DELIVERING TRUSTED NETWORKS

DELIVERING TRUSTED NETWORKS
Table of Contents

EXECUTIVE OVERVIEW

Distributed systems and extended networks make business more productive. But with this added productivity, unprotected corporate data is traveling into potentially dangerous new neighborhoods. As a result, this data is getting "mugged" on an unprecedented scale: The cost of computer crime is rising at an alarming rate according to the Computer Security Institute's annual "Computer Crime and Security Survey". 72% of the 520 respondent companies acknowledged suffering financial losses from security breaches in 1997. The combined lose from computer security crime totaled over $136 million dollars. A 36% increase over 1996 loses. (*Computer Security Institute, 1998*)

Stung by losses, or fearful of being the next victim, corporations are encrypting data so that wherever it may travel on the distributed network (intranet) or public network (Internet) it is unintelligible and unusable to would-be data thieves.

Previously known as slow, cumbersome, and expensive, encryption technology has matured to meet required design characteristics:

- Standards-based
- Fast (supporting wireline speed)
- Easy to manage
- Easy to use
- Low cost

RedCreek Communications meets these requirements in its Ravlin family of encryption products. All of the products in the family are based on the fully scalable Ravlin architecture. This scalability, coupled with Ravlin compliance with the Internet Protocol Security Standard (IPSec) for authentication, firewall access control, and encryption standards, enables network managers to address their security requirements across widely diverse environments.

INTRODUCTION—
DELIVERING TRUSTED NETWORKS

Encryption technology is ancient in computing terms. However, the rapid growth of networks and the desire for new applications to support business needs have forced a near-total redesign of traditional encryption systems. This report discusses selecting encryption products to implement a Trusted Network and provides real world applications in a Trusted Network. A Trusted Network is defined as one that can be depended upon to run critical business applications, because it is known to be reliable, cost-effective, manageable, standards-compliant and, most important, secure.

The concept of the Trusted Network has come into new prominence with the rise of the Internet. The Internet enables organizations to distribute information, collect information, and communicate at minimal cost.

There is only one problem: Due to its total lack of security, the Internet is not a Trusted Network. Internet communications are acceptable for non-critical inter-office communications; however, network managers are increasingly uncomfortable with the idea of sending proprietary information across the Internet without some protection of corporate data. The information can too easily fall into the wrong hands.

Most traditional security systems were designed to protect an organization's data storage systems. But the Internet carries data beyond the electronic barriers into the public arena. The Internet also opens up security holes in electronic barriers so even stored data is now at risk.

To address these problems, the Virtual Private Network (VPN) was created for intra-and inter-company use of the Internet. VPNs rely extensively on new encryption and authentication technologies to ensure the privacy of transmissions. This enables managers to extend Trusted Network security characteristics onto the highly cost-effective Internet.

In this report, RedCreek Communications, a leader in Trusted Networks, looks at VPNs and the new encryption architectures designed to implement them. These systems can protect your information today and, with planning, they will provide the foundation for the emerging business applications of the 21st Century.

SECTION 1
SECURITY AUDITS AND POLICY

Today, the vast majority of all data travels across shared networks (e.g. LANs and Intranets) and, increasingly, over public networks (e.g., the Internet). In either case, the traffic is often highly vulnerable to attack. The first steps in building a secure network are a Security Audit and a re-examination of the business's Security Policy.

THE SECURITY AUDIT

The security audit systematically identifies security vulnerabilities in the network-computing environment.

The audit is predicated on assumptions about the types of attacks that may be mounted, such as wiretaps and sniffing, password guessing, and "spoofing" (Spoofing is when an attacker generates traffic that replicates or resembles traffic from a trusted user or machine).

The likelihood of password guessing and spoofing has increased in recent years, because of the growing power of end user computing platforms and the sophistication of end users. Vulnerability to a wiretap and sniffing attack has increased even more dramatically, because of two important changes in traffic patterns. First, because of increased Internet connectivity, data is much more likely these days than in the past to traverse a public network.

The second change is the tendency toward centralizing servers. Until recently, the rule of thumb was that 80% of network traffic remained on the segment where it originated. Today, with many key servers residing on backbones in data centers, that rule has been reversed: Only 20% of network traffic remains on the segment where it originated *(Source: Cisco Systems, Bay Networks, et al).*

The result is that companies need to be much more concerned about sniffing attacks today than in the past. Internal abuse is responsible for over 70% of all data security problems (*Source: Yankee Group*).

The firewall is the first line of defense against password guessing and casual intrusion attempts. Firewall sophistication is being improved continually to meet the latest hacker innovations and attack strategies. In addition to firewalls, companies may choose to encrypt data leaving a network or a host. Encryption means that, even when data is transmitted outside the firewall (or if a host firewall is somehow penetrated), the data will be unable to read. Encryption may also be used on individual hosts to encrypt files or other data stored on servers and provide protection in the event that the firewall is compromised.

For a wiretap and spoofing attack, data encryption is often the only effective protection. In reality, any time a transmission crosses a shared or public network, it may be intercepted and read unless it is encrypted.

STRATEGY AND POLICY FORMULATION

The Security Audit identifies problems. Security Strategies describe solutions at a high level, while the Security Policy outlines specifically what each employee must do to implement the security strategy. Strategy and policy formulation must deal with costs, determining not only what is desirable, but also what is affordable.

There are three types of costs associated with security:

- Product-related costs, including the purchase price of products, and implementation and training expenses.
- System and network performance degradation due to security functions, such as encryption and access control (e.g. firewalls).
- Reduced productivity due to lost or forgotten passwords, or the need to comply with complex security procedures.

The purpose of security strategy formulation is to find a balance point between strong security and cost. Performance degradation, in particular, is a cost that many end users are unwilling to pay. Thus, a hardware-based encryption device that costs $1,500 may be well worth the price if it helps ensure that software only-based encryption doesn't bog down a $20,000 or $30,000 server.

Organizations must determine how much security they are willing to pay for. For instance, the most airtight solutions for authenticating and authorizing a user requires the user to provide three types of proofs: something you know, something you have, and something you are. "Something you know" includes passwords and user IDs. "Something you have" includes a password from a one-time password generator, as well as a digital certificate or private key that is stored in a secure area on a server or on the local hard disk of a desktop or laptop computer. "Something you are" includes biometric characteristics

such as fingerprints, voice prints, and retinal patterns.

However, due to cost considerations, most organizations opt for solutions based only on something you know (passwords and user IDs), or else on both something you know and something you have (e.g. an encryption system that requires both a hardware encryption/decryption device and a password).

Firewalls are often the next security strategy that organizations consider. This is a holdover from the days when most traffic didn't leave the segment where it originated. By keeping intruders off a critical segment, the organization implemented strong security for 80% of the data on that segment. Today, firewalls are better than ever at keeping intruders out of the areas they guard. However, with 80% of corporate data available throughout the enterprise, the firewall addresses only a small proportion of most organizations' security requirements.

Encryption addresses this growing problem of corporate data transmission trends. It ensures data privacy, even when the data is traversing backbones or public networks. If decryption requires both something you know and something you have, a very strong security solution can be implemented.

SECTION 2
ENCRYPTION SYSTEM REQUIREMENTS

When encryption was a minor factor in most security solutions, organizations could often make due with encryption solutions that slowed communications and increased costs of systems and administration. Today, with encryption fast becoming a ubiquitous feature of data networks, organizations need fast, easy-to-manage encryption systems that operate without user intervention and are impervious to user carelessness.

The following are the primary requirements for providing these features:

- Security
- Performance
- Manageability
- Transparency
- Scalability
- Reliability
- Standards-based
- Low cost

SECURE

Obviously an encryption system only has value if it provides adequate privacy. The many different types of encryption provide protection ranging from minimal to very secure. The encryption system should be appropriate to the value of information, the resources of a likely attacker, and the timeliness of the information.

Conceptually, with sufficient time, weaker encryption schemes can be broken. Computers are the primary attack weapon. With computer power doubling every 18 months (Moores Law), it may seem that any encryption system is very vulnerable. Actually, the widely adopted Data Encryption Standard (DES) normally provides adequate protection in its 56-bit key version.

Triple DES provides even greater security. Triple DES (112-bit or 168-bit), which cycles each message through the encryption process three times, using two or three separate DES keys, is believed to be unbreakable for practical purposes.

COST AND TIME TO BREAK DES KEYS

		TIME TO BREAK KEY		
TYPE OF ATTACKER	BUDGET	40-BIT	56-BIT	168-BIT 3DES
Individual Hacker	$400	5 hours	38 years	too long
Dedicated Hacker	$10,000	12 minutes	556 days	10^{19} years
Intelligence Community	$10 million	0.02 sec.	21 minutes	10^{17} years

(Source: "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security." Blaze, et.al. 1/96; Schneier B. "Applied Cryptography, Second Edition" John Wiley & Sons, Inc. 1996)

FAST

Speed is virtually a prerequisite for doing business. People simply avoid using networks that are not fast and efficient. Encryption has been known, historically, as a real impediment to network speed.

Poor performance has compromised security, since users tend to avoid using a slow encryption system, even when they should. To provide ubiquitous secure environment, encryption must not create any perceptible degradation in speed when compared to clear line transmissions. Companies don't want to force users to choose between a fast or a safe network. The safe (slow) network, and the company's security along with it, will always lose.

MANAGEABLE

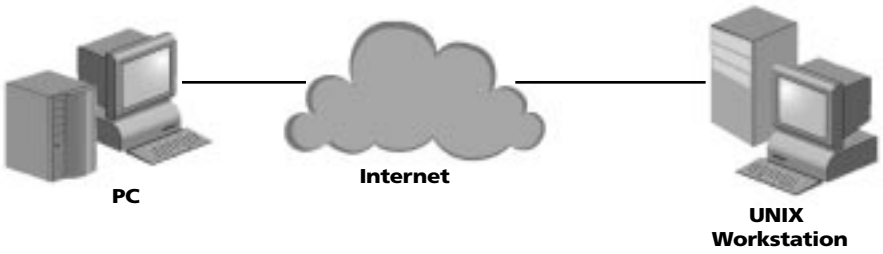
A powerful central management capability keeps management costs down while accelerating management response times. The system should be SNMP-based so that encryption devices can report alerts through enterprise management platforms.

Management systems must facilitate various types of temporary encryption arrangements. For instance, secure VPNs are often set up for temporary workgroups and relationships. Similarly, tunneling often involves very brief network connections that must be dynamically managed.

TRANSPARENT

Encryption systems must be transparent to users as well as to underlying network technologies. Transparency to users means no penalties—no speed degradation and no additional connection tasks.

To other network technologies, transparency means compatibility. In the real world of multiple network types, operating systems, and application environments, the encryption system needs to operate independently. Just as messages cross these different boundaries, so must the encryption that is protecting the messages.



Windows and UNIX are among the dissimilar operating systems on a typical VPN. The encryption solution should be capable of transparently encrypting communications among machines running different operating systems.

SCALABLE

Virtual networks connect sites that range in size from large enterprises, down to one-person and mobile offices. Each of these environments have their own need for bandwidth and connection ports, depending on the number of attached workstations. The encryption solution needs to be available in different design configurations to match the diversity of the site. Yet, collectively these systems need to be capable of functioning as a fully integrated virtual network.

STANDARDS-BASED

Standards-based encryption solutions, because they are based on mature designs that have received industry approval, tend to be more reliable. Moreover, third-party tools and complementary products will be available to enhance encryption products based on standards. In addition, the performance of the combined solution will be dependable. Standards-based encryption solutions also make it easier to replace or upgrade components of the solution without having to replace the entire solution.

LOW COST

Historically, encryption systems have been extremely expensive to purchase, install, and manage. In addition, encryption systems often required expensive hardware upgrades to other network hardware to maintain even minimal levels of performance.

These costs must come down, as encryption becomes a standard feature of networking. A variety of design strategies enable low cost. The most important being scalable, optimized systems built with standardized, low-cost hardware. Thus permitting upgrades and expansion without sacrificing existing investments.

SECTION 3
ENCRYPTION SYSTEM DESIGN OPTIONS

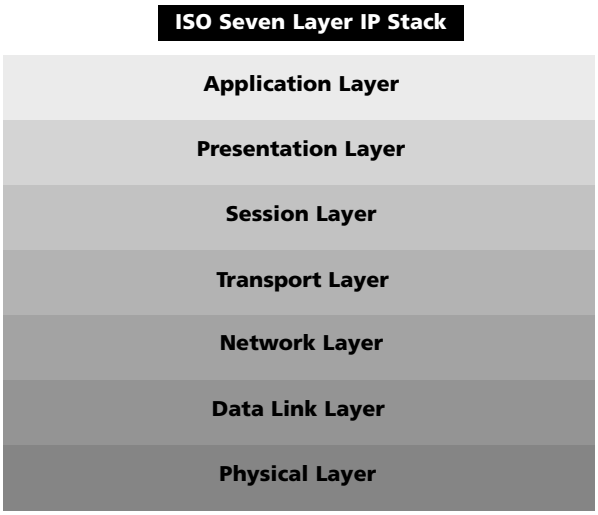
Section 2 looked at the requirement criteria for selecting an encryption system. The requirements for selecting encryption systems are similar to selecting other network components. By contrast, encryption system design options may be less intuitive. This section discusses some of the design options in encryption systems.

APPLICATION-BASED VERSUS NETWORK-BASED

Encryption can be implemented within certain applications. In this environment, communications between devices running identical applications are protected. This type of encryption is often reliable and relatively easy to implement.

The problem with application-based security is one of scale. Once a single-application secure VPN is established, users inevitably want VPN access to additional applications. Some of those applications may offer encryption while others—especially older legacy applications—may not.

The alternative is to base encryption on the Network Layer of the ISO 7 Layer Model. For instance, encrypting all IP packets establishes a tunnel or VPN through the Internet. This approach protects all traffic that passes across a network. Furthermore, it does not preclude additional security at higher levels, such as within the application.

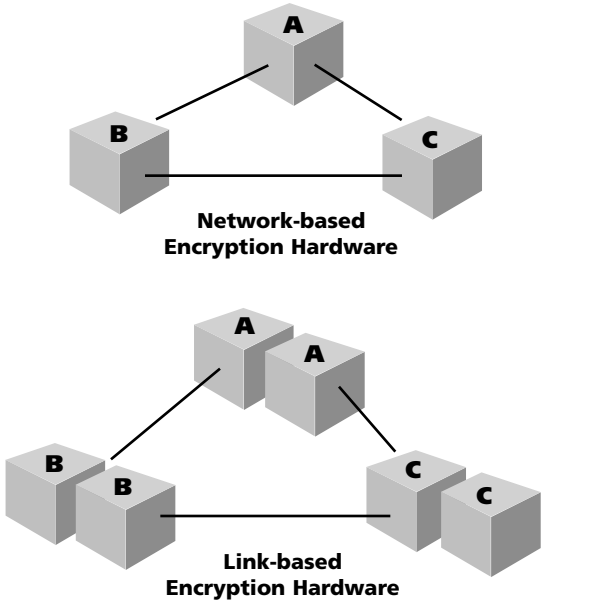


The standard for network-based (ISO network layer) security is the IP security protocol (IPSec), a collection of security standards developed by the Internet Engineering Task Force (IETF), covering encryption, authentication, and key management. IPSec sets up a tunnel through the Internet, manages the tunnel while the connection is in use, and removes the tunnel when it's no longer needed. IPSec can encrypt not only the data payload but also the packet header and address. During tunnel set-up, IPSec protocols authenticate IP datagrams, with key management being supported through the ISAKMP standard (Internet Secure Association Key Management Protocol).

LINK-BASED VERSUS NETWORK-BASED

Early encryption devices were designed to work in pairs, encrypting data that passed over a specific physical link between two computers. Link-based products are still in use, particularly to secure leased line connections. But in most cases they should be re-evaluated based on technologies available today and on the significant cost savings afforded by public networks.

Network-based encryption is independent of physical architecture and was developed to address the need for security throughout a complex network environment. With network-based encryption, one encryption device can handle multiple VPNs.



In the above illustration, network-based encryption requires one encryption device per site (Sites A, B, and C) for a total of three encryption devices. Link-based encryption requires a separate pair of encryption devices for each link. In this example, that means six encryption devices are required.

SOFTWARE-BASED VERSUS HARDWARE-BASED

Encryption is processor-intensive. In software-based encryption, the encryption process runs in a host processor, which can quickly become overloaded if it is also handling other processes. The result is that throughput for encryption and every process on the host can slow to unacceptable levels. This is the same multi-function issue discussed above. In addition, hosts are not optimized for encryption.

In contrast, with hardware-based encryption software and hardware are developed as a dedicated system, other processes won't be affected, and the software can be optimized for the hardware. Optimization enables developers to write fewer lines of code, use less expensive hardware, and produce a faster and more reliable system.

ENCRYPTION ALGORITHMS

The choice of encryption algorithms is a hotly debated issue and one that certainly requires consideration. DES, the most widely used algorithm, has survived years of penetration attempts. During this time it has become a trusted and extremely well defined algorithm.

DES is available in several versions: 40-bit, 56-bit, and Triple DES, which comes in 112-bit and 168-bit versions. In practice 40-bit DES provides privacy from casual hackers, 56-bit DES protects data against serious attack, and Triple DES is stronger than any other encryption system on the market. Banks, for example, have adopted triple DES for financial transactions.

SECTION 4
THE RAVLIN ARCHITECTURE

RedCreek Ravlin is a family of high performance encryption products. All of the products in the family are based on the fully scalable Ravlin architecture.

THE CRYPTOCORE ENGINE

The Ravlin architecture is based on CryptoCore®, a proprietary, patent-pending engine that combines optimized software and parallel processing, implemented with low cost, off-the-shelf components enabling value-priced products. CryptoCore delivers wireline speed through the encryption system. Encryption never slows network throughput, even when encrypting at the Triple DES standard.

SERVICES

Ravlin services include encryption, tunneling, and key management. RedCreek has chosen to adhere to dominant standards, such as IPSec, in each area. This gives RedCreek Ravlin the advantage of being reliable as well as having the broadest possible industry support and interoperability.

Encryption and Authentication—Ravlin uses the DES specification for encryption. RedCreek selected DES because of its strength, its widespread use, and its position as the world's dominant encryption specification. Through the management interface, managers can specify the desired level of DES, 40-bit, 56-bit or 168-bit Triple DES. Along with DES encryption, Ravlin also supports ISO X.509 v3 digital certificates. The use of X.509 digital certificates allows customers to insert their unique X.509 certifications into Ravlin products. This is how Ravlin works within a public key infrastructure (PKI).

Tunneling—Ravlin users can implement IPSec Encapsulated (ESP) Tunneling Mode for even stronger security. In IPSec ESP Tunneling Mode, the entire IP packet (headers and data) is encrypted, with a new IPSec packet wrapped around the outside. By comparison, basic encryption encrypts the payload, but leaves the address in the clear. ESP Tunneling Mode protects against leaving the addresses in the clear and thus protects against an

Ravlin Architecture

attacker capturing the source and destination addresses, where he could use those addresses to attack the private networks of the sender or receiver.

Key Management—One of the important considerations for building VPNs is a reliable method for automatically trading encryption keys over the Internet, a process known as key management. Ravlin implements ISAKMP (Internet Security Association Key Management Protocol). ISAKMP is the key management standard adopted for IPv6 by the IP Security (IPSec) Working Group of the IETF.

SCALABLE PLATFORM

As the architectural diagram shows, each Ravlin implementation is based on a Ravlin platform. Today the Ravlin family includes three different platforms: Ravlin 4, Ravlin 10, and RavlinSoft. All products are interoperable and provide the same levels of security. The different platforms let managers cost-effectively select encryption systems for each connected site based on specific site requirements.

Ravlin 4, with 4Mbps throughput, is designed for LANs, WANs and workgroup environments running at up to T1/E1 speed. Ravlin 10 handles corporate network communications and delivers 10Mbps throughput.

RavlinSoft is a software-only version of Ravlin, designed to run on remote workstations and provide secure connections to corporate resources via the public network.

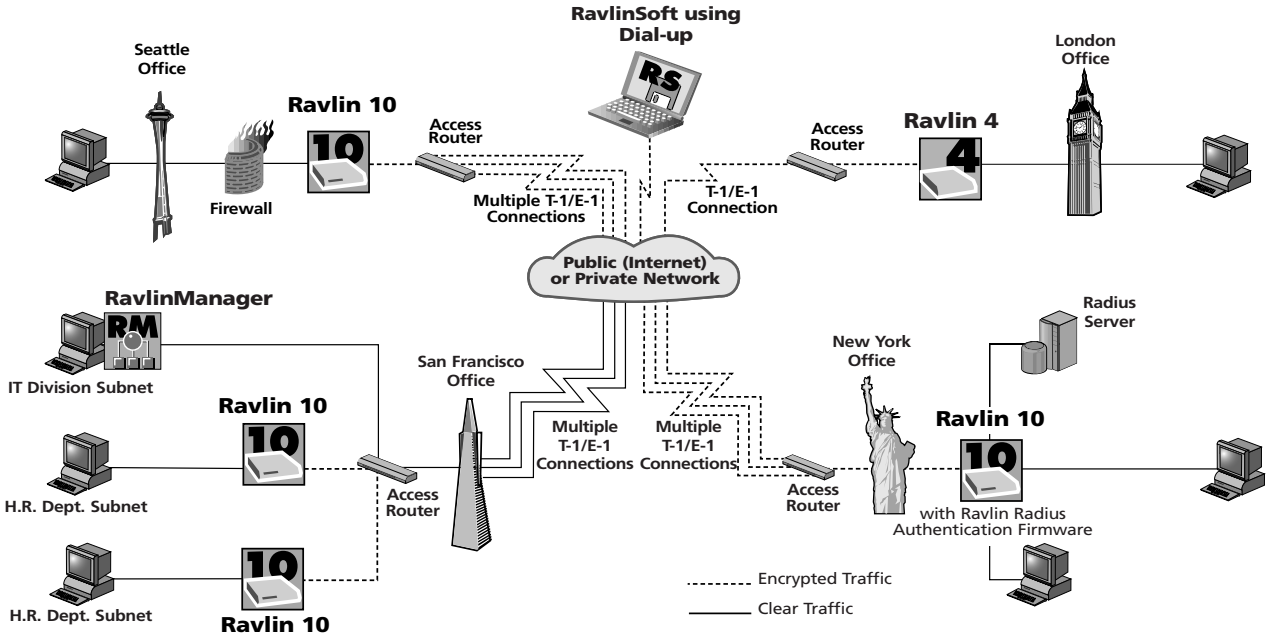
SYSTEM MANAGEMENT

Network managers configure and manage Ravlin secure environments through the RavlinManager. A single RavlinManager can control any number of Ravlin units, whether local or remote. Once secure associations are defined through RavlinManager, the secure VPN operates independently and doesn't require an active RavlinManager.

RavlinManager is fully SNMP-compliant. Operations can be accessed through an SNMP-based management platform. Managers can use SNMP to perform configuration and management tasks, and also use the powerful alert and reporting features of their SNMP management platform to monitor the health of Ravlin systems.

STANDARD EXTERNAL INTERFACES

Ravlin is designed to interoperate with other standard security systems on the network. A Ravlin system can be integrated transparently into existing standards-based networks, and managers can build multi-layered security strategies using best-of-breed products from multiple vendors.



Ravlin In The Network

User/Device Authentication

In the area of user/device authentication, Ravlin supports the following:

- Authentication, Accounting, Auditing: RADIUS
- Tokens: SDI SecurID, Bellcore S/Key, Enigma Logic, Cryptocard
- PKI: LDAP, RADIUS, CiscoCA Enrollment Services, X.509 digital certificates

Standard Firewall Interface

Ravlin operates in conjunction with firewalls. Because of this, network managers can choose a standards-compliant firewall based on specific firewall features and know that the firewall will work with all Ravlin functions.

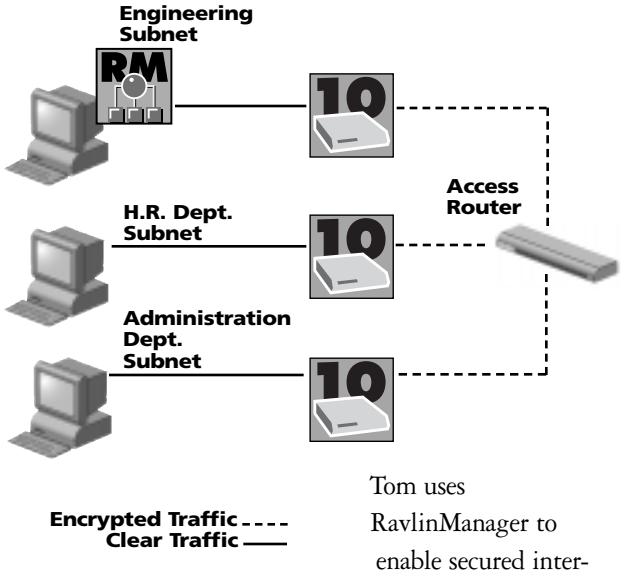
SECTION 5
NETWORK SECURITY IN THE REAL WORLD

Ravlin is designed to be a reliable foundation for corporate network security. To illustrate how it works, we're going to follow a network administrator named Tom as he uses Ravlin to protect his network.

SEGMENTING THE NETWORK (Intranet Security)

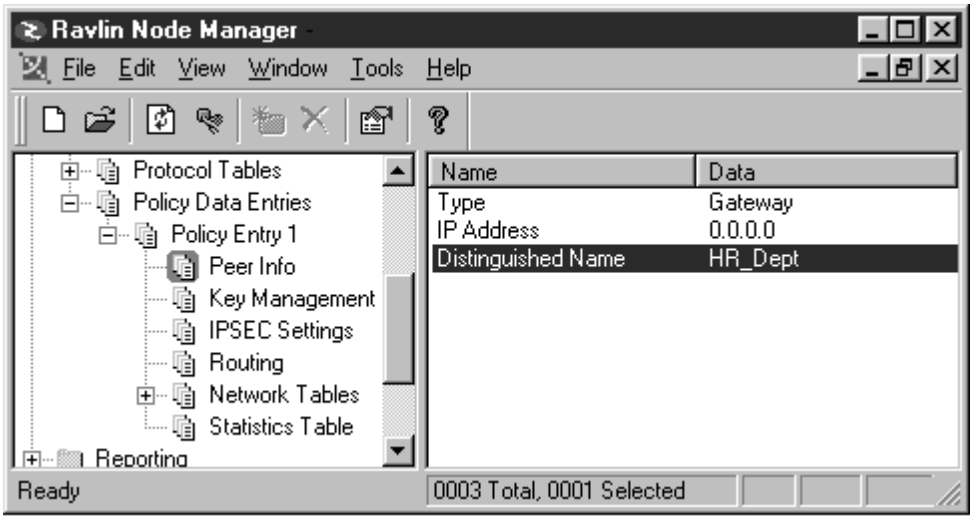
Tom's corporation has a distributed network through which employees send e-mail and share computing resources. Data privacy has typically relied upon authentication using user names and passwords; however, through a recent security audit, the corporation has identified a need for encryption, and authentication based on digital certificates. Tom has been asked to provide this level of privacy among three departments—Human Resources, Administration, and Engineering, which reside on separate subnets within the same corporate LAN.

The corporation is already using RedCreek Ravlin for its communications outside the corporate offices. Tom now decides to use Ravlin encryption to build Security Associations (SAs) among corporate subnets connecting the departments. Tom installs a Ravlin 10 inside each subnet so that network traffic within each subnet is encrypted and a unique SAs established in each department.



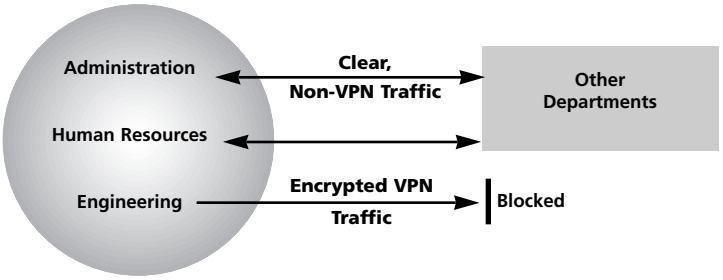
Tom uses RavlinManager to enable secured inter-departmental communication. He designates certain users as Trusted Partners. He then uses the RavlinManager to build Security Associations among those Trusted Partners and some or all of the departments.

After a review, Tom decides to improve security for Administration Department's



executives. Although the whole department is on one network segment, or LAN, the segment includes both corporate executives and administrative services. Tom uses the RavlinManager to build a Security Association between the Administration Department and the HR department, which are on separate subnets. With Ravlin, Tom is able to protect specific communications between Administration Department executives and HR executives. People in other departments cannot intercept the secure communications between the Administration subnet and the HR subnet. Encryption and authentication between the two departments protect those communications.

Ravlin supports two types of network environments: open and closed. Tom configures the Human Resources and Administration networks as open network environments. This means that traffic can be sent to unprotected sites in the clear, while traffic between HR and Administration will be encrypted. Engineering has requested that its traffic always be encrypted; therefore, Tom configures the Engineering network as a closed environment. In this configuration, the Engineering Department can send encrypted traffic to other units in the secure VPN, but traffic to unprotected sites will be blocked.

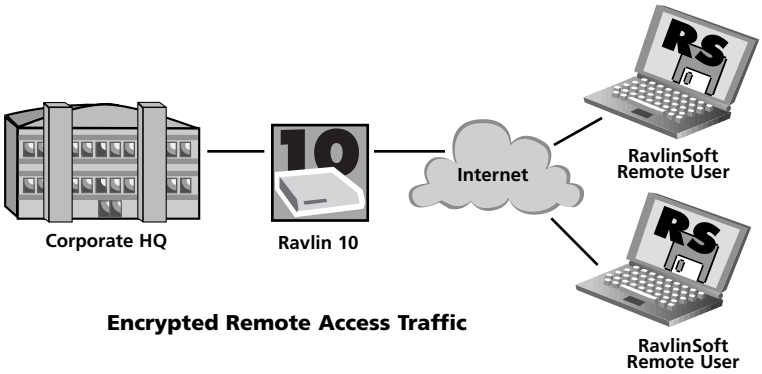


Intra-Departmental Traffic

VPN CONNECTS MOBILE WORKERS (Remote Access Security)

The corporation has traveling workers dispersed throughout the country. They need a secure connection to the corporate network to exchange email and access corporate resources. These workers use dial-up connections to the Internet for network access. Tom decides to use RavlinSoft, the low-cost software version of Ravlin that runs on a PC or laptop, to permit the remote user secure access to the corporate network.

The remote user dials into their Internet Service Provider (ISP) as they normally would. RavlinSoft establishes a Security Association through the Internet to corporate headquarters. To complete the secure connection the user is authenticated by the corporate RADIUS server (if required), which is supported in firmware by the Ravlin 10 at the corporate headquarters. The RavlinSoft client receives a challenge such as "Enter your password," or "Enter your token card code." Once the user enters a response, the response is forwarded via the Ravlin 10 to the RADIUS server. If the RADIUS server accepts the response, the RavlinSoft user is notified and can log in to the network. The RADIUS server thus lets Tom manage authentication, which together with Ravlin encryption creates a Security Association.



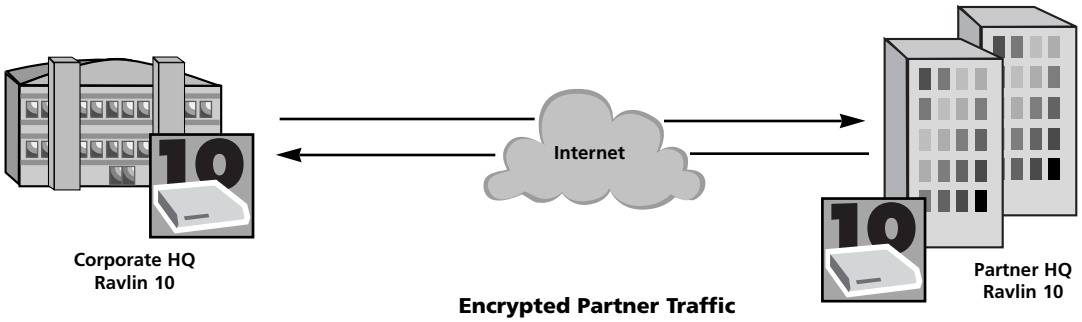
Encrypted Remote Access Traffic

THE PARTNER/SUPPLIER NETWORK (Extranet Security)

Tom's company has established a partnership with another corporation. Tom will use tunneling and encryption to create an Extranet (a VPN that includes sites outside of a single corporation).

As he sets up the partner network, Tom configures a Ravlin 10 to encrypt traffic between Tom's corporation and the partner site. Tom manages this connection with RavlinManager. At the partner site, Tom's counterpart uses her RavlinManager to configure a connection from the partner site to Tom's corporation. Tom has total control over the resources available to the partner at Tom's corporate site, while the partner has the same level of control over the resources available to Tom's corporation at the partner site.

Tom also has several suppliers and has decided to establish a secure Supplier Network (an Extranet with suppliers). The corporation sends a Ravlin 4 to each supplier



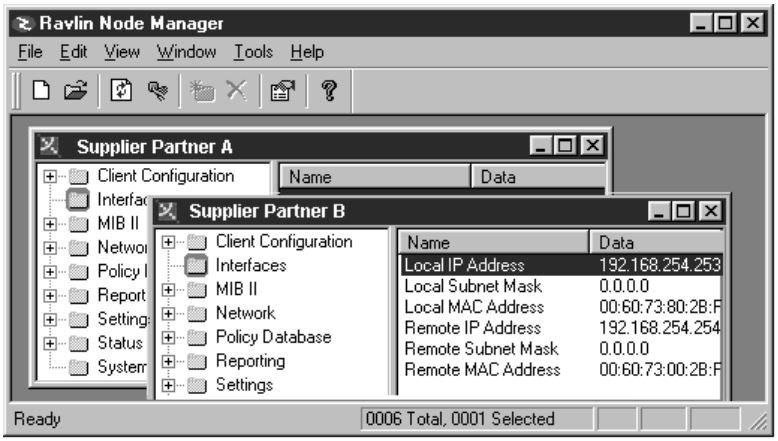
Encrypted Partner Traffic

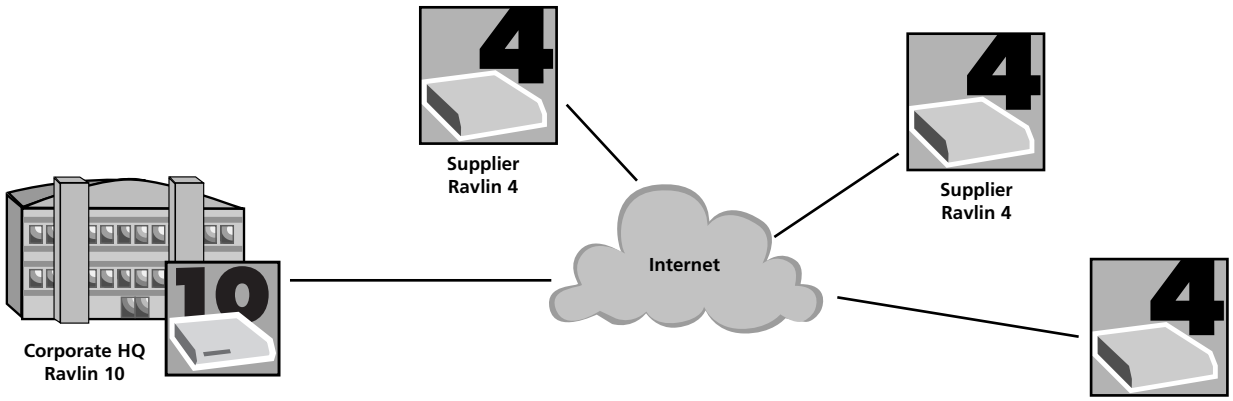
so that the whole Supplier Network/Secure VPN can be managed from the corporation's central site.

Control is a big concern on both sides of the Supplier Network. Suppliers want to be part of the secure VPN, but they want to limit Tom's access to their home network. Tom explains to the supplier that he will build a subnet mask to encompass a server and specific workstations at the supplier's site. The Ravlin 4 will protect only these devices. The supplier's own Ravlin device, as well as authentication and firewalls, should protect the other resources at the supplier's site, where appropriate. These are necessary security precautions for the supplier and will protect its network from any unauthorized access including access from the Supplier Network.

In those cases where suppliers do not want to provide access to Tom, the supplier can use RavlinManager to establish their half of the secure VPN back to Tom's corporation, maintaining control of access to their network infrastructure.

On the corporate side, Tom has control of the RavlinManager that defines the Supplier Network/Secure VPN. He uses this to build Security Associations between the corporation and suppliers. Because he sets the passwords and security IDs for all the units on the VPN, Tom can limit outside access as required. Even if someone has access to their own RavlinManager, without the passwords and security IDs, access would be blocked. If the corporation decided to stop the Security Association between the supplier's site and the corporate home office, Tom could accomplish that with a couple of mouse clicks using RavlinManager.





Encrypted Supplier Network

SECURITY ATTACKS

RavlinManager allows Tom to monitor the network for activity, to perform security audits, and to collect information on security attacks. All of this is done through an SNMP interface that can be integrated into an SNMP-compliant platform manager, such as HP OpenView from Hewlett-Packard or through RavlinManager on a Windows NT® PC.

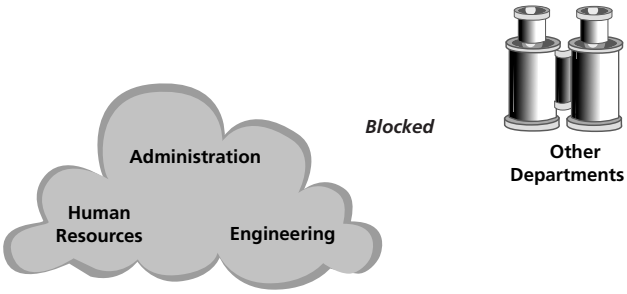
The following examples of security attacks illustrate how the Ravlin encryption product family performs under attack.

SECURITY ATTACK— INTRA-DEPARTMENTAL CONNECTIONS

A disgruntled employee inside the company tries to break into the Security Association between Human Resources and Administration. The attack comes from another department in the company, but within the company's corporate network. Human Resources and Administration are now protected by Ravlin systems, as described earlier in this section.

Using a "sniffer", the attacker is able to capture transmissions between these two departments. However, the Security Association follows the IPSec standard, meaning that the datagrams are encapsulated and encrypted. Thus the attacker is unable to determine the source or the destination of the messages and is also unable to read the messages themselves. The attack fails.

This type of defense eliminates the type of attack known as a "man-in-the-middle" attack in which the attacker talks to system A, pretending to be system B and talks to system B pretending to be system A. Data is protected because it is impossible to distinguish packet origination or destination. This same level of privacy covers anyone who is protected by a Ravlin SA, whether communications are within a corporation, as in the example above, or outside the corporate network on an Intranet or Extranet.

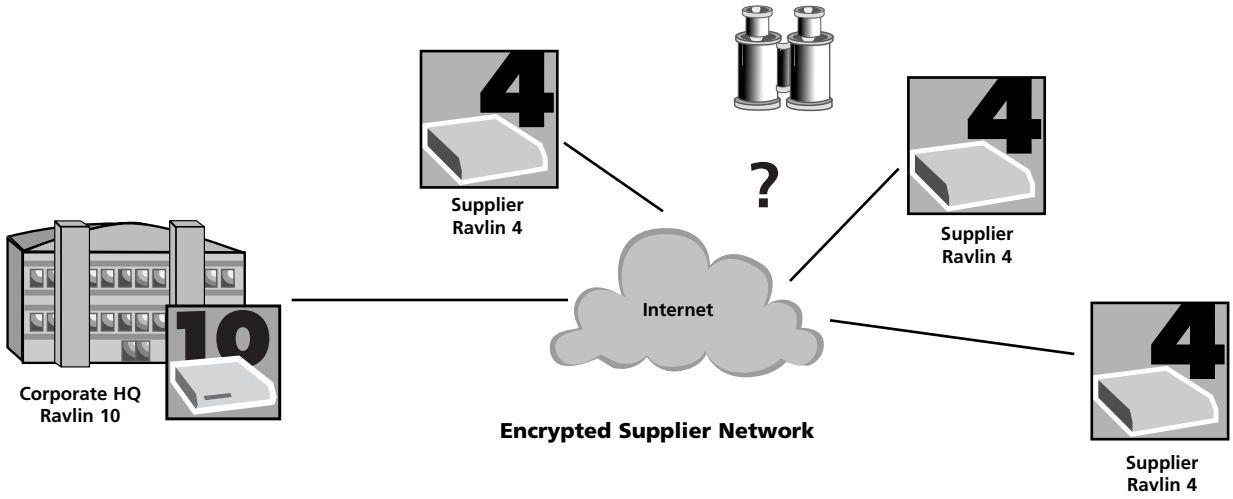


Encrypted VPN Traffic

SECURITY ATTACK— INTERNET TRANSMISSIONS

A person captures an Internet transmission between the corporation and its supplier (where Tom has just set up the encrypted Partner Network). The purpose of the attack is to examine messages, to capture user names and passwords, and to analyze traffic patterns between senders and receivers. (Because keys are exchanged, the attacker can set up a man-in-the-middle attack.)

This attack will fail because the Ravlin system is fully IPSec compliant and Tom has applied ESP Tunneling Mode in building the Suppler Network. In this mode, the original source packet is completely encrypted and encapsulated, including the payload message and the source and destination IP addresses. New routable source and destination addresses are appended to the encrypted packet so that it can move through the Internet.



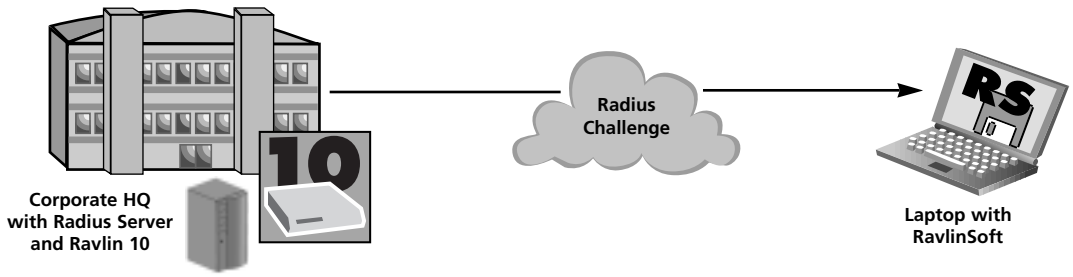
Encrypted Supplier Network

These new addresses, however, simply identify it outside the corporate router and the attacker is unable to identify the actual source and destination. With the whole packet encrypted, the attack is neutralized.

SECURITY ATTACK— RAVLIN-EQUIPPED LAPTOP IS STOLEN

A corporate executive has her laptop stolen while she is traveling. The thief attempts to use the laptop, which contains the RavlinSoft program, to log in into the corporate network and attack online resources.

In this situation, even though the attacker has a copy of RavlinSoft and the system is configured for accessing the corporate network, the attack will fail. As a prerequisite to the secured connection, RavlinSoft passes a request through the Ravlin10 to a RADIUS authentication server at the home office. RADIUS sends back a challenge to the laptop, often for a user name and password. In this case, Tom has also set the RADIUS server to lock-out a user after three failed log in attempts. After the third attempt has failed, RADIUS will send an alarm to Tom informing him of an attempted break-in on the network.



Stolen Laptop Offers No Access

SUMMARY

Computer networking has entered a new phase, characterized by easy access, much heavier use of backbones and public networks, and networks that extend to remote offices, telecommuters, business partners, suppliers, outsourcers and customers.

Under the pressure of these changes, many companies are re-evaluating their security policies, procedures and technology and recognizing the need to make much wider use of encryption technology to protect data wherever it may travel, and despite intrusions.

This report has presented a new model for network security based on encryption technology. To be suitable for widespread deployment, encryption must be fast, manageable, transparent, scalable, robust, standards-based and economical. We call this model the Trusted Network.

Both economy and fault tolerance tend to dictate dedicated, modular hardware devices for servers and backbones. For workstations, on the other hand, inexpensive encryption software running on the host processor may take advantage of spare processing capacity.

RedCreek Ravlin is a scalable family of encryption products designed to meet these exacting new requirements in network security.

For further information please contact RedCreek directly at 1-888-745-3900 or visit our website at http://www.redcreek.com

Written for RedCreek by:
Michael Durr & Associates,
Tel: 941-540-0483