

Firewall Software

Go beyond the world of packet filtering



Today's centrally managed, software-based firewalls go well beyond packet filtering. Although interrogating a network datagram for IP addresses and port numbers is still a prerequisite, vendors are including more functionality. To distinguish between excellent and run-of-the-mill firewalls, you need to look at a product's level of automation, additional features, and ease of management.

Automation

In the past, network administrators spent hours figuring out the optimum order of filter rules. Today's firewalls have predefined rules and actions that let you choose from predefined strength levels (e.g., Paranoid, Intranet, Trusting). Traditional firewalls delineated only a perimeter and perhaps a higher-risk demilitarized zone (DMZ). Now, several products let you assign different levels of trust to perimeter-crossing "zones," so you can prioritize foreign traffic and packets traveling inside the organization.

Configuration wizards help you set up additional rules, define a DMZ, and simplify tasks. Most of today's firewalls check for the latest updates and patches and run periodic checks. Some firewalls are updated almost as frequently as antivirus scanners. Firewall updates include bug fixes, increased functionality, and increased ability to recognize new types of threats.

In many cases, if a firewall notices a persistent threat, the firewall automatically takes action, such as blocking all future requests from the same source or helping track down the offender. Although firewall logs and alerts are still short and to the point, most vendors make expanded explanations of threats available.

Additional Features

One of the best features available is application filtering (aka application-level firewalls or application blocking). Authors of viruses, Trojan horses, worms, and malicious software (malware) have learned that certain IP ports in a firewall (e.g., port 80) are almost always open from the inside out. After an attacker installs a malicious program inside a protected perimeter, the program can search for an open port or attach to an existing proxy client and remain unmolested. Application filtering lets only pre-approved client executables pass through open ports. Look at how the firewall determines what constitutes an approved application: Some firewalls only verify the program's name, but others contain a database of executable traits (e.g., hash algorithms, size, dates, internal coding checks) on each approved application.

Good firewalls not only block unapproved packets but also use Intrusion Detection System (IDS)-like functionality to identify well-known attacks. Firewalls often behave as centralized antivirus managers to distribute forced updates to attached workstations.

Firewalls often act as privacy gateways, block unwanted advertisements and forbidden (e.g., adult,

violent) content, and provide VPN capabilities. Some firewalls include interfacing APIs so that the firewall works with other products that inspect network traffic. Other vendors offer emulated environments so that potentially malicious code can be executed without causing harm. Clearly, today's firewall has to be more than a packet filter.

Centralized Management

Network administrators prefer to manage firewalls from a centralized, Web-based console. Look for products that provide several levels of alerts, logging, and automatically generated statistical reports. The most scalable solutions offer enterprise security policies that automatically generate rule sets and permissions. Of course, automation and good feature sets mean nothing if the firewall doesn't work. Many firewalls are tested, approved, and certified by organizations such as the International Computer Security Association (ICSA).

Future

Future firewalls will be friendlier and more feature-packed, with logs that report only necessary information and improved responses to attacks. Soon, to the dismay of firewall purists, administrators might not even need to know much about protocols and rule sets.

—Roger A. Grimes

InstantDoc ID 25651

Editor's Note: The Buyer's Guide summarizes vendor-submitted information. To find out about future Buyer's Guide topics or to learn how to include your product in an upcoming Buyer's Guide, go to <http://www.winnetmag.com/buyersguide>. To view previous Buyer's Guides on the Web, go to <http://www.winnetmag.com/articles/index.cfm?departmentid=118>.

Compiled by Sue Cooper

Firewall Category	Contact Information	Product Name	Price	Description
Desktop	Agnitum (7) (812) 9632128 http://www.agnitum.com	Outpost Firewall Pro	\$39.95	Supports plugins and filtering at the lowest possible level; protects against active email and Web threats; gives detailed information about all connections and open ports; predefines system and application settings; contains an update utility; lets you block banners and filter content for parental control; provides port-scanning detection and Internet-attack blocking; DNS caching speeds connection times
Enterprise	BorderWare Technologies 905-804-1855 877-814-7900 http://www.borderware.com	BorderWare Firewall Server	Starts at \$1200	Integrated security solution provides Plug and Play (PnP) installation and encrypted remote administration; a proxy server enhances performance for local network access to the Internet
Enterprise	Check Point Software Technologies 650-628-2000 800-429-4391 http://www.checkpoint.com	Check Point FireWall	Starts at \$2000 for 25 nodes	Lets enterprises define and enforce one comprehensive security policy to protect all network resources; innovative architecture delivers a scalable solution to integrate all aspects of network security
Enterprise	Computer Associates 631-342-5224 800-243-9462 http://www.ca.com/etrust	eTrust Firewall	Starts at \$100 per user	ICSA certified; scales to a large number of users; provides both perimeter and internal firewall protection; directly combats insider attacks; a unified console lets you deploy firewalls throughout the enterprise; features intuitive firewall-rule analyzer, stateful packet inspection technology, and application protocols support
Desktop and enterprise	Deerfield.com 989-732-8856 800-599-8856 http://www.deerfield.com	VisNetic Firewall 1.1	From \$69.95 to \$9799.95	Stateful packet-level firewall solution protects Windows-based servers, standalone PCs, and LAN workstations; features Sequence Number Hardening to protect networks against internal and external threats
Enterprise	Firewall Security Solutions 403-266-5895 877-808-8488 http://www.bizguardian.com	BizGuardian VPN Firewall	\$375	Ten-seat industrial-strength integrated IP Security (IPSec) VPN/firewall; installs automatically in minutes; connects branches, suppliers, roving employees, and customers; features secure Web-based management, intrusion-detection, reporting, and management tools
Desktop	InfoExpress 650-623-0260 http://www.infoexpress.com	CyberArmor Suite	CyberArmor Client starts at \$59 per seat; CyberServer is \$4995	Centrally managed distributed firewall extends policy-based security to remote users who access corporate networks through "always-on" configuration; remote-management tools provide flexible control over security policy implementation without end-user intervention
Desktop	Internet Security Systems 888-901-7477 http://www.iss.net	RealSecure Desktop Protector	From \$45 to \$106 per sensor	Provides firewall, intrusion protection, and application control for remote or mobile PCs within the RealSecure ICEcap Manager command environment; blocks improper activity and passes crucial security information to management console for further analysis

Firewall Category	Contact Information	Product Name	Price	Description
Desktop	Network Associates 972-308-9960 888-847-8766 http://www.networkassociates.com	McAfee Desktop Firewall 7.5	From \$30 to \$50 per node	Features console-based centralized management, updates, and graphical reporting; blocks vulnerable connections; protects remote and broadband users; stops internal attacks; prevents use of vulnerable or unauthorized applications and connections
Desktop and enterprise	Ositis Software 925-225-8900 888-946-7769 http://www.ositis.com	WinProxy	From \$59.95 for three users to \$799.95 for unlimited users	Includes a stealth firewall, centralized antivirus protection, Web-site filtering, user privileges, custom alerting capability, robust user restrictions, outgoing virus and SMTP virus scanning, and support for VPN client; supports Internet Connection Sharing (ICS)
Desktop	Privacyware.com 732-212-8110 http://www.privacyware.com	Privatefirewall 3.0	\$29.95	Personal firewall and intrusion-detection application eliminates unauthorized access to your PC; features packet filtering, port scanning, IP tracking, email protection, and Application Control Engine
Desktop	Sygate Technologies 510-742-2600 877-923-7436 http://www.sygate.com	Sygate Personal Firewall PRO 5.0	Starts at \$39.95	Protects at the network, application, OS, and content security layers; effective against blended attacks; features advanced logging capabilities, flexible configuration, a robust UI, simple update mechanisms, and enhanced networking support
Enterprise		Sygate Secure Enterprise 3.0	Contact vendor for pricing	Defines policies based on user, application, and network behavior; protects every Access Point (AP) and endpoint; ensures that antivirus definitions are up-to-date, security settings are correct, and network requests are valid
Enterprise	Symantec 541-335-7000 800-441-7234 http://www.symantec.com	Symantec Enterprise Firewall 7.0	From \$1995 to \$12,995 per server	Ensures fast, secure connections to the Internet and between networks; controls information entering and leaving the enterprise without slowing approved traffic; meets stringent security, interoperability, and industry certification requirements
Desktop		Symantec Desktop Firewall 2.0	From \$23.70 to \$40.20 per node	Protects remote users from attacks and corporate networks from back-door attacks; monitors inbound and outbound communications; features remote installation and compatibility with leading VPNs
Desktop	Tiny Software 408-919-7360 888-994-8469 http://www.tinysoftware.com	Tiny Personal Firewall 3.0	Free for home use; volume license available	Protects PCs inside and outside the corporate firewall; identifies unauthorized code (including ActiveX controls and Java applets) that makes it through the firewall, then prevents suspicious content from accessing system resources; prevents execution of malicious Microsoft Word macros; supports console-based centralized management
Desktop	Zone Labs 415-341-8200 http://www.zonelabs.com	ZoneAlarm Pro 3.0	\$49.95	Includes ad blocking and cookie control; Program Control feature hardens security; users determine which programs can communicate with the Internet, preventing Trojan horses from transmitting user information
Enterprise		Zone Labs Integrity	\$80 per user (one server license included)	Centrally managed endpoint security protects corporate data; includes personal firewall technology to secure endpoint and remote PCs from infiltration; enables "anywhere, anytime" security administration