RAVLIN® 4

Performance is maintained through the use of RedCreek's CryptoCore™ Technology.

PRODUCT OVERVIEW

The RedCreek Ravlin 4 is a cost-effective network security solution that performs encryption and decryption with a throughput of 40% of the theoretical maximum of Ethernet. Network administrators use it to establish private communications within secure intranets (as between corporate divisions, workgroups, branch ofces, and individuals) or within secure extranets (as between customers, suppliers, and strategic partners.) Its low cost lets organizations establish security over private or public IP networks quickly and easily.

The Ravlin 4 is typically installed behind an access router connected to a full-duplex T1/E1 wide-area network (WAN) circuit. It provides data privacy using industry-standard 40-bit/56-bit DES and 168-bit Triple DES encryption. Authentication and access control with DSS (Digital Signature Standard), Dife-Hellman key exchange, X.509 v.3 digital certicates, and ISAKMP/Oakley key management. These security standards are part of the Internet Engineering Task Force (IETF) IP Security Standard (IPSec).

IP SECURITY STANDARD (IPSec)

Ravlin 4 rmware contains all components of the Internet Engineering ask Force (IETF) IP Security Standard (IPSec) for enhanced network security. IPSec is the most secure and comprehensive standard available today for encryption, authentication, key management and anti-replay services.

IPSec protocol interoperability allows the exchange of keys and encrypted communications with all other IPSec compliant products, so customers can use different IPSec vendors for multiple scenarios. RedCreek can provide a list of IPSec interoperability partners.

FAST ENCRYPTION
WIRELINE PERFORMANCE WITHOUT NETWORK DEGRADATION

Third party tested and validated at encryption/decryption speeds of 40% of the theoretical maximum of Ethernet for all packet sizes.

EASE OF IMPLEMENTATION AND ADMINISTRATION

• Integrates easily into existing networks through 10BaseT inputs and outputs. Secure download of product upgrades to Ravlin 4 ash memory. Easy device management through embedded SNMP agent and industry-standard SNMP MIB II.

The Ravlin 4 rmware supports the strongest suite of IPSec network security enforcement features available today. Using RavlinNodeManager to congure the unit, the network administrator can choose between several different secure VPN modes.

ESP (ENCAPSULATED SECURITY PROTOCOL) TUNNEL MODE

This mode provides the highest level of security between gateways while the payload information and the original IP header is encrypted and encapsulated. The original IP datagram is encapsulated in a new IP packet using a new IP address as the source/destination of the packet.

ESP (ENCAPSULATED SECURITY PROTOCOL) TRANSPORT MODE

In ESP Transport mode, only the payload of the original IP datagram is encrypted. Like ESP Tunnel mode, ESP Transport mode uses 40-bit/56-bit DES or 168-bit Triple DES. Ravlin 4 units also support Authentication Header (AH) Transport mode and Authentication Header (AH) Tunnel mode, which use strong authentication and anti-replay to secure IP datagrams without encrypting the data payload. ESP Transport mode uses hashing methods to ensure that the data stream is not modied.

ENCRYPT-IN-PLACE (EIP) MODE

In EIP mode, only the payloads of IP datagrams are encrypted. Like ESP mode, EIP mode can use 40-bit/56-bit DES or 168-bit Triple DES. EIP mode is a RedCreek proprietary secure VPN technology. Although EIP mode is not part of the IPSec standard, it combines high speed with all levels of encryption.

### ANTI-REPLAY SERVICE AND USE OF UNIQUE X.509 v.3 CERTIFICATES

Ravlin 4 uses IPSec anti-replay services to prevent intruders from inserting rogue packets into a data stream. With anti-replay service, each IP datagram passing within the secure association is tagged with a sequence number. On the receiving end, the datagram is blocked if its sequence number does not fall within a pre-specied range of sequence numbers.

The Ravlin 4 supports any unique X.509 v.3 digital certicate for strong user authentication and policy management. This lets network administrators integrate Ravlin 4 units into the Public Key Infrastructure (PKI) programs for additional levels of authentication and strong network security policy management.

STANDARDS-BASED SECURITY AND MANAGEMENT

• Complies with the security standards developed by the Internet Engineering Task Force (IETF) IP Security (IPSec) Working Group

• Ensures information privacy using full 40- bit/56-bit DES (Data Encryption Standard) and 168-bit Triple DES

• Provides access control through the use of International Standards Organization (ISO) X.509 v.3 digital certicates

REDCREEK®

SECURING THE NET

T
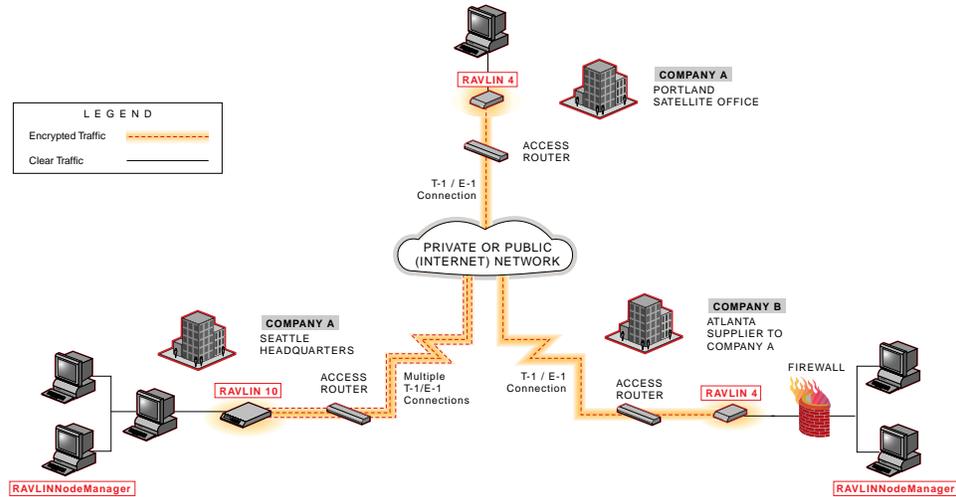
RAVLIN® 4

Using Ravlin to establish Secure Intranets and Secure Extranets

RAVLIN 4 TECHNICAL SPECIFICATIONS

Throughput	40% of the theoretical maximum of Ethernet.
Dimensions	1″ H x 6″ D x 4″ W / 2.54 cm H x 15.24 cm D x 10.16 cm W
Weight	5.9 oz. / 0.2 kg
LAN Interface	Two 10BaseT ports per device
Management Interfaces	10BaseT Ethernet (in-band)
Firmware Upgrades	Download to ash via RavlinNodeManager
Power Requirements	DC power - 9 to 14 volt power supply at 1/2 amp. For use in a 110 - 120 VAC, 60 cycle unconditioned power environment. An international power supply is available.
Safety Certication	CE
EMI/RFI	CISPR EN 55022B

- Veries the sender's identity with Digital Signature Standard (DSS) and Secure HMAC-MD5 and HMAC-SHA-1 Hash Algorithm (SHA) protocols

- Establishes and maintains secure communications using the Internet Security Association and Key Management Protocol (ISAKMP) v.9/Oakley

- Provides enhanced condentiality to IP datagrams through the IP Encapsulating Security Payload (IPESP) Tunneling Mode protocol

- Uses industry-standard SNMP MIB II for device management

- Provides support for the following protocols:

  - Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP) Ping, Address Resolution Protocol (ARP), Simple Network Management Protocol (SNMP)

INTEROPERABILITY

- ISAKMP/Oakley for key management

- Encapsulated Tunneling (IPESP) for interoperability with rewalls

- Standard 10BaseT inputs and outputs to drop into any Ethernet AH network

- Operates at ISO Network layer 3 making it application independent

LOW COST OF OWNERSHIP

- Preserves investments in existing network hardware and software by dropping transparently into the network without requiring modication to the existing network infrastructure.

- Delivers best price and performance for network security products.

- Allows signicant network cost savings by ensuring secure communications and data privacy over public networks like the Internet.

CUSTOMER SUPPORT/SERVICE

RedCreek Communications, Inc. believes that customer advocacy and support are critical to our success. Because of this belief, we offer innovative support programs to assist with installation and conguration of Ravlin products. Traditional technical assistance and support are provided by RedCreek's Customer Support Center. Please reference our Customer Support link: http://www.redcreek.com