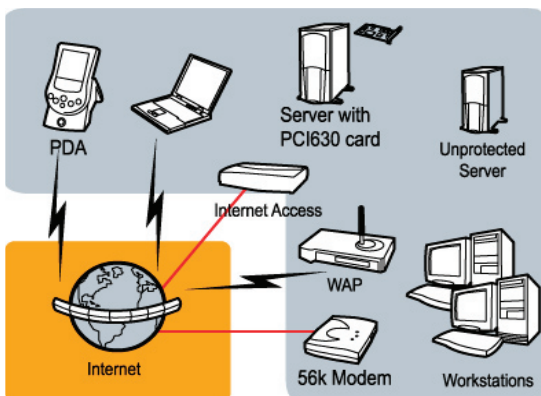


PCI630 Card

VPN/Firewall

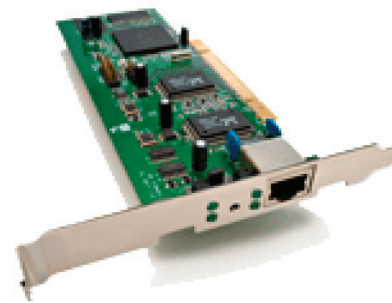
The PCI630 is a cost-effective firewall/VPN solution packaged on a PCI card. By offloading all firewall and VPN processing from the host computer, the PCI630 ensures high performance and throughput with the convenience of remote management and simplified installation. Unlike "co-processing" products, the PCI630 is an advanced, self-contained multi-tasking stateful firewall and VPN appliance. It includes a RISC processor, encryption accelerator for IPsec VPN traffic and two Ethernet interfaces for host and LAN communications. The PCI630 packs the power of an SG firewall/VPN solution while eliminating the cabling, space and power requirements of an external firewall appliance.

Worms and viruses continually exploit popular desktop operating systems making it impossible to connect an unsecured, un-patched computer to the Internet for any amount of time without risking exposure and infection. Businesses can be infected by these worms before being able to download the necessary security patches from vendors such as Microsoft. The primary issue is that the time to locate, download and install critical patches can exceed the infection-free survival time. According to The SANS Institute, survival times of vulnerable Windows XP systems are now as low as 15 to 20 minutes. An SG630 in every computer can alleviate this potentially catastrophic situation.



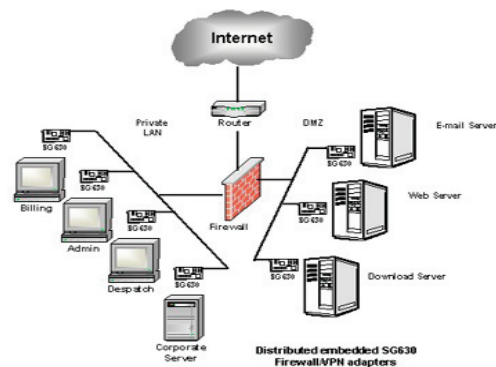
Protect Servers on a DMZ and Hosts within the Data Center

In order to permit transparent public access, Web, e-mail and FTP servers are usually placed on an Internet-facing network or DMZ that imposes relatively few access restrictions. The PCI630 makes it possible to secure each of these servers while preserving transparent access from the Internet. The SG530 can also protect critical servers in the corporate data center or application service provider environment.



Supports a Defense-in-Depth Security Strategy

While perimeter firewalls are effective in stopping incursions from an external network, they cannot prevent attacks that originate within the protected network. Since up to 90% of network attacks are made by disgruntled employees, an effective security policy must include a multi-layered "defense"-in-depth strategy. The PCI630 makes this possible by complementing perimeter defenses with "embedded" firewalls that secure critical servers and host systems.



Multiple PCI630 adapters can be deployed throughout a network to create a robust distributed firewall that continues to operate when host systems fail or become unresponsive. Like all SG firewalls, these can be configured and managed with the SG Central Management System (CMS).

Administrators can define and implement access rules that restrict desktop users to specific servers or network resources based on their user profiles or group affiliations. For example, a human resources manager may be allowed to access employee records on the HR server, but prevented from changing payroll information stored in the accounting system.

In addition, regulatory initiatives, such as the Gramm-Leach-Bliley Act in the United States, impose significant penalties on businesses that fail to address privacy concerns by permitting unauthorized access to personal information. A defense in depth strategy can mitigate this exposure by demonstrating that the organization has conformed to all regulatory requirements.

Wireless & Security

FEATURES:

- Dynamic stateful firewall packaged on a PCI card to secure desktop and server systems
- Fully integrated IPsec VPN
- Full PPTP VPN client and server
- Unrestricted, unlimited user license
- Web console for configuration and management
- Fully interoperable with other SG appliances and other standards-based security devices
- No third-party client software required

PCI630 Card SPECIFICATIONS:

- ICSA-certified dynamic firewall
- Routing
- DHCP - client and server
- PPPoE (for ADSL support)
- NAT - static and dynamic
- NAT/PAT - port forwarding
- Connection sharing
- Anti-intrusion
- Logging (local and remote)
- Traffic shaping (QoS)
- IP aliases
- NTP client and server
- Web management
- CLI (Telnet) management
- Initial setup via either static IP address or dynamic IP address (DHCP client)
- Bridging (802.1d)
- Administration user accounts
- RADIUS/TACACS+
- DNS enhanced caching, masquerading, proxy, multiple DNS server proxying
- RIP, RIPv2
- 100 Mbps routed throughput
- 100 Mbps PPPoE throughput
- 95 Mbps firewall performance
- Status LEDs
- Network port - 1x10/100BaseT
- Memory - 4Mb Flash, 16Mb RAM
- Real time clock
- Power - powered by PCI slot
- Operating temperature 0C to 40C
- Storage temperature -20C to 70C
- Humidity 0 to 95%, non-condensing
- Certification - home and office
- VPN - IPsec
- VPNC-certified interoperability
- Peer-to-peer (initiate and terminate)

RECOMMENDED FOR:

- Security-conscious businesses that wish to deploy a defense-in-depth security strategy
- Environments where the integrity of the host server operating environment cannot be controlled or trusted
- Data centers with Web and application server farms
- Co-location/Web hosting center
- Organizations seeking to demonstrate compliance with regulatory requirements concerning privacy and access to personal information

- Supports aggressive mode
- Dead peer detection
- Compression (deflate/gzip type algorithm)
- DES 56-bit, 3DES 168-bit, AES 256-bit encryption
- Hashes HMAC - MD5 and SHA-1 authentication
- IKE/ISAKMP Diffie-Hellman key exchange
- Diffie-Hellman Groups (1,2,5) and Oakley Groups (14,15,16) to 4096-bits
- X.509 certificates DER, PEM formats
- Pre-shared secrets
- Dynamic IP address end-points
- Dynamic DNS IPsec support
- Authentication up to 2048-bit for RSA key signatures
- Multiple subnets
- NAT traversal
- VPN - L2TP
- IPsec config Wizard
- L2TP over IPsec
- Client: NAT, default route via L2TP
- Server: specify client IP address range
- VPN - PPTP
- v2 client and server
- Pass-through mode also
- MPPE 40 to 128-bit RC4 encryption
- PAP/CHAP/MS CHAPv2 authentication
- L2TP & GRE tunneling extensions
- Warranty - 1 year*

*Except where required to be 2 years by law

Supported Platforms:

- Any PCI-based host, independent of host operating system
- Tested platforms include:
- Windows 2000 server and client
- Windows 2003 server
- Windows XP
- Linux