

www.securecomputing.com

Secure Computing® has been solving the most difficult network and application security challenges for over 20 years. We help our customers create trusted environments both inside and outside their organizations.



Highlights

Compact, powerful, rack-mounted, and secure!

- **Multi-function UTM (Unified Threat Management) security appliance can replace five, six, or more security systems**
- **Lower total cost of ownership for your security infrastructure**
- **The broadest set of attack protections against external attacks**
- **Complete security controls over inbound and outbound employee access**
- **Enterprise strong® appliance technology**
- **High performance, multi-gigabit throughput**
- **Manage hundreds of security appliances with Sidewinder G2® Enterprise Manager**

"Consolidating multiple security functions at a single point within the enterprise network is an increasingly common strategy for IT decision makers. One common aggregation point in the network is at the Internet gateway, where firewalls, VPN termination, and virus filtering are all deployed. Secure Computing's Sidewinder G2 provides a single platform for all of these capabilities and more."

Aberdeen Group
Eric Hemmendinger
Research Director for
security and privacy



SWBR-01-E

Sidewinder G2 Security Appliance

Consolidating the widest variety of Internet security functions in one system

Sidewinder G2 Security Appliance

The Sidewinder G2® Security Appliance is the most comprehensive gateway security appliance in the world, with the strongest credentials of any leading all-in-one firewall or Unified Threat Management security appliance (as tracked by IDC). This market leading Internet security appliance delivers protections for your applications and networks against the entire threat matrix—and at Gigabit speeds. Our appliance consolidates the widest variety of gateway security functions in one system, reducing the complexity of managing a total perimeter security solution. These functions include our unprecedented Application Defenses™ firewall with embedded anti-virus, anti-spam, URL filtering, HTTPS/SSL accelerated termination, traffic anomaly detection, IDS/IPS, and a whole host of other critical protective features.

Sidewinder G2 includes the only firewall that has never had a CERT advisory posted against it in over 10 years—a truly remarkable accomplishment. It recently achieved the highest level of EAL4+ Common Criteria certification possible (far stronger than other vendors' EAL4 ratings). As a result, your Sidewinder G2 provides you with defense-in-depth protections against the entire threat matrix around the clock.

Application Defenses

Secure Computing's Application Defenses strategy is at the heart of the multi-layered defense-in-depth design of the Sidewinder G2 Security Appliance. The ability to face and defeat both known and unknown attacks is the strength of the Sidewinder G2 Application Defenses capabilities. This is achieved through a three-tiered defense-in-depth approach: 1) *Application awareness* ensures in-depth knowledge of a complete breadth of applications; 2) *Application control* enables granular policy controls on a per-rule basis; and 3) *Attack protection* provides in-depth detection of attacks from layer 3 through 7.

Defense in depth

Defense-in-depth combines multiple technologies to accomplish this fundamental strategy, including the following:

- The world's strongest firewall that has never been compromised
- Multi-protocol content filtering, from layer 3 to layer 7
- Both stateful inspection and simple packet filtering engines
- Protocol anomaly detection; traffic anomaly protection
- Advanced network cloaking techniques
- Application and stateful inspection firewall
- Secure MAIL, Web, and DNS gateway services
- Embedded anti-spam* and anti-virus* engines (through industry leading technology partnerships)
- Hardware accelerated HTTPS/SSL termination*
- Both IPSec and clientless SSL* VPN services
- Integrated IDS with real-time alerts and automated Strikeback® response
- High-speed, intrusion preventing application proxies
- Outbound Web access controls with IM & P2P blocking, as well as industry-leading SmartFilter® URL filtering*

Protect yourself against viruses, worms, spyware, DoS attacks, phishing, and more

The Sidewinder G2 defense starts with world-class firewall protection, comprised of hybrid filtering technology. Traffic anomaly detection is part of the intelligence of the Sidewinder G2 Security Appliance, detecting any unusual activity or traffic patterns. Web and mail content inspection is also an important component. Newer viruses and worms, including zero-day worms, often come disguised within e-mail or Web pages. Our anti-virus, anti-spam, mail content scanning, and Web filtering technology protects against these sorts of attacks, as well as related threats of phishing attacks and malware/spyware being secretly injected into your network. Examining e-mail content and file attachments stops malicious software from getting in and keyword & character filters can mitigate trade secrets from getting out. Delivering a full suite of protection for both inbound and outbound traffic truly sets Sidewinder G2 apart.

For DoS attacks, the system's Strikeback detection and automated defense mechanism identifies a DoS attack and drops the attack source IP into a virtual "black hole." This keeps the attack outside the network, and ensures that any future DoS attempts from that address are immediately discarded.

*Items noted with asterisk are add-on modules and must be purchased separately.

Our SecureOS operating system prevents root access and other attacks

At its never-been-compromised core, the Sidewinder G2 Security Appliance runs on our high-speed, high-assurance SecureOS® operating system with patented Type Enforcement® technology.

Type Enforcement technology protects everything in the system; every file, every directory, every application, the hardware's software drivers, the operating system, and against the hacker's dream—root access. This technology prevents the installation of malicious software, buffer overflow attacks, or gaining root access. In contrast to competitive security systems who have many of these vulnerabilities as documented in CERT advisories, ours has none.

Following our heritage of products that have achieved the highest certifications, Sidewinder G2 is ICSA certified and Common Criteria EAL4+ certified against the application firewall protection profile.



Full rack of Sidewinder G2 Security Appliance

Both clientless SSL and IPsec VPN remote access supported

Through the Internet, the enterprise has transcended physical boundaries and has transformed into a more virtual proposition connecting branch offices, telecommuting employees, partners, and customers. Securing these connections is of utmost importance.

Offering both IPsec and clientless SSL VPN solutions, Sidewinder G2 accommodates every type of virtual environment. IPsec is best suited for branch office connectivity; but in an e-commerce environment where there may be thousands, or even millions of connections, a thick-client option is impractical. For these environments, Sidewinder G2's clientless SSL VPN offers simple, reliable, anywhere access to Web applications and Outlook mail. No thick client is required because SSL is embedded in every modern Web browser. And for strong two-factor authentication, choose from Secure Computing's SafeWord® solutions to positively confirm user identity before extending remote access privileges to anyone.

Why IT professionals choose the Sidewinder G2 Security Appliance

With the need for security rising as attacks become more sophisticated and complex, IT professionals face an increasing challenge. An entirely new class of application-specific threats has arisen, circumventing commonly deployed security measures. A growing number of new security products, all designed to meet the evolving threat, are competing for the time and attention of an already over-burdened IT community. To address it all, security managers must now manage an array of multiple security products, including firewalls, anti-virus, anti-spam, VPN, and Web access filtering systems, each with their own management interface, log files, maintenance tasks, and technical support issues.

Configuration errors in security solutions are the greatest vulnerability most networks face today. Moreover, new government regulations (like Sarbanes Oxley and HIPAA), consumer concerns, and demands for accessibility to information must also be addressed. Secure Computing's Sidewinder G2 Security Appliance meets these needs of the rapidly evolving security marketplace head-on. Able to drop seamlessly into any IP network, and interoperable with standard Microsoft services like Active Directory, Sidewinder G2 is an all-in-one security gateway that unifies management of multiple security functions within a single appliance. It greatly reduces the number of point products the IT security manager must buy, deploy, learn, administer, update, and depend upon for their perimeter protection. With 8 appliance platforms to choose from, the new Sidewinder G2 delivers the scalability and strength you need, from your smallest remote office to your highest bandwidth location.

Advanced technology for the IT professional

Sidewinder G2's underlying hardware and networking technology is designed to meet the rigorous requirements of today's IT professionals. Preinstalled and pretuned for ease of installation, the Sidewinder G2 line of high-performance, rack-mounted appliance platforms provides an out-of-box security solution that drops seamlessly into any IP network.

Network-friendly, Sidewinder G2 includes built-in support for all major network "housekeeping" protocols (SNMP, Syslog, LDAP, Active Directory, Radius, OSPF, RIP, NTP, and more). Sidewinder G2 has also begun to support IPv6 networking interoperability for customers adopting this new standard. With its simple Power-It-On!™ deployment features, its remote backup/restore capabilities, centralized logging, and complete health/audit monitoring, Sidewinder G2 is the perfect choice for any organization, especially where remote unattended "lights out" installations are required.

Scalable and highly available

The security appliance line ranges from model 110 (small form factor), to seven additional 1U & 2U model platforms, including our most powerful enterprise-class 4U model 4150. Multi-gigabit stateful inspection and next generation, parallel processing algorithms for application proxies offer gigabit throughput. Sidewinder G2 exclusively integrates Intel network adapters, allowing significant throughput improvements by offloading "checksum" processing from the CPU. Additional performance enhancing features include Jumbo Frame support. Active/Active appliances in a high-availability pair deliver the performance of two appliances performing as one, providing continuous operation 24 x 7 x 365. If you need even more power, the Sidewinder G2's unique one-to-many cluster-management tools make scaling Application Defenses to multi-gigabit rates with rack-clusters as easy as managing a single appliance.

Downtime is not tolerated, so when it's time to upgrade or add features, new software is delivered to you automatically via the Internet. Sidewinder G2 authenticates, self-checks, and even self-installs upgrades for your system (operating system and all application software) with just a single 'click' per your schedule.



POWER-IT-ON!

1



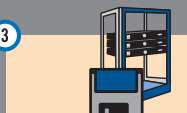
The rack-dense Sidewinder G2 Security Appliance arrives pre-loaded

2



Sit at your desk with the Windows® configuration wizard and answer 15 simple questions, then save to floppy

3



Insert the configuration diskette for the Power-It-On! experience

4



Just a few minutes later, the G2 Security Appliance beeps 4 times to let you know it's up and protecting your network

It's that easy to deploy the world's strongest Security Appliance

Easy to install, easy to own, and always secure

It takes just a few minutes to decide how you want your Sidewinder G2 to work. The Sidewinder G2 Security Appliance uses a Windows-based configuration wizard that asks you a few basic questions about your network and security policy to get you up and running quickly.

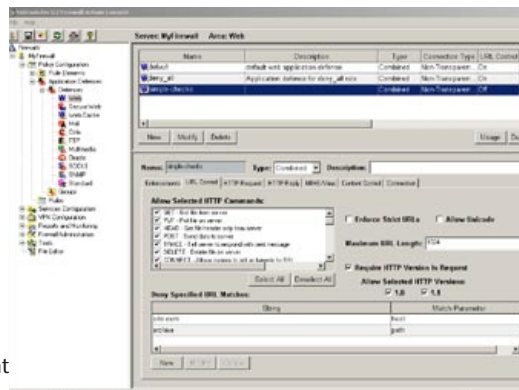
Sidewinder G2 lets you say "goodbye" to emergency security patches, resulting in a much lower total-cost-of-ownership (TCO) as compared to competitive products where patches are regularly required to patch the security system and/or underlying operating system. No one has ever found or reported a flaw on Secure Computing's SecureOS and Type Enforcement technology that required an emergency security patch. Secure Computing's patented security defenses have stood the test of time, defending against even the highest-grade attacks, whether known or unknown. Common Criteria-certified, plus selection by the world's most demanding security organizations, validates that your Sidewinder G2 technology will protect you against both today's and tomorrow's evolving threats.

Policy management

The framework of a good security environment is its underlying policy. Sidewinder G2 facilitates the creation and administration of security policy through a variety of tools:

- Secure Windows-based graphical user interface protected with SSL
- Secure SSH Telnet
- Sidewinder G2 Enterprise Manager (SecureOS-based central management appliance)

All-in-one hybrid security in a single, unified user interface lets you create and distribute policies, reuse policy objects, and modify rules for multiple security functions easily. Using the Sidewinder G2 Enterprise Manager, you can manage up to 400 appliances from a single console, making policy changes on hundreds of appliances instantly with 'object substitution.' Advanced central management features such as delegated administration, policy rollback, and policy adherence facilities are also included.



Single unified user interface for multiple security functions.

The Sidewinder G2 Security Appliance also offers true forensic-quality detail in its audit subsystem, and consolidates the audit streams of multiple security technologies to make life easier for the IT security staff.

Technical support, warranty, and training

Secure Computing's SecureSupport® center provides "Live Answer" assistance 24 hours a day so you can talk to people day or night, not machines. We offer a single point of contact for hardware warranty, operating system, and security appliance administration questions. Secure Computing can also provide onsite support to address any special needs. Numerous training options are available including classroom training or, if travel is not desirable, you can simply log in to Secure Computing's unique e-training facility where administrator training is delivered right to your browser.



Model 110 & 210 - small form factor platform



Model 410 & 510 - small 1U platform



Model 1100 - enterprise 1U platform



Model 2100 & 2150 - 2U platform



Model 4150 - 4U platform

VPN compatibility

- IPSec and IKE protocol compliance verified through ICSA certification
- Extended IKE Authentication (XAUTH) Version 6.0
- X.509 version 3 certificates
- Simple Certificate Enrollment Protocol (SCEP)
- Support for Baltimore, Entrust, Verisign, Netscape, and Microsoft certificates
- Tunnel or transport mode security AES, DES, Triple-DES, MD5, SHA-1 algorithms, and CAST
- PKCS #7, #10, and #12
- FIPS PUB 46-3
- FIPS PUB 140-1
- FIPS PUB 180-1

Administration system requirements

- OS - MS Windows 2000 or XP
- CPU - Intel (1 GHz minimum)
- Memory - 512 MB minimum
- Drives - 300 MB of available disk space, 3.5" 1.44 MB floppy disk drive, CD-ROM drive
- Monitor - 1024 x 768 or higher
- Network interface card - access to your firewall network
- Browser - Internet Explorer 4 or later; Netscape 4.x or later



Physical Specs

	110-small form factor	210-small form factor	410 - small 1U	510 - small 1U	1100 - enterprise 1U	2100 - 2U	4150 - 4U
Ethernet interfaces (base/max)	3/5 - 10/100	3/5 - 10/100	3/4 - 10/100 & Gig	4/4 - Gigabit	4/8 - Gigabit	6/14 - Gigabit	12/24 - Gigabit
Fiber interfaces (option)	N/A	N/A	2	2	2	6	10
User licenses	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unlimited	Unlimited	Unlimited
Recommended users/sizing	Small/Remote office up to 75 users	Small-Medium office up to 150 users	Small-Medium office up to 300 users	Medium Office up to 600 users	Medium to large office	Large office	Enterprise Office
Max. outbound IP addresses	100	200	400	700	Unlimited	Unlimited	Unlimited
Base supported Application Defenses™ protections add-on modules	1 (up to 3 w/performance options)	1 (up to 3 w/performance options)	1 (up to 3 w/performance options)	2 (up to 3 w/performance option)	2 (up to 4 w/performance option)	All 4	All 4
Performance upgrades	2 options	2 options	2 options	1 option	1 option	1 option	1 option
RAID	N/A	N/A	N/A	N/A	RAID 1	RAID 5	N/A
Power supply	Single	Single	Single	Single	Single - Dual option	Dual	Dual

Performance

Stateful Inspection throughput	75 Mbps	170 Mbps	200 Mbps	500 Mbps	1 Gbps	1.2 Gbps	2.4 Gbps
Concurrent connections	10,000 +	50,000	100,000	400,000	500,000 +	750,000+	1,000,000+
Application filtering throughput	75 Mbps	170 Mbps	200 Mbps	200 Mbps	500 Mbps	700 Mbps	850 Mbps
IPSec VPN AES throughput/concurrent connections	60 Mbps/75	80 Mbps/125	160 Mbps/200	160 Mbps/200	300 Mbps/350	300 Mbps/500	350 Mbps/500

Highlights

Three-year hardware warranty included	Next-business-day, onsite parts replacement warranty included with all appliances.						
24 x 7 "live answer" support	Available SecureSupport includes rapid response phone, e-mail, ticket tracking, Web knowledge base, customer escalation.						
Firewall with Application Defenses	Hybrid firewall that provides stateful inspection and deep application-level filters.						
Content filtering & MIME type filtering	Integrated MIME type filters and IM, P2P, Java, and ActiveX blocking.						
Secure DNS & email gateway	Secured DNS server for protecting internal DNS services. Mail filters for key words, phrases, message size, and attachment types.						
Intrusion detection & prevention, DoS, & traffic anomaly detection	Strikeback® intrusion detection, automated response, and real-time alerts; blocks denial of service attacks; protocol anomaly protection and analysis.						
IPSec VPN	ICSA-certified VPN gateway with SoftRemote® VPN client for remote access.						
SecureOS®, protects against known & unknown attacks	High-speed operating system with patented Type Enforcement® technology. No root access possible. Never been compromised. No CERT advisories ever.						
Auto-updates	Feature patches and upgrades automatically downloaded and applied at administrator's preference.						
Cluster management	High-bandwidth cluster management for up to five units managed as one.						
High availability	Stateful, active-active high availability pairs managed as one unit.						
Power-It-On!™ deployment	Wizard-driven start-up simplifies deployment process and gets the appliance up and running in about seven minutes.						
Enterprise Management	Intuitive Windows-based GUI for managing multiple security functions. Compatible with SideWinder G2® Enterprise Manager for managing up to 400 appliances.						
Embedded anti-virus*	Anti-virus filtering for e-mail and Web.						
Embedded anti-spam*	Anti-spam engine captures and analyzes SMTP email using algorithmic technology and includes phishing attack protections.						
Web filtering*	Integrated SmartFilter® URL filtering.						
SSL termination and Clientless - SSL VPN*	Hardware-accelerated SSL decrypts Web traffic for clientless VPN and Application Defense filtering.						

*Add-on modules must be purchased separately. Performance statistics are current as of February 2005 and may include available performance upgrade options.

Secure Computing Corporation: www.securecomputing.com sales@securecomputing.com



Corporate Headquarters
4810 Harwood Road
San Jose, CA 95124 USA
Tel: +1.800.379.4944
Tel: +1.408.979.6100
Fax: +1.408.979.6501

European Headquarters
East Wing, Piper House
Hatch Lane
Windsor SL4 3QP UK
Tel: +44.1753.410900
Fax: +44.1753.410901

Asia/Pacific Headquarters
1604-S MLC Tower
248 Queen's Road East
Wan Chai Hong Kong
Tel: +852.2520.2422
Fax: +852.2587.1333

Japan Headquarters
1st Fl. Bldg.
2-2-1 Toranomon, Minato-ku
Tokyo 105-0001 Japan
Tel: +81.3.5114.8224
Fax: +81.3.5114.8226

© February 2005. Secure Computing Corporation. All Rights Reserved. Secure Computing, SafeWord, SideWinder, SmartFilter, Type Enforcement, Softoken, SecureSupport, SecureOS, MobiPass, G2 Firewall, Bes, SideWinder G2, enterprise strong, PremierAccess, and Strikeback are trademarks of Secure Computing Corporation, registered in the U.S. Patent and Trademark Office and in other countries. G2 Enterprise Manager, Application Defense, RemoteAccess, On-Box, PowerIt-On!, and PowerIt-On! are trademarks of Secure Computing Corporation. All other trademarks used herein belong to their respective owners.