

Key Features

- 1 Gbps, full-duplex performance with DES, Triple DES, or AES encryption
- IPSec standards-based encryption, authentication, digital certificates, and key management
- Expandable to 1,024 IPSec tunnels and 2,048 simultaneous secure connections
- Flexible and scalable network design with VLAN support
- Remote Access Services using DN based access control, NAT Traversal, and Mode Config
- High security with enhanced IKE commands, Perfect Forward Secrecy (PFS)
- Easy installation in existing network environments with gigabit LANs
- Ideal for meshed, hub-and-spoke, and nested networks
- Centralized GUI, certificate-based authentication policy, and centralized policy management through SafeEnterprise Security Management Center

HighAssurance 4000 Gateway

A High-Performance, Site-To-Site, and Remote Access VPN Solution

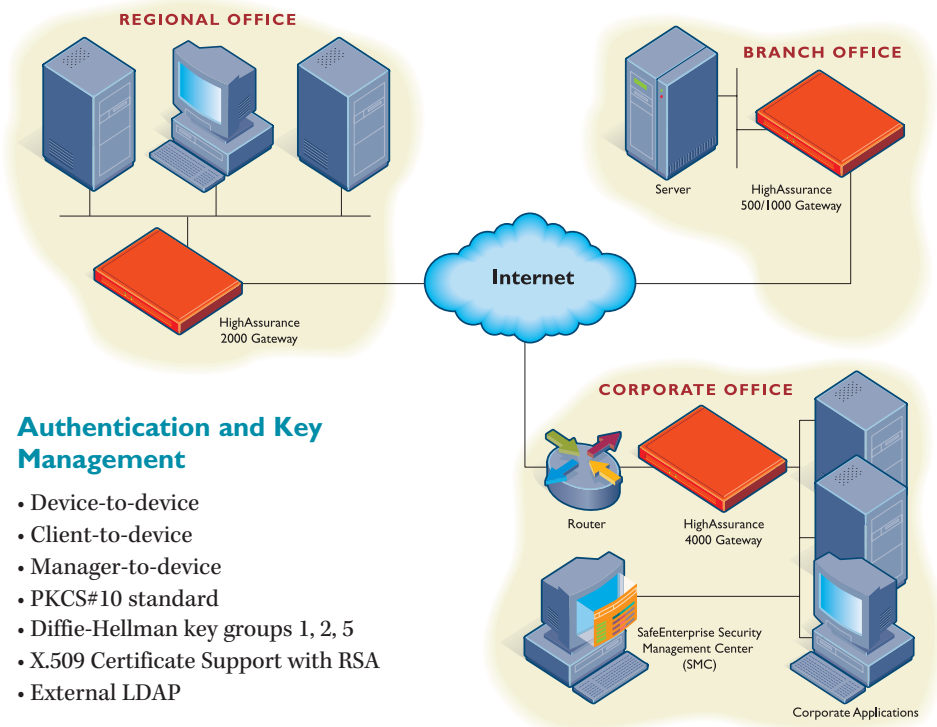


The SafeNet HighAssurance™ 4000 Gateway offers the necessary performance and manageability to drive down the total cost of ownership for network security. Built to meet the scalable demands of today's headquarter and enterprise-class networks, it provides key security and data management features including IPSec VPN tunneling and Network Address Translation while operating at 1 gigabit full-duplex for supporting up to 1,024 IPSec tunnels and a maximum of 2,048 simultaneous secure connections using DES, Triple DES, or AES encryption.

The HighAssurance 4000 Gateway is a dedicated, stand-alone, IPSec solution for site-to-site and remote access virtual private networks (VPNs). The HighAssurance 4000 Gateway maximizes cost and time savings by optimizing security, performance, interoperability, and manageability. It enables companies to move their business communications to the Internet to reduce costs, increase business opportunities, and securely communicate and transact with employees, business partners, and customers. Encryption and security

functions are separated from those of other networking devices because the HighAssurance 4000 Gateway device is a dedicated security device. This is critical when designing the most secure network in meshed and hub-and-spoke network architectures.

Like all SafeNet security appliances, the HighAssurance 4000 Gateway is managed by the SafeEnterprise™ Security Management Center (SMC), a robust, Java™-based policy management software application with secure, flexible, and transparent SNMP-based control and monitoring capabilities. The SMC provides the ability to define integrated security policies that can be distributed across multiple devices and HighAssurance Remote VPN clients.



Authentication and Key Management

- Device-to-device
- Client-to-device
- Manager-to-device
- PKCS#10 standard
- Diffie-Hellman key groups 1, 2, 5
- X.509 Certificate Support with RSA
- External LDAP

IKE Features

- Preshared keys
- DSA authentication (1024 bits)
- RSA (1024 and 2048 bits)
- Quick/Main/ and Aggressive modes
- Mode Config
- NAT Traversal

Encryption

- DES: FIPS 46-2 (56 bit key) CBC mode
- 3DES: ANSI X.952 (168 bit key) CBC mode
- AES: (256 bit key) CBC mode
- IPSec compliant
- RFCs 2405, 2451

Protocol Support

- IEEE Ethernet
- IPSec RFC 2401, 2402, 2406
- IKE RFC 2407, 2408, 2409

Security Management

- Extensive audit logging
- Alarm condition detection

- and reporting
- Configuration and security management
- Secure download of software updates
- Performance monitoring
- Out-of-band (OOB) management

Regulatory

- FCC Part 15, Class B
- UL and CUL
- IEC/EN
- CSA

SafeNet offers distinct levels of support based on the type of support you require. The HighAssurance 4000 Gateway has a one year (12 month) standard, basic warranty. Extended support and maintenance contracts are available. Support is also offered online through our customer support website, express service center, and customer connection center.

Corporate: 4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel: **+1 410.931.7500** or 800.533.3958 email: info@safenet-inc.com

www.safenet-inc.com

Australia +61 3 9882 8322
Brazil +55 11 3392 4600
Canada +1 613.723.5077
China +86 10 8266 3936
Finland +358 20 500 7800
France +33 1 41 43 29 00
Germany +49 18 03 72 46 26 9
Hong Kong +852.3157.7111
India +91 11 26917538

Japan(Tokyo) +81 3 5719 2731
Korea +82 31 705 8212
Mexico +52 55 5575 1441
Netherlands +31 73 658 1900
Singapore +65 6297 6196
Taiwan +886 2 27353736
UK +44 1276 608 000
U.S. (Massachusetts)
+1 978.539.4800

U.S. (New Jersey)
+1 201.333.3400
U.S. (Virginia) +1 703.279.4500
U.S. (Irvine, California)
+1 949.450.7300
U.S. (Santa Clara, California)
+1 408.855.6000
U.S. (Torrance, California)
+1 310.533.8100

Distributors and resellers
located worldwide.

Technical Specifications

IPSec Modes

- Tunnel
- Encapsulated Security Payload (ESP)
- Authentication Header (AH)

Data Integrity

- HMAC-MD5 RFC 2104, 2403, 1321
- HMAC-SHA-1 (FIPS PUB 180-1) RFC 2104, 2404

Management Interfaces

- IEEE Ethernet (OOB remote configuration and management)
- 10/100 Ethernet and RS-232 menu-driven terminal interface
- Remote management protected by a VPN tunnel

Physical Security

- Tamper-evident, extruded/sheet metal construction

Management Platforms

- Microsoft Windows® 2000 and XP
- Linux® 2.4 (Red Hat 7.2)

Electrical/Mechanical/Dimensions

- Two full-duplex Gigabit Ethernet ports with GBIC interfaces
- One RJ-45 10/100 Auto-Sensing Ethernet port
- One RS-232 serial port
- 115-240 VAC @ 50/60Hz, auto-ranging
- Power dissipation: 120 watts (typical)
- Standard 19-inch rack mount design
- Weight: 10 lbs (4.55 Kg)
- Dimensions: 4" H x 17" W x 15" D (10.2 cm x 43.2 cm x 38.1 cm)

Certifications

- FIPS PUB 140-2, Level 2

Environmental

- Operating temperature: 32° to 104° F (0° to 40° degrees C)
- Operating humidity: Up to 90% (non-condensing)
- Operating altitude: -200 to 10,000 feet AMSL

