

# Desktop Firewalls

*Protect your desktops from intrusion*



I can think of three great reasons why desktop firewalls are necessary. First, FBI studies reveal that roughly 50 percent of all network intrusions originate from within a company's own network and are perpetrated by a company employee. Second, border firewalls protect only the network border—if a border is breached for any reason (e.g., bug, misconfiguration), the networks on either side of the border are at risk, and a desktop firewall could help prevent a deeper intrusion. The third reason stems from the surge in the number of telecommuters: A company's border firewall protects mobile users while they're inside the network, but without a desktop firewall, mobile users are vulnerable to intrusion when they take their mobile device outside the network borders.

rules on half a dozen network-border firewalls is a big chore. To change the rules on dozens, if not hundreds, of desktop firewalls is definitely a tedious task—unless your desktop solution supports centralized management. Some vendors offer centralized distribution and management, and others don't. Be sure to consider the time you'll spend initially installing a desktop firewall and subsequently upgrading the product. If you need to manage relatively few desktop firewalls, you probably can't justify the added cost of centralized management. But also take your budget and the future growth of your network into consideration—if you expect your network to grow quickly, you might want to invest now rather than later in a product that has centralized-management capabilities.

Desktop firewalls serve a purpose similar to the purpose that a safe serves in your home. Your home's doors certainly have locks, which serve as your primary means of intrusion prevention. However, you might also install a safe within your home because locked doors aren't foolproof deterrents.

For the most part, you'll spend less money to install and maintain desktop firewalls than you'll spend to recover from an intrusion. This issue's Buyer's Guide provides an overview of available desktop firewall solutions. Many reasonably priced solutions are on the market today.

Because firewalls are rules-based, configuration and manageability are important features. To change

Even if you aren't concerned about centralized distribution and management, you should be concerned about rule configuration. Some products listed in this Buyer's Guide are more intuitive because they offer automated rule generation. For example, when you open a

desktop application that tries to move traffic to or from the local system, some firewalls recognize that action as a potential vulnerability and ask whether you want to let that traffic pass. The firewall might also ask whether you'd like to make the rule permanent or temporary. Such features make it easier for users to use desktop firewalls, but if you plan to use centralized management, automated rule generation probably won't play a big role in which product you choose.

Another key factor in your decision might concern embedded Intrusion Detection Systems (IDSs). Some desktop firewalls can detect common attack types, such as Denial of Service (DoS) attacks. Some of the listed firewalls can immediately shut down DoS attacks, whereas others simply block all traffic for which no rules exist. Consider the firewall's IDS capability compared with the added cost—you might find the additional security well worth the expense.

You should also remember to consider each product's logging features. Firewall logs are invaluable in forensic analysis, so verify that the logging features of the product you're interested in are adequate.

Desktop firewalls aren't that complex to install, configure, and manage, so you might want to download demos of products that have features that seem to meet your needs. Install each product and take it for a serious test drive—there's really no better way to learn exactly how a product works within your environment.

—Mark Joseph Edwards

InstantDoc ID 22241

**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.win2000mag.com/buyersguide>. To view previous Buyer's Guides on the Web, go to <http://www.win2000mag.com/articles/index.cfm?action=buyersguides>.

Compiled by Sue Cooper

Contact Information	Product Name	Price	Description
<b>Biodata Information Technology</b> 646-485-1770 <a href="http://www.biodata.com">http://www.biodata.com</a>	SPHINX 2.0	\$49	Firewall and VPN that isolates Trojan horses and protects PCs from internal network attacks; filters TCP/IP, IPX, NetBEUI, Address Resolution Protocol (ARP), ICQ, and Internet Control Message Protocol (ICMP); operates at the network device interface specification (NDIS) level; protects your network from DoS attacks, Serial Line IP (SLIP), Point-to-Point Protocol (PPP) links, giant pings, and IP spoofing; can identify images and symbols for URL filtering
<b>F-Secure</b> 408-938-6700 888-432-8233 <a href="http://www.f-secure.com">http://www.f-secure.com</a>	F-Secure Distributed Firewall	\$75	Protects your computer while you connect to the corporate LAN in the office, work through the Internet when you're on the road, or telecommute through a broadband connection
<b>InfoExpress</b> 650-623-0260 <a href="http://www.infoexpress.com">http://www.infoexpress.com</a>	CyberArmor Personal Firewall	Contact vendor for pricing	Policy-based personal firewall for systems that connect to enterprise networks; monitors various network and system operations; protects systems on the corporate network or at a remote location; provides a multilayered security architecture to protect against potential attackers; comprises CyberArmor client, CyberServer, Policy Manager, and CyberConsole
<b>Internet Security Systems</b> 650-532-4100 <a href="http://www.networkice.com">http://www.networkice.com</a>	BlackICE Defender	\$39.95	Anti-intruder system that scans your DSL, cable-modem, or dial-up Internet connection for intruder activity; when the software detects an attempted intrusion, it blocks traffic from that source
<b>Network-1 Security Solutions</b> 781-522-3400 800-638-9751 <a href="http://www.network-1.com">http://www.network-1.com</a>	CyberwallPLUS-WS 7.0	\$5995 for 100 workstations	Provides intrusion detection, inspection, and prevention to actively secure Windows 2000, Windows NT, and Windows 98 desktops, laptops, and workstations; centralized management enables common policies to scale across the extended enterprise network
<b>PGP Security</b> 408-988-3832 888-747-3011 <a href="http://www.pgp.com">http://www.pgp.com</a>	PGPfire	Contact vendor for pricing	Proxy and packet-filtering firewall with more than 35 defined proxies; provides flexible, policy-based security; personal intrusion detection stops intruders and Trojan horses; retrieves new policies from Lightweight Directory Access Protocol (LDAP); lets you build deployment packages with predefined policy configurations; sends alerts in case of attack or when your system is compromised; provides remote system-integrity monitoring

Contact Information	Product Name	Price	Description
<b>Sandbox Security</b> (49) (0) 89-800-70-0 <a href="http://www.sandboxsecurity.com">http://www.sandboxsecurity.com</a>	Secure4U 5.3	\$43 for a single-user license	Desktop firewall that works with NT systems; available in three versions: Secure4U 5.0 Enterprise, Secure4U Single User Professional, and Secure4U Lite; doesn't provide its own VPN client, but supports VPN clients from other vendors
<b>Securitae</b> 408-919-7368 888-994-8469 <a href="http://www.securitae.com">http://www.securitae.com</a>	Centrally Managed Desktop Security (CMDS)	\$39 per desktop	Bidirectional enterprise desktop firewall with intrusion detection and an application filter; prevents network users from gaining unauthorized access; features MD5 signature support to stop Trojan horses; remote administration includes transparent security policy configuration for the end user; features user-created, time-sensitive filtering rules to let the desktop communicate with only specific trusted addresses; reports all desktop activity to a central server that has realtime decision-making capabilities; can send log information to a central syslog server for reporting and analysis; runs on Win2K, NT, Windows Me, and Win9x systems
<b>Sygate Technologies</b> 510-742-2600 <a href="http://www.sygate.com">http://www.sygate.com</a>	Sygate Secure Enterprise 2.0	Contact vendor for pricing	Comprises Sygate Security Agent, Sygate Management Server, and Sygate VPN Enforcer; Sygate Security Agent enforces rule-based security on remote and local enterprise devices based on server-defined policies; the security engine combines an application-centric firewall with intrusion-detection capabilities; Sygate Management Server provides a central point of control over all Sygate Security Agents and lets you define, deploy, and monitor security across the network; Sygate VPN Enforcer ensures that users who connect through VPN gateways are running Sygate Security Agent and have the correct security policy
<b>Symantec</b> 541-334-6054 800-441-7234 <a href="http://www.symantec.com">http://www.symantec.com</a>	Symantec Desktop Firewall 2.0	\$27 per node for 500 nodes	Protects remote and mobile users from intruders; secures corporate networks from backdoor attacks through remote connections; provides remote installation and automatic configuration capabilities; supports VPN environments that are optimized for broadband connections
<b>Zone Labs</b> 415-341-8200 <a href="http://www.zonelabs.com">http://www.zonelabs.com</a>	ZoneAlarm Pro 2.6	\$40	Internet security solution that blocks known and unknown threats to protect a PC against outside intrusions and attacks; features realtime alerts and the ability to tailor security to the individual user