NCS TIB 02-3

NATIONAL COMMUNICATIONS SYSTEM

TECHNICAL INFORMATION BULLETIN 02-3

Virtual Private Networks and Their Use in Support of National Security and Emergency Preparedness (NS/EP)

March 2002

OFFICE OF THE MANAGER
NATIONAL COMMUNICATIONS SYSTEM
701 SOUTH COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2198

NCS TECHNICAL INFORMATION BULLETIN 02-3

VIRTUAL PRIVATE NETWORKS AND THEIR USE IN SUPPORT OF NATIONAL SECURITY AND EMERGENCY PREPAREDNESS (NS/EP)

May 2002

PROJECT OFFICER

Dale W Barr Jr.

DALE BARR, JR.
Sr. Electronics Engineer
Technology and Programs Division

APPROVED FOR PUBLICATION:

Peter M. Fonash

PETER M. FONASH
Chief, Technology
and Programs Division

FOREWORD

Among the responsibilities assigned to the Office of the Manager, National Communications System, is the management of the Federal Telecommunications Standards Program. Under this program, the NCS, with the assistance of the Federal Telecommunications Standards Committee identifies, develops, and coordinates proposed Federal Standards which either contribute to the interoperability of functionally similar Federal telecommunications systems or to the achievement of a compatible and efficient interface between computer and telecommunications systems. In developing and coordinating these standards, a considerable amount of effort is expended in initiating and pursuing joint standards development efforts with appropriate technical committees of the International Organization for Standardization, the International Telecommunication Union-Telecommunications Standardization Sector, and the American National Standards Institute. This Technical Information Bulletin presents an overview of an effort which is contributing to the development of compatible Federal and national standards in the area of national security and emergency preparedness (NS/EP). It has been prepared to inform interested Federal and industry activities. Any comments, inputs or statements of requirements which could assist in the advancement of this work are welcome and should be addressed to:

Office of the Manager
National Communications System
Attn: N2
701 S. Court House Road
Arlington, VA 22204-2198

Virtual Private Networks and Their Use in Support of National Security and Emergency Preparedness (NS/EP)

Office of the Manager
National Communications System

March 2002

By
Communication Technologies, Inc.
14151 Newbrook Drive, Suite 400
Chantilly, Virginia 20151
703-961-9080 (Voice)
703-961-1330 (Fax)
www.comtechnologies.com

Executive Summary

Organizations today are looking at using virtual private networks (VPNs) for wide-area intranets. The concept of a VPN is to give an organization the same capabilities as a dedicated network infrastructure, at a much lower cost, by sharing the public infrastructure. A VPN allows the use of a public communications infrastructure in such a manner as to exclude all entities outside a defined community. The communications may consist of a combination of leased lines, dial-up service, packet and cell switched connection-oriented networks, or routed connectionless networks. No matter what the underlying communications scheme, the desired result is to connect separate pieces of an organization, to provide unimpeded communications among the pieces, deny access by any outside organization, and protect the privacy of the information as it traverses the public infrastructure.

This report examines the potential use of VPNs to provide National Security and Emergency Preparedness (NS/EP) capabilities for the National Communications System (NCS) and its member agencies. The intended audience is a manager who is familiar with information technology in general, but not necessarily a specialist in information security.

Current NCS programs do not make use of the Internet as a primary mechanism in support of NS/EP requirements and relies heavily on PSNs. That said the PSN providers are rapidly implementing IP based packet-based data networks for their communications backbones and the NCS is very reliant upon the Internet for day-to-day operations, email, research, etc. The Federal Government dependence on the Internet is expected to grow over the next several years. VPNs may stimulate this trend.

There are several VPN architectures and products, and there are many policies and standards that define and constrain the choice of a particular VPN architecture or product. This report describes several standards and meta-standards - Department of Defense (DoD)'s Joint Technical Architecture (JTA), the Common Criteria (CC), and U.S. Government policies to use evaluated products - that provide useful information about what standards are available and their maturity. A VPN should not be implemented in isolation, but as part of a larger system. This report identifies the related security technologies using the Defense in Depth framework of the Information Assurance Technical Forum (IATF). Security standards for VPNs are emerging, but have not fully matured. VPNs have been identified [14] as one of the key technologies that could be used to protect Government networks and information systems from external threats. VPNs that have been evaluated using the CC have yet to reach the market, but several evaluations are underway.

This report covers various architectures for implementing VPN technology within a network and how VPN technology can be used to provide remote access to a private network. It explores the

differences in the assumed risks at the operational and remote sites. The report also covers some of the specific protocols used to establish a VPN. These include protocols that provide data origin integrity, data integrity, confidentiality, security association management, and key distribution. This report contains descriptions of related technologies including protocols that can be used to create VPNs at the application layer, additional authentication protocols that are needed for remote users, some alternative protocols that have been used to establish VPNs, and new technologies being used at the data link layer. Several VPN architectures have been defined. They have been supplemented with additional capabilities to support remote users. The Internet protocol security (IPSec) standards are complete except for some minor changes, but wide-scale use of VPNs is dependent on the deployment of Public Key Infrastructure (PKI), deployment of the Advanced Encryption Standard (AES), and, to a lesser extent, the deployment of Internet protocol version 6 (IPv6). While some alternative approaches to implementing VPNs have been developed, the IPSec protocols are the preferred choice.

There are some outstanding issues with VPNs that may be of particular interest to the NS/EP community to include the immaturity of quality of service (QoS) capabilities in IP-based networks, lack of interoperability of VPNs, and a lack of evaluated VPN products. As a result, VPNs are not currently able to fully support the needs of the NS/EP community (such as supporting secure voice traffic via STU IIIs), but do hold promise for the future. A better understanding of how to provide QoS in packet-based networks is needed.

The recommendations made to the NCS in this report should accelerate the wide-scale deployment of VPNs. The NCS should heed the recommendation of the Network Reliability Council (NRC) and conduct additional research in QoS in packet-based networks and provide opportunities (such as a pilot deployments of QoS technologies) to gain operational experience with QoS capabilities. The NCS should participate in the efforts within the IETF and ITU-T to develop QoS standards for packet-based networks. Where appropriate, the NCS should require the acquisition of evaluated products.

Table of Contents

List of Figures

List of Tables

1 Introduction

A virtual private network (VPN) is communications method that allows the use of a public communications infrastructure for members of a defined community to communicate freely with other members of the community, and whose information cannot be read by anyone outside the community. VPNs are increasingly being considered by organizations for wide-area intranets. VPNs provide the same capabilities as a dedicated network infrastructure, but at a much lower cost, by sharing the public infrastructure. Communications may be transmitted over a combination of leased lines, dial-up service, packet and cell switched connection-oriented networks, or routed connectionless networks. The desired result is to connect separate pieces of an organization, to provide unimpeded communications among the pieces, deny access by any outside organization, and protect the privacy of the information as it traverses the public infrastructure. There is also an increased need for mobile users, whether telecommuters or employees on travel, to be able to remotely access their office computer networks, while maintaining the privacy of their connections.

This report examines the potential use of VPNs to provide National Security and Emergency Preparedness (NS/EP) capabilities for the National Communications System (NCS) and its member agencies. The intended audience is a manager who is familiar with information technology in general, but not necessarily a specialist in information security.

Section 2 of this report defines the NCS, lists the functional requirements for the NCS, and identifies some important trends in communications technologies.

Section 3 examines VPNs in greater detail. It contains a description of several standards and meta-standards that provides useful information about what standards are available and their maturity. Section 3.1 identifies what VPN standards currently exist. Section 3.2 describes the Department of Defense (DoD)'s Joint Technical Architecture (JTA), the Common Criteria, and the U.S. Government policies to use evaluated products. Several VPN requirements are in the form of Protection Profiles. Section 3.3 describes the current U.S. Government policy of requiring the acquisition of products that have been evaluated using the Common Criteria evaluation process, which includes Protection Profiles. Protection Profiles are the Common Criteria's format for expressing security requirements. Protection Profiles have been created for VPNs and for secure remote access. Section 3.4 identifies some related security technologies, using the Defense in Depth framework. VPNs should not be implemented in isolation, but as part of a larger system. This report identifies the related security technologies using the Defense in Depth framework of the Information Assurance Technical Framework (IATF) Forum. It also provides an additional dimension to the Defense in Depth framework by mapping the relevant technologies to a more traditional audit control framework of prevention, detection, response, and mitigation measures. This section also classifies the related technologies using a framework used by the National Security Telecommunications Advisory Committee (NSTAC) Protecting Systems Task Force.

This report describes various architectures for implementing VPN technology within a network and how VPN technology can be used to provide remote access to a private network. It explores the differences in the assumed risks at the operational and remote sites. Section 4 of this report describes three architectures for implementing VPN technology within a network. This section also describes how VPN technology can be used to provide remote access to a private network.

It describes the differences in the assumed risks at operational and remote sites. It also describes the security objectives that have been established for a remote access site.

This report covers some of the specific protocols developed by the Internet Engineering Task Force (IETF) to provide security services for Internet protocol traffic, and which can be used to establish a VPN. These include protocols that provide data origin integrity, data integrity, confidentiality, security association management, and key distribution. This report contains descriptions of related technologies, including protocols, that can be used to create VPNs at the application layer, additional authentication protocols that are needed for remote users, alternative protocols that have been used to establish VPNs, and new technologies being used at the data link layer. Section 5 of this report describes some of the specific protocols used to establish a VPN. Since several key distribution methods use public key cryptography, a section is included on the Public Key Infrastructure (PKI). The section also describes some related technologies to include protocols that can be used to create VPNs at the application layer, additional authentication protocols that are needed for remote users, some alternative protocols that have been used to establish VPNs, and new technologies being used at the data link layer.

Several issues about VPNs are identified and discussed in Section 6. They include: Quality of service (QoS), Interoperability of VPNs, Management of VPNs, Network address translation (NAT), Intrusion detection systems (IDS), Internet protocol version 6 (IPv6), and the lack of evaluated products.

The status of VPN Standards developed by the Internet Engineering Task Force, Observations and Conclusions on the material presented, and Recommendations are provided in Sections 7, 8, and 9 respectively.

2. Trends Affecting the National Communications System

The National Communications System was established via a presidential memorandum of August 21st 1963 entitled "Establishment of the National Communications System." Executive Order 12472 [1], dates April 3rd 1984, superceded President Kennedy's 1963 memorandum, and broadened the NCS's NS/EP capabilities. The goal of the NCS is to ensure that the national telecommunications infrastructure is responsive to the NS/EP needs of the President and the Federal departments, agencies, and other entities, including telecommunications in support of national security leadership and continuity of government. The infrastructure is capable of satisfying priority telecommunications requirements under all circumstances through the use of commercial, government, and privately owned telecommunications resources. The NCS works to ensure that the infrastructure incorporates the necessary combination of hardness, redundancy, mobility, connectivity, interoperability, restorability, and security to obtain, to the maximum extent practicable, the survivability of national security and emergency preparedness telecommunications in all circumstances.

Table 2-1 summarizes the NS/EP communications requirements.

Table 2-1. NS/EP Communications Functional Requirements [2]

Functional Requirement	Description
Interoperability	Voice and data services must interconnect and interoperate with other government or private facilities, systems, and networks.
Mobility	The ability of voice and data infrastructure to support transportable, redeployable, or fully mobile voice and data communications (i.e., Personal Communications Service (PCS), cellular, satellite, High Frequency (HF) radio).
Nationwide Coverage	Voice and data services must be readily available to support the National security leadership and inter- and intra- agency emergency operations, wherever they are located.
Survivability	Voice and data services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or manmade disaster up to and including nuclear war.
Voice Band Service	The service must provide voice band service in support of presidential communications.
Scaleable Bandwidth	The ability of NS/EP users to manage the capacity of the communications services to support variable bandwidth requirements.
Addressability	The ability to easily route voice and data traffic to NS/EP users regardless of user location or deployment status. Means by which this may be accomplished include "follow me" or functional numbering, call forwarding, and functional directories.

Functional Requirement	Description
Affordability	The service must leverage new public network (PN) capabilities to minimize cost. Means by which this may be accomplished favor the use of commercial off-the-shelf (COTS) technologies and services and existing infrastructure.

The NS/EP community depends heavily on dial-up communications, which includes voice and data, within the public switched network (PSN) to support NS/EP operations. A key responsibility of the NCS is the promotion of assured communications during NS/EP activities. One way of doing this is priority treatment and priority access to the PSN. There are two NCS programs that address the issue of priority treatment and priority access is support of NS/EP communications. Priority treatment is provided under the Telecommunications Service Priority (TSP) program, which addresses priority treatment for restoration and provisioning NS/EP services. Government Emergency Telecommunications Service (GETS) emergency access and priority processing in the long distance segments of the PSN to provide a high probability of call completion service [2].

However, changes are occurring in the underlying public telecommunications infrastructure. Telecommunications service providers are rapidly implementing packet-based data networks (such as the Internet) and plan to transition traffic onto the Next Generation Network (NGN), which combine circuit and packet switched networks [2]. As noted in a report on the Internet by the National Academy of Sciences, "the Internet is a composite of tens of thousands of individually owned and operated networks that are interconnected, providing the user with the illusion that they are a single network" [3]. All of the interconnected networks share a common architecture, which includes the following principles:

- Hourglass architecture. The Internet Protocol (IP) represents the neck of the hourglass and there are multiple applications that operate in the protocol layers above IP and multiple communications technologies at layers below IP that transport packets across the Internet.

- End-to-end architecture. Most of the intelligence is located at the edges of the Internet, while the network provides robust connectivity.

- Scalability. The exponential growth of Internet traffic has demonstrated the scalability of the Internet's architecture.

- Distributed design and decentralized control. A few key functions, namely the allocation of address blocks and the management of top-level domain names in the Domain Name System, are centrally managed. There is no central control of the Internet.

In addition, most Federal departments and agencies now use or have a presence on the Internet. However, few agencies currently depend on the public Internet to support mission critical NS/EP operations. Some agencies do depend on Internet applications, including remote access and secure Web sites, which, if impaired, could affect certain administrative and coordinating capabilities in support of NS/EP operations and functions [4].

Although the Federal Government still heavily relies on dedicated TCP/IP networks, its dependence on the public Internet is likely to grow over the next several years. VPNs may directly or indirectly stimulate increased NS/EP dependence on the Internet by offering added functionality, diversified capabilities, and increased security, and reliability of networked communications and applications [4].

3. Standards and Evaluated Products

There are several VPN architectures and products and, at the most abstract level, policies and standards that define and constrain the choice of a particular VPN architecture or product. This section describes several standards and meta-standards under consideration by the Government. They include but are not limited to: Department of Defense (DoD) Joint Technical Architecture (JTA), the Common Criteria, policies to use evaluated products, and the IATF Forum.

3.1 Joint Technical Architecture

DoD's Joint Technical Architecture (JTA) [5] provides a minimum set of standards that enables the flow of information. JTA specifies a set of primarily commercial specifications and standards that cover information processing, information transfer, content, format, and security. Standards and guidelines in JTA are stable, technically mature, and publicly available. Standards and guidelines that do not yet meet the requirements of the JTA architecture, but are expected to mature to meet them in the near-term (within three years), are cited as "emerging standards" in the expectation that they will be mandated in future versions of the JTA.

Table 3-1 lists selected mandated security standards and Table 3-2 lists emerging security standards from JTA 4.0 that apply to VPNs.

Table 3-1. Selected JTA 4.0 Mandated Security Standards [5]

Security Standard Area	JTA 4.0 Mandated Standard
Security Requirements	ISO/IEC 15408:1999, Information Technology – Security Techniques – Evaluation Criteria for IT Security (parts 1 through 3), 1 December 1999. The same content appears in the Common Criteria (parts 1 through 3), Version 2.1.
Virtual Private Network	None.
Authentication	None.
Cryptographic Modules	FIPS PUB 140-1, Security Requirements for Cryptographic Modules, 11 January 1994.
Cryptographic Algorithms	FIPS PUB 180-1, Secure Hash Algorithm-1, April 1995. FIPS PUB 186-1, Digital Signature Standard (DSS) Digital Signature Algorithm (DSA), December 1998.
PKI Certificates	ITU-T Rec. X.509 (ISO/IEC 9594-8.2), Version 3, The Directory: Authentication Framework, 1997.
PKI Certificate Directories	None.
Internetworking Security	None.
Web Security	Secure Sockets Layer (SSL) Protocol, Version 3.0, 18 November 1996.

Even within the DoD, the implementation of the JTA is limited. A May 2001 report by the DoD Inspector General [6] evaluated DoD's progress in implementing the standards contained in the JTA. The general audit finding was that DoD has not fully realized the JTA objective of improving and facilitating the ability of its systems to support joint and combined operations in an overall investment strategy. In response to the audit findings, DoD reaffirmed its commitment to ensure DoD systems conform to the JTA.

Table 3-2. Selected JTA 4.0 Emerging Security Standards [5]

Security Standard Area	JTA 4.0 Emerging Standard
Security Requirements	None.
Virtual Private Network	Virtual Private Network Protection Profile for Protecting Sensitive Information, Version 1.0, 26 February 2000.
Authentication	IETF RFC 2138, Remote Authentication Dial In User Service (RADIUS), April 1997.
Cryptographic Modules	None.
Cryptographic Algorithms	FIPS PUB 46-3, Data Encryption Standard, 8 January 1999. (This replaces DES with Triple DES, as specified in ANSI X9.52). AES Proposal: Rijndael by Joan Daemen and Vincent Rijmen, 9 March 1999, Version 2.
PKI Certificates	IETF RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999. TWG-98-07, Federal PKI X.509 Certificate and CRL Extensions Profile, 9 March 1998.
PKI Certificate Directories	IETF RFC 2559, Internet X.509 Public Key Infrastructure Operational Protocols: LDAPv2, April 1999. IETF RFC 2587, Internet X.509 Public Key Infrastructure LDAPv2 Schema, June 1999.
Internetworking Security	IETF RFC 2401, Security Architecture for the Internet Protocol, November 1998. IETF RFC 2402, IP Authentication Header, November 1998. IETF RFC 2406, IP Encapsulating Security Payload (ESP), November 1998. IETF RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP), 21 February 1998. IETF RFC 2407, Internet Draft, The Internet IP Security Domain of Interpretation for ISAKMP, November 1998.
Web Security	IETF RFC 2246, The Transport Layer Security (TLS) Protocol Version 1.0, January 1999.

3.2 Common Criteria, VPN, and Remote Access Protection Profiles

The first standard listed in Table 3-1 is the Common Criteria [7]. In January 1996, the United States, United Kingdom, Germany, France, Canada, and the Netherlands released a jointly developed evaluation standard for a multi-national marketplace (Australia, New Zealand, Italy, Spain, Norway, Finland, Greece, and Israel have since adopted the standard). This standard is known as the "Common Criteria for Information Technology Security Evaluation" (CCITSE), and is usually referred to as the "Common Criteria" (CC). The CC defines general concepts and principles of IT security evaluation and presents a general model of evaluation. It presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems.

Under the CC, a Protection Profile (PP) is the document that defines an implementation-independent set of IT security requirements for a Target of Evaluation (TOE). A TOE is defined as an IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation. TOEs are intended to meet common consumer needs for IT security. Consumers can therefore construct or cite a PP to express their IT security needs without reference to any specific product. Protection Profiles have been created for VPNs [8] and for Remote Access to networks [9], [10], and [11].

The CC also identifies a second document, a Security Target (ST). An ST is a set of security requirements and specifications used as the basis for evaluation of an identified TOE. The ST for a TOE is a basis for agreement between the developers, evaluators and, where appropriate, consumers on the security properties of the TOE and the scope of the evaluation. The audience for the ST is not confined to those responsible for the production of the TOE and its evaluation, but may also include those responsible for managing, marketing, purchasing, installing, configuring, operating, and using the TOE.

The process of developing a PP and an ST is illustrated in Figure 3-1. The rest of this section describes this process in greater detail.

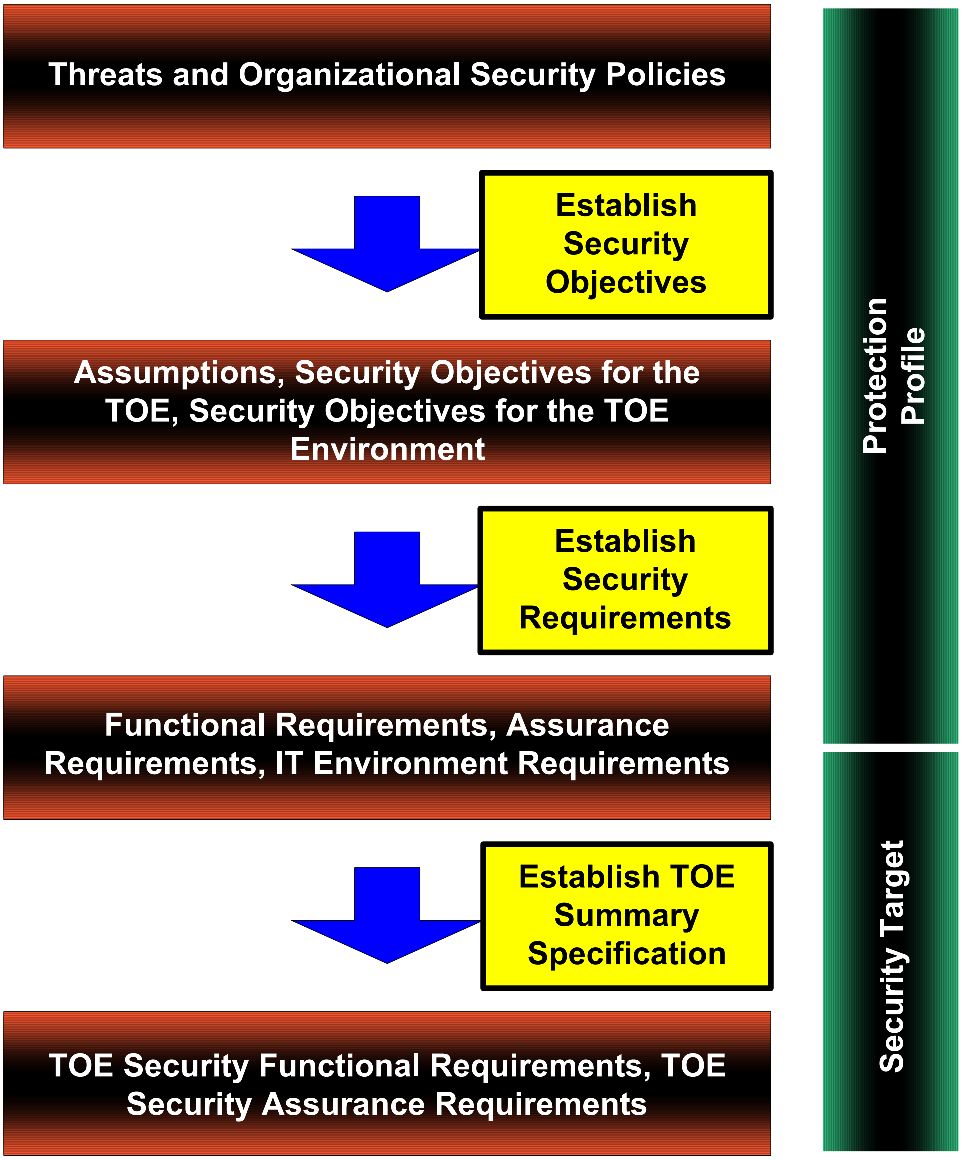
Threats and Organizational Security Policies
Establish Security Objectives
Assumptions, Security Objectives for the TOE, Security Objectives for the TOE Environment
Establish Security Requirements
Functional Requirements, Assurance Requirements, IT Environment Requirements
Establish TOE Summary Specification
TOE Security Functional Requirements, TOE Security Assurance Requirements
Protection Profile
Security Target

Figure 3-1. Protection Profile and Security Target Development Process

The logical relationships established in identifying the security objectives are shown in Table 3-3. The process starts with the definition of the security environment. The threats and security policies that establish the security environment are the basis for identifying assumptions and security objectives. Table 3-3 shows the potential for multiple relationships among threats and policies on one side, and assumptions, objectives, and operating environment requirements on the other. While not specifically required by the Common Criteria, the threats, policies, assumptions, objectives, and operating requirements are written in very abstract terms. This will be illustrated using examples from the Goal VPN PP. The word Goal is used in the title because the PP represents NSA's opinion of what functional security and assurance features near-term VPN implementations should incorporate [8].

Table 3-3. Establishing Security Objectives

	Assumptions	Objectives	Operating Environment Requirements
Threats	✓	✓	✓
Policies	✓	✓	✓

A naming convention for threats, policies, assumptions, objectives, etc. is also generally used where the name given to a threat starts with *T* followed by a period, a name given to a policy starts with a *P* followed by a period, the name given to an assumption starts with an *A* followed by a period, and so forth.

The Common Criteria [7] uses the term threats to include all threats to the assets against which specific protection within the TOE or its environment is required. The CC characterizes a threat in terms of a threat agent, a presumed attack method, any vulnerabilities that are the foundation for the attack, and identification of the asset under attack. The Goal VPN PP identifies a total of 27 threats [8]. Some example threats from the Goal VPN PP are shown in Table 3-4.

Table 3-4. Example Goal VPN Threats [8]

Identifier	Definition
T.ATTACK_DATA	The TOE will encounter data that may contain malicious code. An Authorized User or Unauthorized Agent may use malicious code to attempt to disrupt site security operations or the TOE itself.
T.MASQUERADE_BYPASS	An Unauthorized Agent may bypass identification and authorization mechanisms in order to access or modify information, or utilize system resources. Attack strategies include password guessing, password stealing, password sniffing, all followed by replay, and IP address spoofing.

The Common Criteria [7] uses the term organizational security policies to identify and, if necessary, explain any organizational security policy statements or rules with which the TOE must comply. The Goal VPN PP identifies a total of 21 policies [8]. Some example policies from the Goal VPN PP are shown in Table 3-5.

Table 3-5. Example Goal VPN Organizational Security Policies [8]

Identifier	Definition
P.ACCOUNT	Authorized Users, System and Security Administrators must be held accountable for security relevant actions
P.USAGE	The organization’s IT resources must be used only for authorized purposes.

The Common Criteria [7] uses the term assumptions to describe the security aspects of the environment in which the TOE will be used or is intended to be used. The Goal VPN PP identifies a total of 16 assumptions [8]. Some example assumptions from the Goal VPN PP are shown in Table 3-6.

Table 3-6. Example Goal VPN Assumptions [8]

Identifier	Definition
A.AVAILABLE	Internet, public switched telephone network (PSTN), or other required public network connections are available to the TOE Security Environment (TSE) when required.
A.THREAT_LEVEL	The threat agent is somewhat sophisticated, has minimal though adequate resources, and is willing to take moderate risk.

In Table 3-6, the A.AVAILABLE assumption may raise a concern within the NS/EP community; however, the Protection Profile is describing the security requirements for the VPN that is to be evaluated. The availability of the network that is connected to the VPN is outside the control of the product that is being evaluated.

It is also possible to prepare a Protection Profile for a system in addition to Protection Profiles for individual products used in the system. In a system Protection Profile it would be reasonable to expect that a threat that a network connection becomes unavailable would be addressed by system functions and not treated as an assumption.

The Common Criteria [7] uses the term security objectives for the TOE to define the security objectives for the TOE and the objectives are traced back to aspects of identified threats to be countered by the TOE and organizational security policies to be met by the TOE. The Goal VPN PP identifies a total of 25 TOE security objectives [8]. Some example TOE security objectives from the Goal VPN PP are shown in Table 3-7.

Table 3-7. Example Goal VPN TOE Security Objectives [8]

Identifier	Definition
O.ADMIN	The TOE must provide functions to enable System and Security Administrators to effectively manage and maintain the TOE and its security functions, ensuring that only they can access administrative functionality. This objective extends to remote users who are functioning as the administrator at the RU site.
O.CONFIDENTIALITY	The TOE will provide confidentiality by protecting the content of information released from either the operational user (OU) site or remote user (RU) site destined to other equivalently privileged TOEs. Upon receipt of protected data, the recipient TOE will remove the confidentiality protection invoked by the transmitting TOE.

The Common Criteria [7] uses the term security objectives for the TOE environment to define the security objectives for the TOE environment and they are traced back to aspects of identified threats, organizational security policies, and assumptions not completely countered by the TOE. The Goal VPN PP identifies a total of 18 security objectives for the TOE environment [8]. Some example security objectives for the TOE environment from the Goal VPN PP are shown in Table 3-8.

Table 3-8. Example Goal VPN TOE Operating Environment Requirements [8]

Identifier	Definition
OE.CONNECT	At an OU site connectivity between Authorized Users who do not have equivalent privileges will be regulated by other devices external to the TOE at the OU site, but within the TOE Security Environment (TSE) for the overall system. At an RU site, the authorized user (AU) must use periods processing techniques such as, replacement of hard drives, zeroization of active memory, frequent virus checking, or equivalent techniques whenever connectivity is initiated between AUs who do not have equivalent privileges.
OE.TRAIN	The organization will make every attempt to ensure that AUs and System and Security Administrators (SAs) are adequately trained to the level of their responsibility.

In a Protection Profile there is a second level of decomposition in Figure 3-1 that takes the identified security objectives and assigns them to functional or assurance requirements. The Common Criteria uses the terms TOE security functional requirements to define the functional requirements that the TOE must satisfy in order to meet the security objectives for the TOE and TOE security assurance requirements to identify the supporting evidence needed to demonstrate the TOE meets its security objectives. Optionally, the Protection Profile can include statement of security requirements for the IT environment, which the Common Criteria identifies the IT security requirements that are to be met by the IT environment of the TOE. If the TOE has no asserted dependencies on the IT environment, this part of the PP may be omitted [7]. Again, this is a many to many mapping. In the Goal VPN PP there are 25 TOE security objectives, 183 functional requirements, and 117 assurance requirements [8].

The TOE security functional and assurance requirements statements used in a Protection Profile are selected and tailored from extensive examples in the Common Criteria. Assurance requirements have been grouped into profiles called Evaluation Assurance Levels (EAL). These were created for compatibility with previous security evaluation criteria and to simplify the evaluation process for vendors that have products evaluated. The functional requirements in the Common Criteria are not claimed to be exhaustive, so a Protection Profile may add security functions that are not described in the Common Criteria. Developers of Protection Profiles can also add assurance requirements that are not included in an EAL. Protection Profiles and Security Targets also include a rationale, which is an informal statement that the functions provided are sufficient to satisfy the objectives, that the objectives are sufficient to satisfy the threats and policies, etc [7]. For specific examples of functional requirements, assurance requirements, or the rationale, the reader should obtain one of the referenced Protection Profiles or the Common Criteria.

A third level of decomposition in Figure 3-1 occurs when a specific product is to be evaluated using a Protection Profile. A document called a Security Target is prepared. In a Security Target each functional requirement is mapped to one or more functions performed by the product and each assurance requirement is mapped to a document or the results of some analysis that demonstrates that the product functions perform as claimed. In later sections of this report, Protection Profiles for VPNs and for Remote Access will be used to describe the security objectives for these capabilities. Security objectives provide a high-level overview that is independent of a specific technology or product.

3.3 Acquisition of Evaluated Products

The U.S. government has issued a policy for systems that process national security information. It specifies the purchase of evaluated products. The policy is titled the National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, Subject: National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products [12] and was issued by the National Security Telecommunications and Information Systems Security Committee (NSTISSC) in January 2000. Starting 1 January 2001, systems acquired for processing national security information should give preference to commercial off the shelf (COTS) IA and IA-enabled IT products. The preferred evaluation criteria are the Common Criteria. By 1 July 2002, all COTS IA and IA-enabled IT products acquired to process national security information are required to be evaluated products [12].

While not binding on non-national security systems, departments and agencies are encouraged to consider the acquisition and implementation of evaluated COTS IA and IA-enabled IT products. These products may be appropriate for systems process information that, although not classified, may be critical or essential to the conduct of organizational missions, or for information or systems that are part of critical infrastructures [12]. The National Institute of Standards and Technology (NIST) has also provided similar guidance on the use of evaluated products by Federal organizations [13]. In particular, it cautions that “third party testing and evaluation provides a significantly greater basis for customer confidence than many other assurance techniques.” However, it cautions that “that purchasing an evaluated product simply because it is evaluated and without due consideration of applicable functional and assurance requirements, may be neither useful nor cost effective.”

3.4 Defense in Depth and the IATF

VPNs should not be implemented in isolation, but as part of a larger system. Guidance for including multiple and diverse security capabilities in a system is referred to as Defense in Depth. The IATF Forum provides an overview of Defense in Depth technology objectives. Table 3-9, depicts the technology that applies to each defense in depth layer.

Table 3-9. Defense in Depth Layer and Related Technology [14]

Defense in Depth Layer	Related Technology
Defend the Network and Infrastructure	- Availability of Backbone Networks - Wireless Networks Security Framework - System High Interconnections and Virtual Private Networks (VPNs) - Secure Voice
Defend the Enclave Boundary	- Firewalls - Remote Access - Guards - Network Monitoring Within Enclave Boundaries and External Connections - Network Scanners Within Enclave Boundaries - Malicious Code Protection - Multi-Level Security
Defend the Computing Environment	- Security for System Applications - Host-Based Detect and Respond Capabilities Within Computing Environments
Supporting Infrastructures	- Key Management Infrastructure/ Public Key Infrastructure (KMI/PKI) - Detect and Respond as a Supporting Element

A report by the NSTAC Protecting Systems Task Force (PSTF) on Enhancing the Nation's Network Security [15] does not use the term Defense in Depth, but it does imply the philosophy in its definition of the components of network security. The PSTF report defines the components of network security as follows:

- **Prevention.** Measures taken to preclude or deter an intrusion.

- **Detection.** Measures taken to identify that an intrusion has been attempted, is occurring, or has occurred.

- **Response.** An action or series of actions constituting a reply or reaction against an attempted or successful intrusion. Responses include actions taken to restore a network to its full operating capability following an attack.

- **Mitigation.** Actions taken to make the effects of an intrusion less severe. Mitigation actions include provision of alternative systems, system redundancy, and system fault tolerance.

Referring back to Table 3-9, VPNs, Guards, Multi-Level Security, Security for System Applications and KMI/PKI are examples of prevention type technologies. Network Monitoring, Network Scanners, and Malicious Code Protection are examples of detection type technologies. Examples of response technologies include Host-Based Detect and Respond under Defend the Computing Environment layer and Detect and Respond as a Supporting Element under

Supporting Infrastructures layer. Finally, Availability of Backbone Networks is an example of mitigation technology in Defense in Depth environment.

4. VPN Architectures and Remote Access

The Goal VPN Protection Profile [8] identifies three different architectures for implementing VPN technology within a network environment. The architectures are Site-to-Site, Host-to-Host, and LAN-to-LAN. These connectivity options are also described in the IATF [14], along with several additional variations of the three basic architectures.

The IATF distinguishes between VPNs and remote access. A VPN implies an enclave of users who are protected from the network as a whole by some boundary device. Remote access implies a sole user gaining access to the enclave by some protected means. Although the mechanisms to implement this access may be similar to that used for VPN, the details of the connection are vastly different.

4.1 Site-to-Site

Site-to-site VPNs connect major infrastructures across a public communications infrastructure. The site-to-site VPN architecture is probably the most common. It does not require any changes to the internal network. While it provides protection for communications over external networks, it does not provide any protection on the internal network. Figure 4-1 depicts a site-to-site VPN architecture.

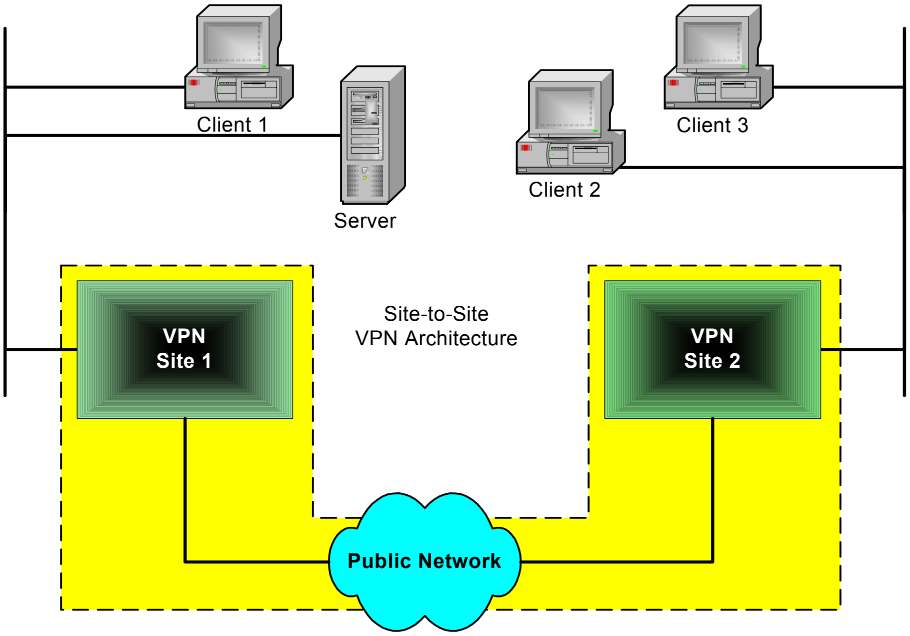

Figure 4-1. Site-to-Site VPN Architecture [8]

In Figure 4-1, all of the clients and the server would appear to be part of a single network and would be unaware that communications between Client 2 and the Server were routed through a tunnel established between the VPNs at Site 1 and Site 2. The INFOSEC glossary [16] defines tunneling as a technology enabling one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network. VPNs establish tunnels through a network infrastructure.

Communications are unprotected from Client 2 to the Site 2 VPN and from the Site 1 VPN to the Server. As a result, a Site-to-Site VPN does not provide protection against an internal threat. Depending on the security services established by the tunnel, the tunnel protects traffic on the public network from various threats. The specific security services are described later in this report in Section 5.1 (integrity) and 5.2. (confidentiality). This configuration can also provide some protection against traffic flow analysis, since the traffic on the public network will have the IP address of the VPNs in the source and destination address fields.

4.2 Host-to-Host

Host-to-host VPNs connect workstations across a shared network or sub-net. The host-to-host VPN architecture is not as common as the site-to-site, but can provide protection against some internal threats as well as external threats. Figure 4-2 depicts a host-to-host VPN architecture.

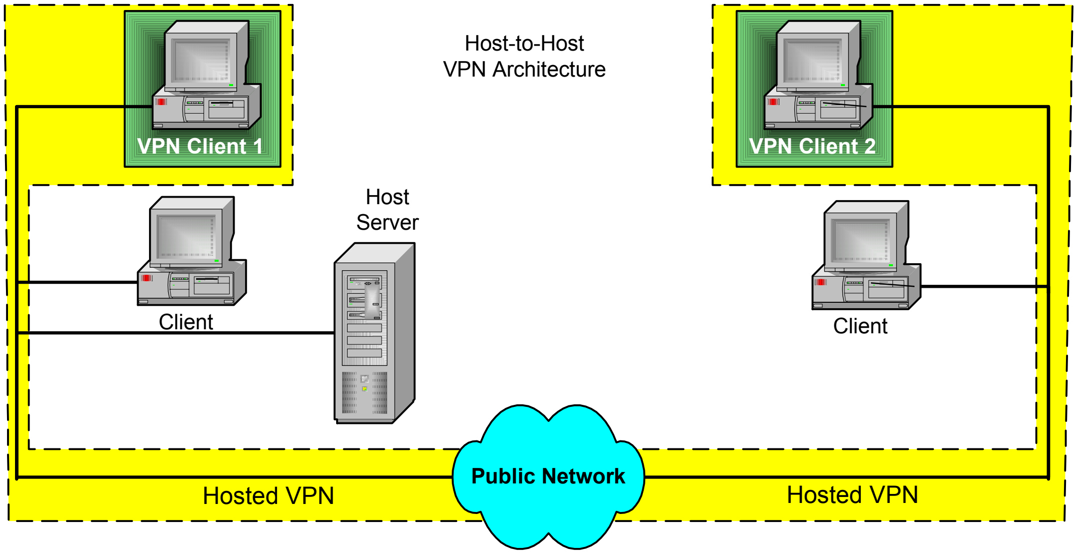

Figure 4-2. Host-to-Host VPN Architecture [8]

In Figure 4-2, Clients 1 and 2 can establish a secure connection between them that can provide protection against internal as well as external threats. Traffic between VPN Client 2 and the Server or non-VPN clients is not protected. Since the VPNs are located at the end points of the network, this VPN architecture does not provide any protection against traffic flow analysis. This is an example of transport mode.

4.3 LAN to LAN

Local Area Network (LAN)-to-LAN VPNs connect sub-nets together across a network that services other entities outside the VPN community. The LAN-to-LAN VPN, which is used to isolate a community of interest (COI) on an internal network, is the least common VPN architecture. This architecture is illustrated in Figure 4-3.

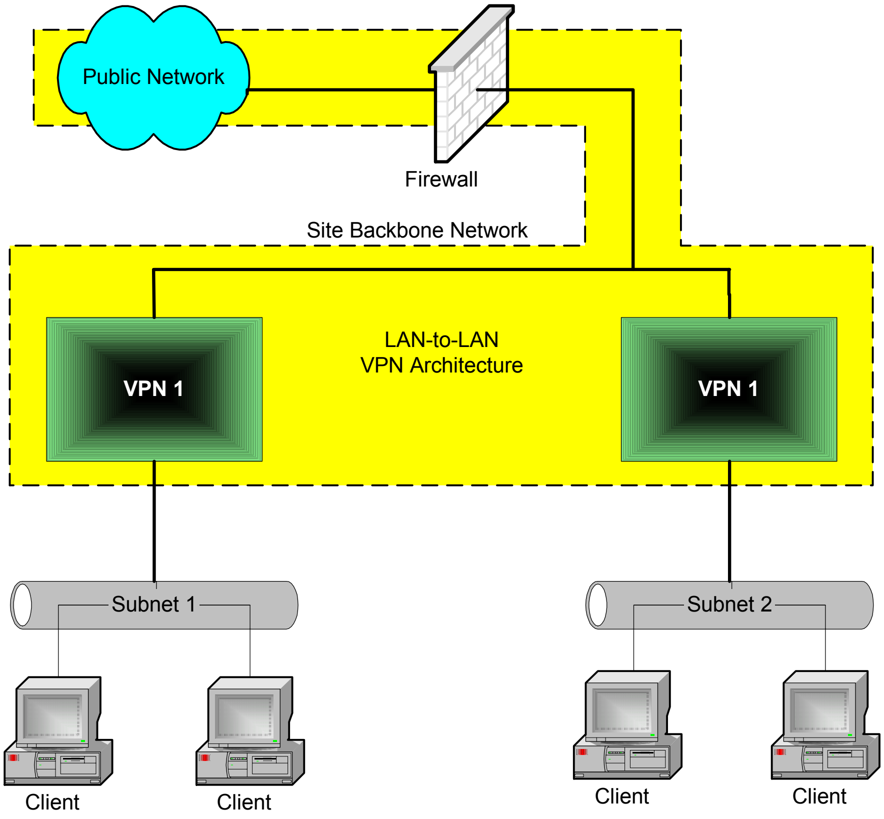

Figure 4-3. LAN-to-LAN VPN Architecture [8]

The LAN-to-LAN VPN architecture is a mixture of the previous two architectures. There is an assumption that the information within the community of interest is more sensitive than the information on the site backbone network. This may mean that the administration and management of the VPNs may be controlled by the subnet administrator rather than the administrator of the site backbone network.

4.4 Remote Access

As noted in Section 4.0, remote access implies a sole user gaining access to the enclave by some protected means and while the mechanisms to implement this access may be similar to that used for VPN, the details of the connection are vastly different [14]. With the advent of telecommuting, remote access to corporate networks is becoming increasingly important. The traditional way of deploying modem pools and remote access servers is expensive because of the dedicated equipment needed before the long-distance telephone costs involved are added. As the Internet has become virtually omnipresent, remote access costs can be greatly reduced by using it as the access infrastructure to the corporate network [17].

The Goal VPN PP describes a number of differences between a VPN that is at an Operational User (OU) site versus a Remote User (RU) site [8]. Figure 4-4 illustrates an RU site connected to an OU site over the Internet. In the figure, at the OU site an Authorized User (AU) does not have physical access to the VPN or other boundary security functions. System administrators (SA) are the only individuals that have physical access to the security boundary functions. At an RU site, which may be a laptop plugged into a phone jack, the AU has full access to the entire environment.

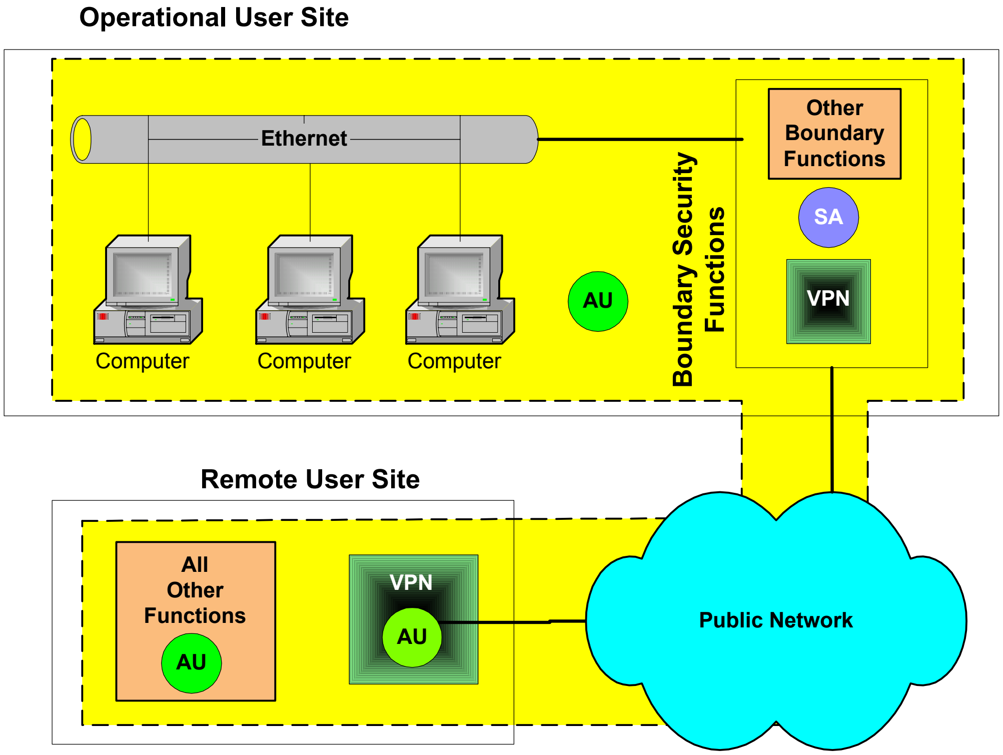

Figure 4-4. Operational vs. Remote User Site [8]

The major issue to be addressed is the inherently dynamic nature of access by a remote user. Typically, security associations cannot be preconfigured because the remote users' address cannot be predicted. A security association is a relationship established between two or more entities to enable them to protect data they exchange. The relationship is used to negotiate characteristics of protection mechanisms, but does not include the mechanisms themselves [23]. Internet Service Providers (ISPs) assign addresses dynamically. At some ISPs it is possible to request fixed addresses for dial-in connections, but only at an extra charge. A remote client needs to be identified by its name rather than by its IP address.

The application of VPN technology to replace existing direct dial-in lines to the corporate network uses the Internet as the access infrastructure. The major design considerations include:

- A VPN solution does not require changes at the servers in the corporate network unless the dial-in traffic is to be protected against attacks on the intranet as well. However, clients have to support the Internet protocol security (IPSec) protocols.

- Because client IP addresses are typically dynamic, clients need to use an identifier other than an IP address to authenticate themselves to the VPN gateway. The Internet Key Exchange (IKE) protocol includes several authentication methods that are not based on a fixed IP address. IKE is described in Section 5.4.

- Dial-in traffic will be encrypted and authenticated. Any traffic that cannot be authenticated will be rejected by the VPN gateway.

- Existing packet filtering rules applied by firewalls, if any, do not interfere with the client IP address filter rules. They can be used without modification.

- Explicit firewall filter rules to protect the corporate intranet against non-VPN traffic are not required because the IPSec authentication will provide this protection.

One requirement of the Goal VPN PP is that the identification of RUs and SAs will be based on the use of hardware identity tokens. The NSTISSI INFOSEC Glossary [16] defines an identity token as a smart card, metal key, or other physical object used to authenticate identity. However, standards for remote user authentication being developed by the IETF IP Security Remote Access working group do not use identity tokens. IETF standards are discussed in Section 7.

Several remote access vendors and the IETF have been in the forefront of this remote access security effort, and the means whereby such security measures are standardized. The Remote Authentication Dial-In User Service (RADIUS) and the Terminal Access Controller Access Control System (TACACS) are two such cooperative ventures that have evolved out of the Internet standardizing body and remote access vendors. See Section 5.7 for more information about RADIUS and TACACS.

Another relevant protection profile is the U.S. DoD Remote Access Protection Profile For SBU-High Environments [9]. For the convenience of specifying those requirements that need only apply to a portion of the remote access system, there are two distinct partitions that have been identified: the RU partition and a Communications Server (CS) partition. An RU contains those parts of the system that a user takes to a remote location, while the CS is the part of the system that remains within the security perimeter of the enclave (referred to as the secure enclave) and connects the secure enclave with the telephone network (TN). Figure 4-5 shows that the system boundary of the remote access system overlaps the system boundary of the secure enclave.

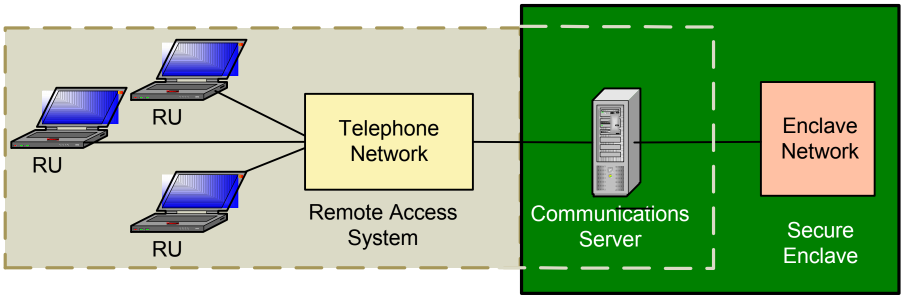

Figure 4-5. System Boundary of Remote Access System [9]

Table 4-1 compares the assumptions made for an OU site versus an RU site in the Goal VPN PP.

Table 4-1. Differences Between an RU and an OU Site [8]

Assumption	OU Site	RU Site
A.ADMIN	At an OU site there are resident system and security administrators.	Limited day-to-day administration of the RU site will be performed by the authorized remote user.
A.ADMIN	OU site administrative responsibilities will be split between a system administrator and a security administrator.	No separation of duties.
A.BACK_UP	Back ups are transparent to the user and performed automatically on a timely basis as determined by site policy.	Back-ups are conducted by the authorized remote user.
A.DESIGN_BYPASS	At an OU site, bypass functions will be performed within a physically controlled boundary protection area, which is accessible to only System and Security Administrators.	At an RU site, bypass functions, if required, will be performed utilizing periods processing techniques.
A.MISUSE_DETECT	Misuse Detection (MD) mechanisms exist outside of the TOE that look for potential misuse (e.g. unauthorized access, unusual modification of information, virus scanning, or unexpected utilization of resources).	MD mechanisms, if any, would be part of TOE.
A.PHYSICAL_SECURITY	At an OU site, the TOE will be located within a physically controlled boundary protection area, which is accessible to only the System and Security Administrators.	The TOE is normally under the supervision of a single individual and may occasionally be left unattended. In addition, the TOE associated with a RU may even be accessed by unauthorized agents (i.e. security inspections at airports, maids in hotels, etc.).

The TN is entirely outside the control of the organization, with the available controls being only what the TN owner voluntarily provides. User access is not controllable and the environment is assumed to be hostile. Because the TN is outside the scope of control for the organization, no security requirements can be attributed to it. Thus, the RU and CS must provide the primary security functions for the remote access system. The system level security objectives for the remote access system identified in the protection profile are listed in Table 4-2.

Table 4-2. Security Objectives for a Remote Access System [9]

Objective	Description
O.ACCESS	The TOE will control access to information that is subject to the enclave security policy, based on the identity of the accountable individuals, such that this policy cannot be bypassed in the TOE.
O.ANTIVIRUS	The TOE will provide for effective malicious code detection and elimination.
O.BANNER	The TOE will provide a banner to notify all users that they are entering a government computer system.
O.CRYPTO_SUPPORT	The TOE must interface with cryptographic support mechanisms, which establish files and configuration parameters and ensures the integrity of these files and parameters.
O.IDENTIFY	The TOE will uniquely identify and authenticate individuals.
O.INTEGRITY	The TOE will apply integrity protection to all information transmitted between the RU and the CS.
O.MANAGE	The TOE will provide adequate management features for its security functions.
O.NO_EAVESDROP	The TOE will prevent, with a strength appropriate for tunneling SBU data across a public network, the disclosure of information during transfers between an RU and the CS.
O.RECEIVE	A CS or a RU will only accept remote commands and data from another CS or RU with which it is mutually authenticated.
O.SECURE_STARTUP	Upon initial start-up of the TOE or recovery from an interruption in TOE services, the TOE must default to a secure state and not compromise its files, configuration parameters, or information being processed before the interruption occurred.
O.SELF_PROTECT	The TOE will protect its security-related functions against external interference or tampering by users, or attempts by users to bypass its security functions.
O.SELF_TEST	The TOE will perform self-tests of its security functions including those required by the site security policy and site procedures.

The objectives listed in Table 4-2 apply to both the RU and the CS. Many of these objectives would apply to any secure system and are not specific to remote access. The objectives that are specific to providing secure remote access include O.CRYPTO_SUPPORT, O.NO_EAVESDROP, and O.RECEIVE. Several additional security objectives are identified in the PP specifically for the RU and the CS [9]. These objectives are listed in Tables 4-3 and 4-4.

Table 4-3. Additional Security Objectives for Remote Unit [9]

Objective	Description
O.MEDIA	The RU will protect sensitive data stored on it such that this data is unavailable while the TOE is not in use.
O.ACCESS	During operation, the RU will limit access to system resources to authorized users.

Table 4-4. Additional Security Objectives for Communications Server [9]

Objective	Description
O.DETECT	The CS will detect unauthorized changes to RU configurations, when an RU connects to the CS.
O.AUDIT	The TOE will provide an audit trail to ensure each authenticated user and TOE administrator can be held accountable for his or her actions in the TOE. The audit trail will be of sufficient detail to reconstruct events in determining the cause or magnitude of compromise should a security violation or malfunction occur.
O.CS_AVAILABLE	The CS will not allow a single user identity to connect to more than one incoming modem port at one time.

The additional objectives for the remote unit reflect that physical security of the RU may be limited. The additional objectives for the CS are to compensate for the lack of physical security in the environment where the RU is operated.

5. VPN Technologies

The primary protocol suite used to create a Virtual Private Network is Internet protocol security (IPSec). As previously noted in Table 3-2, the IPSec standards are identified as emerging standards in JTA 4.0. The Internet Engineering Task Force (IETF) developed the IPSec standards. More information about the IETF's process for developing standards can be found in Section 7. The following IETF Request for Comments (RFCs) are applicable to VPNs and are addressed further in this section as follows:

- RFC 2402. IP Authentication Header (AH)
- RFC 2406. IP Encapsulating Security Payload (ESP)
- RFC 2408. Internet Security Association and Key Management Protocol (ISAKMP)
- RFC 2409. The Internet Key Exchange (IKE)

The IPSec Authentication Header (AH) is addressed in Section 5.1. The Encapsulating Security Payload (ESP) is addressed in Section 5.2. The Internet Security Association and Key Management Protocol (ISAKMP) is addressed in Section 5.3. The Internet Key Exchange (IKE) protocol is addressed in Section 5.4. Since the IPSec protocols make use of public key cryptography for key exchange, a description of the status of the Public Key Infrastructure is included in Section 5.5.

VPNs can also be created at the application layer by using protocols such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS). These are described in Section 5.6. For remote access additional authentication mechanisms are needed beyond what is provided by IKE. Section 5.7 describes two protocols, RADIUS and TACACS. Section 5.8 identifies several protocols that have been used for VPNs, but which are not included as part of the JTA. Some newer data link layer protocols provide a challenge to implement a VPN, primarily because of their high speeds. Section 5.9 identifies two high-speed network technologies.

IPSec is sometimes called a framework [17] because it provides a stable, long-lasting base for providing network layer security. It can accommodate today's cryptographic algorithms, and can also accommodate newer, more powerful algorithms as they become available. IPv6 (discussed in Section 6.6) implementations are required to support IPSec and IPv4 implementations may support IPSec. The IPSec protocols address several major areas:

- **Data origin authentication** verifies that each datagram was originated by the claimed sender.

- **Data integrity** verifies that the contents of the datagram were not changed in transit, either deliberately or due to random errors.

- **Data confidentiality** conceals the clear text of a message, typically by using encryption.

- **Replay protection** assures that an attacker cannot intercept a datagram and play it back at some later time without being detected.

- **Automated management of cryptographic keys and security associations** assures that a company's VPN policy can be conveniently and accurately implemented throughout the extended network with little or no manual configuration. These functions make it possible for a VPN's size to be scaled to whatever size a business requires.

5.1 IPSec Authentication Header

The IP Authentication Header (defined in RFC 2402 [18]) provides connectionless (that is, per-packet) integrity and data origin authentication for IP datagrams, and also offers protection against replay. Data integrity is assured by the checksum generated by a message authentication code, data origin authentication is assured by including a secret shared key in the data to be authenticated, and replay protection is provided by use of a sequence number field within the AH header. In the IPSec vocabulary, these three distinct functions are lumped together and simply referred to by the name authentication.

IPSec identifies two modes of operation: tunnel mode and transport mode. Figure 5-1 shows the addition of an AH header in tunnel mode, as would be used in a Site-to-Site or a LAN-to-LAN VPN architecture. The destination address in the new IP header is the address of the destination VPN. Also note that the authentication function includes the entire packet, except for a few fields in the new IP header (such as time to live, a field that is decremented by each router that handles the packet) that may change in route to the destination IP address. These fields are referred to as mutable fields.

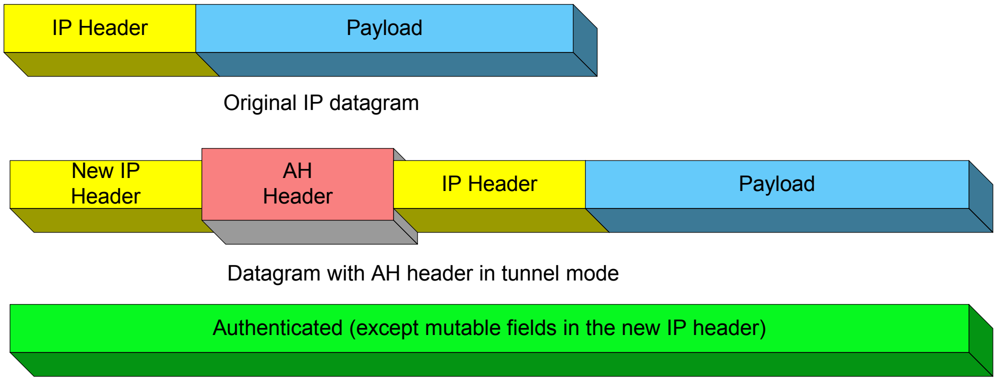
IP Header
Payload
Original IP datagram
New IP Header
AH Header
IP Header
Payload
Datagram with AH header in tunnel mode
Authenticated (except mutable fields in the new IP header)

Figure 5-1. AH Header in Tunnel Mode [17]

The source and destination IP address in the new IP header are included in the authentication function. This allows IP source address spoofing attacks to be detected by the receiver. In order to provide replay protection, an IKE authentication method other than pre-shared secret must be used. This is because the AH header includes a sequence number that requires a new security association to be automatically established when the sequence number field rolls over.

Figure 5-2 shows the addition of an AH header in transport mode, as would be used in a Host-to-Host VPN architecture. The primary difference is that the original IP header is retained. The authentication function still includes the entire packet.

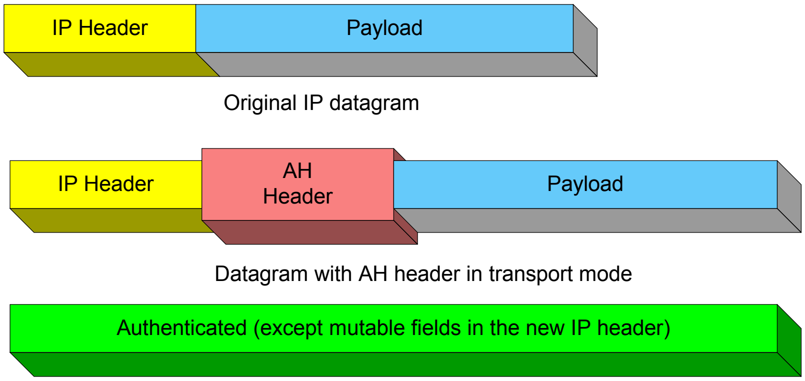
IP Header
Payload
Original IP datagram
IP Header
AH Header
Payload
Datagram with AH header in transport mode
Authenticated (except mutable fields in the new IP header)

Figure 5-2. AH Header in Transport Mode [17]

It should be noted that the authentication function does not provide any data confidentiality. That capability is provided by the Encapsulating Security Payload (ESP) function, described in the next section.

5.2 IPSec Encapsulating Security Payload

The IPSec Encapsulating Security Payload (defined in RFC 2406 [19]) provides data confidentiality (encryption), connectionless (i.e., per-packet) integrity, data origin authentication, and protection against a replay attack. ESP always provides data confidentiality, and can also optionally provide data origin authentication, data integrity checking, and replay protection.

Comparing ESP to AH, one sees that only ESP provides encryption, while either can provide authentication, integrity checking, and replay protection. When ESP is used to provide authentication functions, it uses the same algorithms used by the AH protocol. However, the coverage is different. The authenticated fields do not include the new IP header, so ESP does not provide protection against IP source address spoofing attacks.

Figure 5-3 shows the addition of an ESP header in tunnel mode. The destination address in the new IP header is the address of the destination VPN. Again note that the authentication provided by ESP does not include the new IP header.

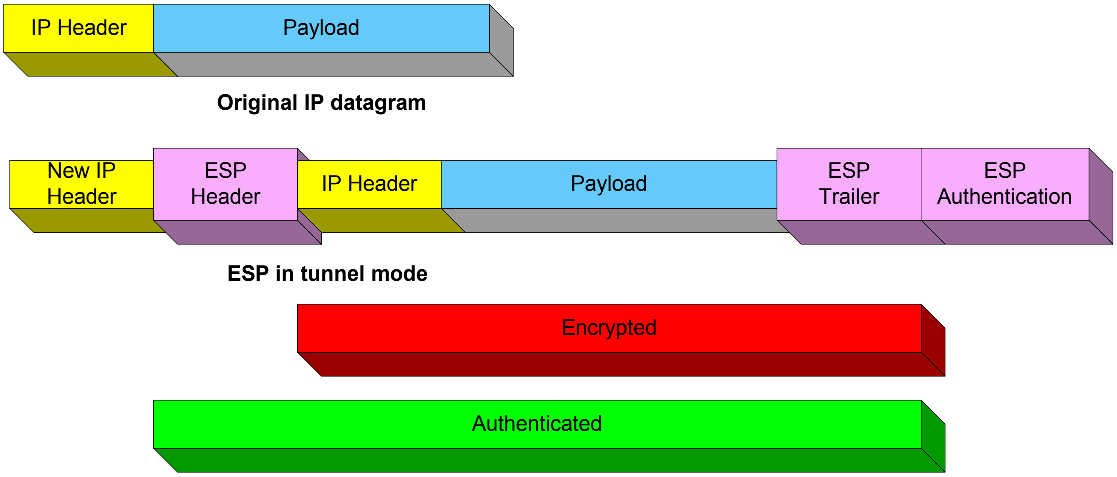

Figure 5-3. ESP Header in Tunnel Mode [17]

Figure 5-4 shows the addition of the ESP header in transport mode. The primary difference is that the original IP header is retained. In contrast with AH transport mode, the authentication does not include the IP header.

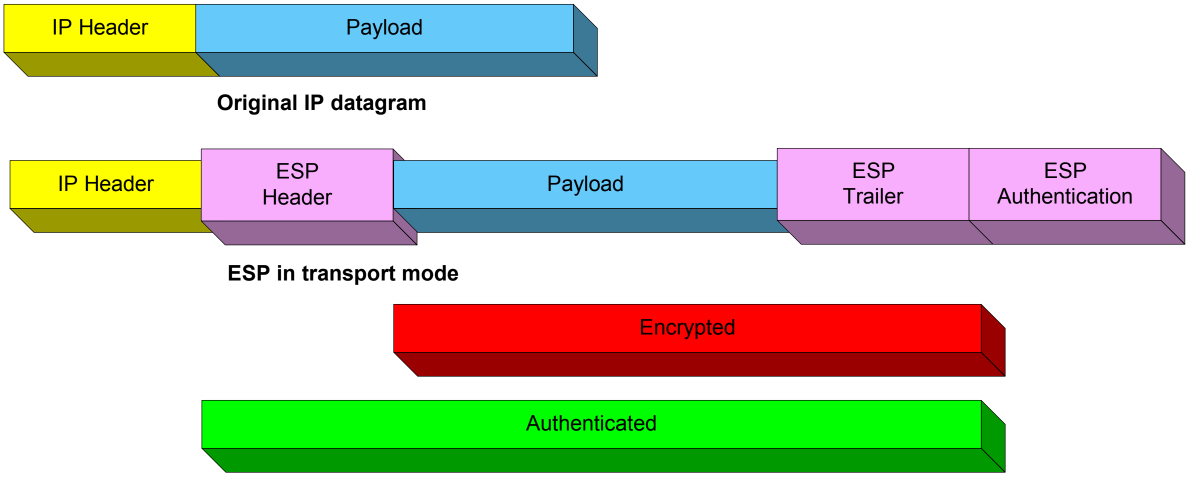

Figure 5-4. ESP Header in Transport Mode [17]

The AH and ESP functions can be used together. One potential combination is to utilize ESP in transport mode and AH in tunnel mode. Figure 5-5 illustrates this combination. Note that the original payload and the ESP trailer are the only portions that are encrypted (the same as ESP in transport mode) and that the AH authentication covers the entire packet, except for the mutable fields in the new IP header.

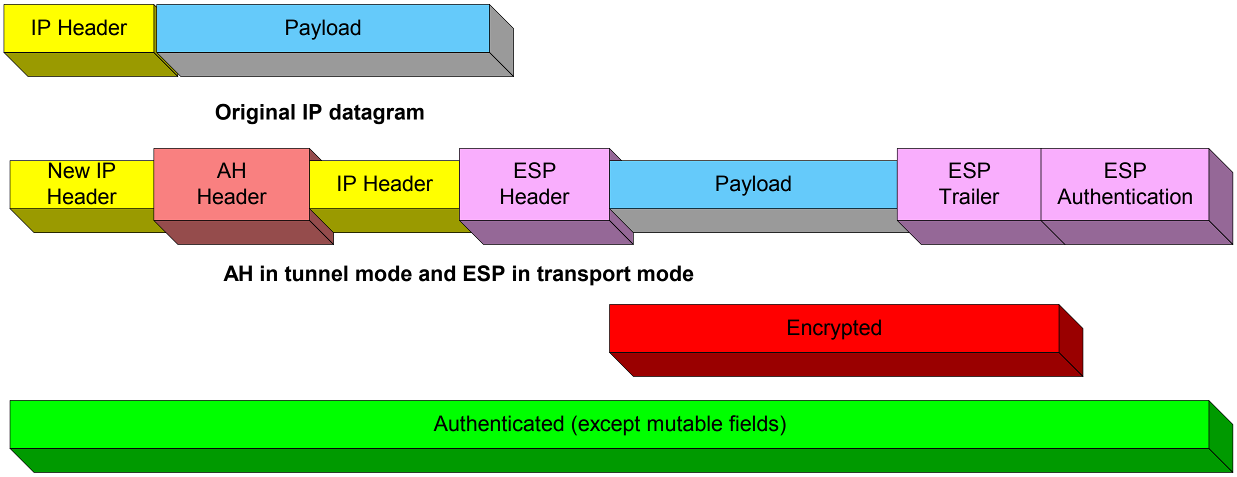

Figure 5-5. AH in Tunnel and ESP in Transport Mode [17]

5.3 ISAKMP

The Internet Security Association and Key Management Protocol (ISAKMP) is described in Request for Comments 2408 [20]. The RFC describes a protocol utilizing security concepts necessary for establishing Security Associations (SA) and cryptographic keys in an Internet environment. An SA protocol that negotiates, establishes, modifies, and deletes SAs and their attributes is required for an evolving Internet, where there will be numerous security mechanisms and several options for each security mechanism.

ISAKMP defines procedures and packet formats to establish, negotiate, modify, and delete SAs. SAs contain all the information required for execution of various network security services, such as the IP layer services (e.g., header authentication and payload encapsulation), transport or application layer services, or self-protection of negotiation traffic. ISAKMP defines payloads for exchanging key generation and authentication data. These formats provide a consistent framework for transferring key and authentication data which is independent of the key generation technique, encryption algorithm and authentication mechanism.

The management of SAs provided by ISAKMP is distinct from key exchange protocols in order to cleanly separate the details of security association management (and key management) from the details of key exchange. There may be many different key exchange protocols, each with different security properties. However, a common framework is required for agreeing to the format of SA attributes, and for negotiating, modifying, and deleting SAs. ISAKMP serves as this common framework.

An SA is a unidirectional (simplex) logical connection between two IPSec systems, uniquely identified by the following three attributes: a Security Parameter Index, an IP Destination Address, and a Security Protocol. The definition of the attributes is as follows:

- Security Parameter Index (SPI) **-** This is a 32-bit value used to identify different SAs with the same destination address and security protocol. The SPI is carried in the header of the security protocol (AH or ESP).

- IP Destination Address - This address may be a unicast, broadcast, or multicast address. However, currently SA management mechanisms are defined only for unicast addresses.

- Security Protocol - This can be either AH or ESP. An SA can be in either of two modes: transport or tunnel, depending on the mode of the protocol in that SA.

For two IPSec systems to communicate there must be two SAs defined, one in each direction. And an SA gives security services to the traffic carried by it either by using AH or ESP, but not both. Therefore, for connections to be protected by both AH and ESP, two SAs must be defined for each direction. In this case, the set of SAs that define the connection is referred to as an SA bundle. The SAs in the bundle need not terminate at the same endpoint. For example, Figure 5-5 could represent a mobile host that has an AH SA between itself and a firewall and a nested ESP SA between itself and a host behind the firewall.

An IPSec implementation maintains two databases related to SAs. They are a Security Policy Database and a Security Association Database and are defined as follows:

- Security Policy Database (SPD) - The Security Policy Database specifies what security services are to be offered to the IP traffic, depending on factors such as source, destination, whether it is inbound, outbound, etc. It contains an ordered list of policy entries, separate for inbound and/or outbound traffic. Entries in this database are similar to the firewall rules or packet filters.

- Security Association Database (SAD) - The Security Association Database contains parameter information about each SA, such as AH or ESP algorithms and keys, sequence numbers, protocol mode and SA lifetime. For outbound processing, an SPD entry points to an entry in the SAD. That is, the SPD determines which SA is to be used for a given packet. For inbound processing, the SAD is consulted to determine how the packet must be processed.

5.4 Internet Key Exchange

The Internet Key Exchange (IKE) protocol is described in Request for Comments 2409 [21]. RFC 2409 describes a hybrid protocol whose purpose is to negotiate, and provide authenticated keying material for, security associations in a protected manner. Processes implementing IKE may be used for negotiating VPNs and also for providing a remote user from a remote site (whose IP address need not be known beforehand) access to a secure host or network. IKE requires two phases be completed before traffic can be protected with AH and/or ESP [22].

During Phase 1, the partners exchange proposals for the ISAKMP SA and agree on one. This contains specifications of authentication methods, hash functions, and encryption algorithms to be used to protect the key exchanges. The partners then exchange information for generating a shared master secret:

- Cookies that also serve as SPIs for the ISAKMP SA
- Diffie-Hellman values
- Nonces (A nonce is a random or non-repeating value that is included in data exchanged by a protocol, usually for the purpose of guaranteeing liveness and thus detecting and protecting against replay attacks [23].)
- Optionally exchange IDs when public key authentication is used

Both parties then generate keying material and shared secrets before exchanging additional authentication information. When all goes well, both parties derive the same keying material and actual encryption and authentication keys without ever sending any keys over the network.

IKE supports client negotiation. Client mode is where the negotiating parties are not the endpoints for which security association negotiation is taking place. When used in client mode, the identities of the end parties remain hidden. Table 5-1 lists the authentication methods supported by IKE.

Three of the authentication methods depend upon the deployment of a Public Key Infrastructure (PKI).

During IKE Phase 2, the partners exchange proposals for Protocol SAs and agree on one. This contains specifications of authentication methods, hash functions and encryption algorithms to be used to protect packets using AH and/or ESP. To generate keys, both parties use the keying material from a previous Phase 1 exchange and they can optionally perform an additional Diffie-Hellman exchange for perfect forward security (PFS).

The Phase 2 exchange is protected by the keys generated during Phase 1, which effectively ties a Phase 2 SA to a particular Phase 1 SA. However, multiple Phase 2 exchanges can co-exist under the same Phase 1 protection to provide granular protection for different applications between the same two systems. For instance, FTP traffic may be encrypted with a stronger algorithm than Telnet, but the keys for Telnet may be refreshed more often than those for FTP. Systems can also negotiate protocol SAs for third-parties (proxy negotiation), which is used to automatically create tunnel filter rules in security gateways.

Table 5-1. IKE Authentication Methods [21]

Authentication method	How authentication is performed	Advantages	Disadvantages
Pre-shared keys	- By creating hashes over exchanged information	- Simple	- Shared secret must be distributed out-of-band prior to IKE negotiations - Can only use IP address as ID.
Digital signatures Rivest-Shamir-Adleman (RSA) or DSS	- By signing hashes created over exchanged information	- Can use IDs other than IP address - Partner certificates need not be available before IKE negotiations	- Requires certificate operations (inline or out-of-band)
RSA public key encryption	- By creating hashes over nonces encrypted with public keys	- Better security by adding public key operation to DH exchange - Allows ID protection with aggressive mode	- Public keys (certificates) must be available before IKE negotiations - Performance-intensive public key operations
Revised RSA public key encryption	- Same as above	- Same as above - Fewer public key operations by using an intermediate secret	- Public keys (certificates) must be available before IKE negotiations

5.5 Public Key Infrastructure

As noted in the previous section, all of the IKE authentication methods require the use of public key cryptography except for pre-shared keys. The limitations of pre-shared keys is that they must be distributed prior to IKE negotiations, the IPSec replay prevention service is not available, and user identity is based on a fixed IP address. Since remote users may not have a permanently assigned IP address, remote users find it difficult to use IPSec without the use of public key cryptography. Pre-shared keys do not scale up well to large networks. This section provides a brief definition of what a PKI includes and provides an assessment of the current state of PKI deployment.

A public key infrastructure is defined as “the set of services and policies that lays the framework for binding a public key to an identity and distributing that binding” [24]. Figure 5-6 provides a graphical view of the entities in a PKI implementation.

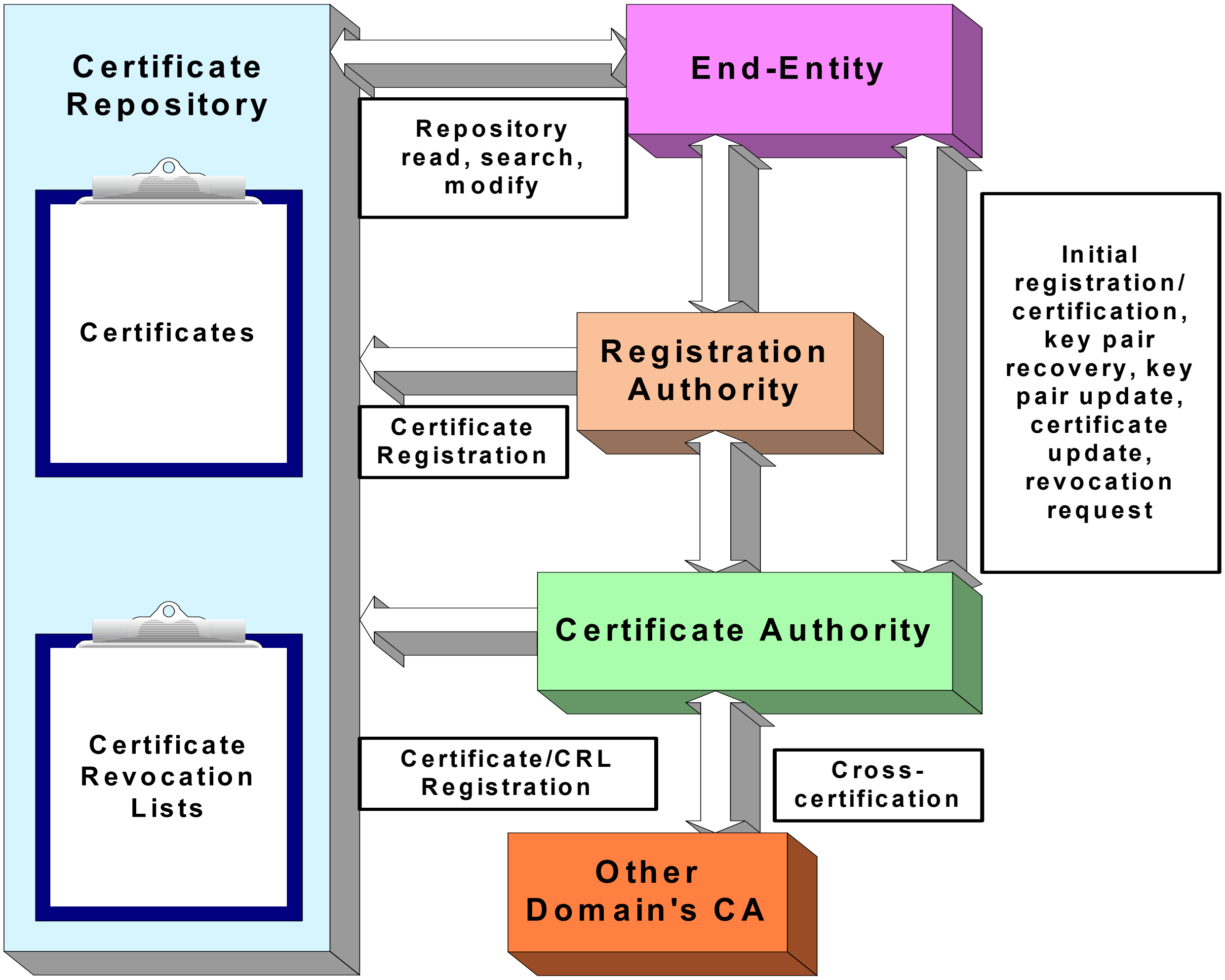
Certificate Repository
Certificates
Certificate Revocation Lists
End-Entity
Repository read, search, modify
Registration Authority
Certificate Registration
Certificate Authority
Certificate/CRL Registration
Initial registration/ certification, key pair recovery, key pair update, certificate update, revocation request
Cross-certification
Other Domain's CA

Figure 5-6. Entities in a PKI Implementation [25]

Table 5-2 provides a definition of each of the entities in Figure 5-6. A user or end-entity only needs to contact the Certificate Authority (CA) or Registration Authority (RA) if it involves a change to a public key certificate, e.g., to have a certificate issued, to update a certificate, or to have a certificate revoked. The purpose of the certificate issuing process is to bind the identity of the individual receiving the certificate to the certificate. If the user only needs to look up the public key of another user, the user can directly search the certificate repository.

Table 5-2. Definition of Entities in PKI Implementation

PKI Entity	Description
End-Entity	A user of PKI certificates or an end-user system that is the subject of a certificate.
Certificate Authority	The signer of the certificates.
Registration Authority	An optional PKI component that acts as a subordinate server of the Certificate Authority. The Registration Authority does not issue certificates or certificate revocation lists.
Certificate Repository	Stores issued certificates and maintains a list of revoked certificates.

A General Accounting Office report on PKI technology [26] concludes: "although progress has been made in seeding PKI technology throughout the government, designing and implementing large-scale systems that use PKI technology remains a daunting task. Full-featured PKI implementations – those that offer all of the security assurances needed for sensitive communications and transactions – are not yet commonplace in either the government or the private sector, and a number of substantial challenges must be overcome before the technology can be widely and effectively deployed."

5.6 Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

The Secure Sockets Layer (SSL) standard specifies a security protocol that was developed by Netscape Communications Corporation, along with RSA Data Security, Inc. The primary goal of the SSL protocol is to provide a private channel between communicating applications, which ensures privacy of data, authentication of the partners and integrity. SSL provides an alternative to the standard TCP/IP socket application programming interface (API) that has security implemented within it. Hence, in theory it is possible to run any TCP/IP application in a secure way without changing the application. In practice, SSL is only widely implemented for Hypertext Transfer Protocol (HTTP) connections, but Netscape Communications Corporation has stated an intention to employ it for other application types, such as Network News Transfer Protocol (NNTP) and Telnet, and there are several such implementations freely available on the Internet [27]. As shown in Table 3-1, SSL 3.0 is identified as a mandatory standard in JTA 4.0.

A good overview of the SSL protocol is provided in [28] and is summarized below. SSL is composed of two layers:

- At the lower layer, there is a protocol for transferring data using a variety of predefined cipher and authentication combinations, called the SSL Record Protocol.

- At the upper layer, there is a protocol for the initial authentication and transfer of encryption keys, called the SSL Handshake Protocol.

An SSL session is initiated as follows:

- On the client (browser) the user requests a document with a special uniform resource locator (URL) that begins https: instead of http:, either by typing it into the URL input field, or by clicking a link.

- The client code recognizes the SSL request and establishes a connection through TCP port 443 to the SSL code on the server.

- The client then initiates the SSL handshake phase, using the SSL Record Protocol as a carrier. At this point there is no encryption or integrity checking built in to the connection.

The SSL protocol addresses the following security issues:

- Privacy: After the symmetric key is established in the initial handshake, the messages are encrypted using this key.

- Integrity: Messages contain a message authentication code (MAC) ensuring the message integrity.

- Authentication: During the handshake, the client authenticates the server using an asymmetric or public key. It can also be based on certificates.

SSL requires each message to be encrypted and decrypted and, therefore, has high performance and resource overhead requirements.

Wagner and Schneier [27] performed an analysis of the SSL 3.0 protocol. They identified a number of minor flaws in the protocol and presented several new attacks on the protocol. They state that the flaws can be corrected without overhauling the basic structure of the protocol.

The following comparison of IPSec to SSL is summarized from [29]. IPSec provides cryptographically strong authentication and encryption for IP traffic and also provides for secure and certificate-based key exchange and refresh using IKE. This section points out the similarities and fundamental differences between IPSec and SSL and explains which are the main areas of use for both protocols.

IPSec and SSL are similar for the following reasons:

- IPSec (via IKE) and SSL provide client and server authentication.

- IPSec and SSL provide data authentication and secrecy, even though on different levels of the protocol stack.

- IPSec and SSL can use cryptographically strong algorithms for encryption and hashing operations and can use certificate-based authentication (IPSec via IKE).

- IPSec (via IKE) and SSL provide key generation and refresh without transmitting any keys in the clear or out of band.

IPSec and SSL are different for the following reasons:

- SSL is implemented as an API between the application and transport layers; IPSec is implemented as a framework at the internetwork layer.

- SSL provides application-to-application security (for instance, Web browser to Web server), IPSec provides device-to-device security.

- SSL does not protect IP headers. This can be an exposure to spoofing and session hijacking attacks. IPSec does protect IP headers.

- SSL does not protect user datagram protocol (UDP) traffic, IPSec does.

- SSL operates end-to-end (i.e., in transport mode) and has no concept of tunneling. This can be a problem when traffic needs to be examined by content inspection and virus scanning systems before it is delivered to the final destination. IPSec can operate both ways, in transport and in tunnel mode.

- SSL can traverse network address translation (NAT) or SOCKS (SOCKet-S), which provides for hiding internal addressing structures or to avoid private IP address conflicts. (See Section 6.4 for a discussion of NAT.) IPSec in transport mode cannot use NAT for that purpose but it can use an IPSec tunnel to achieve the same goal and provide even more security than NAT because that tunnel can also be encrypted.

- Applications need to be modified to use SSL (become SSL aware). This can be a problem when you do not have access to the application source code, or you do not have the time or expertise to change the application. IPSec is transparent to applications.

Murhammer [29] concludes that usually, SSL is fine when only one application is to be secured and that is already available in an SSL-aware version. This is the case with a variety of standard applications nowadays, not only with Web browsers and servers. Also, if one option is to implement 3-tier concepts by employing Web application gateways at the perimeter of the network, SSL is a good choice. If a great number of applications need to be secured, it may be easier to secure the whole network instead of dealing with each application in turn. In this case, IPSec is truly the better choice. Unless you develop your own applications, IPSec is much more flexible than SSL to implement a security policy that requires different levels and combinations of authentication, encryption and tunneling.

Last but not least, the choice of a proper security technology also depends on the business model. If the purpose of your application servers is to be accessible to the public, then a Web-based design and security technology based on SSL may be the right choice. SSL is available on any standard Web browser and that will be the only tool used and required by the users. In this case, everyone is a potential customer. If, however, the circle of users who should be given access to your application servers or networks is more restrictive, then a VPN based on IPSec is more likely the way to go. In this case, the participants and their roles in the data interchange are predefined.

The Transport Layer Security (TLS) Protocol is defined in RFC 2246 [30]. As previously noted in Table 3-2, TLS is identified as an emerging standard in JTA 4.0. The primary goal of the TLS Protocol is to provide privacy and data integrity between two communicating applications. TLS is an update to the SSL standard.

RFC 2246 includes a security analysis of the TLS protocol. The TLS protocol is designed to establish a secure connection between a client and a server communicating over an insecure channel. The analysis makes several traditional assumptions, including that attackers have substantial computational resources and cannot obtain secret information from sources outside the protocol. Attackers are assumed to have the ability to capture, modify, delete, replay, and otherwise tamper with messages sent over the communication channel. It outlines how TLS has been designed to resist a variety of attacks.

TLS supports three authentication modes: authentication of both parties, server authentication with an unauthenticated client, and total anonymity. Completely anonymous connections only provide protection against passive eavesdropping. Whenever the server is authenticated, the channel is secure against man-in-the-middle attacks, but completely anonymous sessions are inherently vulnerable to such attacks. Anonymous servers cannot authenticate clients.

Completely anonymous sessions can be established using Rivest-Shamir-Adleman (RSA) or Diffie-Hellman for key exchange. With anonymous RSA, the client encrypts a pre_master_secret with the server's uncertified public key extracted from the server key exchange message. The result is sent in a client key exchange message. With Diffie-Hellman, the server's public parameters are contained in the server key exchange message and the client's are sent in the client key exchange message.

With RSA, key exchange and server authentication are combined. The public key may be either contained in the server's certificate or may be a temporary RSA key sent in a server key exchange message. When temporary RSA keys are used, they are signed by the server's RSA or Digital Signal Standard (DSS) certificate. The signature includes the current ClientHello.random (a random number), so old signatures and temporary keys cannot be replayed. Servers may use a single temporary RSA key for multiple negotiation sessions.

When Diffie-Hellman key exchange is used, the server can either supply a certificate containing fixed Diffie-Hellman parameters or can use the server key exchange message to send a set of temporary Diffie-Hellman parameters signed with a DSS or RSA certificate. Temporary parameters are hashed with the hello.random values before signing to ensure that attackers do not replay old parameters. In either case, the client can verify the certificate or signature to ensure that the parameters belong to the server. If the client has a certificate containing fixed Diffie-Hellman parameters, its certificate contains the information required to complete the key exchange. Note that in this case the client and server will generate the same Diffie-Hellman result (i.e., pre_master_secret) every time they communicate. To prevent the pre_master_secret from staying in memory any longer than necessary, it should be converted into the master_secret as soon as possible. Client Diffie-Hellman parameters must be compatible with those supplied by the server for the key exchange to work.

Because TLS includes substantial improvements over SSL Version 2.0, attackers may try to make TLS-capable clients and servers fall back to Version 2.0. This attack can occur if two TLS-capable parties use an SSL 2.0 handshake. An attacker might try to influence the handshake exchange to make the parties select different encryption algorithms than they would normally choose. Because many implementations will support 40-bit exportable encryption and some may even support null encryption or MAC algorithms, this attack is of particular concern.

When a connection is established by resuming a session, new ClientHello.random and ServerHello.random values are hashed with the session's master_secret. The resulting connection should be secure and effectively independent from previous connections. Sessions cannot be resumed unless both the client and server agree. If either party suspects that the session may have been compromised, or that certificates may have expired or been revoked, it should force a full handshake.

TLS uses hash functions very conservatively. Where possible, both MD5 and Secure Hash Algorithm (SHA) are used in tandem to ensure that non-catastrophic flaws in one algorithm will not break the overall protocol. Outgoing data is protected with a message authentication code (MAC) before transmission. To prevent message replay or modification attacks, the MAC is computed from the MAC secret, the sequence number, the message length, the message contents, and two fixed character strings. The sequence number ensures that attempts to delete or reorder messages will be detected. If an attacker does break an encryption key, all messages encrypted with it can be read. Similarly, compromise of a MAC key can make message modification attacks possible. Because MACs are also encrypted, message-alteration attacks generally require breaking the encryption algorithm as well as the MAC.

For TLS to be able to provide a secure connection, both client and server systems, keys, and applications must be secure. In addition, the implementation must be free of security errors. TLS is only as strong as the weakest key exchange and authentication algorithm supported, and only trustworthy cryptographic functions should be used. Short public keys, short symmetric encryption keys, and anonymous servers should be used with great caution. Implementations and users must be careful when deciding which certificates and certificate authorities are acceptable; a dishonest certificate authority can do tremendous damage.

5.7 Other Authentication Technologies (RADIUS, TACACS)

As previously discussed in Section 4.4, the current authentication methods supported by IKE do not fully meet the needs of remote and mobile users. In the distributed client/server security database model, a number of communication servers, or clients, authenticate a dial-in user's identity through a single, central database, or authentication server. The authentication server stores all the information about users, their passwords, and access privileges. Distributed security provides a central location for authentication data that is more secure than scattering the user information on different devices throughout a network. A single authentication server can support hundreds of communication servers, serving up to tens of thousand of users.

Communication servers can access an authentication server locally or remotely over wide area network (WAN) connections.

Managing dispersed serial line and modem pools for large numbers of users can create the need for significant administrative support. Since modem pools are by definition a link to the outside world, they require careful attention to security, authorization, and accounting. This can be best achieved by managing a single "database" of users, which allows for authentication (verifying user name and password) as well as configuration information detailing the type of service to deliver to the user (for example, Serial Line IP (SLIP), PPP, telnet, rlogin).

The Remote Authentication Dial-In User Service (RADIUS) [31] was designed based on a previous recommendation from the IETF's Network Access Server Working Requirements Group. An IETF Working Group for RADIUS was formed in January 1996 to address the standardization of the RADIUS protocol; RADIUS is now an IETF-recognized dial-in security solution (RFC 2058 and RFC 2138). As previously shown in Table 3-2, RADIUS has been identified as an emerging standard in JTA 4.0.

The key features of RADIUS are:

- **Client/Server Model**. A Network Access Server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response that is returned. RADIUS servers are responsible for receiving user connection requests, authenticating the user, and then returning all configuration information necessary for the client to deliver service to the user. A RADIUS server can act as a proxy client to other RADIUS servers or other kinds of authentication servers.

- **Network Security**. Transactions between the client and RADIUS server are authenticated through the use of a shared secret, which is never sent over the network. In addition, any user passwords are sent encrypted between the client and RADIUS server, to eliminate the possibility that someone snooping on an unsecure network could determine a user's password.

- **Flexible Authentication Mechanisms**. The RADIUS server can support a variety of methods to authenticate a user. When it is provided with the user name and original password given by the user, it can support PPP Extensible Authentication Protocol (EAP) or Challenge Handshake Authentication Protocol (CHAP), UNIX login, and other authentication mechanisms.

- **Extensible Protocol**. All transactions are comprised of variable length Attribute-Length-Value 3-tuples. New attribute values can be added without disturbing existing implementations of the protocol.

Similar to RADIUS, Terminal Access Controller Access Control System (TACACS) is an industry standard protocol specification, RFC 1492. Similar to RADIUS, TACACS receives authentication requests from a network access server (NAS) client and forwards the user name and password information to a centralized security server. The centralized server can be either a TACACS database or an external security database. TACACS was a mandated standard in earlier versions of the JTA. It has been dropped as a mandated standard from JTA 4.0.

5.8 Other VPN Technologies

The Point to Point Tunneling Protocol (PPTP), Layer 2 Forwarding (L2F), and Layer 2 Tunneling Protocol (L2TP) protocols have also been used to build VPNs. They are not recognized as mandated or emerging standards in JTA 4.0. Some commercial products support one of these protocols and some further standards development of the protocols is ongoing by an IETF working group. They are listed for completeness in this report, but are not described in detail.

5.8.1 Point to Point Tunneling Protocol

PPTP is described in the Internet Engineering Task Force (IETF) Request for Comments (RFC) 2637 [32]. RFC 2637 specifies a protocol that allows the Point to Point Protocol (PPP) to be tunneled through an IP network. PPTP does not specify any changes to the PPP protocol but rather describes a new vehicle for carrying PPP.

5.8.2 Layer 2 Forwarding

L2F is described in IETF RFC 2341 [33]. The traditional dial-up network service on the Internet is for registered IP addresses only. L2F defines a new class of virtual dial-up application that allows multiple protocols and networks utilizing unregistered IP addresses to communicate over the Internet. Examples of this class of network application are support for privately addressed IP, Internet Packet Exchange Protocol (IPX), and AppleTalk dial-up via SLIP/PPP across the existing Internet infrastructure. The status of this RFC has been changed to Historic, a status used to indicate that an RFC is obsolete or has been superseded by a more recent specification [34].

5.8.3 Layer 2 Tunneling Protocol

L2TP is defined in RFC 2661 [35]. L2TP combines the best features of the two tunneling protocols previously described: L2F and PPTP. Traditional dial-up networking services only support registered IP addresses, which limits the types of applications implemented over VPNs. L2TP supports multiple protocols and unregistered and privately administered IP addresses over the Internet. This allows the existing access infrastructure, such as the Internet, modems, access servers, and ISDN terminal adapters to be used. It also allows enterprise customers to outsource dialout support, thus reducing overhead for hardware maintenance costs and toll-free dialing fees, and allows them to concentrate corporate gateway resources.

5.8.4 VPN Related Network Technologies

Asynchronous Transfer Mode (ATM) is a connection-oriented technology, using a small, fixed size cell of 53 bytes, allowing very rapid switching through the network. Before data can flow between two nodes on an ATM network, a virtual path is set up between them. Virtual paths are like pipes between switches within the network. Each pipe contains one or more virtual channels, each of which carries an individual data stream in one direction only. To set up a telephone call, for example, a virtual path is required with two virtual channels, one for each direction. Each virtual channel has its own bandwidth and service requirements [36].

The ATM protocols are developed by the ATM Forum, which is an international non-profit organization formed with the objective of accelerating the use of ATM products and services through a rapid convergence of interoperability specifications. ATM is an International Telecommunications Union-Telecommunication Standardization Sector (ITU-T) standard for cell relay [37].

LAN emulation (i.e., a virtual LAN or VLAN) is not a part of ATM itself. Nevertheless, it is a critical function which uses ATM and which will be needed by most ATM users. When speaking of LAN emulation over ATM, what has usually been meant is that workstations will be ATM endpoints and these will communicate with one another through a central ATM switch (or a network of switches) to which all workstations are connected. That is, ATM will be used to perform the local-area networking function.

The concept of an ATM switched LAN is to construct the system such that the workstation application software “thinks” it is a member of a real shared-media LAN, with as little change to the workstation software as possible, consistent with gaining the extra speed and function ATM brings. A sub-objective is to allow multiple unrelated switched virtual LANs to be constructed over the same ATM network [38].

6 Issues Associated with Implementing VPNs

Several issues associated with implementing VPNs are discussed in this section. They are summarized as follows:

- Quality of service (QoS) is identified as an issue because the NS/EP community needs it and current Internet standards do not support it. QoS is discussed in Section 6.1.

- Interoperability of VPNs is identified as an issue because the large number of optional features in the IPSec protocols may result in products that comply with the IPSec standards, but which cannot interoperate. Interoperability of VPNs is discussed in Section 6.2.

- Management of VPNs is identified as an issue because of the heterogeneous nature of the Internet. No one organization controls it. Management of VPNs is discussed in Section 6.3.

- Network address translation (NAT) is identified as an issue because the use of NAT can cause some IPSec protocols to fail. NAT is discussed in Section 6.4.

- Intrusion detection systems (IDS) are an issue because the use of VPNs can interfere with the ability of an IDS to detect an intrusion. IDS are discussed in Section 6.5.

- Internet protocol version 6 (IPv6) is an issue because it will require widespread implementation of IPSec, will make many more IP addresses available, and has greater QoS capabilities than IPv4. However, it is not clear whether IPv6 will be widely deployed. IPv6 is discussed in Section 6.6.

- The lack of evaluated products is an issue because however secure Protection Profiles are on paper, they will not secure any networks until products are developed that meet their requirements. The lack of evaluated products is discussed in Section 6.7.

6.1 Quality of Service

One of the major criticisms of the shared public Internet is its lack of Quality of Service (QoS) capabilities [24]. Certain applications, however, require that network performance meet specific quality metrics in order to function properly. For example, a voice over IP application may require strict latency and jitter control so that the quality of the voice signal is acceptable. QoS is also an issue of concern to the NS/EP community as it is a way for network traffic to receive priority treatment.

The Internet Architecture Board (IAB), a technical advisory group of the Internet Society, held a workshop on Routing, which included QoS. They reported that "QoS routing, as defined in the differentiated services (diff-serv) working group, allocates network resources based on the user ability to pay for it. If the QoS is a small portion of the bandwith, the premium service of the diff-serv working group can deal with it. If it is not a small portion of the traffic, the operators will have a difficult time provisioning the network in a way that makes money" [39]. QoS as defined by the diff-serv working group does not deal with bandwidth guarantees, but instead with latency guarantees. "A user of the premium service marks packets with a special flag. The marked packets undergo traffic shaping prior to entering the network. After entering the network these packets are queued on priority queues" [39].

Another proposed approach to providing integrated services on the Internet is the IP Integrated Services (IS) Model. IS was developed to optimize network and resource utilization for new applications, such as real-time multimedia, which requires QoS guarantees. Because of routing delays and congestion losses, real-time applications do not work very well on the current best-effort Internet. Integrated Services use the Resource Reservation Protocol (RSVP) for the signaling of the reservation messages. The IS instances communicate via RSVP to create and maintain flow-specific states in the endpoint hosts and in routers along the path of a flow [28].

Guérin and Peris [40] survey QoS mechanisms and directions in packet networks. They conclude that a wide range of mechanisms exist for QoS guarantees in packet networks, which offer a broad choice of trade-offs among complexity, performance, and strength of the guarantees being provided. "There are many unanswered questions when it comes to determining the appropriate QoS model for each environment" [40]. A report by the National Research Council [3] agrees that experts disagree on how to provide QoS: "There is significant disagreement among experts as to how effective quality of service mechanisms would be and which would be more efficient, investing in additional bandwidth or deploying QoS mechanisms." The committee also disagreed on whether QoS is, in fact, an important enabling technology. "Nor can it be concluded at this time whether QoS will see significant deployment in the Internet, either over local links, within the networks of individual ISPs, or more widely, including across ISPs."

The NRC committee [3] favored conducting "research aimed at better understanding network performance, the limits to the performance that can be obtained using best-effort service, and the potential benefits that different QoS approaches could provide in particular circumstances is one avenue for obtaining a better indication of the prospects for QoS in the Internet. Another avenue is to accumulate more experience with the effectiveness of QoS in operational settings; here the challenge is that deployment may not occur without demonstrable benefits, while demonstrating those benefits would depend at least in part on testing the effectiveness of QoS under realistic conditions."

6.2 Interoperability of VPNs

Because of the large number of optional features in the IPSec protocol, compliant implementations of IPSec from different vendors may not be compatible. It is recognized that the transition to IPSec will not occur overnight [41]. Since the IPSec standard offers a large set of optional standards, host systems must be prepared to implement flexible policy lists that describe which systems they desire to speak securely with and which systems they require speak securely to them. The IPSec standards contain a lot of options so that products from one vendor may not interoperate with another vendor's products if they do not implement the same options. The mandatory provisions (e.g., DES and shared secrets for IKE) are limited and are not suitable for managing a large network of VPNs. Table 6-1 lists the mandatory provisions to implement algorithms along with the IPSec protocol. Note that the only mandatory encryption algorithm to provide confidentiality is the Data Encryption Standard (DES), which is no longer considered to be strong against a brute force attack. DES has a 56-bit key. An ad-hoc group of cryptographers and computer scientists issued a report in 1996 stating that a 56-bit key for a symmetric cipher was not adequate [42]. They recommended a 90-bit key as a minimum.

Table 6-1. Mandatory Provisions to Implement Algorithms

IPSec Protocol	Mandatory-Provision-to-Implement Algorithm
AH (RFC 2402)	Keyed-Hash Message Authentication Code (HMAC) with MD5
AH (RFC 2402)	HMAC with secure hash algorithm (SHA)-1
ESP (RFC 2406)	DES in CBC mode
ESP (RFC 2406)	HMAC with MD5
ESP (RFC 2406)	HMAC with SHA-1
ESP (RFC 2406)	NULL Authentication algorithm
ESP (RFC 2406)	NULL Encryption algorithm

Among the optional algorithms to implement in the ISAKMP RFC, the only encryption algorithm supported that also appears in the JTA is Triple DES. There is work underway (described in Section 7) to add the Advanced Encryption Standard (AES) to the list of encryption algorithms supported by IPSec. AES is also listed as an emerging standard in JTA 4.0.

6.3 Management of VPNs

Managing a VPN must consider the underlying network infrastructure [24]. VPNs are constructed of many secure tunnels crossing a shared IP infrastructure. VPN management also includes monitoring the VPN gateways, ancillary servers that support the VPN, and all the security aspects related to the VPN tunnels. Because a VPN is a secure network service, security of the management mechanisms themselves must be addressed.

The most common management protocol used on the Internet is the Simple Network Management Protocol (SNMP) [43]. The SNMP architecture is designed to be modular to allow the evolution of the SNMP protocol standards over time. The SNMP protocol allows a network administrator to manage network resources from a remote node. However, versions 1 and 2 of SNMP have weak authentication mechanisms. As a result, this protocol should never be allowed through a firewall connected to the Internet. A hacker would have the ability to remotely manage and change the configuration of network systems. It would also allow a hacker to rewrite the security policy of the internal network [44]. Examples have been published of how SNMP can be used to gain information about devices on a network and how an attacker can change a systems configuration [45].

6.4 Network Address Translation

Request for Comments 2663 describes IP Network Address Translator (NAT) Terminology and Considerations [46]. The need for IP Address translation arises when a network's internal IP addresses cannot be used outside the network either because they are invalid for use outside, or because the internal addressing must be kept private from the external network.

Network Address Translation (NAT) is usually implemented in a machine that resides at the boundary of a company's intranet, at a point where there is a link to the public Internet. In most cases this machine will be a firewall or router. NAT sets up and maintains a mapping between internal IP addresses and external public (globally unique) IP addresses. Because the internal addresses are not advertised outside of the intranet, NAT can be used when they are private (globally ambiguous) addresses, or when they are public (globally unique) addresses that a company wishes to keep secret.

The weakness of NAT in context to VPNs is that by definition the NAT-enabled machine will change some or all of the address information in an IP packet. When end-to-end IPSec authentication is used, a packet whose address has been changed will always fail its integrity check under the AH protocol, since any change to any bit in the datagram will invalidate the integrity check value that was generated by the source.

Within the IETF, there is a working group that is looking at the deployment issues surrounding NAT. This group has been advised by the Internet Engineering Steering Group (IESG) that the IETF will not endorse any deployment of NAT that would lead to weaker security than can be obtained when NAT is not used. Since NAT makes it impossible to authenticate a packet using IPSec's AH protocol, NAT should be considered as a temporary measure at best, but should not be pursued as a long term solution to the addressing problem when dealing with secure VPNs.

IPSec protocols offer some solutions to the addressing issues that were previously handled with NAT. Address hiding can be achieved by IPSec's tunnel mode. If a company uses private addresses within its intranet, IPSec's tunnel mode can keep them from ever appearing in cleartext form in the public Internet, which eliminates the need for NAT. While NAT became widely used because of the growing shortage of IP addresses in IP version 4, the use of NAT is expected to continue after the widespread implementation of IP version 6.

6.5 Intrusion Detection Systems

A VPN can impede the ability of an intrusion detection system (IDS) to detect an intrusion. Specifically, a gap is created because encrypted messages can contain malicious information that cannot be detected by an IDS [47]. Some intrusion correlation can take place even if the packet payloads are encrypted, although no existing IDS provides this capability. Amoroso [48] identifies some specific techniques available to include the following:

- Covert channel identification
- Session traps
- Brute force or heuristic cryptanalysis
- End-point key management surveillance

Figure 6-1 illustrates several locations that IDS sensors for network-based IDS can be placed in a network:

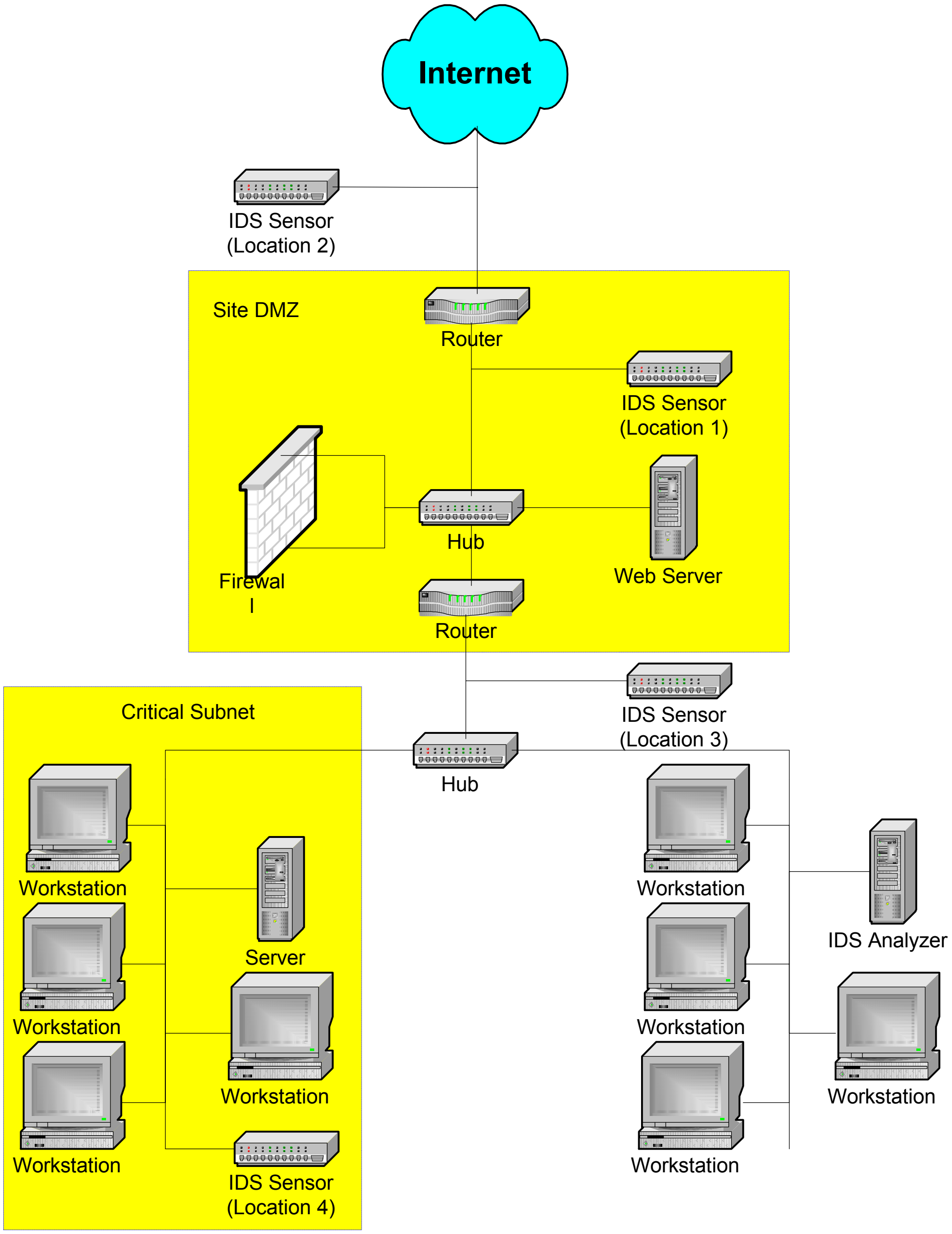

Figure 6-1. Locations for IDS Sensors [49]

In Figure 14, the following sensor locations for a network-based IDS have been identified [49]:

- Location 1: Behind each external firewall, in the network demilitarized zone (DMZ)

- Location 2: Outside an external firewall
- Location 3: On major network backbones
- Location 4: On critical subnets

The impact of VPNs on the placement of IDS sensors can be summarized as follows: for the VPN Site-to-site architecture (described in Section 4.1), only IDS sensors in locations 3 or 4 can scan known signatures. For the VPN Host-to-host architecture (described in Section 4.2), only host-based IDS can scan known signatures. Finally, for the Local Area Network (LAN)-to-LAN VPN architecture (described in Section 4.3), only IDS sensors in location 4 can scan for known signatures.

6.6 IP Version 6

Two previous NCS Technical Information Bulletins (TIB) relating to Internet Protocol Next Generation (IPv6) have been published. They provided an introduction to IPv6[50] and described the IPv6 enhancements and transition issues [51]. This section focuses on what has or has not changed since they were written. IPv6 is defined in Request for Comment (RFC) 2460 [52]. Version 4 of the Internet's basic protocol, IP, was designed to provide only roughly 4.3 billion unique identifiers, a limitation that is becoming increasingly problematic as the number of computers attached to the Internet continues to grow. IPv6 significantly increases the number of addresses available.

The Federal government has made a substantial investment to promote the adoption of IPv6. Examples of efforts to promote the adoption of IPv6 and IPSec include the following [53]:

- The National Science Foundation (NSF) has funded production and distribution of a gigabit asynchronous transfer mode (ATM) switch kit and Internet Protocol version 6 (IPv6) development and source distribution.

- The Department of Energy's (DOE) Energy Sciences network (ESnet) requested and was assigned the first production IPv6 addressing prefix by the American Registry for Internet Numbers (ARIN) and is using it to provide IPv6 services to ESnet users. ESnet, which provides high-speed connectivity to thousands of scientific researchers at more than 30 DOE sites, has established a production IPv6 network initiative called the 6REN to encourage research and education networks worldwide to provide early production native IPv6 service.

- Cerberus, a NIST-designed reference implementation of the latest IPSec specifications, and PlutoPlus, a NIST reference implementation of the IPSec key negotiation and management specifications, are being used by the Internet industry in ongoing research on advanced issues in IPSec technologies.

- NIST's Web-based IPSec interoperability tester, known as IPSec-WIT, enables Internet researchers to conduct interoperability tests anytime and from any location without downloading test software or moving the systems being tested.

- NSA researchers developed and are evaluating Crackerbox, a prototype system software package, to provide packet filtering and basic IP security.

However, a recently published report by the National Research Council [3] describes the current state of implementation of IPv6 as follows: a number of hardware and software products and tools include support for IPv6 and transition strategies to IPv6 have been developed. But the costs of moving to IPv6, reflecting the large number of components needing modification, have dampened enthusiasm for it, and it has seen only limited deployment to date. The low deployment rate, in turn, diminishes the incentives for switching.

A recent article titled "Whatever Happened to the Next-Generation Internet?" [54] observes that "despite apparently compelling arguments for protocol improvement and the increasing availability of IPv6, the world is still nicely served by IPv4. There is no apocalypse looming on the immediate horizon threatening to bring down the Internet." The article concludes with the statement: "deciding whether the Internet should transition to IPv6 or stay with the 1981 standard is largely up to users and system managers. The market will ultimately decide when and if the expected utility of IPv6 (less the high transition cost) exceeds that of the current version."

6.7 Lack of Evaluated Products

It could be stated that a call made using Secure Terminal Units (STU IIIs) is a one-time VPN established for the purposes of that call. However, the definition of a VPN in Newton's Telecomm Dictionary cites a "VPN is a private communication network that uses a private network 'other than the PSTN' as it's WAN Backbone[1]". Further it is not possible to make a STU III call over a VPN as IP does not support the QoS required for secure voice traffic. Additionally, the JTA 4.0 does not list any standards or protocols that support secures voice traffic.

There are currently no VPNs that have been evaluated for compliance with a VPN PP (there are some VPN product evaluations underway). This is in spite of the previously mentioned directive that Federal agencies should purchase evaluated products. Other types of products have been evaluated under the Common Criteria, including operating systems, database management systems, and firewalls.

A vendor panel at a recent IATF Forum meeting [55] was critical of the Common Criteria evaluation process. The vendors represented on the panel included Cisco, Oracle, and Microsoft. Their criticisms included:

- A proliferation of Protection Profiles. There is a tendency for organizations to create their own PP rather than use existing PP. In particular, U.S.-developed PPs diverge from standard CC EALs. Vendors cannot afford to perform multiple evaluations of the same product.

[1] Newton's Telecomm Dictionary, 17th Edition, Feb 2001, pg 759.

- Evaluations take too long. Products can be obsolete by the time an evaluation is completed. While Microsoft recently released Windows XP, the CC evaluation of Windows 2000 has not been completed. The evaluation cycle is about a year.

- Evaluations cost too much. Evaluation laboratories in the U.S. are much more expensive than those elsewhere. Smith [56] reports that estimates for CC evaluations from U.S. labs in 1999 were 100% to 200% higher than estimates from the U.K.

- U.S. Government customers do not buy evaluated products [55]. While the official policy is to buy evaluated products, agencies find ways to evade the directive.

- Commercial customers do not see any benefits in buying evaluated products. While the U.S. Government is a major customer, it has a limited impact on product features wanted by commercial customers. For example, the U.S. Government represents only 5% of Cisco's worldwide business.

The message from several of the vendors on the panel was that they are in business to make a profit. In order to commit the resources to have products evaluated, there need to be sufficient sales of the evaluated products to justify their investment.

An earlier conference paper on "Trends in Government Endorsed Security Product Evaluations" [56] identified 242 product evaluations that were conducted between 1984 and 1999. Only 17% of the evaluations conducted in 1999 were based on the CC, although this should increase in the future. Many of the evaluations occurred in the U.K. The U.K. government has a similar mandate to use evaluated products. The difference is that the mandate is enforced in the U.K.

7. VPN Standards.

There are no specific VPN standards. A VPN is more like a service than a product. So instead of a VPN standard there are protocol standards, such as IPSec, that can be used to create a VPN service. Modules supporting IPSec protocols may be embedded in stand-alone VPN devices or as additions to existing devices, such as firewalls or routers.

An earlier TIB [57] addressed standardization efforts underway by ITU-T. There is an effort underway to develop provider provisioned VPNs (PPVPNs). It has produced a draft Recommendation: Y.I311 - IP VPNs - Generic Architecture and Service Requirements [58]. There is a parallel effort to the ITU-T effort under the IETF. Therefore this report focuses on the standards activity at the IETF.

The primary protocol suite used to create a VPN is Internet protocol security (IPSec). The IPSec standards were developed by the IPSec Working Group of the IETF. The IETF is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The IETF is open to any interested individual [59]. It is the principal body engaged in the development of new Internet standard specifications. The IETF is unusual in that it exists as a collection of meetings and electronic newsgroups, but is not a corporation and has no board of directors, no members, and no dues [60]. The actual technical work of the IETF is done in its working groups, which are organized by topic into several areas (e.g., routing, transport, security, etc.). Much of the work is handled via mailing lists. The IETF holds meetings three times per year [59].

The IETF working groups are organized into areas, and managed by Area Directors, or ADs. The ADs are members of the Internet Engineering Steering Group (IESG). Providing architectural oversight is the Internet Architecture Board, (IAB). The IAB also adjudicates appeals when someone complains that the IESG has failed. The IAB and IESG are chartered by the Internet Society (ISOC) for these purposes. The General Area Director also serves as the chair of the IESG and of the IETF, and is an ex-officio member of the IAB.

Two of the IETF Security Area Working Groups working on VPN-related standards are the IP Security Protocol (*ipsec*[2]) Working Group and the IP Security Remote Access (*ipsra*) Working Group [61]. Sub-IP Area of the IETF also has a working group on Provider Provisioned Virtual Private Networks (*ppvpn*) [62].

The IETF uses a unique standards development process, which is considered by some to be one of the reasons for the success of the Internet. RFC 2026 [34] describes the process used to establish Internet standards. In general, an Internet Standard is a specification that is stable and well-understood; is technically competent, has multiple, independent, and interoperable implementations with substantial operational experience; enjoys significant public support; and

[2] The IETF uses lower case acronyms for working groups and this report follows that convention in order to distinguish between the *ipsec* Working Group and the IPSec protocol standard.

is recognizably useful in some or all parts of the Internet. Figure 7-1 provides a graphical representation of the stages of the Internet standards process described in RFC 2026.

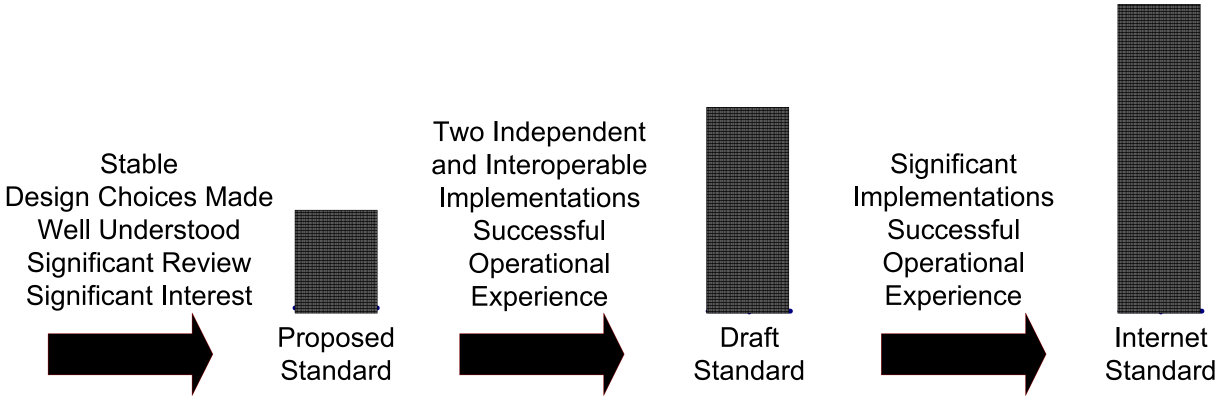
Stable
Design Choices Made
Well Understood
Significant Review
Significant Interest
Proposed Standard
Two Independent and Interoperable Implementations
Successful Operational Experience
Draft Standard
Significant Implementations
Successful Operational Experience
Internet Standard

Figure 7-1. Internet Standards Process [34]

The work of the *ipsec* Working Group is the primary one that has developed the protocols used for VPNs. The *ipsec* working group has completed the planned development of the IPSec standards. However, according to the list of Internet standards [63], all of the IPSec RFCs are still listed as proposed standards. The most recent meeting of the *ipsec* Working Group was at the 6-7 August 2001 IETF meeting. The *ipsec* Working Group agenda included: the progress of the Advanced Encryption Standard (AES) as an RFC, changes in the IKE RFC to support Stream Control Transmission Protocol (SCTP) and NAT/Firewall traversal, Opportunistic IPSec, and IKE Simplification among other topics. The following is a short summary of each of these agenda topics:

- AES is a Federal Information Processing Standard (FIPS) developed by the National Institute for Standards and Technology (NIST) to replace the Data Encryption Standard (DES). The issue of why AES needs to be added to the list of cryptographic protocols supported by IPSec is discussed in Section 6.2.

- The incompatibilities between IPSec and NAT were described in Section 6.4. SCTP is a reliable transport protocol operating on top of a connectionless packet network such as IP. SCTP is designed to transport PSTN signaling messages over IP networks, but is capable of broader applications.

- Opportunistic IPSec is an effort to encourage wider use of IPSec capabilities by leveraging security associations that have been established for other purposes.

- IKE simplification is in its early stages. IKE simplification addresses the VPN interoperability issues described in Section 6.2.

The status of these topics reported in the minutes of the working group meeting are shown in Table 7-1. The addition of the AES to the encryption algorithms supported by IPSec and the

IKE changes to support NAT/Firewall traversal are progressing, and both are needed to support wide-scale use of VPNs by the Federal government.

Table 7-1. Status of Selected Topics Discussed by *ipsec* Working Group [64]

Topic	Status
AES cipher document	There are multiple AES and Cipher Block Chaining (CBC) mode implementations. A draft of AES MAC is planned, and there has been interest in a draft for AES Secure Hash Algorithm (SHA).
Changes to IKE for SCTP compatibility and NAT/ Firewall traversal	Will be taken to the working group e-mail list to allow for comment and then go to working group last call.
Opportunistic IPSec	Support for experimental use of this protocol and to see what the activity and performance characteristics are.
IKE Simplification	It is premature to judge whether to modify or replace IKE. The two proposals discussed at the meeting represent the first steps in this direction.

A second working group of interest is the IP Security Remote Access (*ipsra*) Working Group [65]. The goals of the *ipsra* Working Group are:

- To define a remote access architecture. The entities participating in the remote access and their relationships will be defined in a framework document. This document will be published as an Informational RFC.

- To define a standard mechanism to accomplish human user authentication to an IPSec device running IKE, using legacy authentication mechanisms. One of the goals of introducing this mechanism is to allow for an easy migration path to PKI. The mechanism will be published as a standards-track protocol document.

- To define a standard mechanism to convey user configuration information from the user's own private network to its local IPSec implementation. This mechanism will be published as a standards-track protocol document.

- To provide a standard mechanism to convey user information required for access control from the user's own private network to its local IPSec implementation, while answering the special requirements of remote access users. This mechanism will be published as a standards track protocol document.

The *ipsra* Working Group held its first meeting in March 2000 and is developing several standards track RFCs. At the 7 August 2001 meeting of the *ipsra* Working Group, the primary topic was a Pre-IKE Credential (PIC) Provisioning Protocol [66]. PIC is a bootstrap IPSec authentication via an "Authentication Server" (AS) and legacy user authentication (e.g., RADIUS, described in Section 5.7). The client machine communicates with the AS using a key exchange protocol where only the server is authenticated, and the derived keys are used to protect the legacy user authentication. Once the user is authenticated, the client machine obtains credentials from the AS that can be later used to authenticate the client in a standard IKE exchange with an IPSec-enabled security gateway.

The Sub-IP Area of the IETF also has a working group on Provider Provisioned Virtual Private Networks (*ppvpn*) [62]. The *ppvpn* Working Group is responsible for defining and specifying a limited number of sets of solutions for supporting provider-provisioned virtual private networks (PPVPNs[**]). The work effort will include the development of a framework document, a service requirements document, and several individual technical approach documents that group technologies together to specify specific VPN service offerings. The framework will define the common components and pieces that are needed to build and deploy a PPVPN. The *ppvpn* Working Group will produce a small number of approaches that are based on collections of individual technologies that already exist. Most of the members of the *ppvpn* Working Group appear to work for telecommunications service providers and there is close coordination with an ITU-T draft for PPVPNs. At the August 2001 *ppvpn* Working Group meeting it was reported that there is a good synergy between IETF and ITU-T [67]. The goals of the *ppvpn* Working Group are to submit several documents to the IESG in 2002 to include [62]:

- The framework and the service requirement documents to the IESG for consideration as Informational RFCs.

- The candidate approaches and applicability statements to IESG for publication.

[**] Again, the report is making a distinction between the *ppvpn* Working Group and a PPVPN service.

8. Observations/Conclusions

Current NCS programs do not make use of the Internet as a primary mechanism in support of NS/EP requirements and relies heavily on PSNs. That said the PSN providers are rapidly implementing IP based packet-based data networks for their communications backbones and the NCS is very reliant upon the Internet for day-to-day operations, email, research, etc. The following additional observations and conclusions were found:

- Telecommunications service providers plan to combine circuit and packet-based networks to create their next generation of networks. The Federal Government dependence on the Internet is also expected to grow over the next several years. VPNs may stimulate this trend.

- VPNs have been identified as one of the key technologies needed to defend Government networks. Standards for VPNs are emerging, but have not fully matured, although standards bodies such as the IETF appear to be wrapping up their work on VPN standards.

- Several VPN architectures have been defined. They have been supplemented with additional capabilities to support remote users. Wide-scale use of VPNs is dependent on the deployment of PKI, deployment of AES, and, to a lesser extent, the deployment of IPv6. While some alternative approaches to implementing VPNs have been developed, the IPSec protocols are the preferred choice.

- There are some outstanding issues with VPNs that may be of particular interest to the NS/EP community to include the immaturity of QoS capabilities in IP-based networks, lack of interoperability of VPNs, and a lack of evaluated VPN products. VPNs that have been evaluated using the Common Criteria have yet to reach the market, but several evaluations are underway.

9. Recommendations

VPNs are not currently able to support all of the needs of the NS/EP community, but do hold promise for the future. For example, VPNs cannot support secure voice using STU IIIs. In order to accelerate the wide-scale deployment of VPNs, the NCS should consider the following recommendations:

Recommendation 1: The NCS should sponsor additional research and pilot projects that provide QoS in packet-based networks. A better understanding of how to provide QoS in packet-based networks is needed. While the recommendation of the NRC for additional research in providing QoS in packet-based networks was not specifically directed to the NCS, the NCS should consider the recommendation of the NRC to conduct additional research in QoS in packet-based networks and provide opportunities (such as a pilot deployments of QoS technologies) to gain operational experience with QoS capabilities.

Recommendation 2: The NCS should participate in the efforts within the IETF and ITU-T to develop QoS standards for packet-based networks. The NCS community has an understanding of the QoS requirements for NS/EP and experience with QoS in circuit switched networks. Given the flexible structure of IETF working groups, active participation by the NCS has the potential to effect IETF QoS standards, in particular if NCS has supported research and pilot deployments of QoS capabilities in packet-based networks, as stated in the previous recommendation.

Recommendation 3: The NCS should seek to expedite the deployment of PKI and IPv6. These are prerequisites to the wide-scale deployment of VPNs. Since the pre-shared key authentication method supported by IKE does not scale well in large networks, PKI deployment is needed to permit other IKE authentication methods to be used. Support of IPSec is mandatory in IPv6 and deployment of IPv6 will ensure that all of the devices in an IP packet-based network can support VPNs.

Recommendation 4: Where appropriate, the NCS should require the acquisition of evaluated products. Improvements may be needed in the CC evaluation process to speed product evaluations, but there is no evidence to date that evaluated commercial products are less secure than the unevaluated products on which they are based. The emphasis should be on using existing protection profiles rather than creating PPs specifically for NS/EP applications. While vendors may say that U.S. Government sales of evaluated products are a small portion of their overall sales, the U.K. Government represents a smaller portion of the vendors' sales and their enforcement of a policy to acquire evaluated products has resulted in vendors having their products evaluated. The requirement to purchase evaluated products should consider (as suggested by NIST) the applicable functional and assurance requirements as a product may be neither useful nor cost effective simply because it is evaluated.

Recommendation 5: The NCS should participate in the IPSec and Remote Access working groups in the IETF. In order to support telecommuters and mobile users, there is a need to provide remote access to VPNs. In an NS/EP scenario, remote access is one way to reconnect users with surviving segments of packet-based networks. The IETF working groups are close to finishing their efforts and revisions to the IETF standards to support NS/EP requirements might not occur until a major revision to the IPSec and Remote Access standards are needed.

Recommendation 6: The NCS should investigate methods of ensuring QoS in VPNs such that they can support Secure Voice. To realize secure voice over VPNs, the NCS should support the establishment of standards and protocols that enable QoS required to support secure voice over a VPN. The NCS should be active in research and development of these protocols and standards and submit contributions to the appropriate fora such as ITU-T, IETF, and Committee T1.

Appendix A: Acronyms

AES	Advanced Encryption Standard
AH	Authentication Header
ANSI	American National Standards Institute
API	Application Programming Interface
AS	Authentication Server
CBC	Cipher Block Chaining
CC	Common Criteria
CCITSE	Common Criteria for Information Technology Security Evaluation
CHAP	Challenge Handshake Authentication Protocol
COI	Community of Interest
COTS	Commercial Off-The-Shelf
CRL	Certificate Revocation List
CS	Communications Server
DES	Data Encryption Standard
DoD	Department of Defense
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
ESP	Encapsulating Security Payload
FIPS PUB	Federal Information Processing Standards Publication
GETS	Government Emergency Telecommunications Service
HF	High Frequency
HMAC	Keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
IA	Information Assurance
IAB	Internet Architecture Board
IATF	Information Assurance Technical Framework
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IP	Internet Protocol

Ipsec	Internet Protocol Security
Ipv4	Internet Protocol Version 4
Ipv6	Internet Protocol Version 6
IPX	Internet Packet Exchange Protocol
IS	Integrated Services
ISAKMP	Internet Security Association and Key Management Protocol
ISO	International Organization for Standardization
ISOC	Internet Society
ISP	Internet Service Provider
IT	Information Technology
ITU-T	International Telecommunication Union, Telecommunication Standardization Sector
JTA	Joint Technical Architecture
KMI	Key Management Infrastructure
KMI/PKI	Key Management Infrastructure/Public Key Infrastructure
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC `	Message Authentication Code
MD	Misuse Detection
NAT	Network Address Translation
NCS	National Communications System
NGN	Next Generation Network
NS/EP	National Security and Emergency Preparedness
NSTAC	National Security Telecommunications Advisory Committee
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
NSTISSP	National Security Telecommunications and Information Systems Security Policy
OU	Operational User
PCS	Personal Communications Service
PFS	Perfect Forward Security
PIC	Pre-IKE Credential
PKI	Public Key Infrastructure
PN	Public Network
PP	Protection Profile
PPP	Point-to-Point Protocol
PPVPN	Provider Provisioned VPN
PSN	Public Switched Network
PSTF	Protecting Systems Task Force

QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RFC	Request For Comments
RSA	RSA Security Inc. (Not An Acronym)
RSVP	Resource Reservation Protocol
RU	Remote Unit or Remote User
SAD	Security Association Database
SCTP	Stream Control Transmission Protocol
SHA	Secure Hash Algorithm
SLIP	Serial Line IP
SNMP	Simple Network Management Protocol
SOCKS	Socket-S
SPD	Security Policy Database
SPI	Security Parameter Index
SSL	Secure Sockets Layer
ST	Security Target
STU	Secure Terminal Unit
TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TN	Telephone Network
TOE	Target of Evaluation
TSE	TOE Security Environment
TSF	TOE Security Functions
TSP	Telecommunications Service Priority (NS/EP Usage)
TSP	TOE Security Policy (CC Usage)
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network
WAN	Wide Area Network

Appendix B: Glossary of Terms

Assurance	Grounds for confidence that an entity meets its security objectives [7].
Authentication Header (AH)	An Internet IPSec protocol (RFC 2402) designed to provide connectionless data integrity service and data origin authentication service for IP datagrams, and (optionally) to provide protection against replay attacks [23].
Authorized user (AU)	A user who may, in accordance with the TSP, perform an operation [7].
Certificate Revocation List (CRL)	List of invalid public key certificates that have been revoked by the issuer [16].
Cipher Block Chaining (CBC)	A block cipher mode that enhances electronic codebook mode by chaining together blocks of ciphertext it produces [23].
Community of Interest	A Community of Interest (CoI) is a subset of AUs that either communicate within, or between, Operational User (OU) and Remote User (RU) sites. Communications among and between COI AUs will be protected from both access and modification by non-COI AUs or UAs [8].
Cookie	Data exchanged by ISAKMP to prevent certain denial-of-service attacks during the establishment of a security association [23].
Data Confidentiality Service	A security service that protects data against unauthorized disclosure [23].
Data Integrity Service	A security service that protects against unauthorized changes to data, including both intentional change or destruction and accidental change or loss, by ensuring that changes to data are detectable [23].
Data Origin Authentication Service	A security service that verifies the identity of a system entity that is claimed to be the original source of received data [23].
Diffie-Hellman	A key agreement algorithm published in 1976 by Whitfield Diffie and Martin Hellman [23].
Digital Signature Standard (DSS)	The U.S. Government standard (FIPS PUB 186) that specifies the Digital Signature Algorithm (DSA), which involves asymmetric cryptography [23].
Encapsulating Security Payload (ESP)	An Internet IPsec protocol (RFC 2406) designed to provide a mix of security services - especially data confidentiality service - in the Internet Protocol [23].
Evaluation	Assessment of a PP, an ST, or a TOE against defined criteria [7].
Evaluation Assurance Level (EAL)	A package consisting of assurance components from Part 3 of the CC that represents a point on the CC predefined assurance scale [7].
Hypertext Transfer Protocol (HTTP)	A TCP-based, application-layer, client-server, Internet protocol (RFC 2616) used to carry data requests and responses in the World Wide Web [23].
Identity Token	A Smart card, metal key, or other physical object used to authenticate

	identity [16].
Internet Architecture Board (IAB)	A technical advisory group of the ISOC, chartered by the ISOC Trustees to provide oversight of Internet architecture and protocols and, in the context of Internet Standards, a body to which decisions of the IESG may be appealed. Responsible for approving appointments to the IESG from among nominees submitted by the IETF nominating committee [23].
Internet Engineering Steering Group (ISEG)	The part of the ISOC responsible for technical management of IETF activities and administration of the Internet Standards Process according to procedures approved by the ISOC Trustees. Directly responsible for actions along the "standards track," including final approval of specifications as Internet Standards. Composed of IETF Area Directors and the IETF chairperson, who also chairs the IESG [23].
Internet Engineering Task Force (IETF)	A self-organized group of people who make contributions to the development of Internet technology. The principal body engaged in developing Internet Standards, although not itself a part of the ISOC. Composed of Working Groups, which are arranged into Areas (such as the Security Area), each coordinated by one or more Area Directors. Nominations to the IAB and the IESG are made by a committee selected at random from regular IETF meeting attendees who have volunteered [23].
Internet Protocol (IP)	A Internet Standard protocol (version 4 (RFC 0791) and version 6 (RFC 2460)) that moves datagrams (discrete sets of bits) from one computer to another across an internetwork but does not provide reliable delivery, flow control, sequencing, or other end-to-end services that TCP provides [23].
Internet Protocol Security (IPSec)	IPSec is a framework for a number of security specifications pertaining to VPNs. IPSec's three core components are: 1. The authentication header (AH), which verifies the authenticity of the packet's contents; 2. The encapsulating security payload (ESP), which encrypts a packet before transmitting it. ESP may also encapsulate the original IP packet; and, 3. The Internet Key Exchange (IKE), which governs the exchange of security keys between senders and receivers [8].
Internet Security Association and Key Management Protocol (ISAKMP)	An Internet IPSec protocol (RFC 2408) to negotiate, establish, modify, and delete security associations, and to exchange key generation and authentication data, independent of the details of any specific key generation technique, key establishment protocol, encryption algorithm, or authentication mechanism [23].
Internet Society (ISOC)	A professional society concerned with Internet development (including technical Internet Standards); with how the Internet is and can be used; and with social, political, and technical issues that result. The ISOC Board of Trustees approves appointments to the IAB from among nominees submitted by the IETF nominating committee [23].
IPSec Key Exchange (IKE)	An IPSec key-establishment protocol (RFC 2409) that is intended for putting in place authenticated keying material for use with ISAKMP and for other security associations, such as in AH and ESP [23].

International Telecommunications Union, Telecommunication Standardization Sector (ITU-T)	A United Nations treaty organization that is composed mainly of postal, telephone, and telegraph authorities of the member countries and that publishes standards called "Recommendations" [23].
Layer 2 Forwarding Protocol (L2F)	An Internet protocol (originally developed by Cisco Corporation) that uses tunneling of PPP over IP to create a virtual extension of a dial-up link across a network, initiated by the dial-up server and transparent to the dial-up user [23].
Layer 2 Tunneling Protocol (L2TP)	An Internet client-server protocol that combines aspects of PPTP and L2F and supports tunneling of PPP over an IP network or over frame relay or other switched network [23].
MD5	A cryptographic hash (RFC 1321) that produces a 128-bit hash result and was designed by Ron Rivest to be an improved version of MD4 [23].
Nonce	A random or non-repeating value that is included in data exchanged by a protocol, usually for the purpose of guaranteeing liveness and thus detecting and protecting against replay attacks [23].
Non-repudiation Service	A security service that provide protection against false denial of involvement in a communication [23].
NULL Encryption Algorithm	An algorithm (RFC 2410) that does nothing to transform plaintext data; i.e., a no-op. It originated because of IPSec ESP, which always specifies the use of an encryption algorithm to provide confidentiality. The NULL encryption algorithm is a convenient way to represent the option of not applying encryption in ESP [23].
Operational User (OU)	An employee who functions within an organization's spaces. Typically the OU's job is directly related to the mission and functions of that site. OU's are subject to the supervision (either directly or indirectly) of a senior official at the site [8].
Organizational Security Policies	One or more security rules, procedures, practices, or guidelines imposed by an organization upon its operations [7].
Password Authentication Protocol (PAP)	A simple authentication mechanism in PPP. In PAP, a user identifier and password are transmitted in cleartext [23].
Point-to-Point Protocol (PPP)	An Internet Standard protocol (RFC 1661) for encapsulation and full-duplex transportation of network layer (mainly OSI layer 3) protocol data packets over a link between two peers, and for multiplexing different network layer protocols over the same link. Includes optional negotiation to select and use a peer entity authentication protocol to authenticate the peers to each other before they exchange network layer data [23].
Point-to-Point Tunneling Protocol (PPTP)	An Internet client-server protocol (originally developed by Ascend and Microsoft) that enables a dial-up user to create a virtual extension of the dial-up link across a network by tunneling PPP over IP [23].
Protection Profile (PP)	An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs [7].
Public-Key	A digital certificate that binds a system entity's identity to a public key

Certificate	value, and possibly to additional data items; a digitally-signed data structure that attests to the ownership of a public key [23].
Public-key Forward Secrecy (PFS)	Also called perfect forward secrecy. For a key agreement protocol based on asymmetric cryptography, the property that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the private keys is compromised in the future [23].
Public-Key Infrastructure (PKI)	A system of CAs (and, optionally, RAs and other supporting servers and agents) that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography [23].
Registration Authority (RA)	An optional PKI entity (separate from the CAs) that does not sign either digital certificates or CRLs but has responsibility for recording or verifying some or all of the information (particularly the identities of subjects) needed by a CA to issue certificates and CRLs and to perform other certificate management functions [23].
Remote Authentication Dial-In User Service (RADIUS)	An Internet protocol (RFC 2138) for carrying dial-in users' authentication information and configuration information between a shared, centralized authentication server (the RADIUS server) and a network access server (the RADIUS client) that needs to authenticate the users of its network access ports [23].
Remote User (RU)	An Authorized User (AU) of the RU site [8].
Replay Attack	An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by an adversary who intercepts the data and retransmits it, possibly as part of a masquerade attack [23].
Rivest-Shamir-Adleman (RSA)	An algorithm for asymmetric cryptography, invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman [23].
Secure Hash Standard (SHS)	The U.S. Government standard (FIPS PUB 180) that specifies the Secure Hash Algorithm (SHA-1), a cryptographic hash function that produces a 160-bit output (hash result) for input data of any length < 2**64 bits [23].
Secure Sockets Layer (SSL)	An Internet protocol (originally developed by Netscape Communications, Inc.) that uses connection-oriented end-to-end encryption to provide data confidentiality service and data integrity service for traffic between a client (often a web browser) and a server, and that can optionally provide peer entity authentication between the client and the server [23].
Security Association (SA)	A relationship established between two or more entities to enable them to protect data they exchange. The relationship is used to negotiate characteristics of protection mechanisms, but does not include the mechanisms themselves [23].
Security Function (SF)	A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP [7].
Security Function Policy (SFP)	The security policy enforced by an SF [7].
Security Objective	A statement of intent to counter identified threats and/or satisfy identified organization security policies and assumptions [7].

Security Parameters Index (SPI)	The type of security association identifier used in IPSec protocols. A 32-bit value used to distinguish among different security associations terminating at the same destination (IP address) and using the same IPSec security protocol (AH or ESP). Carried in AH and ESP to enable the receiving system to determine under which security association to process a received packet [23].
Security Target (ST)	A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE [7].
Simple Network Management Protocol (SNMP)	A UDP-based, application-layer, Internet Standard protocol (RFC 2570, RFC 2574) for conveying management information between managers and agents [23].
SOCKS	An Internet protocol (RFC 1928) that provides a generalized proxy server that enables client-server applications - such as TELNET, FTP, and HTTP; running over either TCP or UDP - to use the services of a firewall [23].
Target of Evaluation (TOE)	An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation [7].
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP [7].
TOE Security Policy (TSP)	A set of rules that regulate how assets are managed, protected and distributed within a TOE [7].
Transport Layer Security (TLS)	TLS Version 1.0 is an Internet protocol (RFC 2246) based-on and very similar to SSL Version 3.0 [23].
Transport Mode	Protection applies to (i.e., the IPSec protocol encapsulates) the packets of upper-layer protocols, the ones that are carried above IP [23].
Tunnel Mode	Protection applies to (i.e., the IPSec protocol encapsulates) IP packets [23].
Unauthorized Agent (UA)	Any person (or process acting on behalf of a person) that is not authorized, under the TOE site security policy, to access the TOE resources or information processed by the TOE. This person includes anyone from a “hacker” to a determined foreign adversary, and Security Administrators, System Administrators or Authorized Users who are untrustworthy, do not possess COI privileges or lack the need to know [8].
User Datagram Protocol (UDP)	An Internet Standard protocol (RFC 0768) that provides a datagram mode of packet-switched computer communication in an internetwork [23].
Virtual Private Network	A network that is secured by using cryptographic techniques to provide communication between users across networks with unknown security. It is called “virtual private” because the organization utilizing this technology achieves private network security on a public backbone [8].
Zeroize	Use erasure or other means to render stored data unusable and unrecoverable, particularly a key stored in a cryptographic module or other device [23].

Appendix C: References

[1] President of the U.S., "Executive Order 12472: Assignment of National Security and Emergency Preparedness Telecommunications Functions,". Washington, DC: U.S. Government, 1984.

[2] "Information Technology Progress Impact Task Force Report on Convergence," President's National Security Telecommunications Advisory Committee, Washington, DC May 2000.

[3] National Research Council Committee on the Internet in the Evolving Information Infrastructure Computer Science and Telecommunications Board Commission on Physical Sciences Mathematics and Applications, *The Internet's Coming of Age*. Washington, DC: National Academy Press, 2000.

[4] Network Group, "Internet Report: An Examination of the NS/EP Implications of Internet Technologies," President's National Security Telecommunications Advisory Committee, Washington, DC June 1999.

[5] "Joint Technical Architecture," U.S. Department of Defense, Washington, DC Version 4.0, April 2 2001.

[6] "Use of the DoD Joint Technical Architecture in the Acquisition Process," Office of the Inspector General, U.S. Department of Defense, Washington, DC, Audit Report D-2001-121, May 14 2001.

[7] "Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model,"., 2000.

[8] National Security Agency, "A Goal VPN Protection Profile for Protecting Sensitive Information," A Goal VPN Protection Profile for Protecting Sensitive Information, http://www.ietf.org/, 2000.

[9] B. Green, J. Gurzick, S. Hutchens, J. Meehan, A. Streeter, and M. Alexander, "U.S. DoD Remote Access Protection Profile for SBU-High Environments," Booz·Allen & Hamilton Inc., Linthicum, MD, Protection Profile May 27 2000.

[10] E. Williams, J. Kubik, and A. Forbes, "Cryptographic Communication System (CCS) Protection Profile," Booz·Allen and Hamilton, Linthicum, MD November 21 2000.

[11] G. R. Black, J. M. Boone, J. Myers, and E. A. Schneider, "U.S. DoD Remote Access Protection Profile for High Assurance Environments," National Security Agency,, Ft. Meade, MD May 2000.

[12] "National Information Assurance Acquisition Policy," National Security Telecommunications and Information Systems Security Committee, Ft. Meade, MD NSTISSP No. 11, January 2000.

[13] E. A. Roback, "Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products," National Institute of Standards and Technology, Gaithersburg, MD, Special Publication 800-23, August 2000.

[14] National Security Agency, "Information Assurance Technical Framework," National Security Agency, Ft. Meade, MD September 2000.

[15] "Protecting Systems Task Force Report on Enhancing the Nation's Network Security Efforts," National Security Telecommunications Advisory Committee, Washington, DC May 2000.

[16] "National Information Systems Security (INFOSEC) Glossary," National Security Telecommunications and Information Systems Security Committee, Washington, DC NSTISSI No. 4009, September 2000.

[17] M. Murhammer, T. Bourne, T. Gaidosch, C. Kunzinger, L. Rademacher, and A. Weinfurter, "A Comprehensive Guide to Virtual Private Networks, Volume I: IBM Firewall, Server and Client Solutions," IBM, Research Triangle Park, Redbook SG24-5201-00, 1998.

[18] S. Kent and R. Atkinson, "IP Authentication Header," Request for Comments: 2402, The Internet Society, http://www.ietf.org/, 1998.

[19] S. Kent and R. Atkinson, "IP Encapsulating Security Payload (ESP)," Request for Comments: 2406, The Internet Society, http://www.ietf.org/, 1998.

[20] D. Maughan, M. Schneider, M. Schertler, and J. Turner, "Internet Security Association and Key Management Protocol (ISAKMP)," Request for Comments: 2408, The Internet Society, http://www.ietf.org/, 1998.

[21] D. Harkins and D. Carrel, "The Internet Key Exchange (IKE)," Request for Comments: 2409, The Internet Society, http://www.ietf.org/, 1998.

[22] M. W. Murhammer, H. J. Lee, A. Schmid, O. Atakan, Z. Badri, and B. J. Cho, "A Comprehensive Guide to Virtual Private Networks, Volume II: IBM Nways Router Solutions," IBM, Research Triangle Park, Redbook SG24-5234-01, 1999.

[23] R. Shirey, "Internet Security Glossary," RFC 2828, The Internet Society, http://www.ietf.org/, 2000.

[24] R. Yuan and W. T. Strayer, *Virtual Private Networks: Technologies and Solutions*. Upper Saddle River, NJ: Addison-Wesley, 2001.

[25] H. Johner, S. Fujiwara, A. S. Yeung, A. Stephanou, and J. Whitmore, "Deploying a Public Key Infrastructure," IBM Corporation, Austin, TX, Redbook SG24-5512-00, February 2000.

[26] "Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology," U.S. General Accounting Office, Washington, DC, Audit Report GAO-01-277, February 2001.

[27] D. Wagner and B. Schneier, "Analysis of the SSL 3.0 Protocol," Analysis of the SSL 3.0 Protocol, Counterpane Systems, Inc., http://www.counterpane.com/, April 15 1997.

[28] A. Rodriguez, J. Gatrell, J. Karas, and R. Peschke, "TCP/IP Tutorial and Technical Overview," IBM, Research Triangle Park, NC, Redbook GG24-3376-06, August 2001.

[29] M. W. Murhammer, O. Atakan, Z. Badri, B. Cho, H. J. Lee, and A. Schmid, "A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management," IBM, Research Triangle Park, Redbook SG24-5309-00, 1999.

[30] T. Dierks and C. Allen, "The TLS Protocol Version 1.0," Request for Comments 2246, The Internet Society, www.ietf.org, January 1999.

[31] C. Rigney, A. Rubens, W. Simpson, and S. Willens, "Remote Authentication Dial In User Service (RADIUS)," Request for Comments: 2138, The Internet Society, http://www.ietf.org/, April 1997.

[32] K. Hamzeh, G. S. Pall, W. Verthein, J. Taarud, W. A. Little, and G. Zorn, "Point-to-Point Tunneling Protocol (PPTP)," Request for Comments: 2637, The Internet Society, http://www.ietf.org/, 1999.

[33] A. Valencia, M. Littlewood, and T. Kolar, "Cisco Layer Two Forwarding (Protocol) "L2F"," Request for Comments: 2341, Internet Society, http://www.ietf.org/, 1998.

[34] S. Bradner, "The Internet Standards Process," The Internet Standards Process, The Internet Society, http://www.ietf.org/, 1996.

[35] W. M. Townsley, G. S. Pall, B. Palter, A. Rubens, A. J. Valencia, and G. Zorn, "Layer Two Tunneling Protocol "L2TP"," Request for Comments: 2661, The Internet Society, http://www.ietf.org/, 1999.

[36] J. E. Smallwood, "An Introduction to ATM," *Computing and Control Engineering Journal*, pp. 233-245, 1998.

[37] "About ATM Technology," About ATM Technology, The ATM Forum, http://www.atmforum.com/, September 2001.

[38] H. J. R. Dutton, "Asynchronous Transfer Mode (ATM) Technical Overview," IBM International Technical Support Organization, Raleigh, NC SG24-4625-00, 1995.

[39] S. Deering, S. Hares, C. E. Perkins, and R. Perlman, "Full Report on the 1998 IAB Routing Workshop," Full Report on the 1998 IAB Routing Workshop, Internet Engineering Task Force, http://www.ietf.org/, January 15 1998.

[40] R. Guérin and V. Peris, "Quality-of-Service in Packet Networks: Basic Mechanisms and Directions," *Computer Networks*, vol. 31, pp. 169-189, 1999.

[41] D. Piper, "The Internet IP Security Domain of Interpretation for ISAKMP," Request for Comments: 2407, The Internet Society, http://www.ietf.org/, 1998.

[42] M. Blaze, W. Diffie, R. L. Rivest, B. Schneier, T. Shimomura, E. Thompson, and M. Wiener, "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security,", January 1996.

[43] D. Harrington, R. Presuhn, and B. Wijnen, "An Architecture for Describing SNMP Management Frameworks," Request for Comments: 2571, The Internet Society, http://www.ietf.org/, May 1999.

[44] "An Introduction to the Internet and Internet Security," Communications Security Establishment, Ottawa, Canada NITSM 2/95, September 1995.

[45] J. Romanski, "Using SNMP for Reconnaissance," Using SNMP for Reconnaissance, SANS Institute, http://www.sans.org/, August 12 2000.

[46] P. Srisuresh and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations," Request for Comments: 2663, The Internet Society, http://www.ietf.org/, August 1999.

[47] J. Allen, A. Christie, W. Fithen, J. McHugh, J. Pickel, and E. Stoner, "State of the Practice of Intrusion Detection Technologies," Software Engineering Institute, Pittsburgh, PA CMU/SEI-99-TR-028, January 2000.

[48] E. G. Amoroso, *Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Traps, Trace Back, and Response*. Sparta, NJ: Intrusion.Net Books, 1999.

[49] R. Bace and P. Mell, "NIST Special Publication on Intrusion Detection Systems (Draft)," National Institute of Standards and Technology, Gaithersburg, MD February 12 2001.

[50] Communication Technologies Inc., "Internet Protocol Next Generation (IPv6)," Office of the Manager, National Communications System, Arlington, VA, Technical Information Bulletin 97-1, January 1997.

[51] Communication Technologies Inc., "Internet Protocol Next Generation (IPv6) Enhancements and Transition Issues," Office of the Manager, National Communications System, Arlington, VA, Technical Information Bulletin 97-2, June 1997.

[52] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," Request for Comments: 2460, The Internet Society, http://www.ietf.org/, 1998.

[53] "Information Technology: The 21st Century Revolution," Interagency Working Group on IT R&D National Science and Technology Council, Washington, DC October 11 2000.

[54] M. Weiser, "Whatever Happened to the Next-Generation Internet?," *Communications of the ACM*, vol. 44, pp. 61-68, 2001.

[55] "Vendor Perspective on NSTISSC Policy Number 11, Protection Profiles, and CC Evaluations in Secure System Development," presented at IATF Forum, Laurel, MD, 2001.

[56] R. E. Smith, "Trends in Government Endorsed Security Product Evaluations," presented at National Information Systems Security Conference, Baltimore, MD, 2000.

[57] ARTEL Inc., "ITU-T GII Standardization Initiative," Office of the Manager, National Communications System, Arlington, VA, Technical Information Bulletin 99-5, June 1999.

[58] "IP VPNs - Generic Architecture and Service Requirements," IP VPNs - Generic Architecture and Service Requirements, ITU - Telecommunication Standardization Sector, Study Group 13, http://nbvpn.francetelecom.com/, 2001.

[59] "Overview of the IETF," Overview of the IETF, The Internet Society, http://www.ietf.org/, 2001.

[60] S. Harris, "The Tao of IETF - A Novice's Guide to the Internet Engineering Task Force," Request for Comments: 3160, The Internet Society, http://www.ietf.org/, 2001.

[61] "Active IETF Working Groups," Active IETF Working Groups, The Internet Society, http://www.ietf.org/, 2001.

[62] "Provider Provisioned Virtual Private Network (ppvpn) Working Group," Provider Provisioned Virtual Private Network (ppvpn) Working Group, The Internet Society, http://www.ietf.org/, 2001.

[63] "Official Internet Protocol Standards," STD 1, The Internet Society, http://www.rfc-editor.org/, 2001.

[64] B. Fraser, J. Linn, and G. Huang, "IPsec Working Group Meeting Minutes," IPsec Working Group Meeting Minutes, The Internet Society, http://www.ietf.org/, 2001.

[65] "IP Security Remote Access (ipsra) Working Group," IP Security Remote Access (ipsra) Working Group, The Internet Society, http://www.ietf.org/, 2001.

[66] P. Hoffman, "IPSRA Meeting minutes," IPSRA Meeting minutes, The Internet Society, http://www.ietf.org/, 2001.

[67] "PPVPN Working Group Minutes from 51st IETF Meeting," PPVPN Working Group Minutes from 51st IETF Meeting, The Internet Society, http://www.ietf.org/, 2001.