

SECUREIRON SECURITY TRAFFIC MANAGERS



HIGH-PERFORMANCE, SEVEN-LAYER SECURITY
— NETWORK WIDE

FEATURES

- ▶ **Networkwide security**—Purpose-built, high-performance, high-availability, networkwide security traffic manager
- ▶ **Seven-layer security**—Highly advanced, seven-layer security for protection against emerging application threats
- ▶ **Intrusion prevention**—High-performance intrusion prevention that includes highly customizable signatures
- ▶ **Application rate limiting**—Granular application rate limiting to prevent attacks and abuse of critical resources
- ▶ **Application-specific protection**—Application-specific protection for Web, DNS, SIP, VoIP, and e-mail attacks, including network-based spam mitigation
- ▶ **DoS protection**—Superior denial of service (DoS) protection against SYN flood attacks up to 3.6 million SYN/sec (wire speed 2.5 Gbps) and support for more than 30 DoS signatures
- ▶ **Traffic monitoring**—Always-on real-time traffic monitoring with standards-based hardware-assisted sFlow
- ▶ **Stateful capacity**—Industry's highest stateful capacity, supporting as many as 5 million concurrent flows
- ▶ **Stateful security**—Stateful security with high availability and hitless failover for zero enforcement downtime
- ▶ **Firewall clustering and availability**—Highly transparent firewall clustering and high availability to scale firewall performance
- ▶ **Firewall offload**—Firewall offload includes support for wire-speed access control lists (ACLs), high-performance, stateful IP Network Address Translation (NAT), and advanced DoS
- ▶ **Scalability and high performance**—Choice of performance models that are scalable to multi-Gigabit secure throughput

Overview

Organizations increasingly rely on IP networks to deliver applications that are critical to business productivity and profits. Securing this infrastructure against debilitating attacks from malicious users is necessary to ensure sustained business operations. Mobility, convergence, and Web-centric applications are rendering centralized security models ineffective. Today, organizations require distributed, network-wide, security architectures to protect against threats from outside the network and to minimize vulnerabilities inside the network. Furthermore, the line between Internet and intranet is fading fast as users become more mobile and less identifiable. In such an open infrastructure, the threats are not concentrated at a single entry point at the network perimeter, but are network wide. Attacks are also becoming more sophisticated and exploiting application-level vulnerabilities to cripple critical IP services.

The Foundry Networks® SecureIron™ traffic managers deliver high-performance Layer 2 through 7 switching and security, enabling organizations to achieve a highly secure and scalable network and application infrastructure. These security traffic managers are designed to protect against network- and application-layer threats network wide—at the network perimeter, inside the data center, and within the enterprise LAN. The SecureIron traffic managers are specially built for inline networkwide deployment to provide perimeter-like security enforcement inside the LAN against threats within the enterprise network. The SecureIron traffic manager family comprises two performance models: SecureIron 100 and SecureIron 300. Foundry's SecureWorks™ software suite powers the SecureIron, protecting the network and applications against high-speed attacks.

The SecureIron traffic managers enforce highly customizable security policies and prevent intrusions, transparently protecting against attacks targeting any IP application. These switches also feature specialized security protection for Web, Domain Name System (DNS), Voice over IP (VoIP), Session Initiation Protocol (SIP), and e-mail applications.

The SecureIron devices include Foundry's innovative third-generation security processor and advanced ASIC technology, which help deliver superior security without sacrificing network and service performance. Built on Foundry's proven JetCore® ASIC architecture, the SecureIron 100 and SecureIron 300 provide outstanding scalability and performance as well as high-density connectivity through a choice of 10/100, Gigabit, and 10-Gigabit Ethernet interface modules. The JetCore ASIC supports wire-speed ACLs and hardware-assisted, standards-based sFlow network monitoring to increase traffic visibility, manageability, and security. The SecureIron devices include a dedicated processor for reliable device management and control, ensuring device access even under extreme load. Installing a second active security management module doubles the baseline performance.

The SecureIron traffic managers perform deep packet inspection on traffic flows to identify malicious content and intrusions, and to take user-configured corrective action on offending flows.

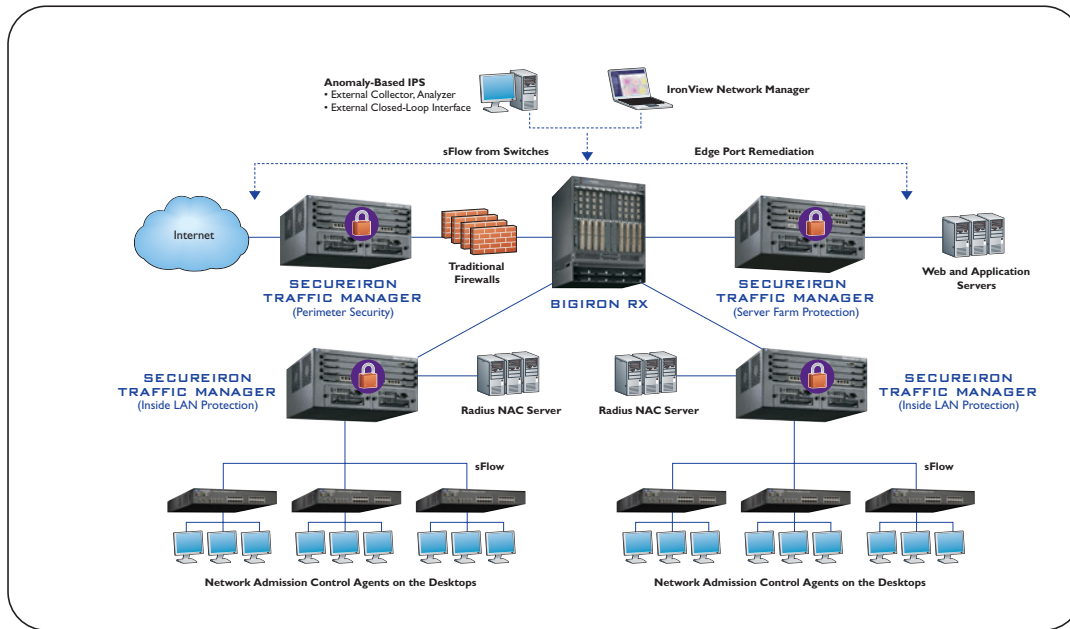
Additionally, the switches enforce a comprehensive set of Layer 2, 3, and 4 security policies to prevent many network and transport-layer DoS attacks. By using advanced rate limiting at the application level, the SecureIron prevents seemingly legitimate IP flows from being the vehicle for resource abuse and attacks.

Secure DNS is critical for all IP services. The SecureIron includes a unique DNS proxy server that has authority for DNS domains, and the SecureIron intelligently responds to client DNS queries by considering the health and availability of IP addresses associated with the DNS domain. This feature enhances overall DNS security and is a foundation for supporting high-availability applications, disaster recovery, and location transparency for a consistent user experience from geographically separated data centers.

The SecureIron's extensive and customizable policies at layers 2, 3, and 4-7 on specific flows help optimize security and network performance simultaneously. Security policies may be granularly applied to traffic from specific network segments, users, or end devices. Security policies also may be targeted to specific application services, server resources, or users. The SecureIron supports hardware-based access control and can block bad flows at wire speed without affecting overall traffic performance.

The SecureIron traffic managers provide maximum security protection and nonstop enforcement. To protect against session loss during device failures, the SecureIron traffic managers have advanced modes of high availability with real-time flow state synchronization and hitless failover between a pair of devices. If one device fails, the backup device takes over traffic processing and security enforcement without losing existing sessions or connectivity. Foundry's hitless, high availability is a superior alternative to solutions that fail-to-wire and permit all traffic without security enforcement.

The SecureIron devices are simple to configure and easy to manage using the industry-standard command line interface (CLI), built-in secure Web browser, standards-based SNMP, and Foundry's IronView Network Manager (INM).



► Figure 1: Seven-Layer Security, Network Wide

SecureIron Platform Highlights and Benefits

- **Modular design**—Highly modular and resilient design with future port expandability and performance upgradeability
- **Redundant power supplies**—Support for redundant, hot-swappable, and front-serviceable power supplies
- **Hot-swappable modules**—Hot-swappable modules and expansion slots for hot-pluggable management and line modules to add performance and port density
- **Dual-management modules**—Optional second active management module for redundancy and doubling the performance
- **Integrated SSL traffic security**—Optional service module future upgrade to add integrated and scalable security enforcement on Secure Sockets Layer (SSL)-encrypted traffic
- **Investment protection**—A unique platform to meet current and future needs for features, performance, and scalability
- **Reliability**—Resilient switching and routing foundation with advanced ASIC-based architecture and highly reliable embedded real-time operating system
- **Flexible connectivity**—Copper and fiber gigabit media options, and support for high-density gigabit over copper

Feature Set for High-Performance Security

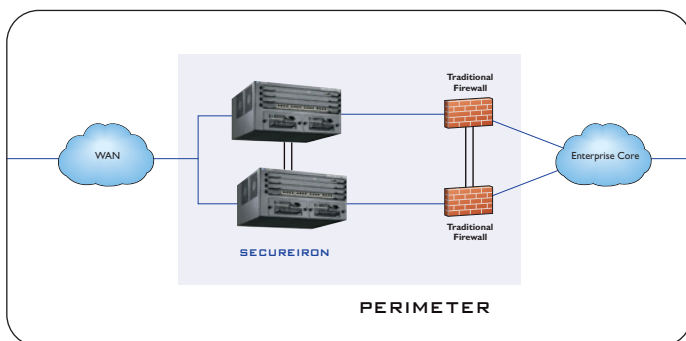
- **Wire-speed hardware access control**—Enforce access policies using standard and extended ACLs at wire speed on every port. Eliminate the need to expend security processing capacity to analyze disallowed traffic and flows. Dynamically migrate access policies from other devices with easy-to-use industry-standard ACL format.
- **DoS security against more than 30 signatures**—Prevent DoS and distributed DoS (DDoS) attacks at the MAC, IP, and TCP/UDP layers by filtering traffic using more than 30 signatures, including TCP, ICMP, and UDP attacks and floods. Use customizable DoS signatures to block traffic that has illegal protocol headers, flags, and payload.
- **SYN-Guard TCP SYN/ACK flood protection**—Prevent deadly TCP SYN and ACK flood attacks from taking down critical Web, e-mail, and other TCP services. Gain protection against multi-gigabit-rate wire-speed SYN flood attacks using hardware-assisted SYN-Guard™, which blocks illegal TCP connections.
- **Firewall clustering and high availability**—Increase firewall performance by distributing the traffic load across multiple firewalls. Overcome scalability limitations, increase throughput and performance, and improve resiliency by eliminating the firewalls as single points of failure. Cap the investment in legacy firewalls.
- **Deep packet inspection and filtering**—Prevent application-level attacks and intrusions from affecting service by using the SecureIron's high-performance deep packet inspection. Use the highly customizable and comprehensive content filtering rules to identify and block malicious content in application flows. Apply deep packet inspection rules to targeted flows, users, and services to optimize performance while increasing security protection.

- ▶ **Intelligent DNS proxy and DNS security**—Use DNS security features to protect a DNS service hosted on external dedicated servers. Filter on the basis of domain, query type, and other DNS message content to block attacks and illegal DNS traffic. Use the intelligent DNS proxy server to eliminate the need for an external DNS server, and provide intelligent replies to DNS clients with healthy and responsive IP addresses. Enable redundancy across multiple sites for critical IP services with intelligent DNS proxy.
- ▶ **Connection and application rate limiting**—Enforce desired user and host behavior by limiting the number and rate of IP flows. Prevent abusers from accessing services using automatic and manual hold-down. Limit the number of flows permitted to specific servers and applications to match resource availability with load. Extend the benefits to all TCP and UDP applications, including Web, DNS, e-mail, and VoIP.
- ▶ **Bandwidth abuse prevention**—Limit the amount of bandwidth used by a given user, or a group of users, to prevent abuse of shared bandwidth resources. Define bandwidth limits granularly down to each source IP. Ensure that legitimate users of critical applications are served without downtime or poor response time.
- ▶ **SIP and VoIP application security**—Validate SIP messages with application-level inspection, and allow only valid SIP communication over predefined UDP ports. Rate limit and filter SIP messages to prevent DoS and other attacks and abuse, and to allow only predefined SIP methods. Use deep packet inspection to filter SIP messages from malicious or illegal content.
- ▶ **E-mail spam mitigation**—Block spam at the edge of the network on the basis of IP reputation lists. Download reputation lists as large as 8 million IP addresses and prefixes (representing tens or hundreds of millions of addresses) in real time, and block e-mail traffic from known spammers. Protect other applications from attacks by identified e-mail abusers.
- ▶ **Application access policy enforcement**—Classify user source IP addresses into service access groups and enable selective access to applications by appropriate users. Augment hardware ACLs with granular and scalable application access policy lists to control application access to the individual host and user level. Scale policy lists to 8 million IP addresses and prefixes.
- ▶ **High-performance and stateful IP NAT**—Keep internal hosts, servers, and other devices private and secure with high-performance IP NAT. Use dynamic and static NAT to prevent internal hosts from being exposed to the public networks. Prevent device failures from disrupting NAT flows and traffic by using hitless NAT failover to a standby device.

- ▶ **Redundancy and high availability with hitless failover**—Deploy two SecureIron traffic managers in active-standby mode for redundancy and high availability during a device failure. Ensure no downtime for traffic flow and security enforcement by using stateful and hitless failover to the standby device. With real-time synchronization of session /flow state between the devices, there is no disruption of existing flows through the device pair when one fails.
- ▶ **Extensive actions on filtered traffic**—Log, alert, mirror, redirect, block, reset, hold down, or drop traffic matching deep packet inspection rules. Configure a combination of actions on filtered traffic to comply with organizational security and operation needs. Enable connection logging to identify every flow through the device for auditing.
- ▶ **Always-on traffic monitoring and visibility using sFlow**—Gather traffic statistics on every port all the time using standards-based sFlow technology to gain visibility into the network traffic. Use traffic trend analysis to identify unusual user or network activity, and take corrective action with dynamic security policy configuration and enforcement.

SecureIron Traffic Management Solutions for Network Wide Security

Foundry's SecureIron is uniquely designed to meet the demands of multi-gigabit traffic rates and the diverse needs of many organizations, including enterprises, service providers, and managed security providers to achieve seven-layer security, network wide. The SecureIron is well suited for deployment at the network perimeter, inside the LAN, and within the data center to protect against threats from external and internal users.



▶ Figure 2: Perimeter Front End

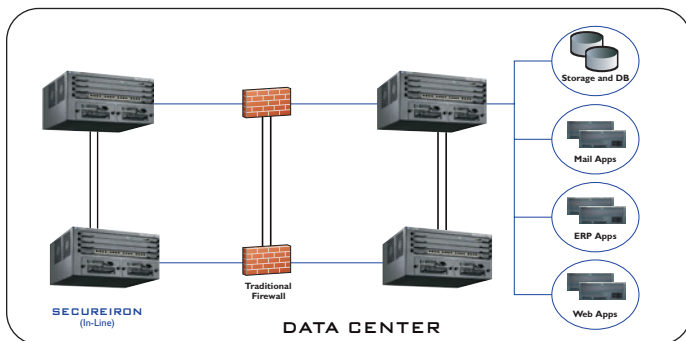
PERIMETER SECURITY SOLUTION

Organizations have relied on firewall solutions at the perimeter to manage and control access to specific resources and applications inside the network. Now organizations can cap their firewall investment and extend the life of these devices by using the SecureIron traffic managers as a front end to the firewalls.

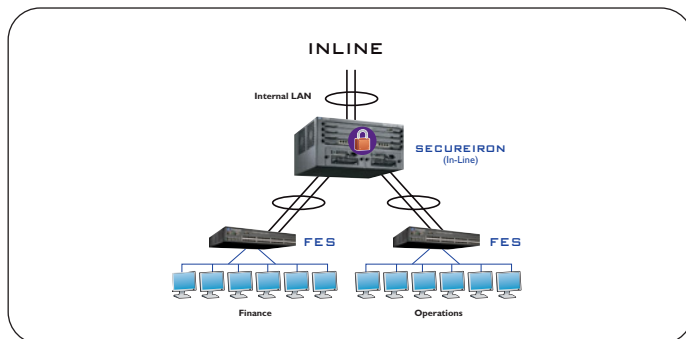
The SecureIron traffic managers augment the firewalls, delivering high-performance protection against not only network-layer and DoS attacks, but also against application-level attacks carried in seemingly legitimate traffic. Additionally, the SecureIron off-loads firewalls by relieving them of IP NAT and access control functions. To scale firewall performance, the SecureIron offers a high-availability firewall clustering solution. The end result is more robust perimeter security protection and life extension of firewalls for maximum return on investment.

DATA CENTER SECURITY SOLUTION

Every organization's most critical application, server, and storage infrastructure resides in the data center, and these assets are the high-value targets of most attacks and malicious exploits. The SecureIron traffic managers go beyond the network-layer protection offered by most firewalls, blocking threats and attacks against applications and application data. Using innovative, hardware-assisted DoS protection solutions, the SecureIron protects



► Figure 3: Data Center Security



► Figure 4: Inside the LAN—Inline

server farms from multi-gigabit TCP attacks. Additionally, the switches use highly customizable application-layer filters to block malicious messages and content from reaching the servers. The SecureIron includes application-specific signature definitions and policy enforcement for Web, DNS, VoIP, and e-mail applications.

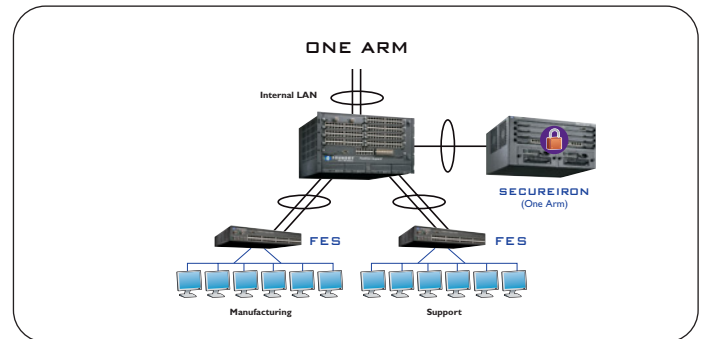
INTERNAL LAN SECURITY SOLUTION

Network users and host machines inside the LAN have long been considered to be safe and trusted. As these users become diverse, more connected, and increasingly mobile, the trust boundary no longer extends to the edge of the network. The LAN edge is essentially as untrusted a source for threats and attacks as the network perimeter connecting to the Internet.

Foundry's SecureIron traffic managers provide seven-layer protection to traffic entering and leaving the enterprise LAN edge. They also offer the edge devices superior protection from network-originated attacks, and vice versa. With the advanced layer 2/3 switching and routing foundation, the SecureIron traffic managers are well suited for inside-the-LAN deployment.

Performance is a key consideration when deploying security solutions inside the LAN because of the high-bandwidth links and their usage. To optimize network and service performance while enforcing needed security policies, the SecureIron traffic managers can be deployed either inline (see Figure 4) or as one-arm (see Figure 5).

Inline implementation is suited for networks that require all traffic to be inspected and subject to security policy enforcement. Performance-sensitive networks can benefit from segmenting the traffic into trusted and untrusted flows, and diverting only untrusted flows to the SecureIron to security policies on these flows. With the choice of these options, Enterprises can achieve an optimal balance of performance and security protection.



► Figure 5: Inside the LAN—One-arm

Technical Specifications

LAYER 2 FEATURES AND SECURITY PROTECTION

- 32,000 MAC addresses
- 802.1d Spanning Tree Protocol
- 802.1w Rapid Spanning Tree Protocol
- 802.1p prioritization
- Policy-based VLANs
- Port-based VLANs
- 802.1q VLAN tagging
- MAC filters
- Port mirroring
- sFlow

LAYER 3 AND 4 SECURITY PROTECTION

- ACLs
- Extended ACLs
- Spoof attacks
- Land attacks
- SYN floods
- ACK floods
- Smurf attacks
- Ping of death
- Connection open/close
- ICMP unreachable
- ICMP redirect
- SYN fragment
- Malformed TCP packets and SYN messages
- Illegal TCP options
- Illegal IP options
- IP options filtering
- Protocol enforcement
- UDP flood
- TCP flood
- Port scanning
- IP scanning
- Information tunneling
- Signature scanning and filtering

INTRUSION PREVENTION AND SIGNATURE BLOCKING

- Deep packet scan
 - Forward
 - Reverse
 - Bidirectional
- TCP flows
- UDP flows
- Fixed and variable offset for signatures
- Bounded scan (between fixed offsets or variable strings) to detect specific occurrence of signatures and not any occurrence
- Action upon signature match
 - Log
 - Counter
 - Reset
 - Drop
 - Mirror
 - Redirect
- Virus scan (mail and HTTP attachments)

APPLICATION-SPECIFIC SECURITY

- DNS
 - DNS proxy server
 - Replies to DNS queries
 - IP health check for DNS proxy
 - DNS rate limiting
 - DNS Layer 7 filtering
 - DNS query type
 - Domain and host
 - DNS recursive/nonrecursive query blocking
 - DNS payload scanning (deep packet scan)
- SIP/VoIP
 - SIP protocol validation
 - SIP header validation
 - SIP rate limiting
 - SIP method filtering
 - SIP DoS prevention
- Web/HTTP
 - URL filtering
 - URL rewrite
 - HTTP header filtering
 - HTTP method
 - HTTP version
- E-mail spam
 - Blacklists
 - Whitelists
 - Retroactive list enforcement
 - Real-time list download

LAYER 4 RATE LIMITING

- Concurrent connection
- Connection rate
- Maximum connection to service
- Maximum connection to destination host
- Bandwidth enforcement per flow
- Manual hold-down
- Connection logging
- TCP, UDP, and ICMP

IP NAT

- Inside NAT
- Outside NAT
- Static NAT
- Dynamic NAT
- Port address translation
- NAT stateful failover
- Protocols with dynamic ports
 - FTP
 - RTSP
 - Others

FIREWALL CLUSTERING AND HIGH AVAILABILITY

- Load distribution
- Health monitoring
- Automatic failover
- Multiple security zones (DMZs)
- VPN load distribution and failover

STANDARDS COMPLIANCE

- 802.3 10BaseT
- 802.3u 100BaseTX, 100BaseFX
- 802.3z 1000BaseSX
- 802.3z 1000BaseLX
- 802.1q VLAN tagging
- 802.1d bridging
- 802.1w RSTP
- 802.1ad link aggregation
- 802.3 Ethernet-like Management Information Base (MIB)
- Repeater MIB
- Ethernet interface MIB
- SNMPV2c
- SNMP MIB II

NETWORK MANAGEMENT

- Integrated industry-standard CLI
- SSHv2
- Web-based GUI (HTTP and HTTPS)
- Telnet
- SNMP
- RMON
- IronView Network Manager (INM)
- HP OpenView

SAFETY AGENCY APPROVALS

- EN 60950/EN 60825/IEC 950
- UL 1950-CSA 950 Electromagnetic Emission Certification
- FCC Class A-EN 55022/CISPR-22 Class A/VCCI Class A
- CE Mark

IMMUNITY

- Generic: EN 50082-1
- ESD: IEC 61000-4-2; 4 kV CD, 8 kV AD
- Radiated: IEC 61000-4-3; 3V/m
- EFT/Burst: IEC 61000-4-4; 1.0 kV (power line), 0.5 kV (signal line)
- Conducted: IEC 61000-4-6; 3V

ENVIRONMENTAL

- Operating temperature: 32° F to 104° F (0° C to 40° C)
- Relative humidity: 5% to 90% @ 104° F (40° C), non-condensing
- Operating altitude: 6,000 ft (2,000 m) maximum
- Storage temperature: 9° F to 158° F (-25° C to 70° C)
- Storage altitude: 15,000 ft (4,500 m) maximum
- Storage humidity: 95% maximum relative humidity non-condensing

MOUNTING OPTIONS

- 19" universal EIA (Telco) rack
- Tabletop



SecureIron System Summary and Specifications

SECUREIRON TRAFFIC MANAGERS

Note: Performance and capacity are doubled when a second active management module is added to a SecureIron system

	SECUREIRON 100	SECUREIRON 300
Stateful session capacity (bidirectional flows)	1,000,000	5,000,000
Layer 4 flows per second	50,000	150,000
Layer 7 flows per second	15,000	45,000
SYN flood protection	1,000,000 SYN/sec	3,000,000 SYN/sec
Throughput		
Layer 2/3	Wire speed	Wire speed
Layer 4	2.0 Gbps	6.0 Gbps
Layer 7 (one way)	350 Mbps	1.0 Gbps
Layer 7 (two way)	180 Mbps	550 Mbps
L2 switching capacity	56 Gbps	
Maximum ports (expandability)		
10/100	48	
Gigabit	48	
10-Gigabit	6	
Total	64	
Physical dimensions	8.75" h x 17.5" w x 15" d (22.2 cm x 44.5 cm x 38.1 cm)	
Weight	60 lbs fully loaded (29.9 kg)	
Power requirements	4-slot chassis with single (1) power supply: input voltage and current power supply rating -70 to -40VDC: 17A 100 to 120VAC (auto-ranging): 8A 200 to 240VAC (auto-ranging): 4A AC line frequency: 47-63 Hz	

Ordering Information

PART NUMBER	DESCRIPTION
SecureIron Traffic Manager Platforms	
SCI100	4-slot chassis equipped with one SSM6-1 (security switch management module), one AC power supply (redundant power supply optionally available)
SCI300	4-slot chassis equipped with one SSM6 (security switch management module), one AC power supply (redundant power supply optionally available). This model has three times the performance of the SCI100
SCI100-DC	4-slot chassis equipped with one SSM6-1 (security switch management module), one -48V DC power supply (redundant power supply optionally available)
SCI300-DC	4-slot chassis equipped with one SSM6 (security switch management module), one -48V DC power supply (redundant power supply optionally available). This model has three times the performance of the SCI100
SecureIron Traffic Manager Line Module Options	
J-B2Gx	2-port 1000BaseX (mini-GBIC) JetCore line module
J-B4Gx	4-port 1000BaseX (mini-GBIC) JetCore line module
J-BxG	8-port 1000BaseX (mini-GBIC) JetCore line module
J-B16Gx	16-port 1000BaseX (mini-GBIC) JetCore line module
J-B16GC	16-port 100/1000BaseT (RJ-45) JetCore line module
J-B48E-A	48-port 10/100BaseTX (RJ-45) double-wide JetCore line module
J-B24FX	24-port 100BaseFX JetCore line module
J-B2404CF	24-port 10/100BaseTX (RJ-45) and 4-port Gigabit (copper and fiber combo) double-wide JetCore line module
B10Gx1	1-port 10-Gigabit Ethernet base module (optics required)
B10Gx2	2-port 10-Gigabit Ethernet base module (optics required)
SecureIron Traffic Manager Management Module Options (Redundant, Dual-Active, Upgrade)	
SSM6-1	Security switch management module with one security traffic processor and one management processor
SSM6	Security switch management module with three security traffic processors and one management processor
SecureIron Traffic Manager Mini-GBIC Options	
E1MG-SX	1000BaseSX mini-GBIC optic, MMF, LC connector
E1MTG-SX	1000BaseSX mini-GBIC optic, MMF, MTRJ connector
E1MG-LX	1000BaseLX mini-GBIC optic, SMF, LC connector
E1MG-LHA	1000BaseLHA mini-GBIC optic, SMF, LC connector
E1MG-LHB	1000BaseLHB mini-GBIC optic, SMF, LC connector, 150 km maximum reach
E1MG-TX	1000BaseTX mini-GBIC copper, RJ-45 connector
SecureIron Traffic Manager 10-Gigabit Optics	
10G-XNPK-SR	850nm serial XENPAK plug-in transceiver (SC), target range of 300m over MMF
10G-XNPK-LR	1310nm serial pluggable XENPAK optic only (SC) for up to 10 km over SMF
10G-XNPK-ER	1550nm serial pluggable XENPAK optic only (SC) for up to 40 km over SMF





Foundry Networks, Inc.
Corporate Headquarters
4980 Great America Parkway
Santa Clara, CA 95054

U.S. and Canada Toll-free:
1-888-TURBOLAN (887-2652)
Tel: +1 408.586.1700
Fax: +1 408.586.1900
info@foundrynet.com
www.foundrynetworks.com

Although Foundry has attempted to provide accurate information in these materials, Foundry assumes no legal responsibility for the accuracy or completeness of the information. More specific information is available on request from Foundry. Please note that Foundry's product information does not constitute or contain any guarantee, warranty or legal binding representation, unless expressly identified as such in duly signed writing.

© 2006 Foundry Networks, Inc. All Rights Reserved. Foundry Networks, BigIron, FastIron, NetIron, SecureIron, ServerIron, AccessIron, IronPoint, Terathon, JetCore, EdgeIron, IronView, sFlow, IronShield, MetroLink, IronWare, TrafficWorks, Power of Performance and the 'Iron' family of marks are trademarks or registered trademarks of Foundry Networks, Inc. in the United States and other countries. All others are trademarks of their respective owners. FDRY_DS-042_SCI_2006_01_Rev02

