Recent Industrial Developments of VPN (Virtual Private Network)

VPN의 최근 산업계 동향

S.O. Hwang (황성운) Internet Service Department (네트워크소프트웨어연구팀 연구원)
Y.B. Choi (최영배) Internet Service Department (네트워크소프트웨어연구팀 선임연구원)
J.S. Lee (이준석) Internet Service Department (네트워크소프트웨어연구팀 선임연구원)
K.S. Yoon (윤기송) Internet Service Department (네트워크소프트웨어연구팀 책임연구원, 팀장)
M.J. Kim (김명준) Internet Service Department (인터넷서비스연구부 책임연구원, 부장)

VPN (Virtual Private Network) is an effort to get some of the advantages of public network – cost saving, scalability, flexibility, and efficient network management as well as some advantages of private dedicated network – fast speed and less security threats. We introduce protocols to implement VPN, pros and cons of VPN, and its application areas. We also explain some tasks and classification criteria that should be considered in deploying VPN, available commercial products and recent industrial trends of VPN.

I. Background

The Internet has become a popular, low-cost backbone infrastructure. But despite the worldwide communications revolution created by the Internet, it is not an appropriate medium for business communications due to problems of guaranteeing reliability and quality of service (QoS), operational manageability, and security. The 1996 annual report from the Computer Emergency Response Team (CERT) lists more than 2,500 reported security incidents affecting nearly 11,000 sites. The most serious types of attacks included IP spoofing, in which intruders create packets with false IP addresses and exploit applications that use authentication based on IP; and various forms of eavesdropping and packet sniffing, in which attackers read transmitted information such as logon information and database contents. VPN technology emerged as a solution for these problems, among them, with a special emphasis of security aspect. VPN can be defined as a set of computer systems and protocols that provides an effort of a private network using public network. An effort implies guaranteed bandwidth and secure transmission.

The organization of this paper is as the following. Section II describes typical implementations of VPN. Section III explains VPN and IPSEC in the view of benefits of VPN, issues in VPN development, VPN application fields, standard protocols for VPN security, and characteristic of VPN as a policy based network. Section IV explains major tasks required to deploy VPN. Section V shows a guide to VPN classification. Section VI describes VPN commercial products and shows features

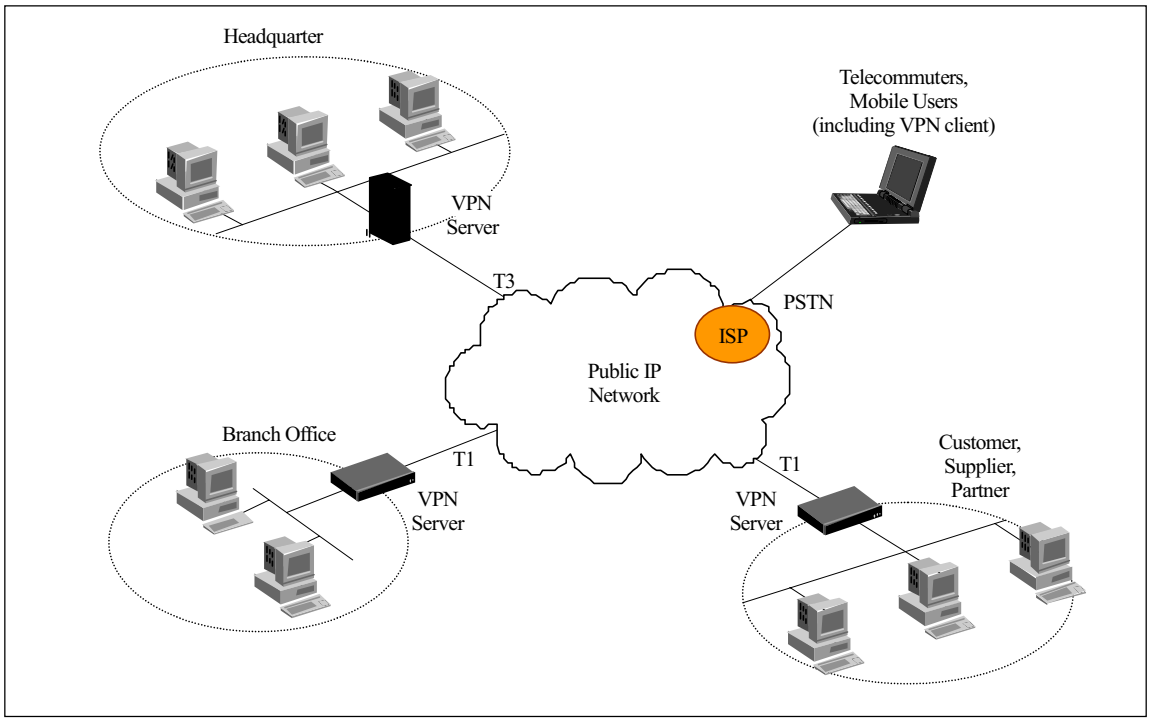

Fig. 1. Different VPN configuration types.

of major VPN products currently available. Section VII finally concludes this report summarizing recent trends of VPN technology.

II. Typical VPN Implementations

Although there are as many types of VPN implementations as what issue they are facing, what problems they are going to solve through VPN, what benefits of VPN they are bearing in mind, most VPN configurations can be grouped into the following three primary categories (See the following Fig. 1):

- Intranet VPNs between two internal corporate offices (typically headquarter and branch offices);
- Remote Access VPNs between a corporation and remote or mobile employees;
- Extranet VPNs between a corporation and its strategic partners, customers, and suppliers.

III. VPN and IPSEC

In response to the above mentioned security issues, the Internet Architecture Board (IAB) included authentication and encryption as necessary security features in the next generation IP, which has been issued as IPv6. Fortunately, these security capabilities were designed to be usable with the current IPv4 and the future IPv6. Within the Internet Engineering Task Force (IETF) formally established by IAB, the IP Security (IPSEC) working group started developing a flexible framework for providing network layer security in June, 1993. IP SEC protocols will be required as part of IPv6, but optional in IPv4. But they are being widely implemented for IPv4. In particular, nearly all vendors of firewall or security software have supported

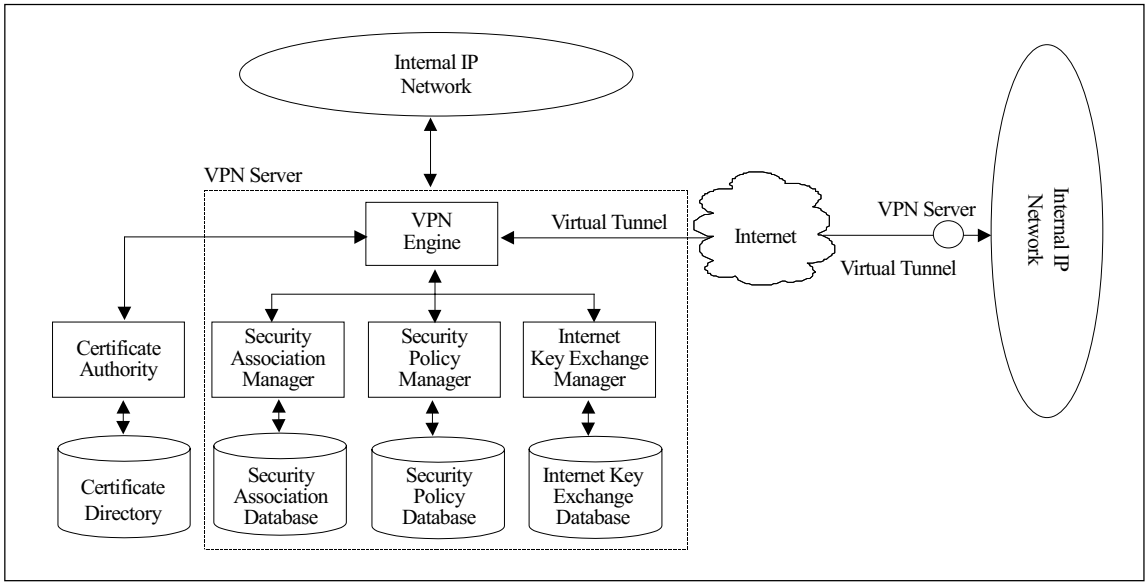

Fig. 2. VPN componental architecture using IPSEC.

or developed. There are also several open source IPSEC projects. For example, S/WAN (Secure Wide Area Network) [12] project started in December, 1996 to ensure that IPSEC products will interoperate. The high-profile example of IPSEC in a VPN is the AIAG (Automotive Industry Action Group). The AIAG – consisting of General Motors, Ford, Chrysler and their suppliers and business partners - selected IPSEC & Oakley for VPN standard in March, 1996. The AIAG created the ANX (Automotive Network Exchange) project to move their considerable EDI (Electronic Data Interchange) traffic from more expensive dial-up systems and leased lines to an IP-based VPN. Figure 2 shows the componental architecture of VPN using IPSEC.

In this section, III.1 describes nine benefits of VPN. III.2 describes some of the issues in VPN development. III.3 shows various VPN application fields. III.4 describes related standard protocols for VPN security. Finally, III.5 describes characteristics of VPN as a policy based network.

1. Benefits of VPN

The following are some expected benefits of VPN:

A. VPN is Transparent to Applications.

Since most of VPN technologies is applying under the transport layer (TCP, UDP), there is no need to change application software on a user or server system. For example, IPSEC is implemented in a router or firewall. Even if IPSEC is implemented within end systems, the upper layer software, such as an application, is not affected.

B. VPN Can be Transparent to End Users.

There is no need to train users about security mechanisms, issue keying material on a per-user basis or revoke keying material when users leave the organization. All these activities are performed systematically on behalf of end users by network or security managers who are responsible for the corporate network management.

C. VPN Can even Provide Security for Individual Users If Needed.

This is useful for off-site workers, as well as for setting up a secure virtual subnetwork within an organization for sensitive applications.

D. Saving Cost

One of the promises of VPNs is to save costs over leased line WAN (Wide Area Network) connections and reduce the cost of dial-up operations. VPN savings grow as the network size increases. Costs associated with private line networks are not linearly related to the number of branch offices, because a private network should be added for each office to which the new office will be connected. However, with Internet communications, adding a new office to the network simply requires you to connect the office to the Internet, rather than connecting it to every other office. Therefore, the larger the wide area network, the larger the savings gained by using the Internet.

E. Flexibility

The Internet brings a degree of flexibility to corporate communications that has never before been available. Corporations can add branch offices to their network simply by setting up Internet access. The low access price enables corporations to connect branch offices to their network that previously had no access at all. And the Internet provides instant access to global trading partners and customers as well.

F. Central Management

For a fully-meshed branch office network, private lines can be a nightmare. You must manage lines between each of the offices. For a 10-site network, you must manage 45 PVCs (Permanent Virtual Circuit). For a 150 site network you need 11,175 PVCs. With the Internet, however, you need only provide each office with Internet access – you do not need to manage individual lines.

G. Global Connectivity

As the economy continues to become more global, corporate networks need to grow beyond its national borders. The fiber infrastructure for quality private lines is simply unavailable in many countries. The Internet, on the other hand, is ideal for international connectivity. The Internet Protocol (IP) can run over any communications infrastructure.

H. Scalability

As demand for remote access increases within your organization, you will have no need to buy and install more ports. It is simply a matter of ordering new access accounts from your service provider.

I. Better Remote Access

The need for remote access facilities is growing at an exceptional rate, as the demands of telecommuters, support personnel, and road warriors grow. Infonetics Research Inc. [8] reports the percentages of employees accessing corporate networks remotely is growing: the number of mobile workers grows 114 % by 2000 and the number of telecommuters grows 154 % by 2000. Traditional, corporate-administered remote access facilities with dial-up modem lines will not be able to keep up with such demands. This growth is introducing two major problems: 1) the costs associated with remote access including long distance charges, the capital expenditures on remote access equipment are growing considerably. The Internet remote access scenario results in 62 % operational cost savings when compared with the private line scenario,

resulting in a capital investment pay back period of just 2.8 months, expects TimeStep [9] in the report 'The Business Case for Secure VPNs.' 2) Management is becoming increasingly complex. It is because that remote access requires intense user support and a lot of network management time, due in part to the poor reliability of remote access facilities.

2. Issues in VPN Development

Besides the advantages of VPN, we can think of some issues to be resolved. Some of them are QoS, security services, user transparency, collaboration with existing network environments, policy management, interoperability, and performance:

A. QoS

How can it provide users with their desired bandwidth? VPN should consider these QoS requirements driven by the application. It is because VPN is based on the public, uncontrollable data networks such as Internet. Many network managers think that the Internet is not yet capable of providing adequate, peak or scalable bandwidth. So guaranteed bandwidth and non-graded QoS should be managed in the VPN deployment.

B. Strong Network Security Services

Customers using VPN services demand the same level of security they have come to expect using traditional leased-line private networks. VPN service providers should have various security schemes to achieve private-network-like security over public IP, ATM or Frame Relay backbones.

C. Collaboration with Existing Network Environments

VPN technology should be independent of specific architecture and be compatible with Internet protocol. And it also provides a better security service by collaborating with the existing security systems.

D. Policy Management

Policy management [2, 4, 5] covers multiple domains including service management, class of service, QoS as well as security. For instance, VPN security policy consists of authentication, authorization and cryptographic attributes (e.g., key length negotiations and certificate validation), etc. It is a set of mechanisms that allow a VPN customer to control and manage the use of network resources based on the end user and/or application.

E. Interoperability

Because VPN technology uses encryption as the basis for its security, interoperability [1, 3] among vendors is a major concern. For VPNs to be interoperable, the "VPN policy" must be consistent throughout the enterprise. More importantly, the outside client must adhere to a subnet of VPN policies to allow secure communications. IPSEC standard is focusing this interoperable security, which allows partner companies to link their respective VPNs together, even though their encryption systems were manufactured by different vendors.

F. Performance

Crytographic processing (encryption, decryption, authentication, etc.) is known as computationally intensive. For example, Diffie-Hellman and RSA public key cryptography require multiple rapid multiplications. This, coupled with the increasing need for simultaneous connections, may also lead to some bottlenecks which heavily affect the entire Intranet. However, there are several ways to address this problem. One is to determine the optimum level of security suitable for your en-

terprise. Another solution is to use a dedicated server for VPN. Not only will it improve performance, but using a separate machine for the VPN will add yet another layer of security to your system. Another is to use a hardware-based VPN solution, though in this case you may have compatibility problems with existing hardware.

3. VPN Application Fields

Some of application fields in VPN technologies are as the following:

- Automobile company with part manufacturers, suppliers, and distributors
- Insurance company with multiple insurance agents, home offices, and hospitals
- Electronic activities such as electronic stock trading or electronic auction (broker, customer, bidder)
- Large company with a headquarter and multiple branch offices, e.g., multi-national company
- Banking with many clients and branch offices
- ISP (Internet Service Provider): Internet broadcast company
- Online ordering service
- Electronic Post

4. Standard Protocols for VPN Security

There are several different technical approaches to implementing VPNs over the Internet. Table 1 shows the representative standard protocols for VPN. Microsoft's PPTP is a free, Windows-centric tunneling protocol that is simple to implement and handles multiple protocols, but lacks solid security features. L2TP is similar to PPTP, but provides better authentication. SOCKS provides better access to encryption, but operates at a higher level than IPSEC.

Neither PPTP nor L2TP specify inherent encryption or key management mechanisms in their published specifications. The current (July 1997) L2TP draft standard recommends that IPSEC be used for encryption and key management in IP environments, and the next draft of the PPTP standard may do the same. In particular, PPTP and L2TP are more suitable for multi-protocol non-IP environments. Although both PPTP and L2TP do not provide packet authentication and packet encryption, IPSEC provide them using AH, ESP header. Unlike PPTP and L2TP, IPSEC also provide key management such as ISAKMP/Oakley, SKIP.

For the above reasons, IPSEC is the best VPN solution for IP environments, as it includes strong security measures, notably encryption, authentication, and key management, in its standards set. It is already being implemented in IPv4 which is the current IP protocol used in the Internet. It is also strongly supported by a user group consisting of manufacturers and suppliers, for example, the ANX. Another protocols such as VTP, AMP, SOCKS are supported by only a small number of vendors at this point. SSL is an upper-layer protocol commonly used by Web browser clients and servers to provide peer authentication and encryption of application data. SSL is an end-to-end protocol, and therefore will be implemented typically in the client and the server, but it is not implemented in the intermediate machines such as routers or firewalls.

5. VPNs Are Policy Based Networks

VPNs require each data stream to be processed as it enters and exits the public WAN to ensure security and to optimize performance and manageability. The collection of services which is applied to each data stream in a VPN is a policy. Generally, policies apply to individual users or groups of users (e.g.,

<Table 1> Standard protocols for VPN security.

OSI Layer	Security Protocol	Features
Layer 2	L2F (Layer 2 Forwarding)	• Proposed by Cisco • Provide authentication for each end of the tunnel unlike PPTP. • Access server authenticates VPN user based on domain name and user ID only • No encryption provided • Hardware-based L2F scale better than protocols like PPTP
	PPTP (Point to Point Tunneling Protocol)	• Proposed by Microsoft • Designed for Dial-up VPN • Not strong authentication, encryption • Support TCP/IP, IPX, NetBEUI • Support 2 modes: client enabled and ISP enabled • Support only Windows 95 clients and NT server • Support single point-to-point tunnel
	L2TP (Layer 2 Tunneling Protocol)	• Proposed by Cisco, Microsoft, and 3COM • Combination of PPTP and L2F • Support TCP/IP, IPX, AppleTalk • Generally combined with IPSEC protocol for better security services • Support flow control • No UNIX or non-Windows versions as with PPTP • Support single point-to-point tunnel
Layer 3	IPSEC (Internet Protocol Security)	• Open framework proposed by IETF • Lowest layer that can provide end-to-end security • Support two security protocols: AH, ESP • Need key management protocol and database for SA (SAD, SPD) • Easier to implement and often faster to operate • Support multi-point tunnel
	VTP	• Proposed by Bay Network • Guarantee speed of line using Frame Relay • Provide dynamic tunnel assignment strategy
	ATMP (Ascend Tunnel Management Protocol)	• Proposed by Ascend Communications • Software based on the TCP/IP protocol suite • Completely transparent to the clients • Originating caller may use native TCP/IP or IPX server
Layer 4	SOCKS V5	• Proposed by NEC and now an IETF standard • Operated at the application level • A framework for client-server applications in TCP/UDP domain • Provide convenience and a variety level of security • High security but low performance (speed) because it adds a layer of security • Provide message integrity and privacy • Extremely useful for secure extranet VPNs
	SSL (Secure Socket Layer)	• Transaction security standard developed by Netscape Communications • Encryption of a session, authentication of a server, authentication of a client (optional), message authentication are provided

senior management, sales personnel, specific business partners, etc.) and include specific security, QoS, and management features. A list of such VPN features, along with the related technologies and key standards are presented in Table 2 [11].

IV. Major Tasks Required to Deploy VPN

As with any sophisticated technology, successful VPN implementation demands careful coordination

<Table 2> Technologies and standards to Implement VPN policies.

VPN Requirement	Related Technologies	Common/Standard Implementations
Secure data over the public IP network	Packet encryption, Packet authentication, Key management	IPSEC, DES, 3DES, IKE
Verify user identity	User authentication, Cross certification	PKI (X.509), tokens, RADIUS
Generate VPNs policy	Policy data model, Policy specification language, Directory services	LDAP, NDS
Access control / Network protection	Firewall, Intrusion detection, Virus checking	Packet filtering, stateful inspection, application proxy, content filtering
Connect private LANs over public IP network	Network Address Translation (NAT)	RFC 1631
Maximize available bandwidth	Compression	STAC, LZS
Match available bandwidth to business priorities	Bandwidth management	CBQ, Rate Control
Manage business traffic using policies	QoS, Service level management	Diff-Serv, COPS, MPLS, etc.

of a set of interrelated tasks from the initial design requirements through the day-to-day operations and support. The following divides VPN implementation tasks into 4 classes: network design, security design, network and security integration, and operations and support.

A. Network Design

- Existing network and applications audit
- Analysis of enterprise-wise network component
- Identification of VPN applications (intranet, extranet, remote access, hosting)
- Determination of bandwidth and QoS policies
- Service Level Agreement (SLA) definition
- Determination of public & private addressing schemes, translations & naming services
- Identification of VPN device placement relative to existing routers, firewalls, etc.
- Determination of internal/external segment, i.e., Intranet and Internet
- Determination of routing topology in VPN network

B. Security Design

- Enterprise-wise security analysis and audit
- Security policy management (definition, distribution, review)
- Determination of encryption, authentication, key management, access control, and filtering policies
- Determination of Public Key Infrastructure (PKI) requirements
- Determination of VPN protocols: L2TP, PPTP, IPSEC, SOCKS, etc.

C. Network and Security Integration

- Initial installation and configuration of devices: Routers, VPN service units, firewalls, bandwidth management devices, authentication servers, directory servers, etc.
- Verification and check-out

D. Operations and Support

- VPN activity and performance monitoring
- Security monitoring and reporting
- Certificate authority management
- Remote site and user support
- Change management
- Capacity planning

V. VPN Classification Guide

All VPNs are not the same. They vary in purpose, size, scope, and complexity. There is consid-

erable variation in VPN implementations, especially in view of the many permutations and combinations of features, technologies, and standards available. The classification scheme detailed in the table of Appendix [11] is intended to help users and service providers to quickly determine the types of VPN technologies they'll need to deploy based on the applications they intend to support, the VPN services to be provided, and the size and scale of the network. In the table, VPN was classified to 5 classes (Type 0-4) according to the features such as typical users, typical information needs, scalability and bandwidth needs, and technologies and products. Some pros and cons for each VPN class were added.

VI. VPN Commercial Products

The following Table 3 indicates ICSA-certified IPSEC products. For each company, major products are listed with platform and features. The ICSA (International Customer Service Association) [7] is completely independent organization which is giving security assurance services through product certification programs and establishing better security practices through management of multiple security-focused consortia. The ICSA Program for IPSEC Product Certification has the objective to enable multi-vendor virtual private networks on the Internet that can provide interoperability along with the security functions of data source authentication, data integrity and confidentiality.

VII. Recent VPN Technology Trends

In this report, we tried to cover what is related to VPN as much as possible. As we can infer from the above, VPN is not a fragmental technology but a composite technology. It means that if we want to get the expected effect of VPN, we are supposed to assess various VPN-constituent technologies as well as our own business environment (needs) in advance. It is because there may be lots of corresponding, suitable VPN technologies according to each different business requirements. Finally, we conclude this report summarizing some of the recent trends of VPN technology as the following:

ⓐ Most of VPN commercial products support IPSEC, the Internet standard protocol. Due to the related companies' implementation and interoperability activities as well as international standardization activity, this trend is believed to keep going. Above all, when we consider interoperability of VPN technology, IPSEC seems to be established as an industrial VPN standard finally.

ⓑ Most of companies which are producing VPN-related products are security software producers, therefore they have a tendency to add some VPN functions to their existing firewall system. Some others are network equipment producers and they also tend to add VPN function to their routers. In addition to them, government research institutes, universities, telecommunication companies, etc. are researching or implementing VPN technologies, independently or jointly.

ⓒ Most VPN products support user authentication and entity authentication based on public-key algorithms and they are deploying public key infra structures from other companies, which are largely represented by VeriSign (http://www.verisign.com) and Entrust (http://www.entrust.com), GTE Cybertrust (http://www.cybertrust.com), and Baltimore (http://www.baltimore.com).

ⓓ Companies strongly expect VPN promisingly in the sense that (1) considerable corporate-wide

network cost saving is possible using less-cost Internet backbone (2) it provides network security mechanism which is one of outstanding issues on the Internet (3) it plays a secure pseudo-private net

<Table 3> ICSA-certified IPSEC products (continued on next page).

Company	Product	Platform	Features
AXENT Technologies, Inc. http://www.axent.com/	Raptor Firewall's VPN Server v6.0 for NT	Windows NT 4.0	• VPN technology supported in Raptor Firewall 6.0 • Protocol: swIPe or IPSEC • Key mgmt: ISAKMP/Oakley • Support NAT • Encryption: DES, 3-DES, RC2 • Integrity alg.: MD5, SHA1 • Auth: pre-shared secret
Check Point Software Technologies, Inc. http://www.checkpoint.com/	Firewall-1 v4.0	• Windows NT • Solaris	• VPN technology supported in FireWall-1 v4.0 • Protocol: IPSEC • Key mgmt: ISAKMP/Oakley, SKIP, manual IPSEC • Encryption: RC4, CAST, DES, 3-DES, RSA, DH keys • Integrity alg: CBC-DES-MAC, MD5, SHA-1 • Auth: pre-shared secret or digital certificate (PKI support)
Cisco Systems http://www.cisco.com/	Cisco IOS v11.3.3	IOS	• Context-based Access Control (CBAC) • Java blocking • Denial-of-Service detection and prevention • Encryption: DES, 3DES • Protocol: IPSEC, L2TP, L2F
Information Resource Engineering, Inc. http://www.ire.com/	Safenet/Soft-PK v1.0	Windows 95	• Support Client-to-Client (dial-up), Client-to-Gateway communication • Protocol: IPSEC • Key mgmt: ISAKMP/Oakley • Encryption: DES, 3-DES • Integrity alg: MD5, SHA-1 • Auth: pre-shared secret or digital certificate (PKI support)
Network Associates, Inc. http://www.tis.com/	Gauntlet GVPN Internet Firewall v.4.1a	BSDI	• Tightly integrated with Gauntlet Firewall • Protocol: IPSEC • Key mgmt: ISAKMP/Oakley • Encryption: DES, 3-DES, CAST • Integrity alg: MD5, SHA-1 • Auth: digital certificate (PKI support) • Native Support for Multiple PKI vendors (Entrust, VeriSign)
Northern Telecom Limited http://www.nortelnetworks.com	Contivity Extranet Switch v2.11	Proprietary Hardware	• Support remote access VPNs • Provide VPN service with working service providers
RADGUARD Ltd http://www.radguard.com/	• ClPro VPN Hardware v1.12 • Software v3.22 VB3	Proprietary Hardware	• Hardware-based VPN system • 100 Mbps multi-site network encryption • Integrated firewall and NAT
RedCreek Communications Inc. http://www.redcreek.com/	Ravlin 10/5100 Software v 3.10	Proprietary Hardware	• Protocol: IPSEC • Key mgmt: ISAKMP/Oakley • Encryption: DES, 3-DES • Integrity alg: MD5, SHA-1 • Auth: Digital Signal Standard (DSS) • Easy device management through SNMP MIB II
Shiva Corporation http://www.shiva.com/	LanRover VPN Gateway v 6.5	Proprietary Hardware	• Hardware-based, wire-speed encryption • Support of multi authentication schemes: RADIUS, SecureID, challenge/response, Entrust Ready, Windows NT Domains • Load balancing and failover across multiple gateways

<Table 3> ICSA-certified IPSEC products (continue).

Company	Product	Platform	Features
TimeStep Corporation http://www.timestep.com/	PERMIT/Gate 2500/4500 v1.1	Proprietary Hardware	• Support intranets, extranets, and Internet remote access • Protocol: IPSEC • Key mgmt: ISAKMP/Oakley • Encryption: DES, 3-DES, RC5, Blowfish, CASH, IDEA • Integrity alg: MD5, SHA-1 • Auth: signature, pre-shared secret • CA: Entrust/Manager
	PERMIT/Client v1.1	• Windows 95, 98 • NT 4.0	• Support Internet remote access • Protocol: IPSEC • Key mgmt: ISAKMP/Oakley • Encryption: DES, 3-DES, RC5, Blowfish, CASH, IDEA • Integrity alg: MD5, SHA-1 • Auth: signature, pre-shared secret • CA: Entrust/Manager
VPNet Technologies, Inc. http://www.vpnet.com/	VSU-1010 VPN Service Unit v 2.0	Proprietary Hardware	• Protocol: IPSEC • Key mgmt: ISAKMP/Oakley, SKIP, manual • Encryption: DES, 3-DES • Integrity alg: MD5, SHA-1 • Auth: signature, pre-shared secret, token • Support NAT • Compatible digital certificate by VeriSign, GTE Cybertrust, Entrust, and Frontier Technologies

work between the company and its partners (4) investment-return period is very short compared with other technologies as several months (5) it is gearing with the electronic commerce which is explosively increasing on the Internet.

ⓔ A VPN product consists of several components: VPN server, VPN client, Certificate Authority, LD AP server, Key Management Server, etc. So many VPN providers support VPN service with other providers. For instance, provider A supports VPN client device (remote access support) and provider B support VPN server device (security association support).

ⓕ Companies requiring security facilities install and operate a firewall. Several problems can occur if currently used firewalls are replaced by IPSEC. First of all, the performance issue will be raised. So, what kind of relationships with firewalls IPSEC products should have will be a considerable one. Currently, the trend is that companies developing firewalls are developing IPSEC products and also adding the IPSEC functions to firewalls.

ⓖ To resolve the interoperability issue using IP SEC in the VPN, first of all, the interoperability between source security policy and destination security policy should be established. The IETF is now working on the Security Policy Protocol (SPP) and Security Policy Specification Language (SPSL). SPP is a protocol dealing with security policy and SPSL is a language for security policy specification. If these IETF drafts are standardized, somehow the infrastructure on the interoperability for the secure communications over the Internet will be established.

ⓗ To resolve the interoperability for the VPN, first of all, a base policy data model should be established. Based on this model, the standardization on the structure of directory based schema for the

policy based VPN configuration and administration with IPSEC can be established. Also, the considerations on the coordination of LDAP which is a policy information access protocol with SPSL which is a security policy specification language used to represent policy information itself is necessary.

Acronyms

AH	Authentication Header
ATM	Asynchronous Transfer Mode
COPS	Common Open Policy Service
DES	Data Encryption Standard
DiffServ	Differentiated Services (See http://www.ietf.org/html-charters/diffserv-charter.html.)
DSL	Digital Subscriber Line
ESP	IP Encapsulating Security Payload
FT-1	Functional T-1
ICSA	International Customer Service Association
IKE	Internet Key Exchange
ISDN	Integrated Services Digital Network
LDAP	Lightweight Directory Access Protocol
MPLS	Multi-Protocol Label Switching
OC3	Optical Carrier level 3
OSI	Open Systems Interconnection
PSTN	Public Switched Public Network
RSA	Rivest, Shamir and Adleman
SA	Security Association
SAD	Security Association Database
SPD	Security Policy Database
TCP	Transmission Control Protocol
T-1 (DS1)	T-carrier multiplexer, level 1 (1.544-Mbps digital channel)
T-1C	T-carrier multiplexer, level 1C
T-2	T-carrier multiplexer, level 2
T-3 (DS3)	Carrier multiplexer, level 3 (45-Mbps digital channel)
UDP	User Datagram Protocol

Appendix

<Table 4> VPN classification guide (continued on next page).

VPN Class	Typical Users	Typical Information Needs	Scalability & Bandwidth Needs	Technologies/ Products	Pros/Cons
Class 0	Small companies with remote workers (small manufacturing, services, etc.)	• Email • Internal database • File access	• 1 site • Up to 50 remote users • Internet access at site via DSL or FT1 • Dial access for remote sites	• PPTP • Windows 95/98/NT • Software VPN solutions on standard PC platforms • Packet filtering	+ Simplest and lowest cost to implement + Good way to "trial" remote access - No site-to-site - Inflexible (point to point) - Longest meantime-to-repair (if server fails)
Class 1	Small to mid size companies with multiple locations (small to mid-sized manufactures, services, etc.)	• Email • Internal database • File access	• 2 to 10 sites • Up to 250 remote users • Internet access at site up to T1 • Dial access for remote sites	• IPSEC (DES, IKE) • Password user authentication • Hardware VPN gateway (wire-speed T1 with 250 sessions) • Remote access client software • Simple firewall or packet filtering	+ Easy to design & install + Low cost + Site-to-site & remote access + Hardware gives security without performance loss - Extranets not supported if IPSEC is not interoperable
Class 2	Medium size companies with high-value intellectual property: (design	• Email, internal database & file access • Product design	• Up to 10 sites • Up to 500 remote users • Up to T1/multi-T1 at main site	• IPSEC (3DES, IKE) • Network Address Translation • Strong user authentication (e.g., soft tokens)	+ Higher security + Manageable cost + Site-to-site & remote access

<Table 4> VPN classification guide (continue).

VPN Class	Typical Users	Typical Information Needs	Scalability & Bandwidth Needs	Technologies/ Products	Pros/Cons
Class 2	services, media, etc.)	• Project plans	• Up to T1 for branch sites • Dial access for remote sites	• Firewall at main site • RADIUS server • Hardware VPN gateway (wirespeed T1, wirespeed multi-T1 with 500 sessions) • Remote access client software	- Additional administration (RADIUS, Firewall, etc.) - No extranets (requires interoperability) - No real-time applications
Class 3	Medium to large companies with their business partners & customers (medical, manufacturing, insurance, e-commerce)	• Email, internal database & file access • Design information • Supply chain info & transactions • E-commerce	• 100's of sites • 1,000's of remote users • FT1 to multi-T1 at branches • Multi-T1/T3 at main site • QoS/SLAs for intra-company sites • Dial, ISDN, xDSL, or cable modem access for remote users	• Certified interoperable IPSEC (3DES, IKE) • Network Address Translation • Strong user authentication (smart cards, tokens) • Firewall at main site and large branches • LDAP directory server • Certificate services (PKI) • Hardware VPN gateway at multiple performance levels (wirespeed T1, wirespeed multi-T1, wirespeed multi-T1with 1000+ sessions)	+ Support extranets + Support time-sensitive e-commerce transactions - Require corporate security policy - Require sophisticated design skills - Require significant ongoing administration & management
Class 4	Large multinational companies with extended business partner chain and high degree of outsourcing (medical, insurance, government, financial, etc.)	• Email, internal database & file access • Supply chain info & transactions • E-commerce • Voice & video	• 1000's of sites • 10,000's of remote users • FT1 to Multi-T1 at branches • QoS/SLAs for intra-company, sites • Dial, ISDN, xDSL, or cable modem access for remote users	• Certified interoperable IPSEC (3DES, IKE) • Network Address Translation • Strong user authentication (smart cards, tokens) • Firewall at main site and large branches • LDAP directory • Certificate services (PKI) • Hardware VPN gateways at multi performance levels (wirespeed T1, wirespeed multi-T1, wirespeed T3 or OC3 with 5000+ sessions) • Bandwidth management • Multi VPN service levels • Real time QoS & SLAs • Remote client software with auto-policy distribution	+ Support extranets + Highest security + Support real-time voice & video + Support e-commerce transactions + Scalable admin + Multiple partner relationships - Most complex & expensive - Require extensive network & security skills - Significant ongoing management effort

References

[1] An LDAP Schema for Configuration and Administration of IPSEC Based Virtual Private Networks (VPNs), IETF draft-ipsec-vpn-policy-schema-00.txt, Oct. 9, 1998.

[2] Security Policy System, IETF draft-ietf-ipsec-sps-00-txt, Nov. 18, 1998.

[3] Security Mechanisms for the Internet, draft-ietf-iab-secmech-01.txt, June 1999.

[4] Security Policy Protocol, draft-ietf-spp-00.txt, July 1 1999.

[5] Security Policy Specification Language, draft-ietf-ipsec-spsl-01.txt, July 1, 1999.

[6] http://www.entrust.com

[7] http://www.icsa.com

[8] http://www.infonetics.com

[9] http://www.timestep.com

[10] http://www.verisign.com

[11] http://www.vpnet.com

[12] http://www.xs4all.nl/~freeswan