Trusted Network
CyberSecurity
NetCrypt S10

Small & Compact IP Encryptor

NetCrypt S10 is a small and compact IP encryptor that enables user to leverage on public Ethernet/IP infrastructure to connect to multiple sites in a secure manner.

NetCrypt S10 employs AES algorithm for data confidentiality, Secure Hash Algorithm (SHA) for integrity protection as well as Internet Key Exchange (IKE) protocol for key derivations and authentications. The built-in Firewall performs packet filtering and supports NAT/PAT features.

Supporting up to 20 tunnels with a maximum encrypted throughput of 30Mbps, NetCrypt S10 is ideal for securing video streaming from surveillance camera, securing the SCADA network link, and mobile vehicle wireless inter-offices connectivity.

NetCrypt S10 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 S10 allows local and remote monitoring of devices, and firmware field-upgrading to ease new features introduction, algorithm updates and maintenance.

Key Features

- Small and compact
- 30Mbps throughout aggregate
- IPSec standards-based encryption, authentication, digital certificates and key management
- Supports AES algorithm for data confidentiality
- Supports 20 concurrent IPSec tunnels
- Easy deployment in existing network with 10/100 Mbps LANs
## Specifications

| **Network Interfaces** | Trusted port: 1 x Ethernet RJ45 10/100 Mbps auto-sensing port  
| | External port: 1 x Ethernet RJ45 10/100/1000 Mbps auto-sensing port |
| | Support Layer 2 and Layer 3 encryption capability  
| | IP Compression  
| | QoS support  
| | Traffic flow confidentiality |
| **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-SHA1  
| | HMAC-SHA2 (256, 384, 512 bit) |
| **Performance** | Zero-loss encrypted throughput up to 30Mbps (depending on IP packet size and used encryption mode)  
| | Support 20 concurrent IPSec tunnels |
| **Management** | Interfaces:  
| | - 10/100 Mbps Ethernet RJ45 (remote management and local configuration)  
| | - RS232 local console interface (DB9 to RJ45)  
| 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: 32mm(H) x 130mm(W) x 150mm(D)  
| | Weight: 700 grams  
| | Power Supply: External 7.5VDC, 3A, 100-240VAC, 47-63 Hz  
| | Adaptor  
| | Power Rating: 15W max |
| **Environmental** | Operating Temperature: 0°C to 45°C  
| | Storage Temperature: -20°C to 70°C  
| | Humidity: Relative 95%, non-condensing |
| **Regulatory** | EMC/EMI: FCC Part 15 Class B |
| **Optional Feature** | Supports customized algorithm loading feature |