

IP Security: Building Block for the Trusted Virtual Network



intel[®]



Table of Contents

Executive Summary

The Growth of Computer Crime	2
<i>As the Internet Grows, So Does the Threat</i>	2
<i>Definition of the Trusted Virtual Network</i>	3
An Inside Job	3
The Need for a New Security Model	4
<i>Elements for Building a Trusted Virtual Network</i>	4
<i>IPSec: An Essential Building Block</i>	5
What Is IPSec?	5
<i>How It Fits the Virtual Network</i>	5
<i>How It Works</i>	6
<i>Enhanced Security and Cost Savings</i>	7
<i>IPSec-related Work by Intel</i>	7
Conclusion	7
<i>Initial Deployments</i>	8
For More Information	8

Executive Summary

Companies are placing a growing volume of valuable and sensitive information on the Internet, extranets and intranets. As this data proliferates, it poses an increased risk to corporate security.

A recent study (FBI/CSI Computer Crime & Security Survey, 1999) shows that most security breaches occur within the Local Area Network (LAN). While traditional solutions such as firewalls will continue to be used to protect the perimeter of the corporate enterprise, additional layers of protection will be needed. An overall industry effort will be required to create the various pieces needed for a comprehensive, multi-layer solution.

Intel plans to provide key building blocks to support this effort. A significant piece will be IPSec (Internet Protocol Security), a standard defined by the IETF (Internet Engineering Task Force) that provides IP

network layer protection. Implemented at the network interface, IPSec will help enable the trusted, connected PC. It can also be used to create a common protocol for building VPNs (Virtual Private Networks).

This white paper discusses the need for a network-level, standards-based security solution and describes the factors that make IPSec an ideal technology for this purpose. It should be of interest to the IT manager and CIO as well as those involved in hardware and software development.

The Growth of Computer Crime

Millions of people are getting connected to the Internet and doing business in the electronic world. Business-to-business electronic commerce today represents about \$100 billion. This number is expected to grow to almost \$1 trillion by the year 2002 (Forrester Research, 1998). More

and more business data, much of it critical or sensitive in nature, will be placed online as a result of this growth.

The evolution of the new electronic economy is placing increased value on the Internet. The business community has realized that in addition to traditional sources of value, such as cash and equipment, there is now an equally important source of value in a company's intellectual capital — the sum total of its knowledge and information. Oftentimes the value of this intellectual capital dwarfs the value of a corporation's hard capital. This new form of wealth is attracting a new kind of criminal activity.

As the Internet Grows, So Does the Threat

The Internet is changing today's business model in ways that facilitate commerce but can compound security problems. Traditionally, the enterprise consisted of LANs linked by leased lines or other private media to form a closed system. Today, there is a new, more open business model consisting of one "virtual network."

The new business model is enabled in part by a growing number of extranets, where suppliers and customers can work together on the network. Implementing an extranet requires a company to put its intellectual capital out onto the Internet. There, the valuable data can theoretically be accessed by anyone.

Corporations are also turning to the Internet as a WAN connectivity solution that is less expensive than paying leased line charges.

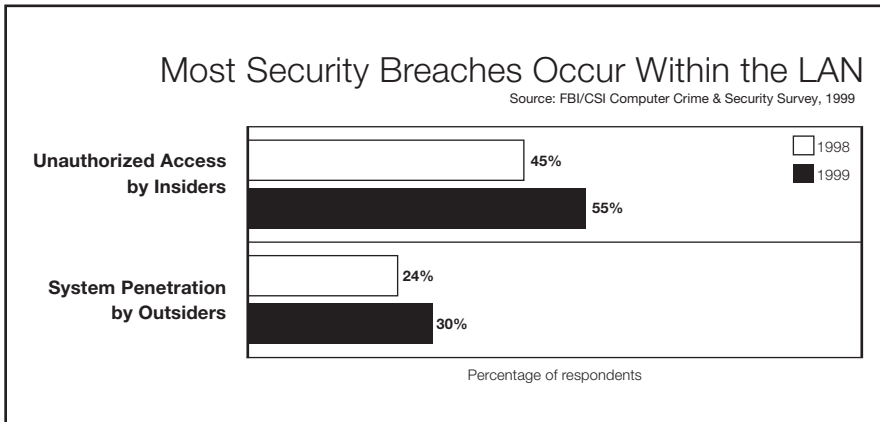


Figure A

In effect, this solution incorporates a form of public communication into the boundaries of the enterprise.

In addition, many companies are using their corporate LANs as more critical business tools. Just as more data is now exposed to other companies on an extranet, more data is also exposed to employees on the LAN today.

Security breaches can be intentional or unintentional. People who have access to a corporate network, but are unfamiliar with a company's policies and procedures, can make mistakes and accidentally damage critical data.

Definition of the Trusted Virtual Network

With the rise of e-Business, a fundamental change in the nature of our communications infrastructure is dictated. Closed networks, whose access were once limited only to desktop workstations, are now open to remote employees, suppliers and partners. This is the difference between e-Commerce and e-Business.

The former is about selling products on the Web, while the latter is about seamlessly integrating communications with others. Doing so requires us to open our networks to the world.

While this certainly speeds business operations, it brings with it other perils. It can leave data open to unintended access. The ease with which anyone may install and use a "sniffer" program to monitor LAN traffic serves as a pointed reminder of data vulnerability. Consider the following examples:

- Two high-tech firms partner on a new product and must trade highly secret design data. Doing so requires each firm to allow sensitive data to travel on the other's LAN, over which they have no control. How will each firm assure the other that the design data will not be compromised?
- There is an increasing trend towards the use of contract or temporary employees. The level of trust in, knowledge of, or control over these individuals is not as strong as with permanent employees. How can a company protect itself from a

An Inside Job

According to the FBI/CSI 1999 Computer Crime & Security Survey, 30% of companies polled reported system penetration by outsiders. But even higher crime rates were reported from within the traditional perimeter of the enterprise. According to the same study, 55% experienced unauthorized access by insiders within the past year (up 10% from 1998). (Figure A)

Insider security threats can come from disgruntled employees and contractors. They can also come from suppliers and customers, often inadvertently. Examples cover a wide spectrum:

- A temporary contract employee, who receives a permanent offer at a rival firm, accesses the company's client list in hopes it will provide a "head start" in the new position
- A manufacturing company allows one of its suppliers to access production-planning data on its network, which opens up the possibility that the production data server can become an unintended gateway into other parts of the network
- A trainee attempts to access a human resources department server and change his test scores by identifying himself as the training course instructor

Obviously, sensitive data generated by human resource departments, financial departments, executive staff and compartmentalized teams can be vulnerable to insider abuse even at the LAN or workgroup level. A very high price tag is attached to these "inside jobs." The FBI/CSI survey shows that insider crime is a very expensive type of computer crime, costing companies about \$142,000 per incident.

skilled temporary employee who may attempt to access and retain certain sensitive files?

- A supplier who has been tied into a company's production planning data can only access a certain server that contains the data. However, that server is tied to the rest of the company's LAN. How can the company ensure that an employee of the supplier won't use this server access as a gateway to sensitive data on the LAN?

In each of these cases, the sensitive data faces vulnerabilities *inside* the network's firewall or intrusion detection system—in most cases by people who were authorized to be inside these defenses. With the new paradigm of open networks for e-Business, these types of network protection are important but not alone sufficient.

To operate an e-Business intranet and extranet safely, *a company must protect their data at the source* by securing data traveling on the LAN. This will allow them to create the Trusted Virtual Network that will make their e-Business thrive.

The challenge is that, given its lineage, a network is a fundamentally open and insecure place. For the new business model to be successful, the one virtual network must become the trusted virtual network.

The Need for a New Security Model

One piece of the solution is already in place—the firewall. Typically located at the enterprise perimeter, the firewall controls access to the corporation's electronic resources by filtering out IP packets based on a set of rules. Until now, this type of security solution has been an effective protection method because threats to corporate assets have commonly been on the outside trying to get in.

A simple analogy helps show why this protection is incomplete. When it comes to their physical premises, businesses not only protect the perimeter of a building, but also use interior devices such as motion sensors to protect against a thief who is already inside.

The same principle applies to the network. Additional layers of security are needed to complement each other.

Elements for Building a Trusted Virtual Network

A new approach is needed to keep pace with the security needs of the electronic business model or virtual network (See Figure B). The elements of the virtual network include:

- **LAN security at the desktop and server level.** Most business network communication occurs between a server and its client desktops, and between the desktops in the workgroup. This is also where the greatest inside security threat lies. Authentication, integrity and encryption, implemented in the network interface card, could be used to secure these communications.
- **Access control at the router/ firewall and the mobile PC.** For example, an employee outside the perimeter of the enterprise might need to get into the network to participate in activities as part of a workgroup. In addition to the protection provided by a firewall at the

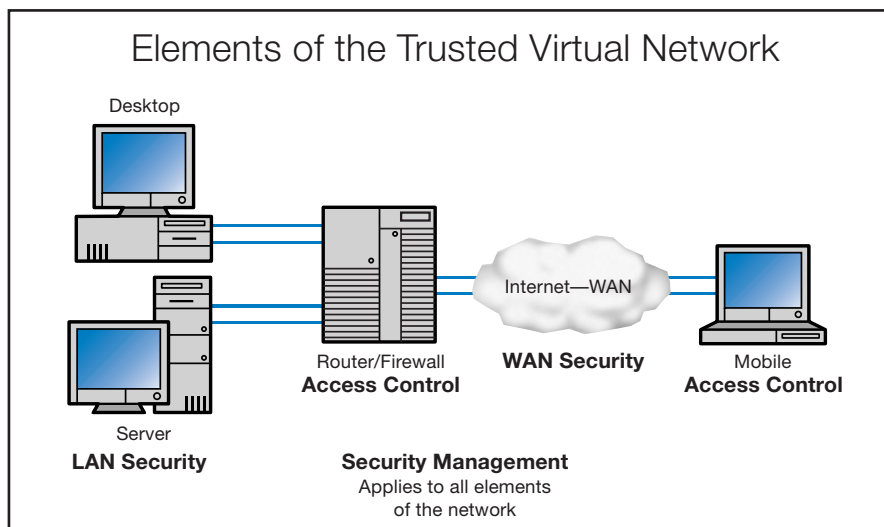


Figure B

perimeter, a Virtual Private Network could be created for protecting communications over the Internet.

- **WAN/Internet security.** A corporation might have a field office that many people at the headquarters campus need to reach on a daily basis and vice-versa. This communication could take place over the Internet, a dedicated WAN or both, but in any case the corporation would need to guard the communications channel against security breaches from the inside and outside.
- **Security management throughout the network.** Today, companies typically use many different security measures across the enterprise. Often they are proprietary solutions that cannot be easily coordinated. In the future, all of the security solutions in the enterprise should be managed in a coordinated way, and ideally they should be developed on common building blocks so that they are interoperable.

To be successful, the solutions must be based on industry-wide standards and globally consistent government policy. They must also be affordable, deployable, scalable and interoperable with the legacy installed base of network infrastructure.

A common management interface for the enterprise, along with manageable rules and policies, will be essential in order to ensure end-to-end security. What is a security management policy? One example might be a “when and how to encrypt” policy by which 168-bit encryption is required when communicating highly sensitive material, but only 56-bit encryption is required for moderately sensitive

material. The sensitivity of the communication is determined by evaluating the type of application, sender’s address or port number, criteria that are easy for network interface cards and other devices to read.

IPSec: An Essential Building Block

An emerging answer to many of these questions is a technology called IPSec (Internet Protocol Security). Open and standards-based, IPSec is becoming widely adopted and is expected to become a de facto basic building block of the trusted network.

IPSec runs at Layer 3 in the protocol stack. As a result, it is transparent to applications, unlike security technologies that run at other layers. This means IPSec is relatively easy and inexpensive to implement, since applications can take advantage of it without having to be altered and users would not have to be retrained.

What Is IPSec?

Defined by the Internet Engineering Task Force (IETF), IPSec is a standard that provides a common means of authentication, integrity and IP encryption. It offers two modes of operation—tunnel mode and transport mode.

One of the principal strengths of IPSec is that encrypted packets can be routed and switched on any network that supports IP traffic. No upgrade to the network elements is necessary. This enables the packets to traverse the LAN, extranet and Internet easily and transparently.

It also means that end stations and applications will not require any modifications. Since IPSec is transparent to the application layer, for example, it can be used in conjunction with existing application layer security software. In addition, VPN solutions using IPSec as the basis for a common protocol can interoperate, opening up new possibilities for securely sharing data.

Benefits of IPSec to the End Customer

- Less expensive branch office connectivity
- Faster, more efficient links to customers and suppliers
- More secure corporate LANs, including better protection against inside threats

How It Fits the Virtual Network

As a basic building block at the network layer, IPSec fits well into the model of tomorrow’s trusted virtual network, playing a key role in LAN security, access control and WAN security. Uses might include the following types of network communications and configurations:

- Peer-to-Peer
- Client-Server
- Protected Workgroup
- Protected Enterprise
- Protected Inter-Enterprise
- VPN and Remote Access

The Network Interface Card (NIC) is an especially useful place to implement IPSec technology. This is the place where end station data is turned into useful security

management information, where data can be queued in order of priority before transport, and where hardware acceleration can be used to the greatest advantage to help facilitate encryption.

An encrypted audio/video stream from a server to its clients provides a good example of the benefits of hardware acceleration. Users would experience much better network performance if the stream were decrypted on an IPSec enabled NIC, instead of via decryption software only. Hardware acceleration in the NIC can help improve network performance by accelerating the many math cycles required by encryption and decryption algorithms. By offloading the process onto a NIC, problems are avoided (See Figure C).

How It Works

As defined by the IETF, IPSec utilizes two principal elements to protect network communications:

- An authentication header (AH) for providing source authentication and data integrity, to ensure the data will not be available to an unauthorized station and will not be altered en route.
- An encapsulated security payload (ESP) to provide confidentiality, ensuring that data will not be intercepted, read or copied.

What are the specific mechanisms for applying these elements? IPSec operates on IP packets as follows:

IPSec AH

For AH transport mode, an AH header is inserted between the IP header and the payload. This provides the Security Parameter Index (SPI), sequence number and other authentication data required.

IPSec ESP

In Encapsulated Security Payload (ESP) transport mode, an ESP header is inserted between the IP header and IP payload. An ESP trailer and authentication MAC are added to the end of the packet. In tunnel mode ESP, the entire packet is encrypted and appended to a new ESP header and IP header, with an authentication trailer added.

Transport Mode Uses

Transport mode is typically used in peer-to-peer communications to provide intranet security. The IP header remains unaltered, so it can be read and used by any standards-based device or software. The data packet is encrypted so that the contents of the IP packet are protected.

Tunnel Mode Uses

Tunnel mode is used for remote access and site-to-site security, including VPNs. By placing the packet into a whole new wrapper, it hides the topology of the protected sites.

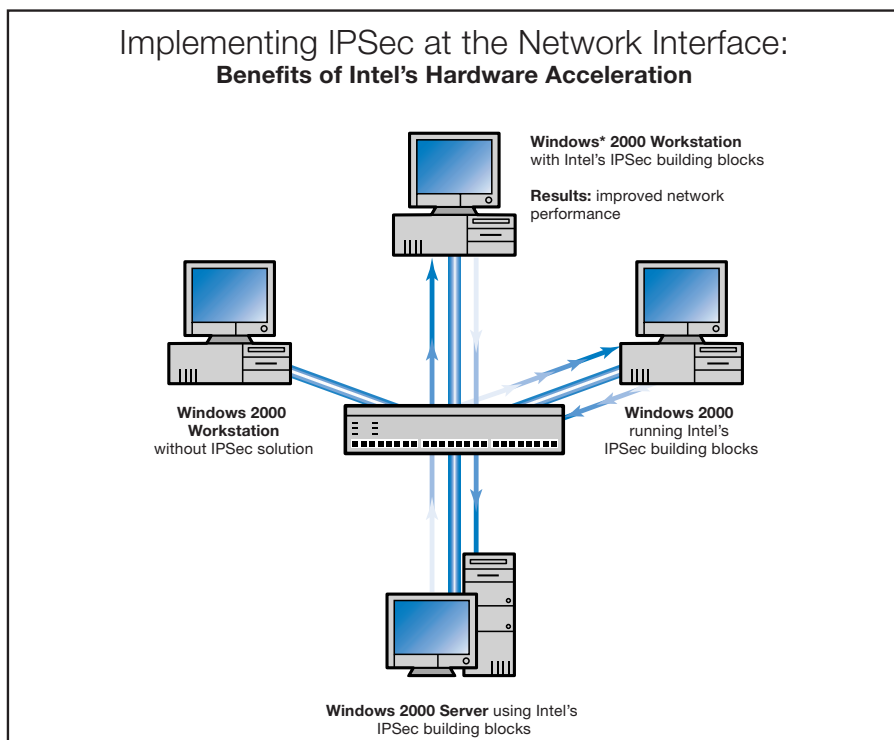


Figure C

Enhanced Security and Cost Savings

Enhanced, multi-layered security and significant cost savings are among the benefits of IPSec implementation in a trusted virtual network.

Intranets/Branch Office Connectivity

Large corporations can save money as more and more IPSec VPN solutions are implemented. Remote users can utilize the Internet via an ISP instead of dial-up lines for access to the corporate network. Accessing a local ISP for connection and using IPSec for encryption can significantly lower telephone charges and equipment costs.

Extranets

IPSec offers the ability to create virtual, protected links through the Internet to customers, vendors and other business partners. Faster, more efficient order-placement, reduced warehousing, lower sales costs and many other benefits of online commerce can help generate savings in this arena.

Corporate LANs

IPSec can be used to create trusted virtual workgroups to help protect sensitive corporate data. For example, the Research and Development Department can be protected from other departments that do not have a "need to know" with respect to this group's confidential information. Or, employee records residing in the Human Resources Department can be protected from unauthorized access.

IPSec-related Work by Intel Corporation

Intel is currently developing IPSec technologies for PC and server platforms, the LAN and the corporate enterprise, and has introduced an entry-level IPSec solution.

The Intel® PRO/100 S Management and Server Adapters are Intel's new IPSec-enabled network adapters, featuring the new Intel® 82594ED network encryption co-processor. Developed in collaboration with Microsoft, these adapters offload the IPSec encryption from the host CPU to the encryption co-processor. Thus, data travelling on the LAN is protected without sacrificing network performance, as is typically the case when using encryption. With offloading enabled, throughput is increased while CPU utilization is reduced, allowing the host CPU to focus on other computing tasks.

The new Intel PRO/100 S adapters currently support the IPSec capabilities of Windows 2000. Please see www.intel.com/network/os for the most current information on IPSec support for other operating systems.

While IPSec is the mechanism for protecting communication, the "When and how to protect" and "When and how to authenticate" decisions are determined by management policy. IPSec must be well managed to be effective, as e-Business expands and the number of companies sharing data and resources grows exponentially.

For this reason, Intel Corporation and Microsoft Corporation have announced the Network Interface Services (NIS) initiative, designed to deliver greater ease and flexibility in the management of network connections for server, desktop and mobile systems.

The initiative enables multi-vendor interoperability and provides an open interface standard based on the Common Interface Model (CIM). Currently it is being evaluated by the Distributed Management Task Force (DMTF). The goal is to bring advanced services for Quality of Service and security, including IPSec, into a common data model.

By delivering security building blocks and helping to promote common policies worldwide, Intel is working with others in the industry to make the vision of the Trusted Virtual Network a reality.

Conclusion

The prospects for the new electronic business model, the Trusted Virtual Network, hold exciting possibilities for a wide variety of industries.

By most accounts, IPSec is well on its way to becoming the new framework for network security. IT professionals will begin to see IPSec capabilities deployed in 1999, and it is expected to become a fully deployed, integral part of the network in the year 2000.

Initial Deployments

Administrators should consider performing initial deployments of this capability and begin learning how to manage this new building-block technology in the network infrastructure. A workgroup-based deployment model is the simplest, most logical way to roll out IPSec security in a controlled manner.

- It allows the administrator to start by securing the parts of the network that are most sensitive—for example, the financial or human resources department.
- It can be scaled to any level, because an IPSec policy server can manage any number of workgroups.
- Another major benefit is ease of management due to the relatively small size of workgroup units (usually 10 to 100 nodes).

For initial deployments of Intel's IPSec solution, the security workgroup model is recommended. After determining critical data paths, the administrator selects workgroup elements. A typical security workgroup includes:

- Web, application or file servers as appropriate
- One or more client systems including connected desktop computers

To be fully effective, IPSec must be integrated into a company's security administration and network management policies. This task cannot be accomplished in a vacuum, but should be part of an overall management strategy. Anyone associated with technology should start to investigate how IPSec will impact their business both at the tactical and strategic levels.

For More Information

Visit www.intel.com/network.

Additional information about the IPSec standard is available at www.ietf.org

Information in this document is provided in connection with Intel products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications.

Intel may make changes to specifications and product descriptions at any time, without notice. For the most current product information, please visit <http://www.intel.com/network>

Copyright © 1999 Intel Corporation. All rights reserved.

*Third-party brands and names are the property of their respective owners.

1299/HB/KR/5K

NP1412.03

