



LOCKED DOWN. FREED UP.

BORDERGUARD 5000

HIGH ASSURANCE VPN APPLIANCE WITH INTEGRATED PKI

The BorderGuard™ 5000 family offers a wide range of capacity models while preserving backwards compatibility with previous models of the highly regarded BorderGuard VPN product line. Top-end models offer strong cryptographic performance measured in hundreds of megabits per second. Gigabit Ethernet interfaces, available with some models, provide for physical layer compatibility in almost any network where high-speed VPN features are required.

The BorderGuard 5000 series builds upon its reputation for ironclad security and reliability. Its predecessors have been deployed in support of the most demanding missions around the world without a single security breach. Additionally, an extended version of Virtual Router Redundancy Protocol (VRRP) is available for the BorderGuard 5000 providing both chassis and total path redundancy with automatic failover.

Used with the BorderGuard Management Console, it can deliver rapid VPN deployment and reduced total cost of operation. The Management Console offers GUI drag and drop automation of VPN definition, BorderGuard setup, public-key exchange, and on-going configuration management. The VPN administrator has access to a real-time, central, secure management interface that displays the status of the network.

Like previous BorderGuard models, the BorderGuard 5000 includes a built-in RSA public-key infrastructure (PKI) that will generate, exchange, and use digital certificates for all BorderGuard VPN authentication. Each BorderGuard has a unique non-replicable RSA public-key identity that provides VPN connection authentication far stronger than the shared secret authentication offered by other VPN products. Since the PKI is included, there is no need for stand-alone PKI or digital certificate services. The BorderGuard 5500 and 5600 models offer an extended RSA key length of 4,096 bits.

The BorderGuard 5000 supports an optional, removable USB-based SmartCard cryptographically mated to the chassis. Removing the SmartCard disables the chassis boot firmware. This feature adds an additional security option for “safeing” units in transit or when unattended.

- Strong Public Key Authentication
- Built-in Digital Certificates
- Secure Pocket PC Client
- Powerful and Versatile Filtering/Redirects
- Hardware Accelerated AES Encryption
- Common-Criteria Certified Secure Central Management
- Compact Rack Mountable Design - 1U
- Auto-Sensing Ports 10/100/1000 Ethernet
- Extensive Audit Capability
- Redundant Configurations

