SECURE COMPUTING

www.securecomputing.com

NETWORK GATEWAY SECURITY
Product Overview

Sidewinder Product Family

Secure Computing® is a global leader in Enterprise Gateway Security solutions. Powered by our TrustedSource™ technology, our award-winning portfolio of solutions help our customers created trusted environments inside and outside their organizations.

Highlights

- **Gigabit-speed application firewall**
- **3-4 times faster than leading "deep inspection" firewalls**
- **Combines 5 or more individual security systems in one appliance**
- **Only firewall with reputation-based global intelligence**
- **Next-generation IPS (intrusion prevention) with ASIC acceleration**
- **Positive security model: Automatically stop zero-hour attacks**
- **Real-time event monitoring, alerting, and reporting**

COMMON CRITERIA EAL4+ CERTIFIED

"Products based upon the positive security model dramatically reduce an organization's attack surface by automatically eliminating exposure to all sorts of attacks – unknown as well as known. Unless countermeasures capable of preventing unknown attacks are employed, the result will be steadily increasing occurrences of successful attacks!"

Unknown Attacks: A Clear and Growing Danger
Mark Bouchard–Missing Link Security Services, LLC

SECURE COMPUTING Sidewinder Network Gateway Security

Web vers. 7/18/07

Sidewinder Appliances: Industry's Strongest Firewall Protection

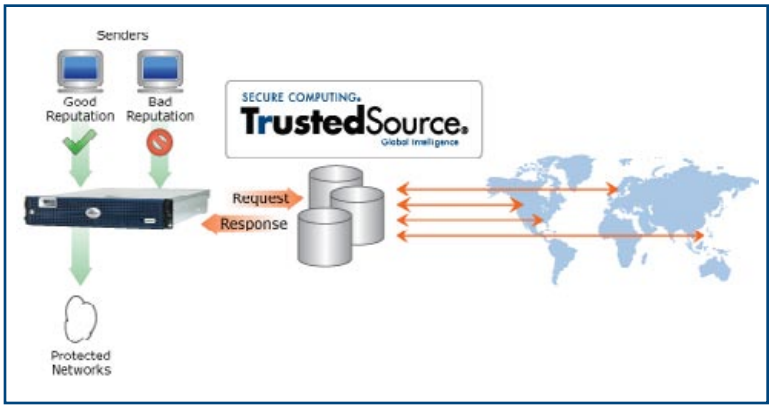
Consolidating all major perimeter security functions in one system, Secure Computing's Sidewinder® Network Gateway Security appliance is the strongest self-defending perimeter firewall in the world. Built with a comprehensive combination of high-speed application proxies, TrustedSource™ reputation-based global intelligence, and signature-based security services, Sidewinder defends networks and Internet-facing applications from all types of malicious threats, both known and unknown. Enterprises use Sidewinder to secure access to their networks and protect Internet-facing applications, as well as monitor and manage employee use of the Internet, kill hidden attacks in packet streams, block viruses and spyware in file transfers, and create a forensic-quality audit trail for regulatory compliance and reporting.

IDC, a leading analyst firm, defines Sidewinder as a Unified Threat Management (UTM) security appliance. These security appliances integrate multiple security functions with a firewall under one unified management to improve the security posture of networks while simultaneously reducing equipment and administration costs. Broadly deployed in the largest government and corporate networks in the world, Sidewinder is a multi-function firewall appliance that delivers true enterprise-class features and performance, while most other UTM devices are only appropriate for small to mid-sized organizations. It's multi-gigabit performance capabilities and hardware monitoring and redundancy features allow its multiple security functions to run simultaneously, including its multi-layer firewall, TrustedSource reputation services, ASICs-accelerated IPS, anti-virus, anti-spyware, anti-spam, URL filtering/blocking, VPN encryption services, and more.

Security products should be more secure than the work stations, network devices, and servers that they protect. Sidewinder is the only network gateway appliance to have ever achieved the pre-eminent EAL4+ Common Criteria certification for application layer firewalls. Its unique, unequalled CERT advisory record and zero emergency security patches over the 11+ year life of Sidewinder set it apart from all other enterprise firewalls. Sidewinder customers have never been interrupted by emergency security patch projects so common place in the security industry today where security products themselves need to be continually patched for security vulnerabilities. Not having to apply emergency security patches to Sidewinder delivers *tremendous time savings* and is yet one more reason why Sidewinder's self-defending design is so confidently trusted by our customers.

TrustedSource Reputation-Based Security with Global-Intelligence

Sidewinder is the *first and only* firewall that offers reputation-based security for the edge of networks. Sidewinder now incorporates a bi-directional global intelligence feed from Secure Computing's industry-leading reputation service, TrustedSource. This enables Sidewinder to make proactive security decisions based on the real-time known behavior of IP addresses worldwide.



Our TrustedSource global intelligence centers analyze over 100 billion mail messages worldwide each month, and continually assign each IP sender a numeric reputation score ranging from good to bad. This dynamic scoring system provides Sidewinder with a unique new layer of comprehensive protection.

Sidewinder customers benefit from this real-time data feed reputation service because it allows Sidewinder appliances to automatically drop huge volumes of unwanted and infected mail at

Our SecureOS Operating System Delivers the Most Hardened Appliance

Sidewinder is uniquely built to defend itself from future unknown attacks. At its never-been-compromised core, the Sidewinder Network Gateway runs on our high-speed, high-assurance SecureOS® operating system with patented Type Enforcement® technology.

Type Enforcement technology protects everything in the Sidewinder system: every file, every directory, every hosted application, as well as defends against the hacker's dream goal—"get root access." SecureOS also prevents the execution of foreign software, buffer overflows, and other known and unknown attacks. That's why Sidewinder has gained a word-of-mouth reputation as being the world's strongest firewall.

Complementary Products:

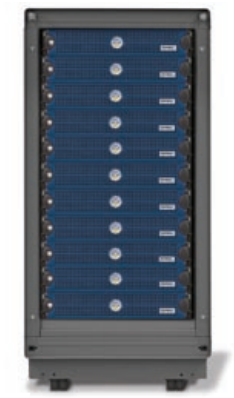
SECURE COMPUTING® TrustedSource™ Global Intelligence

SECURE COMPUTING® SmartFilter® Web Gateway Security

SECURE COMPUTING® SafeWord® Identity and Access Management

SECURE COMPUTING® Webwasher® Web Gateway Security

SECURE COMPUTING® IronMail® Messaging Gateway Security



Full rack of Sidewinder appliances

the outer edge of our customers' networks. By rejecting connections from known bad senders of spam, or machines that have been taken over and turned into malware-distributing zombies, Sidewinder can eliminate well over 60% of the ever-increasing mail traffic flooding into today's networks. As a result, huge volumes of unwanted mail can be rejected before it reaches your critical mail servers, providing the following high-value benefits:

- Saves on messaging servers' processing time
- Increases available network bandwidth
- Minimizes networking infrastructure expenses
- Improves overall security posture

Defending Applications and the Positive Model of Security

Two defensive approaches against both known and unknown attacks exist today: The negative security model and the positive security model.

The **negative security model** approach identifies bits of traffic already known to be threatening. Anti-virus and intrusion detection/prevention systems are classic examples of this approach, which both depend upon checking traffic flows against attack signatures. With threats increasing at such a rapid pace, this results in less and less time to react to new attacks, and a steady increase of successful attacks over time. The **positive security model** approach, on the other hand, understands and allows only legitimate, acceptable traffic elements and denies everything else. Current estimates say about 70% of all new malware is focused on application-oriented vulnerabilities, and network-layer firewalls were never designed to deeply protect against this method of delivering attacks.

At the heart of Sidewinder, are over 40 application-specific proxies, including deeply aware application flitering for email, Web, Oracle, Citrix, SQL, VoIP, and other high-use Internet protocols. Each proxy can be configured according to the customer's unique use of their applications, which forms the baseline against which all traffic is checked. These intelligent application-specific filters enable you to tightly define only the allowed use of these applications (on a per-rule basis) and then pass only the allowed traffic through at gigabit speeds. Even the default application security configurations straight out-of-the-box have zero tolerance for suspicious and undesirable traffic that does not strictly conform to safe industry practice or RFC compliance, including the ability to filter out unidentified threats even before security patches or attack signatures are available.

Application proxies are simply the best layer 7 security technology when both high-speed and high-security are required. To learn more about the positive model of security and application proxies, please visit our Secure Computing Web site.

IPS Signature-Based Application Defenses

Sidewinder excels at stopping unknown attacks with our application-specific proxies and TrustedSource proactive global intelligence services. Sidewinder also includes best-of-breed signature-based defenses for over 200,000 known viruses and attacks. Out-of-the-box, all signature-based services are tightly integrated into the appliance software. You simply switch these services on to keep signatures updated automatically at the network perimeter to ensure that known threats do not leak inside the network. What sets Sidewinder's virus and IPS attack signature-based security services apart is our commitment to offering only best-of-breed attack signature services from industry security leaders. Compare our best-of-breed solutions to many others who use open-source and/or poorly updated and maintained signature services.

Poor and incomplete implementations of IPS services within firewalls today are the norm. In stark contrast, the granular ability within Sidewinder to apply highly current, pre-organized service groups of IPS signatures against specific connection flows on a rule-by-rule basis puts Sidewinder in an IPS class by itself. In addition, Sidewinder benefits from rapid-response global analysis sensors all around the Internet that aggressively analyze Internet traffic for newly emerging attacks twenty-four hours a day. The global IPS service automatically builds IPS attack signature candidates for packets analyzed to be malicious, and at speeds and accuracy levels far outpacing general industry practice. Following immediate human review of all automatically constructed IPS signature candidates, the new attack signatures are broadcast to Sidewinder appliances around the world, strengthening our customers' ability to rapidly defend against all classes of Internet threats—both known and unknown.

Editor's Choice Award Communications Week 2006

COMMON CRITERIA EAL4+ CERTIFIED

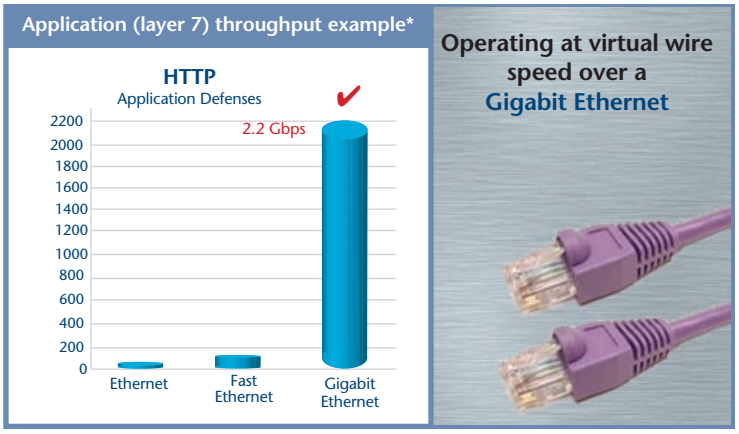
Best MidMarket Products 2006

SC Magazine Awards 2007 Winner

ICSA labs Certified

Why IT Professionals Choose Sidewinder Network Gateway Security

Sidewinder's underlying hardware and networking technology is designed to meet the rigorous requirements of today's most demanding IT professionals. Sidewinder appliances are always current to the latest state-of-the art technology including 64-bit architectures, Intel dual-core processors, RAID and redundant power supplies, active/active high availability pairs, comprehensive hardware diagnostics tools, and more. Pre-installed and pre-tuned for ease of installation, the Sidewinder line of high-performance, rack-mounted appliance platforms provide an out-of-box security solution that drops seamlessly into any IP network.



The Sidewinder appliance line includes nine models ranging from the cost-effective branch office model 110 (mini-1U platform), to our most powerful enterprise model 4150 (5U platform), to a new rugged appliance for heavy industry and military applications. Please reference our separate datasheet on the rugged appliance options.

Active/active appliances in a high-availability (HA) 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's unique one-to-many cluster-management tools make scaling consolidated attack protections to multi-gigabit rates with rack-clusters as easy as managing a single appliance.

New feature patch updates are delivered to you automatically via the Internet. Sidewinder authenticates, self-checks, and even self-installs upgrades for your system with just a single 'click' per your schedule.

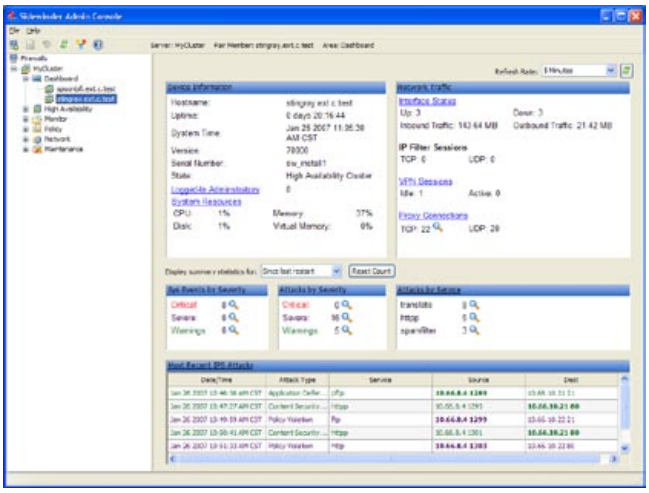
Event Monitoring, System Management, and Regulatory Compliance

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

- Feature rich and easy Windows-based user interface
- Central management appliances (optional)
- Central event monitoring and reporting software (optional)

Sidewinder helps you meet today's stringent government compliance regulations because it is the most highly credentialed firewall in the Common Criteria community. And Sidewinder's complementary SecurityReporter product generates over 800 easy-to-understand reports, many designed specifically for SOX, GLBA, and HIPAA.

To learn more, please visit our Secure Computing Web site.



Real-time attack monitoring dashboard

110/210 - mini 1U platform

410/510 - small 1U platform

1100 - enterprise 1U platform

2100/2150 - 2U platform

4150 - 5U platform

IPSec 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 140-2
- 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 - mini 1U	 210 - mini 1U	 410 - small 1U	 510 - small 1U	 1100 - enterprise 1U	 2100 - 2U	 2150 - 2U	 4150 - 5U
Ethernet interfaces (base/max)	4 -10/100	4 -10/100	4/6 - 10/100	4/6 – Gigabit	8/14 – Gigabit	8/20 - Gigabit	8/20 - Gigabit	14/26 - Gigabit
Fiber interfaces option (max)	N/A	N/A	4	4	4	6	6	6
User licenses	Unrestricted	Unrestricted	Unrestricted	Unrestricted	Unlimited	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	Medium to large office	Large office	Enterprise Office
Max. outbound IP addresses	100	200	400	700	Unlimited	Unlimited	Unlimited	Unlimited
Base supported Application Defenses™ protections add-on modules	1 (up to 3 w/perfor-mance options)	2 (up to 3 w/perfor-mance option)	1 (up to 3 w/perfor-mance options)	2 (up to 3 w/per-formance option)	2 (up to 4 w/per-formance option)	2 (up to 4 with performance option	2 (up to 4 w/perfor-mance option)	All 4
Performance upgrades	2 options	1 option	2 options	1 option	1 option	N/A	1 option	N/A
RAID	N/A	N/A	N/A	N/A	RAID 1	RAID 1	RAID 5	RAID 5
Power supply	Single	Single	Single	Single	Single - Dual option	Single - Dual option	Dual	Dual

Performance								
Packet filtering throughput (TCP)	150 Mbps	180 Mbps	275 Mbps	650 Mbps	1.6 Gbps	1.8 Gbps	2.6 Gbps	3.2 Gbps
Stateful throughput	140 Mbps	170 Mbps	250 Mbps	600 Mbps	1.5 Gbps	1.7 Gbps	2.4 Gbps	3 Gbps
Concurrent connections	10,000 +	50,000	100,000	500,000	1,000,000	1,200,000	1,600,000	2,000,000
Application filtering throughput	100 Mbps	140 Mbps	230 Mbps	250 Mbps	1.2 Gbps	1.3 Gbps	1.8 Gbps	2.25 Gbps
IPSec VPN AES throughput/concurrent connections	60 Mbps/75	80 Mbps/125	160 Mbps/200	160 Mbps/250	240 Mbps/350	300 Mbps/400	350 Mbps/500	400 Mbps/600

Highlights		
Three-year hardware warranty included	Next-business-day, onsite parts replacement warranty with models 410/510/1100/2100/2150. Advanced replacement hardware warranty with models 110/210.	All models
24 x 7 “live answer” support	Available SecureSupport includes rapid response phone, email, ticket tracking, Web knowledge base, customer escalation.	All models
Only firewall with TrustedSource™* security	Hybrid firewall provides stateful inspection and deep application-level filters with reputation-based service for comprehensive protection against unknown attacks.	All models
Content filtering & MIME type filtering	Integrated MIME type filters and IM, P2P, Java, and ActiveX blocking.	All models
Intrusion Prevention signature service*	Comprehensive attack signatures updated in real-time with available ASIC-based hardware acceleration.	All models
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.	All models
IPSec VPN	ICSA-certified VPN gateway with SoftRemote® VPN client for remote access.	All models
SecureOS®- Self-Defending Platform, EAL4+ Common Criteria	High-speed operating system with patented Type Enforcement® technology. No root access possible. Never been compromised. Unequalled CERT advisory record.	All models
VLAN policy enforcement	Security policy enforcement against virtual network segments using 802.1q tag recognition.	All models
Cluster management	High-bandwidth cluster management for up to five units managed as one.	All models
High availability	Stateful, active-active high availability pairs managed as one unit.	All models
Security event monitoring and reporting	Sidewinder SecurityReporter correlates and consolidates audit streams from multiple appliances.	All models
Central Management*	Central management appliance available for managing enterprise-wide policies & monitoring of hundreds of Sidewinder appliances.	All models
Embedded anti-virus*/anti-spyware	Anti-virus/anti-spyware filtering for email and Web.	All models
Embedded anti-spam*/anti-fraud	Anti-spam/anti-fraud engine captures and analyzes SMTP email using algorithmic technology and includes phishing attack protections.	All models
Web site blocking and reporting	Integrated SmartFilter® URL filtering.	All models
SSL decrypt*	Software or ASIC-accelerated SSL Web traffic is decrypted for performing application filtering.	All models
DHCP client support	Small business locations sitting behind cable & DSL modems are easily integrated with Sidewinder.	All models

**Add-on modules, central management, SecurityReporter must be purchased separately. Note: Performance statistics are current as of February 2007 and may include available performance upgrades.*

SECURE COMPUTING®
Sidewinder®
Network Gateway Security

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

Corporate Headquarters
San Jose, CA USA
Tel: +1.800.379.4944
Tel: +1.408.979.6100

European Headquarters
Berkshire, UK
Tel: +44.0.870.460.4766

Asia/Pacific Headquarters
Wan Chai, Hong Kong
Tel: +852.2598.9280

Japan Headquarters
Tokyo, Japan
Tel: +81.3.5339.6310