

NetCrypt S20



Compact & High Performance IP Encryptor

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

NetCrypt U1000



High Performance IP Encryptor

NetCrypt U1000 is a high performance IP encryptor that enables the user to leverage on public Ethernet/IP infrastructure to connect to multiple sites in a secure manner. NetCrypt U1000 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 300 tunnels with a maximum encrypted throughput of 500Mbps, NetCrypt U1000 is ideal for deployments as a security gateway in a corporate LANs, site-to-site VPN and site-to-site wireless inter-offices connectivity.

Key Features

- High-assurance IP encryptor with Firewall capabilities
- 500Mbps throughput aggregate
- IPSec standards-based encryption, authentication, digital certificates and key management
- Supports AES algorithm for data confidentiality
- Supports 300 concurrent IPSec tunnels
- Easy deployment in existing network environment
- 19" rack mountable (Optional Chassis Runner)

Specifications

Network Interfaces	Trusted LAN 1, Trusted LAN 2, External and Management (4 x Gigabit ports): - Fiber optic: LC connector, multi-mode/single-mode - Copper: Ethernet RJ45
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) Load Balancing (Active/active 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 500Mbps (depending on IP packet size and used encryption mode) Support 300 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: 44mm(H) x 430mm(W) x 511mm(D) Power Supply: 110/230VAC @ 50/60 Hz Auto-ranging Power Rating: 300W max Weight: 8.7 KG
Environmental	Storage Temperature: -20°C to 70°C Operating Temperature: 0°C to 40°C Humidity: Relative 95%, non-condensing
Regulatory	EMC/EMI: FCC Part 15 Class B
Optional Feature	Supports customized algorithm loading feature

NetCrypt U2000



High Performance IP Encryptor

NetCrypt U2000 is a high performance IP encryptor that enables the user to leverage on public Ethernet/IP infrastructure to connect to multiple sites in a secure manner. NetCrypt U2000 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 800 tunnels with a maximum encrypted throughput of 1Gbps, NetCrypt U2000 is ideal for deployments as a security gateway in a corporate LANs, site-to-site VPN and site-to-site wireless inter-offices connectivity.

With the flexibility to use industry standard Simple Network Management Protocol (SNMP) network management system, NetCrypt U2000 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
- 1Gbps throughput aggregate
- IPSec standards-based encryption, authentication, digital certificates and key management
- Supports AES algorithm for data confidentiality
- Supports 800 concurrent IPSec tunnels
- Easy deployment in existing network environment
- 19" rack mountable (Optional Chassis Runner)

Specifications

Network Interfaces	Trusted LAN 1, Trusted LAN 2, External and Management (4 x Gigabit ports): <ul style="list-style-type: none">- Fiber optic: LC connector, multi-mode/single-mode- Copper: Ethernet RJ45
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) Load Balancing (Active/active mode) Priority Based Redundant Secure Nodes
Authentication	Pre-shared Key RSA Public Key Signature (up to 4096 bit)
Key Management	Support Internet Key exchange (IKEv2) 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 1Gbps, aggregated (depending on IP packet size and used encryption mode) Support 800 concurrent IPSec tunnels
Management	Interfaces: <ul style="list-style-type: none">- Fiber optic/RJ45 (remote management and local configuration)- RS232 local console interface Security/Configuration: <ul style="list-style-type: none">- 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: 44mm(H) x 430mm(W) x 511mm(D) Redundant Hot-Swap PSU: 110/240VAC @ 50/60 Hz Auto-ranging Power Rating: 300W max Weight: 8.8 KG
Environmental	Storage Temperature: -20°C to 70°C Operating Temperature: 0°C to 40°C Humidity: Relative 95%, non-condensing
Regulatory	EMC/EMI: FCC Part 15 Class B
Optional Feature	Supports customized algorithm loading feature

NetCrypt R100



Ruggedized High Performance IP Encryptor

NetCrypt R100 is a ruggedized IP encryptor with operating temperature of up to 55°C. NetCrypt R100 enables the user to leverage on public Ethernet/IP infrastructure to connect to multiple sites in a secure manner. NetCrypt R100 employs AES algorithm for data confidentiality, Secure Hash Algorithm (SHA) as well as Internet Key Exchange (IKE) protocol for integrity protection and user authentication. The built-in Firewall performs packet filtering and supports NAT/PAT features.

Supporting up to 80 tunnels with a maximum encrypted throughput of 100Mbps, NetCrypt R100 is ideal for deployments as a security gateway in mobile vehicle, outdoor deployment, corporate LANs, site-to-site VPN and site-to-site wireless inter-offices connectivity.

NetCrypt R100 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 R100 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 80 concurrent IPSec tunnels
- Easy deployment in existing network
- Ruggedized and suitable for outdoor deployment

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) Load balancing (Active/Active 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 80 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 - Supports up to 3-factor authentication
Security Features	Tamper-resistant chassis Anti-tamper detection and response
Physical Characteristics	Dimensions: 44mm(H) x 420mm(W) x 285mm(D) (Rack mountable) Power Supply: External 18-32VDC, 100-240VAC Adaptor, 2.2A 50/60 Hz (60W nominal)
Environmental	Operating Temperature: -10°C to +55°C Storage Temperature: -20°C to +70°C Humidity: 95%, non-condensing
Induced (Mechanical) Environment	Vibration: IEC 61373 @ 1999 Shock: IEC 60068-2-27 @ 2008
Regulatory	EMC/EMI: FCC Part 15 Class B
Optional Feature	Supports customized algorithm loading feature