MILTOPE
A company of ST Engineering North America

NETCRYPT S20

NetCrypt S20 is a compact IP encryptor that enables the user to leverage on public Ethernet/IP infrastructure to connect to multiple sites in a secure manner. NetCrypt S20 employs AES algorithm for data confidentiality, Secure Hash Algorithm (SHA) for integrity protection as well as internet key exchange (IKE) protocol for keys derivations and authentications. The built-in Firewall performs packet filtering and supports NAT/PAT features.

Supporting up to 50 tunnels with a maximum encrypted throughput of 100Mbps, NetCrypt S20 packs a big punch in a small foot print. It is ideal for deployments as a security gateway in a small office corporate LANs, site- to-site VPN, mobile vehicle and site-to-site wireless inter- offices connectivity.

NetCrypt S20 is interoperable with NetCrypt series of IP encryptor, allowing user to form a secure VPN between the corporate HQ and remote sites/branch offices. With the flexibility to use industry standard Simple Network Management Protocol (SNMP) network management system, NetCrypt S20 allows local and remote monitoring of devices, and firmware field- upgrading to ease new features introduction, algorithm updates and maintenance.

KEY FEATURES

- High-assurance IP encryptor with Firewall capabilities
- 100Mbps throughput aggregate
- IPSec standards-based encryption, authentication, digital certificates and key management
- Supports AES algorithm for data confidentiality
- Supports 50 concurrent IPSec tunnels
- Easy deployment in existing network with 10/100/1000 Mbps LANs
- Slim and Compact

SPECIFICATIONS

NETWORK INTERFACES	Trusted LAN 1 and Trusted LAN 2 ports: 2 x Ethernet RJ45 10/100/1000 Mbps auto-sensing port External port: 1 x Ethernet RJ45 10/100/1000 Mbps auto-sensing port
NETWORKING FEATURES & PROTOCOLS	IP Security/Encapsulating Security Protocol Support Layer 2 and Layer 3 encryption capability IP Compression QoS support Traffic flow confidentiality IPv4
HIGH AVAILABILITY FEATURES	Failover (Active/Passive mode) Priority Based Redundant Secure Nodes
AUTHENTICATION	Pre-shared Key RSA Public Key Signature (up to 4096 bit)
KEY MANAGEMENT	Support Internet Key exchange (IKE v2) DH supports up to 8192 bit Supports ECDH (up to P-521 bit) Group Transport Protection: The device has the option of providing encryption and data integrity protection to all key exchange traffic including the initial key exchange traffic
ENCRYPTION ALGORITHM / MODES	AES-CBC (256 bit)
HASH ALGORITHM	HMAC-SHA2 (256, 384, 512 bit)
PERFORMANCE	Zero-loss encrypted throughput up to 100Mbps (depending on IP packet size and used encryption mode) Support 50 concurrent IPSec tunnels
MANAGEMENT	Interfaces: • 10/100/1000 Mbps Ethernet RJ45 (remote management and local configuration) • RS232 local console interface Security/Configuration: • Extensive audit logging • Alarm detection and logging • SNMP v2c network management (operates with standard SNMP network management station) • Supports up to 3-factor authentication
SECURITY FEATURES	Tamper-resistant chassis Anti-tamper detection and response
PHYSICAL CHARACTERISTICS	Dimensions: 30mm(H) x 230mm(W) x 150mm(D) Power Supply: External 12VDC, 3.4A, 100-240VAC, 50/60 Hz Adaptor Power Rating: 40W max Weight: 1.25 KG
ENVIRONMENTAL	Storage Temperature: -20°C to 70°C Operating Temperature: 0°C to 40°C Humidity: Relative 10% - 95%, non-condensing
REGULATORY	EMC/EMI: FCC Part 15 Class B
OPTIONAL FEATURE	Supports customized algorithm loading feature