



**LOCKED DOWN. FREED UP.**

# **BORDERGUARD® 6000**

## **SECURE COMMUNICATIONS PLATFORM**

### **BEST IN CLASS INTEROPERABILITY AND SECURITY**

The BorderGuard 6000 Secure Communications Platform builds on a decade-long legacy of offering the best combination of price, performance, reliability, and security in the industry.

BorderGuards have been deployed around the world in support of the most demanding secure communications applications without a single security breach. In addition to iron-clad security, BorderGuards are known for their reliability — enhanced by total path redundancy and automatic failover for complete peace of mind.

### **INTEROPERABILITY AND FLEXIBILITY**

The versatile BorderGuard 6000 can leverage your existing public key infrastructure (PKI), including X.509 certificate authorities as well as OCSP and CRL checking. Administrators are relieved of the tedious task of manually configuring certificate authority hierarchies by the BorderGuard 6000 automatic path discovery and path validation mechanisms. For flexibility, the BorderGuard 6000 includes its own built-in PKI that can be used independently.

Supporting geographically and technologically diverse organizations has never been easier. The BorderGuard 6000 is ready to deploy with minimal setup. To meet the rising demand for wireless devices, the BorderGuard 6000 offers seamless roaming that allows users to maintain a VPN tunnel across wireless access points.

The BorderGuard 6000 is compliant with the important Federal Government directive HSPD-12 and is compatible with any PKCS#11 smart card or USB token.

### **IRON-CLAD SECURITY**

BorderGuards are configured as perfect firewalls. The only packets forwarded from external connections to inside ports are the packets that have been cryptographically authenticated. Conversely, the only packets that leave the BorderGuard 6000 are those that are encrypted and sent to an authenticated destination in the VPN. BorderGuards do not respond to unauthenticated sources.

Blue Ridge Networks™ developed Tunnel-Lock™ to lock down remote access devices to only one possible destination — the corporate network via the VPN tunnel. Tunnel-Lock is applied during the installation process and cannot be disabled. This unique feature eliminates the possibility of backdoor attacks.

- DISA JITC and Army TIC Certified
- Secure All IP-Based Communications — Wireless and Wired
- DoD PKI / Standards-Based Authentication — X.509, OCSP, CRL
- HSPD-12 Compliant Two-Factor Authentication
- Central Management
- PKCS#11 Smart-Card Compatible
- Seamless Wireless Interface Roaming
- Red List Revocation Capability
- IEEE 802.1Q VLAN Support
- Dynamic End-Point Security Policies
- Hardware Accelerated AES Encryption
- Extended RSA Keys — 2048 and 4096
- Built-in PKI Included

Strong two-factor authentication with Key-Guard™ combined with the BorderGuard 6000 auto-enrollment capability scales to meet the escalating needs of the organization and offers a higher level of security than password-only systems while maintaining user convenience.

Mutual Authentication — the appliance itself has a unique RSA public key digital certificate-based identity. Each BorderGuard 6000 within the VPN must mutually authenticate using these certificates. Password or "shared secret" modes of authentication are not secure and not supported by the BorderGuard 6000. The Blue Ridge Networks method of mutual authentication eliminates the possibility of an attacker inserting himself into the VPN via identity spoofing or a man-in-the-middle attack.

### REMOTE MANAGEMENT

The BorderGuard 6000 Management Console is a pre-configured appliance that drops into your network, centrally

and securely managing all site-to-site and remote access connections. It supports standard digital certificates and with the Blue Ridge Networks Red List function, administrators can revoke access to specific users in real time, even for users employing external certificate authorities.

### TESTED AND TRUSTED

Over the years, Blue Ridge Networks earned numerous certifications and equipment validations, including Common Criteria, FIPS 140-2, DISA JITC and Army TIC, HIPAA, and DoD SPOCK. Contact one of the security experts at Blue Ridge Networks for a complete demonstration of the BorderGuard 6000 and to discuss your unique secure communications requirements.

## BORDERGUARD 6000 SPECIFICATIONS

#### DIGITAL CERTIFICATES

- X.509
- Built-in RSA-based

#### CERTIFICATE REVOCATION

- OCSP
- CRL
- Red List

#### ENCRYPTION ALGORITHMS

- Data Encryption Standard (DES)
- Triple DES
- IDEA
- AES 128, 192, 256

#### DATA INTEGRITY

- MD5
- HMAC SHA-1, SHA-256

#### DATA INTEGRATION

- LDAP Version 3
- X.509 digital certificate authority

#### VLAN SUPPORT

- IEEE 802.1Q

#### PUBLIC KEY CRYPTOGRAPHY

- RSA and Diffie-Hellman
- 512, 1024 bit keys
- 2048, 4096 bit keys (Extended RSA)

#### VPN CLIENT PLATFORMS

- Pocket PC (128 MB RAM)
- Secure Thin Client
- Windows XP (SP1 and later)
- Windows 2000 (SP3 and later)

#### ROUTING

- RIP
- OSPF

#### INTERFACE ROAMING

- Windows 2000 (SP4 and later)
- Windows XP (SP2 and later)

#### PHYSICAL DIMENSIONS

- Height: 1.74 in. (4.42 cm)
- Width: 17.0 in. (43.2 cm)
- Depth: 12.0 in. (30.5 cm)
- Weight: 8.2 lbs. (3.72 kg)
- Rack units: 1U

#### POWER REQUIREMENTS

- 100-120 VAC / 200-240 VAC
- 2 amps maximum; 50/60 Hz

#### OPERATING ENVIRONMENT

- Temperature: 5° to 45° C (41° to 113° F)
- Humidity: 10% to 90% (non-condensing)
- Altitude: -150 to +10,000 feet



MODEL	10/100 ETHERNET PORTS	10/100/1000 ETHERNET PORTS	MAXIMUM AES256 THROUGHPUT (MBPS)	MAXIMUM CONCURRENT TUNNELS	MAXIMUM RSA KEY
6100	2	0	20	150	2048
6200	3	0	45	300	2048
6400	3	0	100	600	2048
6500	1	2	200	1,000	4096
6600	1	2	400	3,000	4096
6800	4-16	4-16	2400	24,000	4096