Dynamic Virtual Private Networks: A Security Solution for Enabling Business Intranets

A White Paper

Dr. Alexander Cavalli,
VP, Strategic Development
TradeWave Corporation
September 4, 1996

"Based on Internet technology, intranets are becoming an essential part of corporate information systems today. However, the Internet was not originally designed with businesses in mind. It lacks the technology required for secure business communications and transactions. . ."

Dynamic Virtual Private Networks: A Security Solution for Enabling Business Intranets

A White Paper

Contents

Dynamic Virtual Private Networks: A Security Solution for Enabling Business Intranets

A White Paper

Dr. Alexander Cavalli

Abstract

Based on Internet technology, intranets are becoming an essential part of corporate information systems today. However, the Internet was not originally designed with businesses in mind. It lacks the technology required for secure business communications and transactions. A challenge therefore arises for businesses with intranets: how to establish and maintain trust in an environment which was designed from the beginning for open access to information. More specifically, a way has to be found to secure an intranet without impinging on its inherent benefits of flexibility, interoperability and ease of use.

TradeWave believes that the most appropriate and successful answer to this challenge will be a dynamic Virtual Private Network (VPN) based on our TradeVPI™; applications and services. Unlike traditional VPNs that offer limited or inflexible security, a dynamic VPN provides both extremely high levels of security and, equally important, the flexibility to accommodate dynamically changing groups of users and information needs. Our dynamic VPN can offer this flexibility based on a unique agent-based architecture as well as other features.

Because information can now be made available in such a flexible and fine-grained fashion, a company's files, documents or data that had to be locked away in the past can now be accessed either in whole or in part to carefully selected groups of users in precisely determined ways. As a result, a dynamic VPN is an intranet enabler. It enables an intranet to offer more resources and services than it could otherwise, thereby allowing the business to make more use of its information resources.

The Challenge: Trust in an Open, Changing Environment

The Promise of the Intranet

Intranets are becoming an essential component in corporate information systems today. An intranet is a corporation's internal network that uses Internet technology to communicate and share information.

In order to accommodate new, changing and expanding groups of users and provide these users with information in a number of ways, intranets should deliver several benefits, including flexibility, interoperability, ease of use and extendibility. In particular, they should be open and standards-based, so information can be read by different users with different applications on different platforms.

However, the benefits promised by intranets lead to an important challenge for businesses using this technology: how to establish and maintain trust in an environment which was designed originally for free and open access to information. The Internet was not designed with business security in mind. It was designed by universities as an open network where users could access, share and add to information as easily as possible. A way has to be found to secure an intranet for businesses without impinging on the intranet's inherent benefits. Indeed, an ideal solution must provide not only the highest levels of security but also security in such a way that users can easily access, modify and share more information, not less, under carefully controlled and maintained conditions.

Understanding Security Needs

In thinking about the challenge of trust in an open, changing environment, we will examine the security needs first. Security for an intranet is based on several hardware and software components. Specific mechanisms and technology will vary, but what is sometimes called "industrial-strength" security must always satisfy the following five basic needs:

- Privacy, with the ability to scramble or encrypt messages across an unsecured network
- Access control, determining who is given access to a system or network, as well as what and how much information someone can receive
- Authentication, which verifies the identity of the two companies executing the transaction
- Integrity, ensuring that files or messages have not been altered in transit
- Non-repudiation, which prevents the two companies from denying that they sent or received a file

Accommodating Change

Along with "industrial-strength" security, an intranet must also be able to accommodate changing information needs involving multiple groups of users arranged in multiple ways on an ongoing, dynamic basis. User groups might include employees according to department, rank or location. Other user groups might include members of organizations, subscribers to services, corporate vendors, or the general public. One person might also be a member of several groups concurrently. At the same time, membership in each group is constantly changing as members join or leave groups.

.

In addition, an intranet must accommodate different forms of information, whether Web pages, files or other forms. Finally, an intranet must accommodate changing technology and increasingly complex information systems.

The Solution: A Dynamic VPN

To meet the challenge of establishing and maintaining trust in an open, changing environment, TradeWave believes that the best strategy is to implement what we call a dynamic Virtual Private Network (VPN).

In general, any VPN is a process whereby the public network (the Internet) is secured in order to function as if it were a private network. As such, a VPN is not defined by specialized circuits or routes. Rather, it is defined by security mechanisms and procedures that allow only appointed users access to the VPN and the information that flows through it.

VPNs are not new. What makes TradeWave's VPN the appropriate solution for intranet security is its dynamic nature. By dynamic, we mean its ability to accommodate open, changing business environments. This ability is based on a unique architecture and set of features found in TradeVPI, which is TradeWave's VPN solution.

Capabilities of a Dynamic VPN

TradeVPI is a set of applications and related services. TradeVPI allows a business to create and deploy a dynamic VPN solution with the following capabilities:

- Provides "industrial-strength" security
- Accommodates dynamically changing communities of users
- Provides the ability to exchange information in various forms (Web pages, files, etc.)
- Accommodates different users with different browsers, applications, operating systems, etc.
- Allows users to join groups or administrators to assign identities in a controlled but simple fashion
- Maintains integrity over time, regardless of administrative turnover, changes in technology or the increasing complexity of the corporate information system

The Reward: Enabling Intranets for Business

A dynamic VPN based on TradeVPI offers businesses the ability to use intranets and Internet technology with the assurance that communications and transactions will be protected by the highest levels of security.

At the same time, a dynamic VPN allows businesses to extend their communications and information access in a controlled, yet versatile, fashion. Instead of being designed primarily to "lock out" certain users with limited or inflexible security schemes, a dynamic VPN is designed to provide the highest level of freedom in a secure environment. As a result, the largest number of users can do the greatest amount of work with the broadest range of information. Because information can now be made available in such a dynamic and fine-grained fashion, a company's files, documents or data that had to be locked away in the past can now be accessed either in whole or in part to carefully selected groups of users in precisely determined ways.

As a result, a dynamic VPN is actually an intranet enabler. It enables an intranet to offer more resources and services than it could otherwise, thereby allowing the business to make more use of its information resources.

Speaking in business terms, a company implements a dynamic VPN for the same reasons it implemented an intranet in the first place: flexible

communications, interoperability, extendibility, ease of use, etc. A dynamic VPN simply allows a company to receive these intranet benefits to a full and appropriate degree. Conversely, without a dynamic VPN, a company will not receive the full benefits of intranet technology, nor can it receive an adequate return on its investment in this technology.

Security Mechanisms and Methods

In order to better understand how VPNs work, including TradeWave's TradeVPI, we need to first examine some of the basic elements of a secure network system.

Encryption Mechanisms

Ensuring the privacy of messages, encryption can be offered in two different forms, private key and public key. Private- or symmetric-key encryption is based on a key (or algorithm) being shared between two parties. The same key both encrypts and decrypts messages. Kerberos and the Data Encryption Standard (DES) are traditional private-key technologies. A private-key mechanism is a proven, relatively simple method of encryption. The main problem is in sharing the key: How can a key that is used for security be transmitted over an unsecured network? The difficulties involved with generating, storing and transmitting keys (called key management) can limit private-key systems, especially over the Internet.

In 1976, two computer scientists, Whitfield Diffie and Martin Hellman, developed a theory of public-key encryption which offered a solution to the problem of how to transfer the private key. Later, RSA Data Security, Inc. created an algorithm to make public-key cryptography commercially viable.

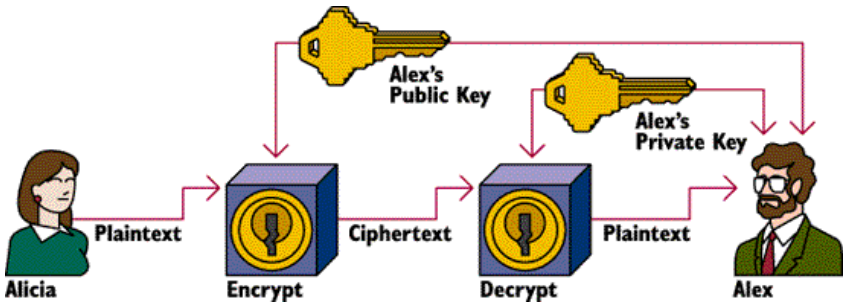

Figure 1: Public Key Encryption

As illustrated by Figure 1, in a public-key solution such as Entrust™; from Entrust Technologies, there are two keys - a private key and a public key which is made publicly available. In addition, a one-time symmetric key is generated for each transaction. To send a message, the sender, Alicia, first encrypts it by using the one-time symmetric key. This key is then encrypted, using the public key of the recipient, Alex. Keep in mind that anything encrypted with a public key can only be decrypted with the recipient's private key. This means that the symmetric key (and therefore the message that it has encrypted) is now secure for transmission over the Internet or an intranet. When the message arrives, Alex decrypts the one-time symmetric key using his own private key. Then, using the symmetric key, he decrypts the message.

The main advantage offered by public-key technology is increased security. Although slower than some private-key systems, public-key encryption generally is more suitable for intranets for three reasons: 1) It is more scalable

to very large systems with tens of millions of users, 2) It has a more flexible means of authentication, and 3) It can support digital signatures. Public-key technology also enables non-repudiation enforcement to verify the transmission or receipt of a given transaction.

Authentication, Digital Signatures and Certificate

In any business transaction, both parties need to offer a guarantee of their identity. Sometimes, authentication is as simple as providing a password. In an intranet, authentication can be accomplished in a number of ways, using encryption technologies that are also used for authentication. These technologies include SPKM (Simple Public-Key Mechanism), developed by Entrust Technologies, S-HTTP (Secure HyperText Transport Protocol) developed by Enterprise Integration Technologies, and SSL (Secure Sockets Layer) Protocol developed by the Netscape Communications Corporation. Each of these authentication protocols uses the RSA algorithm.

Authentication requires, among other things, a digital "signature." The process begins with a mathematical summary called a "hash" which acts as a "fingerprint" of the message. The message contents cannot be changed without altering the hash code. This hash code is then encrypted with the sender's private key and attached to the message. When the message has been received, the hash code attached to the message is compared to another hash code or summary calculated by the recipient. If the two match, then the recipient knows that the message has not been altered and its integrity has not been compromised. The recipient also knows that the message came from the sender, since only that sender has the private key that encrypted the hash code.

DSS (Digital Signal Standard) is a U.S. government standard that provides data integrity assurance and data origin authentication. DSS also serves as a legally binding signature for electronic transactions.

Keys for digital signatures are filed in a public-key directory, made up of "certificates" for every user. These certificates are like the signature cards in a bank and are used to verify identities. A trusted Certification Authority (CA) manages and distributes these certificates, in addition to distributing electronic keys.

Access Control Lists

Access Control Lists determine who is given access to a local or remote computer system or network, as well as what and how much information someone can receive. Related information resources on the network can be organized in a hierarchical fashion, and Access Control Lists can specify access for everything up to a certain level of the hierarchy. Access Control Lists can also specify access for both certain users and certain groups of users. In addition, access control mechanisms can be distributed on the network. The mechanisms do not have to reside on the same host as the website. This means that administrators can physically operate the access control services on a separate host, allowing multiple websites to make use of the same access control mechanisms.

Threats and Control Points

Now that we have looked at some of the basic elements of network security, let's examine the problems in maintaining this security. A key concept in understanding good network security is the idea of a control point. A control point is a tool or process designed to meet a specific threat; it acts as a countermeasure against a particular threat. For example, a door lock is a control point intended to keep unauthorized people out. Most physical security systems consist of multiple control points working together to make a

complete security package. In a building security system, there are distinct control points for the issuance of badges, the guard stations, video cameras, revocation of badges, security codes, hand-scanner installations, door locks and so on. Security is compromised if any one of its control points is absent or not working.

A network security system is built on the same principles. Like a physical security system, a network security system consists of a set of control points working together to form an integrated security package. Each control point is designed to meet a particular threat.

Many security problems that have been publicly reported are caused not by poor security technology but by either a lack of completeness in establishing control points or a failure to maintain a control point with the proper policies and procedures.

Traditional VPN Solutions

VANs

As we mentioned before, VPNs are not new. Value Added Networks (VANs), a type of VPN, have been available for years. A VAN is based on private, closed, leased-line or dial-up access. Organizations such as IBM (through Advantis) and General Electric Information Services currently offer EDI capabilities based on VANs. VANs offer the advantages of fast, high-volume transfer of data. They also provide this exchange of data over a secure network.

At the same time, VANs are limited in several ways. They are proprietary solutions which restrict users to specific hardware and software platforms. They also require dial-up connections or dedicated telephone lines, which can be expensive. In addition, companies have to belong to the same VAN to execute transactions. Currently, thousands of companies belong to VANs, but that number is a tiny fraction of the hundreds of thousands of companies who now have a connection to the Internet. Both companies in a VAN also have to agree on a standard EDI format for purchase orders, shipping notices, freight bills, invoices and other electronic forms. Standard formatting can be a problem for one or both companies if it involves the redesign and reorganization of existing forms.

In short, a VAN, while proving a secure platform for communications, can limit companies in terms of who they might do business with and how they might do business.

Routers, Firewalls and Encrypted Routers

A VPN can be based on routers and firewalls. Routers are computers that control traffic on a network. A firewall is a method of protecting one network from another network. It sits between the internal network and the outside network to block unauthorized traffic. When a user sends a message, it flows through the firewall and onto the Internet. The firewall will block traffic from this user if he is not authorized to visit the Internet, or if he is using an unauthorized protocol.

A VPN based on routers and firewalls can be constructed for within-network and network-to-network traffic. However, routers don't distinguish between communities of users, so users on two networks have to use user names and passwords. This procedure makes a single logon very difficult. In addition,

user names and passwords can be read by outsiders in transit between networks, so transmissions need to be encrypted as well.

With encrypted routers, communications can be undertaken between networks with a fair degree of security. A system using routers and firewalls does not include unilateral or mutual authentication: a user does not have to offer proof of identity beyond user names and passwords. Routers also typically share the same symmetric key. This means that security can be compromised by someone using a stolen key.

More significantly, a router system is too brittle to accommodate multiple, dynamic groups of users. Any changes in the system are difficult to make and/or compromise security.

How TradeVPI Works

TradeWave's dynamic VPN consists of a network security platform and a set of applications that use this security platform. The diagram below shows how the pieces work together to make a dynamic VPN solution.

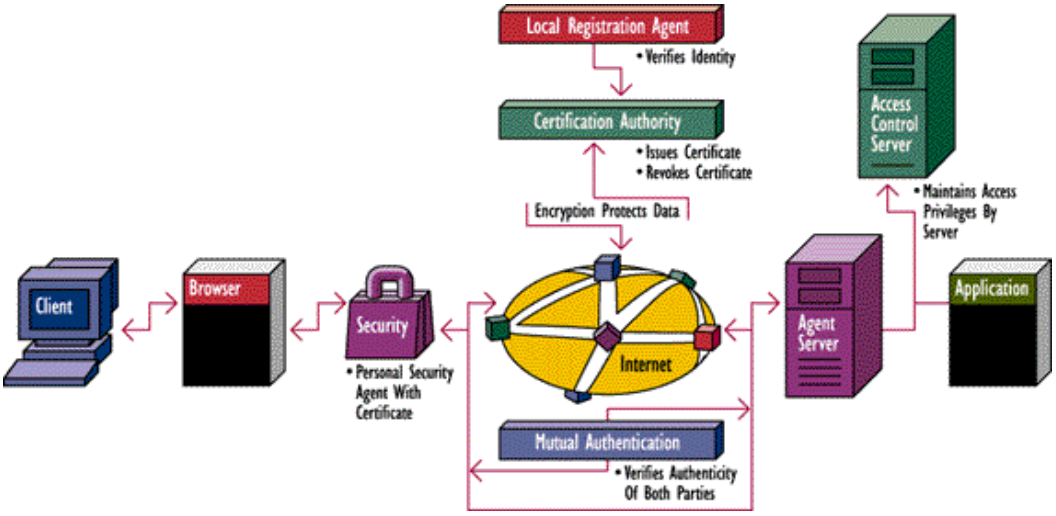

Figure 2: A Dynamic VPN

The example in Figure 2 steps through the pieces of a dynamic VPN by imagining a secure HTTP (Web) communication. TradeVPI, however, is not application-specific and will work with other Internet applications, as well as with corporate-specific applications written to conform to it.

Joining the VPN

Before actually using the VPN, a user or service must first join the VPN by registering with the CA. A trusted corporate employee, called a Local Registration Agent, approves all registration requests. Strong security procedures ensure that only appointed users are registered and receive certification. The CA ensures that revoked certificates are posted and available so that service can be denied when these certificates are used.

Using TradeWave's VPN

Users and services send and receive information continuously within a VPN. However, the basic steps of each interchange are the same. The following steps illustrate a user requesting information from a server by clicking a mouse on a hyperlink.

1.	A user requests information using a desktop application, such as an Internet browser	Information exchange starts when a user sends information to another user or requests information from a server. The VPN can incorporate proprietary applications. However, it must also offer applications that take advantage of the Internet, and particularly the World Wide Web. In this case the user has accessed a hyperlink within some Web document. This hyperlink, however, is secure and can be accessed only by authorized users.
2.	The application secures and sends the message	When the client and server detect that security is required to transmit the request and to see the new document, they engage in a mutual authentication protocol. This step verifies the identities of both parties before any further action is taken. Once authentication occurs, but before the application sends the request, it secures the message by encrypting it. Additionally, it can attach the user's electronic certificate, or signature. Encrypting the information protects its confidentiality and integrity. The signature, if sent, will be used for auditability. To enable the interoperability of multiple security mechanisms, the security functions must be based on well-defined standards, such as the Internet standard Generic Security Services Application Programming Interface (GSSAPI).
3.	The message is transmitted over the Internet	For the request to reach the server, it must leave the LAN, get out onto the Internet at large, and reach the server at someone else's site. This trip might traverse one or more firewalls before the request reaches its destination. Once past the firewall, the request is passed along the Internet pathways to reach its destination.
4.	The received message must pass security	When the message reaches its destination, it might have to traverse another firewall. This firewall will carefully screen incoming traffic, ensuring that it conforms to corporate policy before passing it on through to the internal network. The message is transferred to the server. Because the client and server have already executed the mutual authentication step, the server knows the identity of the client user when it receives the request.
5.	For requests, the user's access rights are verified	As in all corporate networks, all users cannot have access to all corporate information. In a dynamic VPN, the system must be able to restrict what can and cannot be accessed by each user. The server must determine if the user has access rights to the requested information. It does this using an access control mechanism, preferably a separate server. The access control server restricts access to information at the document level. So, even if the user presents a valid certificate, he may be denied access based on other criteria (e.g., corporate information policies).
6.	The requested information is secured and returned over the	If the user has access rights to the information requested, the information server encrypts the information and, optionally, its certificate. Keys established during the mutual authentication step are used to encrypt and decrypt the message. The user now has his secured document.

Internet

An Analogy: An Employee ID and Badge System

TradeWave's VPN solution can be understood as the computerized equivalent of a corporate employee ID and badge system. In the same way that the Human Resources or Security department might verify an employee's identity and assign that person a unique employee number, a VPN verifies a user's identity and issues a unique "distinguished name" which is used for all access to and movement within the system. In the same way also that a company keeps track of who has a badge and where they can go with it, the VPN tracks, manages and deploys keys and certificates. Just as lost badges can be reissued by a company, lost keys can be recovered by the Certification Authority.

Furthermore, in the same way that access to buildings or certain areas is controlled by various levels of security clearance, the VPN checks Access Control Lists against user names and passwords to authorize access to networks and to certain documents and files. In addition, just as employees leaving the company permanently will turn in their badges, with their individual badge codes placed on a list of revoked users, VPN Access Control maintains a list of revoked users and denies these users future access to the system.

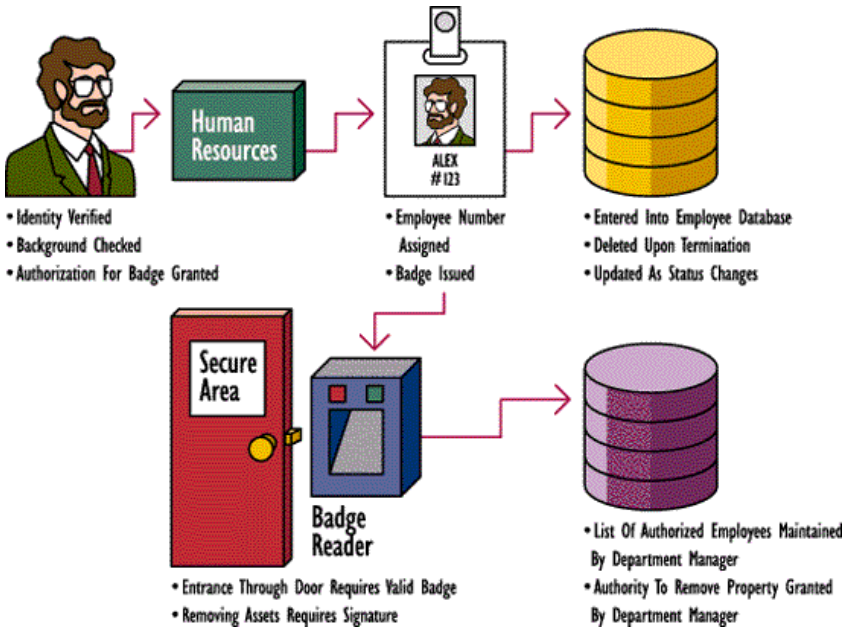

Figure 3: ID and Badge System Analogy

The analogy is not exact: A VPN monitors and controls access to information on a constant basis, not just when a user "enters the door." Badges are not used for encrypting communications, and badges do not determine or control different types of information access. However, the analogy is useful in illustrating the fact that TradeWave's VPN can deal with changing and overlapping communities of users on a dynamic basis. The analogy can also serve to remind us that encryption - one of the first elements that might come to mind in discussing network security - is actually only one part of a dynamic VPN solution, however important that part might be. A dynamic VPN actually consists of a number of complex processes involving trust, verification,

management and other functions - not just coding and decoding messages.

TradeVPI's Agent-based Architecture and Extendibility

A critical aspect of TradeWave's VPN is its agent-based architecture. TradeWave agents are stand-alone software entities or modules that communicate via standard protocols. Because TradeWave has architecturally "decoupled" its agents from other applications, a business can change or expand its intranet - including expansion across platforms - without having to reengineer its intranet system. More specifically, this architecture allows a business to select and use any browser, any server and any application with its dynamic VPN.

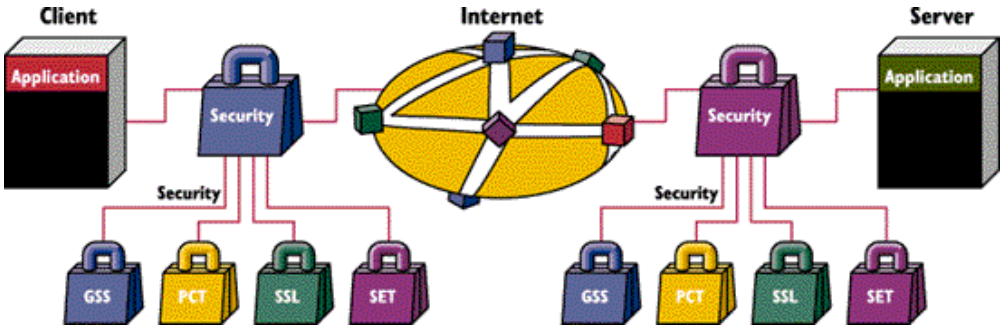

Figure 4: Agent-based Architecture

TradeWave agents can:

- Be inserted easily into an existing legacy computer communications stream with a minimal disruption to the system
- Easily embody capabilities not in the existing system
- Be updated quickly
- Incorporate multiple security protocols, thereby supporting a system where multiple levels of security are required

In addition, agent-based architecture provides a solution to a traditional problem in corporate information systems: the conflict between enterprise-wide standards on the one hand and the local adoption of technology for specific needs on the other. An agent-based architecture allows, for example, departments to use the browsers they want without disturbing enterprise-wide security standards.

TradeAttachés

An additional benefit of agent-based architecture is the ability of TradeVPI to use a variety of software modules called TradeAttachés. These modules can be added to a TradeVPI system to increase its functionality and interoperability. For example, TradeAttachés permit the VPN to expand to include different security protocols without disturbing the browser or server.

New security functions are available immediately with this system. TradeVPI can also manage several security TradeAttachés simultaneously, so the VPN can support multiple security platforms at the same time.

Conclusion

TradeWave believes that in order for businesses to receive the full benefits of

intranets and Internet technology, a dynamic VPN needs to be implemented. Because a dynamic VPN can establish trust in open environments and accommodate the information needs of a business in a flexible, finely controlled manner, a business with a dynamic VPN can provide access to more information and allow a greater range and diversity of communication, both within the company and among companies on the Internet.

TradeWave is an ideal partner for providing Internet security solutions. Founded in 1991, the company has been a pioneer in the development of practical solutions for Internet-based, business-to-business information management and exchange, advertising, security and financial settlement. We introduced the first commercial Web browser and the first WAIS Internet navigators to include security (WAIS preceded the Web technology as the layperson's method of using the Internet.) We also developed the first browser-and-search Internet directory.

More recently, TradeWave has been selected to provide the security infrastructure for the electric utilities industry project, Open Access Same-time Information System (OASIS). Participation in this groundbreaking project demonstrates the Federal Energy Regulatory Commission's approval of, and the utilities industry's confidence in, TradeWave's solutions.

A VPN Checklist

The following capabilities and features are important in developing a dynamic VPN solution.

General Capabilities:

- Provides "industrial-strength" security
- Accommodates dynamically changing communities of users
- Able to exchange information in various forms (Web pages, files, etc.)
- Accommodates different users with different browsers, applications, operating systems, etc.
- Allows users to join groups or administrators to assign identities in a controlled but simple fashion
- Maintains integrity over time, regardless of administrative turnover, changes in technology or the increasing complexity of the corporate information system

Specific Features:

Administrative

- Transparent key update and recovery, certificate revocation and renewal, and key/certificate disabling
- Single sign-on
- An online, Web-based service for registering and managing users and secure services
- An option for bringing key management and administration in-house
- Support for secure MS mail and cc:Mail using the same system as used for Web applications (i.e., TradeAgent with Netscape or Microsoft browsers and servers)
- U.S. government FIPS-PUB 140-1 accreditation for encryption software
- Cross-certification for multiple CAs

Access Control

- Distributed Access Control mechanism
- Application independence, with support for access controlling arbitrary resources (in addition to Web documents and CGI applications
- Access Control based on strongly authenticated user identities, including organizational wildcarding
- Support for user groups, including nested groups
- Support for user identities from multiple CAs (for cross-certification)

Standards

- Support for DSS digital signatures (DSA/SHA)
- Support for 64-bit CAST symmetric encryption
- Use of ANSI X9.17 random number generation IETF GSSAPI-based application toolkit

Glossary of Internet and Internet Security Terms

Access Control

A process that determines who is given access to a local or remote computer system or network, as well as what and how much information someone can receive.

Authentication

A process verifying that users are who they say they are. An example of authentication is requiring users to identify themselves with a password.

Authorization

The process that grants access to a local or remote computer system, network or to online information.

Browser (also "navigator")

Software used to find, retrieve, display and move easily among various kinds of Internet resources, including text, video, graphics, etc.

Certification Authority

The entity or service that distributes electronic keys for encrypting information and electronic certificates for authenticating user and server identities.

Client

A computer or software that requests a service of another computer system or process (a "server"). For example, a workstation requesting the content of a file from a file server is a client of the file server.

DES (Data Encryption Standard)

A standard encryption technique that translates data into an unbreakable code for public transmission. It uses a binary number as the encryption key. This key, preferably chosen randomly for each session, is used to create the encryption pattern.

Digital Certificates

A public-key directory entry that has been "signed" or validated by a certification authority. Digital certificates are used to verify digital signatures.

Digital Signature

A coded message added to a document or data that guarantees the identity of the sender.

DSS (Digital Signal Standard)

A standard that provides data integrity assurance and data origin authentication. It also serves as a legally binding "signature" for electronic transactions.

Electronic Commerce

The use of an information infrastructure through which businesses can speed the exchange of information, improve customer service, reduce operating costs and increase global competitiveness.

EDI (Electronic Data Interchange)

A set of standards for exchanging orders and other business transactions by electronic format. EDI is often supported by Value Added Networks (VANs).

Email (Electronic Mail)

The method by which computer users can exchange messages with each other over a network.

Encryption

The manipulation, or encoding, of information to prevent anyone other than the intended recipient from reading the information. There are many types of encryption, and they are the basis of network security.

Firewall

A server or collection of components that supervises all traffic in and out of a network, permitting only traffic which is authorized by local security policy to pass.

FTP (File Transfer Protocol)

A protocol that allows computer users to exchange large documents with other users. Commonly, it is used to retrieve files from online archives of accumulated software and data.

GSSAPI (Generic Security Service Application Programming Interface)

An Internet standard interface which forms a link between a variety of user or vendor client/server applications (such as the World Wide Web) and a variety of security mechanisms (including both private-key and public-key security).

Hash Code

A unique, mathematical summary or "fingerprint" of a document that serves to identify the document and its exact contents. Any change in the hash code is an alert that the document's contents have been altered.

Internet

A worldwide system of computer networks. Networks connected through the Internet use a particular set of communication standards, known as TCP/IP, to communicate.

Kerberos

A distributed security system developed by the Massachusetts Institute of Technology. It uses private-key security.

Private-Key Security

Also known as symmetric-key security, this method is based on both parties having the same encryption key, as in secret-key cryptography. The client and server share a key to encrypt and decrypt information on a network. A common implementation of private-key security is the Kerberos distributed security system (see Kerberos).

Public-Key Security

Also known as asymmetric-key security or public-key encryption technology, this is a mechanism for securely distributing encryption keys that are used to "lock" and "unlock" data across an unsecured path. Public-key security is based on encryption key pairs, in contrast to methods based on having a single, shared key, as with private-key security.

Router

A computer that controls traffic on a network.

RSA

An encryption mechanism by RSA Data Security that uses a private and a public key. RSA is also used for authentication.

Server

A computer or software that provides resources, such as files or other information, to client software running on other computers.

S-HTTP-(Secure HyperText Transport Protocol)

A protocol and security mechanism that uses public-key technology to encrypt sensitive data and to verify user and/or server authenticity.

SPKM

A security protocol developed by Entrust Technologies that uses public-key technology to encrypt sensitive data and to verify user and/or server authenticity.

SSL (Secure Sockets Layer) Protocol

A security protocol developed by the Netscape Communications Corporation to encrypt sensitive data and to verify server authenticity.

TCP/IP (Transmission Control Protocol/ Internet Protocol)

The suite of protocols developed by the U.S. Department of Defense in the 1970s to support the construction of world-wide internetworks. Today, millions of users are connected to the Internet via software which uses the TCP/IP Internetworking Protocol suite.

VPN (Virtual Private Network)

An Internet-based system for information communication and enterprise interaction. A VPN uses the Internet for network connections between people and information sites. However, it includes stringent security mechanisms so that sending private and confidential information is as secure as in a traditional closed system.

WAIS (Wide Area Information Servers)

A system that lets users look up information in public databases available on the Internet. Many of the information-searching services available on the Internet use a WAIS search engine.

World Wide Web ("the Web")

A client/server system for finding and retrieving Internet information. To access the Web, you run a browser program, which can get documents from sources all over the world. Browsers usually can also search documents and databases. The documents the browsers display include hypertexts, which are documents that include highlighted cross-references (or links) to other documents. Select a link

and the document to which it is pointed is displayed. The document can be text, graphics, sound, video or other multimedia formats.