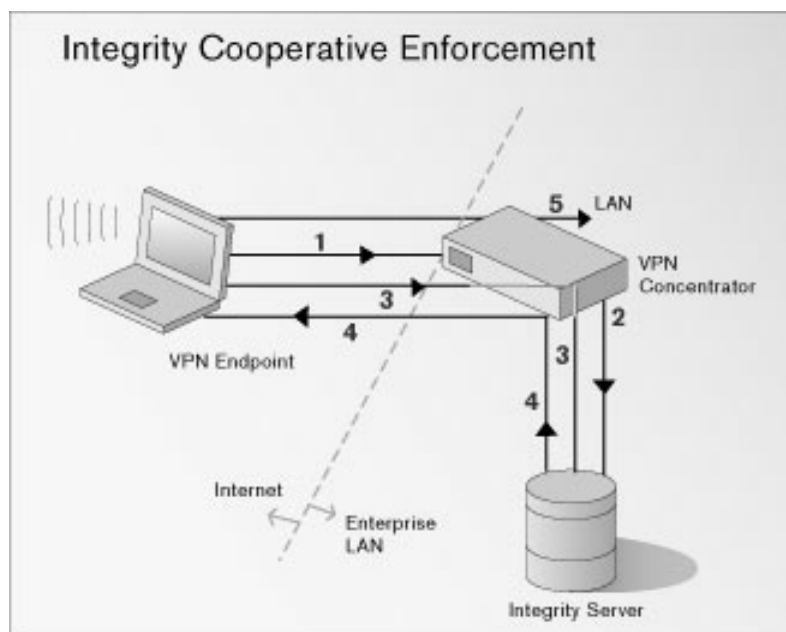
Zone Labs Integrity

Enterprise Endpoint
Security

Architectural
Overview

Page
7

// Trusted Zone //



may provide the resources necessary to bring their machine into compliance.

Each step can be described as follows:

1. The VPN client software, which resides on the same PC as the Integrity client, connects to the VPN Connector, passing necessary information regarding the Integrity client.
2. The VPN Connector informs the Integrity Server of the new client connection and provides client connection information.
3. The Integrity client, via the VPN Connector, establishes a connection with the Integrity Server.
4. The Integrity Server determines whether the client is in compliance with security policy, and, if it is, it instructs the VPN concentrator to open the connection and provide necessary connection details. If the client is not in compliance, the Integrity Server will instruct

the VPN concentrator to restrict the session to the network sandbox.

5. The VPN client passes connection details to the Integrity client and signals that policy enforcement should begin immediately and the client can now enter the enterprise LAN.

Once the connection has been established, the server continues to monitor the state of the client via the heartbeat messages sent from client to server. This process is described in greater detail in the "Heartbeats and Policies" section later in this document.

IEEE 802.1X/EAP Cooperative Enforcement

In addition to Zone Server Protocol (ZSP), Integrity's gateway interface uses the Extensible Authentication Protocol (EAP) to provide Cooperative Enforcement for those devices

which support EAP. This includes numerous switches, routers, wireless access points and network access servers, as well as most Windows operating systems.

Integrity leverages the core function of EAP, which is to extend the authentication of PPP sessions with the addition of secure authentication schemes such as smart cards, certificates, and now Cooperative Enforcement. The Integrity Server and gateway communicate with the EAP enabled devices and RADIUS servers to ensure that the access through the device is only gained by those users who meet specific criteria as defined by the Integrity policy's Cooperative Enforcement rule set. Integrity client supports endpoint operating systems that are EAP enabled by the addition of Cooperative Enforcement to the list of authentication methods for 802.1x and LAN adapter configurations. The Integrity client endpoint EAP integration

Zone Labs Integrity

Enterprise Endpoint
Security

Architectural
Overview

Page
8

// Trusted Zone //

takes the form of a wrapper dll which utilizes the underlying MD5, Smart Card or Certificate configuration, and transports that information along with the Integrity compliance checks, to the Integrity Server via the access point and the Integrity gateway interface. This means that the endpoint authentication is a combination of compliance information as well as MD5, Smart Card or Certificates. The standard Integrity restriction and termination rules apply to the EAP integration as well. Each step can be described as follows:

1. The network client software, which resides on the same PC as the Integrity client, connects to the Network Access Server, passing necessary information regarding the Integrity client.
2. The Network Access Server informs the Integrity Server (in this case, with the embedded Integrity Gateway) of the new client connection and provides client connection information.

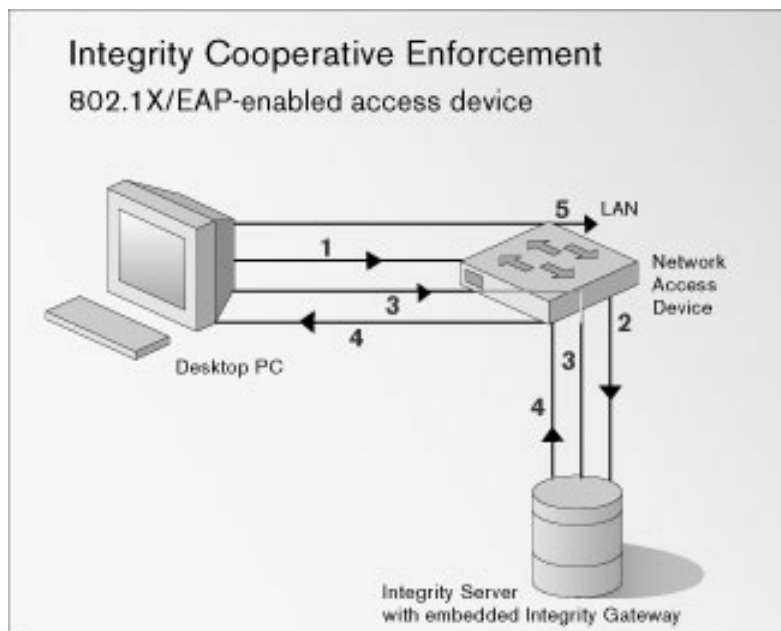
3. The Integrity client, via the Network Access Server, establishes a connection with the Integrity Server.
4. The Integrity Server determines whether the client is in compliance with security policy, and, if it is, it instructs the Network Access Server to open the connection and provide necessary connection details. If the client is not in compliance, the Integrity Server will instruct the Network Access Server to restrict the session to the network sandbox.
5. The network client passes connection details to the Integrity client and signals that policy enforcement should begin immediately and the client can now access the enterprise LAN.

Antivirus Enforcement

As a part of maintaining endpoint security, the Integrity system has the ability to enforce the use of antivirus software on client machines. In addition to ensuring the antivirus application is installed and running on the client, the antivirus enforcement feature provides the ability to enforce versioning of the antivirus application's engine and virus definitions file. Among other things, this enables administrators to quickly respond to emerging virus threats by creating a policy that requires end users to keep their antivirus software updated.

Advanced Cooperative Enforcement

In addition to the built-in support for antivirus enforcement, Integrity provides the ability to enforce the use or presence of any endpoint software with Advanced Cooperative Enforcement. Advanced Cooperative Enforcement enables the Integrity administrator to create policy rules that check for the presence of specified files, registry entries, or



running applications. Policy compliance can then be determined by the presence or absence of these items on the endpoint PC. In this way, Advanced Cooperative Enforcement can validate an endpoint's security even outside the scope of Integrity security functionality by ensuring the endpoint is running other software mandated by policy. For instance, Advanced Cooperative Enforcement allows an administrator to require that operating system and application patches have been installed on end user systems.

Heartbeats & Policy

The heartbeat messages mentioned earlier are sent from the Integrity client to Integrity Server at intervals specified by the system administrator to provide information on the current state of the client. Information contained in the heartbeat includes connection details, client type and version, number of pending alerts, and antivirus enforcement specifics. If Integrity Server determines that the client is not in compliance with security policy (e.g., failure to enforce latest policy or out-of-date antivirus software) in an environment with Cooperative Enforcement, it will instruct the gateway device to place the client in restricted mode and ultimately to terminate the client connection if it remains in a state of non-compliance.

Integrity Server

Integrity Server is the heart of the Integrity system. It provides the following services necessary to establish and manage this comprehensive endpoint security system:

- Interface with Integrity client software running on client machines.
- Interface with network access devices.
- Server administration, including user catalog management

and a policy management interface for creating security policies and associating policies with users and groups.

- Advanced reporting capabilities providing the feedback necessary to drive the security policy lifecycle.

Integrity Client Interface

The Integrity Server and Integrity client maintain a constant connection to one another using a secure TCP socket. The subsystem that manages these connections in the Integrity Server is known as the connection manager. The purpose of Integrity Server's connection to the Integrity client is threefold:

1. Enable Integrity Server to monitor the client to ensure that it remains compliant with security policy. If a client is deemed to be non-compliant, Integrity Server will instruct the gateway device to restrict or terminate out-of-compliance client connections.
2. Ensure connected clients are always running the most up-to-date security policy. When an administrator modifies or assigns a policy for one or more connected clients, that new policy is immediately pushed out to clients. This ensures the shortest possible time from security policy conception to actual enforcement.
3. Allow the Integrity Server to request and receive security log uploads. This enables administrators to perform near-real-time analysis of endpoint security events.

The advantage of Integrity's connection-based architecture over a connectionless, client-polling architecture is it allows for real-time, bi-directional exchange of information between client and server. This means, for example, that policy updates can be pushed from server to client immediately, without waiting for the next polling interval, as would be the case in a connectionless architecture.

The communications between Integrity Server and the Integrity client occur using an XML-based protocol via Secure

Zone Labs

Integrity

// Trusted Zone //

Enterprise Endpoint
Security

Architectural
Overview

Page
10

Sockets Layer (SSL), and involve the exchange of digital certificates to ensure privacy, integrity, and authentication.

The connection manager architecture combines vigilance with scalability. In general, each Integrity client heartbeat efficiently fits into a single Ethernet frame, preventing network congestion. The TCP connection provides for bi-directional communication, which enables the Integrity Server to call back to the client at any time to push policy updates or request log uploads.

The Integrity Monitor console within Integrity Server works hand-in-hand with the connection manager to provide a graphical representation of the activity of currently connected clients. Integrity Monitor provides administrators with real-time information on connected clients, server load, and other relevant details.

Gateway Interface

The gateway interface enables Cooperative Enforcement™ by managing the connection between the Integrity Server and the gateway device. Like the connection with the Integrity client, the connection with the gateway device uses an XML-based protocol called Zone Server Protocol (ZSP), which is protected using SSL security. ZSP provides a means for the Integrity Server and the gateway device to exchange information such as client connection status, user identity, policy compliance, and state transitions.

Server Administration

Integrity Server provides a rich, Web-based interface for administering configuration details. Because the interface is Web-based, corporate IT departments may manage enterprise security policy from virtually any administrator workstation, without the need to install specialized client software. At the

back end, Integrity Server uses Java Database Connectivity (JDBC) drivers to connect to a variety of back-end relational database management systems (RDBMS). Integrity Server's administration tools also have the capacity to interface with external management tools, such as SNMP-based applications like Tivoli and OpenView, and notification tools, such as Envoy and NotifyMe. Integrity Server administration capabilities can be divided into three categories: general administration, user management, and policy management.

General Administration

General administration deals with the configuration and maintenance of information pertinent to the specific environment in which Integrity Server is operating. Details such as gateway devices, RDBMS, and directory/authentication servers are controlled using this interface.

User Management

Integrity Server has the ability to import users and groups from NT Domain, LDAP, and RADIUS directory/authentication server platforms. In particular, Integrity is certified to support integration with RSA SecurID token-based authentication, Funk Steel Belted RADIUS, Microsoft Active Directory, Novell eDirectory Server, and Netscape Directory Server. This broad authentication support ensures that Integrity integrates with the most common user management and authentication systems. Imported authentication information is used to populate Integrity Server's own internal user information that is used by Policy Studio to relate policies with specific users and groups.

Policy Management

Integrity Server provides the Policy Studio tool for building security policies and associating policies with specific users or groups. Administrators have the ability to centrally control policies both at the high level, such as by specifying trusted appli-

Zone Labs

Integrity

// Trusted Zone //

Enterprise Endpoint
Security

Architectural
Overview

Page
11

cations and networks, as well as at a low-level, such as by blocking specific IP addresses and ports.

Integrity Server provides several default policies that may be used as a starting point for policy design. These default policies range in security from open to restrictive (and provide several shades of gray in between) so that you can start from a point that most closely matches your needs.

Program Observation

In order to build a database of known applications, the Integrity client provides a feature known as Program Observation. Program Observation keeps track of each application that accesses the network and reports the list of applications back to the Integrity Server. This provides the administrator the ability to maintain a complete catalog of all applications used in the enterprise to access the network, and provides a means to allow known good applications and to block known undesirable applications from accessing the network.

Application Reference Checking

Integrity also uses Application Reference Checking to block unknown applications and components. With this approach, administrators use an Integrity disk scanning tool to compile a database of approved enterprise applications installed on one or more reference PCs. Application Reference Checking automatically compares newly-discovered client applications and components against this central reference list before allowing network access. Integrity can automatically block exceptions to this list, or apply whatever access rules the administrator desires.

With Program Observation and Application Reference Checking, when an administrator marks an application as either allowed or blocked, this information is communicated back to the client in the policy. Administrators may apply a set of rules to individual applications. Alternatively, administrators

may apply a common set of rules to related applications and components—Web programs, for example. This flexibility simplifies the maintenance of application control and security policies.

Reporting

Key to the proper maintenance of a security policy lifecycle is the ability to analyze the strengths and potential vulnerabilities of the network's endpoint security policies on an ongoing basis. Because the nature of security threats and individual network usage is in a constant state of change, it's important to have tools available that enable administrators to easily collect data, analyze the data, and make the necessary adjustments to security policy. Integrity Server collects data by retrieving access logs from each client device running an Integrity client, and policy adjustments are managed using Policy Studio. Data analysis is performed using Integrity Server's reporting tools, which provide a collection of pre-packaged reports for managing policy. Additionally, all of the data used by Integrity's reporting system is stored in an industry-standard SQL database, allowing organizations the ability to customize reports.

Dynamic Failover Support

Because Integrity Server is intended to be a mission critical component of network security, it supports dynamic failover to enable high availability. When configured for dynamic failover, one Integrity Server will serve as the "active" server while one or more additional Integrity Servers will operate in "passive" mode. When the active server goes offline for any reason, this will be detected by one of the passive servers, which will then take over the active role. The back-end database is used to keep state information constantly in sync between the active and passive servers.

Zone Labs

Integrity

// Trusted Zone //

Enterprise Endpoint
Security

Architectural
Overview

Page
12

Integrity SDK

Zone Labs has surfaced a number of these generic interfaces as an external Software Developer's Kit (SDK) intended for use by third party VPN, firewall, and gateway vendors to integrate their solutions with Integrity. Contact Zone Labs' Business Development office for further information on the Integrity SDK.

International Support

Integrity has been designed with the global enterprise in mind with an architecture that supports most character sets used worldwide. Character strings within the Integrity Server are stored in double-byte Unicode format. Communication between Integrity Server and Integrity client employs the UTF-8 character set. Character strings within the client are stored in ANSI multi-byte format. All display strings on Integrity Server and Integrity clients are stored as separate resources to facilitate translation. This architecture enables the Integrity platform to target almost any locale required by the market.

Integrity Clients

The Integrity client is the desktop client-resident portion of the Integrity system, responsible for implementing the security policy provided by Integrity Server. The client software is the key to any enterprise endpoint security system; without the absolute strongest client security, all other security infrastructure is merely window dressing. To this end, the Integrity clients are built on the same TrueVector engine platform as Zone Labs' award-winning PC security products, ZoneAlarm and ZoneAlarm Pro.

For administrative flexibility, Integrity supports two forms of client software installs and operates in two modes either as the purely administrator managed Integrity Agent or a client that combines central management with end-user administration,

Integrity Flex.

Integrity Agent: Central Control of the Desktop

Integrity Agent is designed to function with only a minimal user interface, providing information regarding known and active policies but no ability for the end user to customize security settings. The interface presented to the end user can range from none to a minimal tray icon and status window. Integrity Agent is recommended for enterprises wishing to take complete control over desktop security without interfering with the end-user's normal desktop experience.

Integrity Flex: Enhanced End User Productivity

Integrity Flex extends the capabilities of the Integrity Agent client, enabling local policy management in addition to providing information on Integrity security policies. Integrity Flex is recommended for enterprises wishing to give end users the flexibility to control their own security policy when disconnected from the corporate network, without compromising corporate policy when they are connected. Furthermore, it offers the option to simultaneously combine a user's security settings with active enterprise policies for enhanced security and a better user experience thanks to a patent-pending policy arbitration technology. In essence, policy arbitration combines two policies and enforces the most restrictive of each of the policy elements on a setting-by-setting basis. This ability means there are no compromises necessary when it comes to combining the security needs of end users and corporate security policy.

Client Deployment

Zone Labs provides a single, self-contained installer executable for client deployment. This installer can be pushed out to desktops via any enterprise software distribution mechanism, such as SMS, Tivoli and OpenView. Client installations can also be customized by deploying a configuration file along with the installer executable and/or by executing batch file commands after product installation. Initial client deployment does not typ-

Zone Labs

Integrity

// Trusted Zone //

Enterprise Endpoint
Security

Architectural
Overview

Page
13

ically require a reboot of the client machine, although subsequent installations will require a reboot after install.

User Authentication

The Integrity client identifies and authenticates the user in one of two ways:

1. The client first obtains the Windows domain identity credentials of the currently logged in user. If there is a match for this user in the Integrity Server's user catalog, the user is logged into the Integrity Server and provided the appropriate policy.
2. Failing Windows domain authentication, the Integrity system can be configured for proxy login. Proxy login presents the user with a login dialog into which they may type their user name and password. This information is sent securely to the Integrity Server, with authentication confirmed against NT Domain, Active Directory, RADIUS or LDAP user directories. If authentication is successful, the user is provided with the appropriate policy. Policies may be assigned by individual user based on NT Domain, RADIUS or LDAP credentials, or administrators may assign policies to grouped or individual IP addresses, an approach that speeds and simplifies central policy deployment, management, enforcement and monitoring.

Integrity Technologies

To promote maximum robustness and flexibility, Integrity is built using technologies with a proven track record in Internet communications and security. These include:

- **Java:** Integrity Server is built in 100% Java, which affords a great deal of flexibility on the server in terms of platform and operating system.
- **C/C++:** Integrity clients are built in a combination of C and

C++, the world's most popular programming languages. Building the client pieces in C/C++ provides the highest level of control and performance required for the Integrity client.

- **HTML:** The interface for Integrity Server's administrative tools is implemented using HTML so that configuration of Integrity Server is possible from practically any administrator workstation with a Web browser.
- **XML:** The protocols for communication between Integrity Server and Integrity clients and between Integrity Server and the gateway devices are based on industry standard XML. This allows for greater extensibility and ease of development.
- **TCP/IP:** Communication between all of the components of the Integrity system uses standard TCP sockets, supported by practically all network infrastructures.
- **SSL:** Component communication over TCP is protected using secure sockets layer (SSL), leveraging this standard public key infrastructure encryption technology for the utmost in connection privacy.
- **TrueVector Technology:** Integrity clients leverage the patented security technologies that have proven successful on millions of desktops worldwide.
- **802.1X/EAP:** Integrity Server integrates with network access devices that support this emerging authentication standard in order to provide Cooperative Enforcement of enterprise policy across the LAN.

System Requirements

Please see the Zone Labs Integrity Datasheet for currently supported platforms, gateways, databases, and authentication servers.

Zone Labs Integrity

// Trusted Zone //

Enterprise Endpoint
Security

Architectural
Overview

Page
14

Summary

The Integrity system represents the state of the art in enterprise endpoint security. The combination of proven client security technology, central management of security policy, and the ability to leverage existing IT infrastructure makes for a powerful and compelling solution to the problem of securing ever-growing numbers of fixed and mobile network endpoints. By associating an Integrity server with one or more gateway devices, Integrity will scale to the entire enterprise. The industry-proven strength of the client's TrueVector technology means never having to compromise on client security. The ultimate benefit of Integrity is peace of mind: knowing that your enterprise network and data are protected from potentially huge losses due to targeted attacks.

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
Düsseldorfer Str. 40a
65760 Eschborn, Germany
tel +49 6196 773 670
fax +49 6196 773 6777



www.zonelabs.com

© 2003 Zone Labs, Inc. All rights reserved. Zone Labs, TrueVector, ZoneAlarm, and Cooperative Enforcement are registered trademarks of Zone Labs, Inc. The Zone Labs logo, Zone Labs Integrity and IMsecure are trademarks of Zone Labs, Inc. Zone Labs Integrity protected under U.S. Patent No. 5,987,611. Reg. U.S. Pat. & TM Off. Cooperative Enforcement is a service mark of Zone Labs, Inc. All other trademarks are the property of their respective owners. v.11.17.03