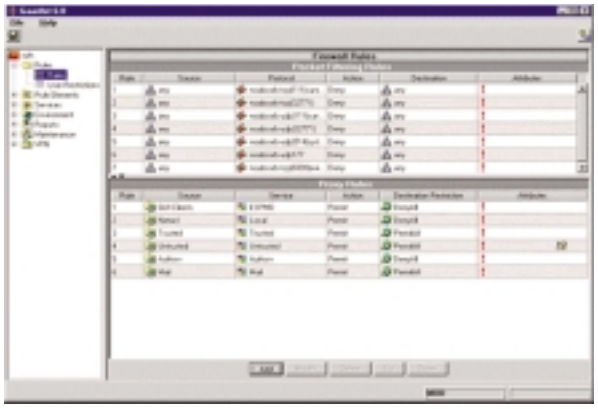
Gauntlet Firewall and VPN 6.0

PGP Security, Protecting Your Privacy

Ultimate Security in One Comprehensive Software Solution

Your network...it's never been more important, complex, and widespread. Today's network is all about business. It's about sharing information—and helping your company succeed in a highly competitive world. In today's on-line economy, you need to ensure the integrity and privacy of all the data that flows into and out of your network infrastructure—for all your users, regardless of location.

Gauntlet Firewall and Gauntlet Virtual Private Networking (VPN) help you meet these formidable challenges—all in a single, comprehensive software solution that includes the award winning McAfee Anti-Virus software, and SurfPatrol's CyberPatrol. Compatible with existing infrastructures, this robust, highly scalable package delivers a cost-effective, easy-to-deploy, and simple-to-manage solution that can reside at single or multiple locations, making it ideal for small, medium, and large networks.



Gauntlet 6.0 lets you add, modify, or delete firewall rules quickly and easily.

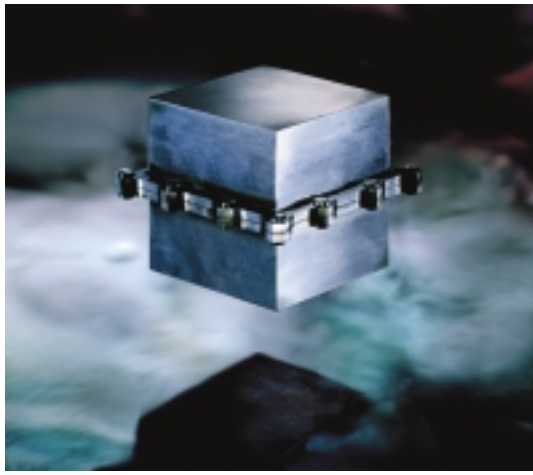
Flexible Performance and Security

Gauntlet Firewall's unique architecture supports the most extensive data inspection methods available today. Including packet screening rules, application proxies, and adaptive proxies, Gauntlet Firewall gives you unparalleled data inspection set-up flexibility. Now you can choose high-data throughput, high security, or a combination of both, which saves you time and overall business costs when designing and implementing a network security policy.

To balance lower-level security concerns with high data throughput needs, you can create packet-screening rules. Gauntlet Firewall supports both traditional "stateless" packet screening, as well as new "forward with reply" packet screening. "Forward with reply" rules remember TCP/IP state connections and once permitted by the rule, all subsequent packets for the connection flow through the firewall until the rule is terminated. Packet-screening rules operate at the network layer of the OSI seven-layer model using source, destination IPs, and ports, as well as protocol IDs, TCP/IP flags, and hardware interfaces to determine if packets can pass through the firewall.

Choosing Security Policy Enforcement

For the utmost security, choose from more than 35 application proxies—the most offered in the industry. Application proxies, transparent to users, authenticate and enforce protocols. Operating at the application layer of the OSI seven-layer model, application proxies can enforce decisions based on specific data, for example, file names, URLs, and sender and recipient names, rather than relying solely upon packet headers as employed in packet-screening rules. This capability enables numerous protective measures when viewing web sites, exchanging email, and transferring files between trusted and untrusted sources using the HTTP, SMTP, and FTP application proxies, giving you the highest possible level of security.



Features & Benefits

- Supports Solaris 8 (32-bit and 64-bit) and HP-UX 11.0 (64-bit only)
- Single Rule View lets administrators see-at-a-glance firewall security policies
- Single sign-on support provides one-time user authentication for access to all network services/applications
- Virtual client identity allows a remote VPN user to access local applications while outside the corporate network
- Tightly integrated Firewall and VPN makes Gauntlet VPN configuration easy
- Enhanced McAfee Auto-Update function provides automatic virus updates
- RTSP Proxy supports RealAudio G2 and Apple QuickTime multimedia applications
- UDP Proxy support allows connectionless-oriented protocols to penetrate the firewall without direct connection to computers behind the firewall
- Enhanced McAfee scanning engine improves anti-virus performance scanning by 40 percent over previous versions
- Improves Hypertext Transfer Protocol (HTTP) performance by 10 percent over previous versions
- Optional Global Enterprise Management System (GEMS) enables global deployment, administration, and management of up to 500 firewalls/VPNs from a single console

PGP SECURITY

A Network Associates Company

Or, you can choose to implement adaptive proxies that combine packet screening speed and the security offered by application proxies. Adaptive proxies switch between operating at the network layer and the application layer of the OSI seven-layer model. Gauntlet's patent-pending adaptive proxy technology performs initial packet checks at the application layer. Once complete, subsequent packets travel through the network layer, thereby increasing data throughput speed. With adaptive proxies, you can maximize both speed and security.

Integrating Data Privacy Throughout Your Network

Gauntlet VPN uses your Internet infrastructure to transmit and receive encrypted data from remote users, trusted business partners, and other corporate sites—without compromising security. A VPN uses encryption to provide sender-to-receiver data integrity and privacy. If the data is intercepted, the unintended recipient receives an unreadable, scrambled message.

Integrated with Gauntlet Firewall, the ICSA IPsec certified Gauntlet VPN software provides interoperability with all other IPsec certified industry offerings. It's this interoperability that makes it easy to integrate Gauntlet VPN into your existing network infrastructure.

Gauntlet VPN supports user authentication via preshared secret- or certificate-based authentication, as well as DES, 3DES, and CAST encryption standards. Gauntlet VPN provides automated support for Certificate Authorities (CAs) from VeriSign, Entrust, and iPlanet (Netscape). To make user access and authentication easier for remote users, Gauntlet VPN is the first commercial VPN to offer virtual client identity. Virtual client identity assigns an internal IP address to remote users, which gives them easy access to corporate resources and eliminates common routing and access privilege problems.

Delivering Expected Firewall Capabilities—and More

Fail-over Protection to Support Mission-critical Firewall Servers

Through Legato Cluster Enterprise software, Gauntlet Firewall supports failover for mission critical firewall servers—24 hours a day, seven days a week. Fail-over protection lets you set up two firewalls—a primary firewall and a secondary firewall. If the primary firewall ever fails, the secondary standby firewall assumes primary firewall duties.

Content Filtering to Define Internet Access

Gauntlet Firewall lets you define your Internet access policy. You can block employees from designated URLs or set specific access parameters. Or, using the CyberPatrol content-filtering program included with Gauntlet, you can simply select the content types you want to filter, and CyberPatrol automatically blocks these URLs.

Load Balancing to Distribute Network Traffic

Gauntlet Firewall supports Cisco, F5, and Radware, which provides certified load balancing to accelerate data throughput. Third-party configuration guides included with Gauntlet, make it easy to set up firewall load balancing.

Authentication Support to Ensure User Identity

Gauntlet Firewall supports all major authentication systems: RADIUS, Secure ID, S/Key, CryptoCard, LDAP, and DSS.

Anti-virus Software to Protect Your Network

Doing business in today's on-line economy doesn't mean you need to put your valuable network resources and data at risk. Gauntlet Firewall works with McAfee Anti-virus software to detect, treat, or discard viruses and other malicious code before they penetrate your network.

Masquerading to Protect Internal Addresses

Gauntlet Firewall provides Internet Protocol (IP) address masquerading to hide private network IP addresses from the outside world. It also converts illegal IP addresses on trusted hosts into legal IP addresses to facilitate Internet communications.

Platform Requirements

For Sun:

Solaris 8 32-bit operating system and 64-bit operating system

- UltraSPARC system or higher
- 128 MB RAM minimum
- 2 GB free disk space
- CD-ROM

For Hewlett Packard:

HP-UX 11.0 64-bit operating system

- HP PA-RISC system
- 256 MB RAM minimum
- 4 GB free disk space
- CD-ROM

For more information on products, worldwide services, and support, contact your authorized PGP Security sales representative or visit us at:

3965 Freedom Circle
Santa Clara, CA 95054-1203
Tel (888) 747-3011
Fax (888) 203-9258

www.pgp.com

PGP SECURITY

A Network Associates Company

1-TNS-UNI-005 6/01