RAVLIN® 10

WIRELINE PERFORMANCE
ENCRYPTION SPEEDS FOR ETHERNET NETWORKS

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

PRODUCT OVERVIEW

The RedCreek Ravlin 10 is a cost-effective network security solution that performs encryption and decryption with a throughput of the theoretical maximum of Ethernet (or "wire" speed). Network administrators use it to establish private communications within secure intranets (between corporate divisions, workgroups, branch ofces, and individuals) or within secure extranets (between customers, suppliers, and strategic partners.) Its low cost allows organizations to establish security over private or public IP networks quickly and easily.

The Ravlin 10 provides data privacy using industry-standard 40-bit/56-bit DES and 168-bit Triple DES encryption. Authentication and access control are provided using 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). The Ravlin 10 maintains the theoretical maximum of Ethernet (or "wire" speed) through the use of RedCreek CryptoCore® technology.

The Ravlin 10 supports RavlinSoft Clients running on Windows® 95, Windows NT® 4.0, and Windows for Workgroups 3.11 systems, allowing remote communications over public and private networks. Organizations can also purchase enhanced rmware to allow strong RADIUS user authentication for standard remote software. Ravlin RADIUS Authentication provides interoperability with user authentication hardware tokens that have standard RADIUS interfaces.

The Ravlin 10 rmware has all mandatory components of the Internet Engineering Task Force (IETF) IP Security Standard (IPSec) for enhanced network security.

IP SECURITY STANDARD (IPSec)

IPSec is the most secure and comprehensive standard available today for encryption, authentication, key management, and anti-replay services.

IPSec protocol interoperability lets Ravlin products exchange 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 upon request.

The Ravlin 10 rmware supports the strongest suite of IPSec network security enforcement features available today. Using RavlinNodeManager, the Ravlin 10 rmware gives the network administrator or security manager a choice of several secure VPN operational modes.

ESP (ENCAPSULATED SECURITY PROTOCOL) TUNNEL MODE

ESP Tunnel mode provides the highest level of security between gateways. The original IP datagram is encapsulated in a new IP packet using a new IP address as the source/destination of the packet. ESP Tunnel mode uses 40-bit/56-bit DES or 168-bit Triple DES encryption.

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 10 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 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 uses 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 10 uses IPSec anti-replay services to ensure that rogue packets cannot be inserted into a Ravlin protected 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.

FAST ENCRYPTION WIRELINE PERFORMANCE WITHOUT NETWORK DEGRADATION

- Third party tested and validated at encryption/decryption speeds of 100% of media throughput for all packet sizes.

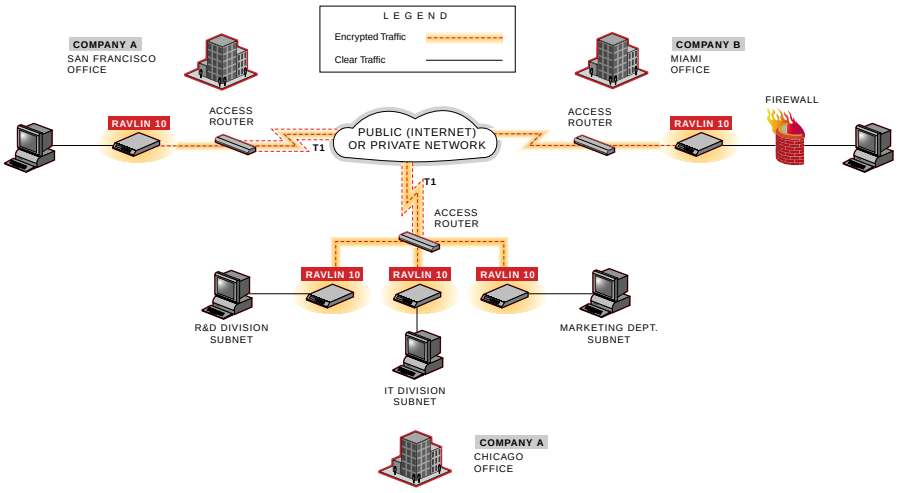
EASE OF IMPLEMENTATION AND ADMINISTRATION

- Integrates easily into existing networks through 10BaseT inputs and outputs
- Secure download of product upgrades to Ravlin 10 ash memory
- Easy device management through industry-standard SNMP MIB II
- Automatically congures to operate in an IP network through Dynamic Host Conguration Protocol (DHCP)

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 and 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

RAVLIN® 10



Using Ravlin to establish Secure Intranets, Secure Extranets and Secure Remote Access.

RAVLIN 10 TECHNICAL SPECIFICATIONS

Throughput	The theoretical maximum of Ethernet (or "wire" speed)
Dimensions	1.75" H x 11" D x 8.75" W / 4.45 cm H x 27.94 cm D x 21.59 cm W (Two Ravlin 10s t side by side on a standard IU 19 inch rack shelf.)
Weight	2lb. 3 oz./1.0 kg
LAN Interface	Two 10BaseT or RS-232 AUI Ethernet ports per device
Management Interfaces	Front panel, 10BaseT Ethernet, RS-232
Firmware Upgrades	Download to ash via RavlinNodeManager
Power Requirements	DC power - 9 to 14 volt power supply at 1 amp. For use in a 110-120 VAC, 60 cycle unconditioned power environment. An international power supply is available.
Safety Certication	CE
Tamper Evident Status	FIPSs 140-1, level 2
EMI/RFI	CISPR EN 55022B
Option	Remote Access Feature
IPSec Compliant	ICSA Certication

- 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), Dynamic Host Conguration Protocol (DHCP), Internet Control Message Protocol (ICMP) Ping, Address Resolution Protocol (ARP), Simple Network Management Protocol (SNMP)
  - RADIUS support with optional rmware at additional cost

INTEROPERABILITY

- ISAKMP/Oakley for key management
- Encapsulated Tunneling (IPSec IPESP) for interoperability with rewalls
- Standard 10BaseT inputs and outputs to drop into any Ethernet 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

REDCREEK®
RedCreek Communications®, Inc.
3900 Newpark Mall Road
Newark, CA 94560
Main: 510.745.3900/888.745.3900
Fax: 510.745.3999
World Wide Web: www.redcreek.com

SD-00010 A 10/98