FAA-STD-045A
March 11, 2005

U.S. Department of Transportation
Federal Aviation Administration

Standard Practice

NATIONAL AIRSPACE SYSTEM (NAS) COMMUNICATIONS SECURITY PROTOCOLS AND MECHANISMS

A. Approved for public release; distribution is unlimited

FOREWORD

This standard establishes the security architecture, protocols, and mechanisms for use in the National Airspace System (NAS) data communication architecture to provide secure communications between NAS systems. The security architecture described in this standard is based on the Open System data communication architecture that is described in FAA-STD-039c.

The NAS will consist of various processors and communication network sub-systems from assorted vendors. A well-defined security architecture and standardized security mechanisms are required to ensure that NAS operational systems are protected in accordance with FAA Telecommunication and Automated Information Security Policy Orders.

This document was prepared in accordance with FAA-STD-005e.

TABLE OF CONTENTS

TABLE OF FIGURES

1 SCOPE

FAA-STD-045a covers approved protocols and mechanisms for ensuring secure data communication within the NAS. This standard discusses security for the NAS systems founded upon the OSI architecture reference model and Internet Protocol Suite.

Networks based upon X.25 and Aeronautical Telecommunication Network (ATN) are covered by the previous version of this standard, FAA-STD-045.

Naming and Addressing information is not covered in this document. Refer to the applicable Interface Requirements Documents (IRDs) and Interface Control Documents (ICDs) for requirements for naming and addressing.

Interoperability and conformance testing is not applicable to this document.

1.1 PURPOSE

This standard documents a set of security requirements based on NAS-SR-1000 and FAA security policy for NAS data communication systems. It makes use of best industry practices for ensuring security in order to protect NAS data communication networks and systems from malicious tampering. By using such accepted practices, this standard ensures interoperability of current and future NAS systems that implement Commercial Off The Shelf (COTS) products. Also, this standard will help the acquisition and implementation of future systems by providing a finite set of security mechanisms that are approved for all data communication systems within the NAS.

This standard is based on the NAS open system layered architecture in the FAA-STD-039c.

2 APPLICABLE DOCUMENTS

The following documents form a part of this standard to the extent specified herein. In the event of conflict between the documents referenced herein and the content of this standard, the content of this standard shall be considered the superseding document.

2.1 GOVERNMENT DOCUMENTS

FAA-STD-005e	Preparation of Specifications, Standards and handbooks, 1996
FAA-STD-039c	National Airspace System (NAS) Open System Architecture and Protocols, April 2003
FAA-STD-045	National Airspace System (NAS) Communication Security Protocols and Mechanisms, May 2004
FAA Order 1370.82	Information Systems Security Program, June 2000
FAA Order 1600.66	FAA Telecommunications and Information Systems Security Policy, July 1994
NAS SR-1000	NAS System Requirements Specification
NIST FIPS 46-3	Data Encryption Standard, October 1999
NIST FIPS 140-2	Security Requirements for Cryptographic Modules, June 2001
NIST FIPS 180-2	Secure Hash Standard (SHS), August 2002
NIST FIPS 197	Advanced Encryption Standard, November 2001
NIST FIPS 198	The Keyed-Hash Message Authentication Code (HMAC), March 2002
NIST Special Publication 800-41	Guidelines on Firewalls and Firewall Policy, January 2002
NIST Special Publication 800-49	Federal S/MIME V3 Client Profile, November 2002

2.2 NON-GOVERNMENT DOCUMENTS

RFC-1510	The Kerberos Network Authentication Service (V5), September 1993
RFC-1928	SOCKS Protocol Version 5, March 1996
RFC-1929	Username/Password Authentication for SOCKS V5, March 1996

RFC-1961	GSS-API Authentication Method for SOCKS Version 5, June 1996
RFC-2246	The TLS Protocol Version 1.0, January 1999
RFC-2401	Security Architecture for the Internet Protocol, November 1998
RFC-2402	IP Authentication Header, November 1998
RFC-2403	The Use of HMAC-MD5-96 within ESP and AH, November 1998
RFC-2404	The Use of HMAC-SHA-1-96 within ESP and AH, November 1998
RFC-2405	The ESP DES-CBC Cipher Algorithm With Explicit IV, November 1998
RFC-2406	IP Encapsulating Security Payload (ESP), November 1998
RFC-2407	The Internet IP Security Domain of Interpretation for ISAKMP, November 1998
RFC-2408	Internet Security Association and Key Management Protocol (ISAKMP), November 1998
RFC-2409	The Internet Key Exchange (IKE), November 1998
RFC-2412	The OAKLEY Key Determination Protocol, November 1998
RFC-2440	OpenPGP Message Format, November 1998
RFC-2451	The ESP CBC-Mode Cipher Algorithms, November 1998
RFC-2510	Internet X.509 Public Key Infrastructure Certificate Management Protocols, March 1999
RFC-2631	Diffie-Hellman Key Agreement Method, June1999
RFC-2632	S/MIME Version 3 Certificate Handling, June 1999
RFC-2633	S/MIME Version 3 Message Specification, June 1999
RFC-2634	Enhanced Security Services for S/MIME, June 1999
RFC-2661	Layer Two Tunneling Protocol “L2TP,” August 1999

RFC-2817	Upgrading to TLS Within HTTP/1.1, May 2000
RFC-3031	Multi Protocol Label Switching Architecture, January 2001
RFC-3168	The Addition of Explicit Congestion Notification (ECN) to IP, September 2001
RFC-3268	Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS), June 2002
RFC-3369	Cryptographic Message Syntax (CMS), August 2002
RFC-3370	Cryptographic Message Syntax (CMS) Algorithms, August 2002
RFC-3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), December 2002
RFC-3437	Layer-Two Tunneling Protocol Extensions for PPP Link Control Protocol Negotiation, December 2002
RFC-3546	Transport Layer Security (TLS) Extensions, June 2003

2.3 OTHER PUBLICATIONS

Internet Draft	draft-ietf-secsh-transport-17.txt, SSH Transport Layer Protocol, October 2003
Internet Draft	draft-freier-ssl-version3-02.txt, The SSL Protocol, Version 3.0 November 18, 1996

ICAO Doc. 9705-AN/956, 3rd Edition 2002, Manual of Technical Provisions for Aeronautical Telecommunication Network (ATN): Subvolume VIII

White Paper	Securely Transitioning Mixed IPv4/IPv6 Networks Configured for IPSec, prepared by ACB-250 for ASD-130, October 2003

2.4 DOCUMENT SOURCES

Contact the following organizations to get copies of applicable documents or standards.

FAA specifications, standards, and publications
Contracting Officer, Federal Aviation Administration
800 Independence Avenue, S.W.
Washington, DC 20591

Request should clearly identify the desired material by number and date; state the intended use for the material.

Federal or military documents
Standardization Document Order Desk
700 Robbins Avenue, Building 4D
Philadelphia, PA 19111-5094

Non Government Documents
Copies of the Requests for Comments (RFC) can be obtained from the Internet Engineering Task Force Web site at www.ietf.org.

Other Publications
Copies of the Internet Drafts can be obtained from the Internet Engineering Task Force Web site at www.ietf.org.

3 DEFINITIONS AND ACRONYMS

3.1 ACRONYMS

3DES	Triple Data Encryption Standard
AH	Authentication Header
ATM	Asynchronous Transfer Mode
ATN	Aeronautical Telecommunication Network
CA	Certification Authority
DES	Data Encryption Standard
ESP	Encapsulating Security Payload
FAA	Federal Aviation Administration
FDDI	Fiber Distributed Data Interface
FR	Frame Relay
FTI	FAA Telecommunication Infrastructure
ICD	Interface Control Document
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPS	Internet Protocol Suite
IPSec	Internet Protocol Security
IRD	Interface Requirements Document
ISAKMP	Internet Security Association and Key Management Protocol
L2TP	Layer 2 Tunneling Protocol

MD5	Message Digest 5
MPLS	Multi-Protocol Label Switching
NAS	National Airspace System
OpenPGP	Open Pretty Good Privacy
PKI	Public Key Infrastructure
PPP	Point to Point Protocol
RFC	Request for Comments
S/MIME	Secure/Multipurpose Internet Mail Extensions
SA	Security Association
SHA-1	Secure Hash Algorithm 1
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VPN	Virtual Private Network

3.2 DEFINITIONS

Bastion Host

Strongly protected computer in a network protected by a firewall (or is part of a firewall) and is the only host (or one of only a few hosts) in the network that can be directly accessed from networks on the unprotected side of the firewall.

Certification Authority (CA)

Entity that issues digital certificates (especially X.509 certificates) and vouches for the binding between the data items in a certificate.

Internet Protocol Security (IPSec)

Security architecture and an associated protocol set specified by the IETF to provide security services for Internet Protocol traffic.

Proxy Server

Computer process — often used as, or as part of, a firewall — that relays a protocol between client and server computer systems, by appearing to the client to be the server and appearing to the server to be the client

Public Key Infrastructure (PKI)

System of CAs (and, optionally, other supporting servers and agents) that performs a set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography.

Secure Sockets Layer (SSL)

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

Security Association

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.

Tunneling

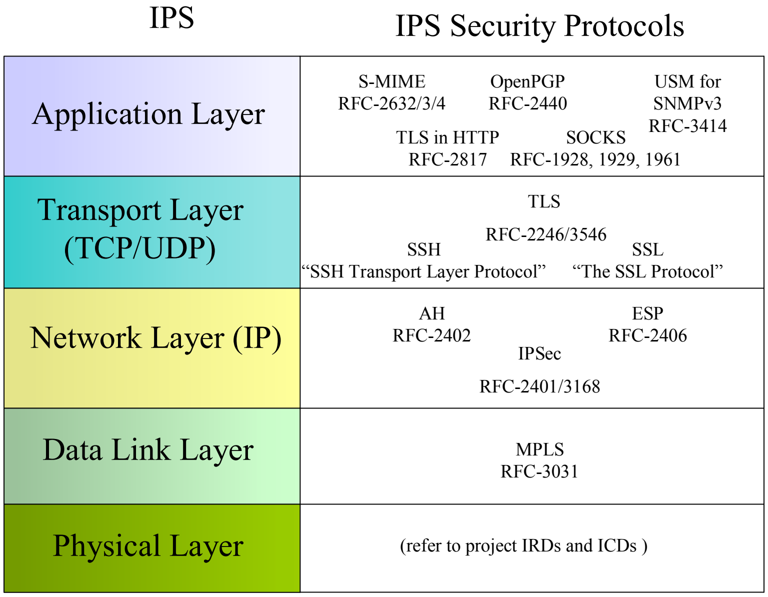
Communication channel created in a computer network by encapsulating (carrying, layering) a communication protocol's data packets in (on top of) a second protocol that normally would be carried above, or at the same layer as, the first one.

Virtual Private Network (VPN)

Restricted-use, logical (i.e., artificial or simulated) computer network constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network.

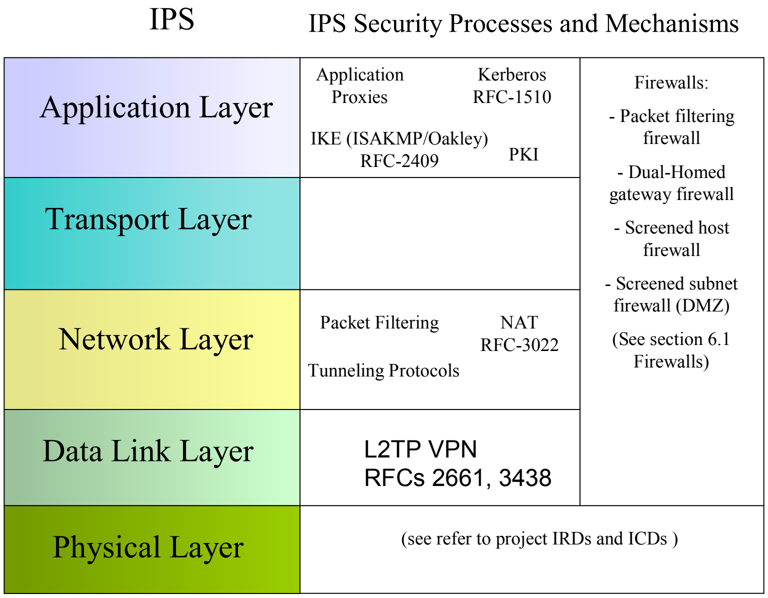
4 REQUIREMENTS

This section specifies general requirements for implementing security communications protocols within NAS networks and end-systems. This standard's protocols and practices are based upon the 5-layer Internet Protocol Suite (IPS) architecture, as described in FAA-STD-039c as a 5-layer model, which includes Application, Transport, Network, Link, and Physical Layers. This document allocates security protocols and services across the layers of that model. The IPS security protocols are depicted in Figure 1, while security options are shown in Figure 2.



IPS	IPS Security Protocols
Application Layer	S-MIME RFC-2632/3/4 OpenPGP RFC-2440 USM for SNMPv3 RFC-3414 TLS in HTTP RFC-2817 SOCKS RFC-1928, 1929, 1961
Transport Layer (TCP/UDP)	TLS RFC-2246/3546 SSH "SSH Transport Layer Protocol" SSL "The SSL Protocol"
Network Layer (IP)	AH RFC-2402 ESP RFC-2406 IPSec RFC-2401/3168
Data Link Layer	MPLS RFC-3031
Physical Layer	(refer to project IRDs and ICDs)

Figure 1 Security protocols within IPS



IPS	IPS Security Processes and Mechanisms	
Application Layer	Application Proxies Kerberos RFC-1510 IKE (ISAKMP/Oakley) RFC-2409 PKI	Firewalls: - Packet filtering firewall - Dual-Homed gateway firewall - Screened host firewall - Screened subnet firewall (DMZ) (See section 6.1 Firewalls)
Transport Layer		
Network Layer	Packet Filtering NAT RFC-3022 Tunneling Protocols	
Data Link Layer	L2TP VPN RFCs 2661, 3438	
Physical Layer	(see refer to project IRDs and ICDs)	

Figure 2 IPS Security Options

Since most current data communication, and almost all future NAS data communication, are based on IPv4 or IPv6, this standard uses RFC-2401: “Security Architecture for the Internet Protocol” as a basis for the network security standard described in this document.

All security systems implemented within NAS must comply with FAA Order 1370.82 and FAA Order 1600.66.

4.1 APPLICATION LAYER SECURITY

Application layer security is enabled with the use of bastion hosts, ISAKMP algorithms, S/MIME, Kerberos, HTTPS (i.e., HTTP over SSL), SOCKS, OpenPGP, USM for SNMPv3 and Public Key Infrastructure (PKI).

The bastion host is a highly secure server that accepts all incoming traffic from the firewall. It relays and forwards protocols and services to network resources in its domain, as authorized by the implemented security policy. As part of a firewall system, bastion hosts may host proxy servers for various upper-layer protocols (e.g., HTTPS) within filtering routers.

Public Key Infrastructure (PKI) provides a trusted and efficient way of issuing, revoking and managing public key certificates. PKI provides authentication, non-repudiation, and confidentiality to data transmitted over untrusted networks. Without the efficient, automated, reliable PKI, the transport and network layer protocols, such as IPSec and

TLS, would need to implement manual key exchange policy, which would be impractical for large networks.

ISAKMP/Oakley supports automated negotiation of Security Associations (SA), automated generation of cryptographic keys, and automatic refresh of cryptographic keys. Without the automation process of generating cryptographic keys IPSec would not be feasible.

The S-MIME protocol ensures a secure method to send and receive email over untrusted networks, such as the Internet. S-MIME uses of the cryptographic services, such as cryptographic key exchange, message encryption and decryption, source authentication, non-repudiation, along with the MIME mail standard to ensure security of mail transfer.

The OpenPGP protocol digitally signs and encrypts messages into objects. These objects are then securely transmitted over the untrusted media. The OpenPGP protocol is well suited for the store and forward applications, such as FTP.

Kerberos is a popular authentication scheme on a widely distributed network, particularly for single sign-on setups. It is able to authenticate which services client is allowed to use, which objects, and what type of access to those object is allowed to that client. Kerberos provides all that information on the client tickets issued by the Kerberos server.

HTTPS and SOCKS protocols provide for the creation of secure sessions at the application level. HTTPS establishes a secure session over SSL via Web browsers, while SOCKS protocols is an enabler for proxy servers.

USM for SNMPv3 provides for verification of message, verification of user, time of message generation, data integrity, data confidentiality, and many other features that insure secure use of SNMP.

4.2 TRANSPORT LAYER SECURITY

Security of data communication in the IPS Transport Layer is achieved with the use of Secure Socket Layer (SSL) Version 3.0, Transport Layer Security (TLS) Version 1.0, and Secure Shell (SSH) protocols.

SSL Version 3.0 is an Internet protocol (originally developed by Netscape Communications, Inc.) that uses connection-oriented end-to-end encryption to provide data confidentiality services and data integrity services 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. The most common application of SSL is for securing HTTP connections, referred to as HTTPS.

TLS Version 1.0 is an Internet protocol based on and very similar to SSL Version 3.0. These two protocols do not interoperate directly, but TLS client/servers can be set to a compatibility mode to emulate SSL. Additionally, TLS encryption and authentication methods are strictly specified by the governing PKI.

SSH provides support for secure login and file transfer. SSH provides authentication, encryption and compression of data in the transport layer.

These protocols will provide for the secure sessions on top of the TCP or UDP transport layer protocol that will enable secure transmission of information between two host systems. Transport Layer security protocols are most effective when used in concert with higher and lower layer security protocols.

4.3 NETWORK LAYER SECURITY

IPSec protocol is the primary protocol that provides secure exchange of data between two communicating network layers. IPSec provides for authentication, replay protection, integrity checking of IP packets. There are four security components in IPSec:

- Security Protocols — Authentication Header (AH) and Encapsulating Security Payload (ESP). AH provides authenticity guarantee for packets, by attaching strong crypto checksum to packets. ESP provides confidentiality and integrity by encrypting data.
- Security Associations — what they are, how they work, how they are managed, and associated processing
- Key Management — manual and automatic (i.e., Internet Key Exchange (IKE))
- Algorithms for authentication and encryption

Each one of the components can be used as a stand alone, but a combination of the four will provide significantly robust security.

The IPSec protocol uses Security Associations and tunneling to ensure secure transfer of data between two IPSec systems. Security Associations (SA) are unidirectional (simplex) logical connection between two IPSec systems that label this connection with security parameters (e.g., authentication/encryption algorithms). Tunneling or encapsulation is a technique where original packet is wrapped into new packet where the original packet is the payload and to which a new header is added.

While Authentication Header (AH) and Encapsulating Security Payload (ESP) are implemented at the Network layer, the IKE is implemented at the Application layer. The IKE consists of three parts: ISAKMP, Oakley, and SKEME. ISAKMP provides a framework for authentication and key exchange but does not define them. Oakley describes a series of key exchanges — called "modes" — and details the services provided by each (e.g., perfect forward secrecy for keys, identity protection, and authentication). SKEME describes a versatile key exchange technique that provides anonymity, non-repudiation, and quick key refreshment.

4.4 LINK LAYER SECURITY

Link layer security is provided with the use of MPLS on data communication systems such as L2TP, Frame Relay (FR), FDDI, ATM, and PPP. Link Layer Security is not implemented on systems that are based on IPSec.

4.5 PHYSICAL LAYER SECURITY

Physical layer security is not in scope of this document. For information concerning Physical layer security refer to the “Information Security Guidelines for NAS Subsystems Using the Internet Protocol Suite” along with the project IRDs and ICDs.

5 DETAILED REQUIREMENTS

This section of the document describes the detailed security requirements for select capabilities in each of the 5 layers of the IPS stack. Implementation of particular capabilities shall be at the discretion of particular project IRDs and ICDs.

Security requirements for the ATN-compliant systems shall be implemented in accordance with ICAO Doc. 9705, Ed. 3, Subvolume VIII.

5.1 DETAILED REQUIREMENTS FOR APPLICATION LAYER

This section describes security protocols and mechanisms used to provide secure data communication at the application layer.

5.1.1 Public Key Infrastructure (PKI)

Implementation of PKI v3 shall be done in accordance with the RFC-2510.

5.1.2 Internet Key Exchange (IKE) Protocol

The IKE shall be implemented in accordance with RFC-2409.

5.1.2.1 ISAKMP

The Internet Security Association and Key Management Protocol ISAKMP is an application layer key exchange protocol.

An Internet IPsec protocol [RFC-2408] is used 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.

ISAKMP shall be implemented in accordance with RFC-2407 and RFC-2408.

5.1.3 Open Pretty Good Privacy (OpenPGP)

OpenPGP provides data integrity services for messages and data files by using these core technologies:

- Digital signatures
- Encryption
- Compression
- Radix-64 conversion

In addition, OpenPGP provides key management and certificate services, but many of these are beyond the scope of this document.

OpenPGP implementation shall be in accordance with RFC-2440.

5.1.4 S/MIME

The Secure/Multipurpose Internet Mail Extensions (S/MIME) version 3 shall be implemented in accordance with RFC-2631, RFC-2632, RFC-2633, and RFC-2634, RFC-3369, RFC-3370.[1]

5.1.5 USM for SNMPv3

The User-based Security Model (USM) for the Simple Network Management Protocol version 3 (SNMPv3) shall be implemented in accordance with RFC-3414.

5.1.6 Kerberos

Kerberos authentication and authorization system shall be implemented according to RFC-1510.

5.1.7 Proxy Servers

Proxy servers shall be implemented with the SOCKS protocol in accordance with RFC-1928, RFC-1929, and RFC-1961.

5.2 DETAILED REQUIREMENTS FOR TRANSPORT LAYER

This section describes security protocols and mechanisms used to provide secure data communication at the transport (TCP/UDP) layer.

5.2.1 Transport Layer Security (TLS) Protocol

Transport Layer Security Protocol shall be implemented in accordance with the RFC-2246 and RFC-3546.[2]

Implementation of ciphersuites, in addition to TLS Protocol, shall be in accordance with RFC-2712 (in particular for Kerberos support) and RFC-3268 for AES implementations.

Upgrading of HTTP for TLS shall be done in accordance with RFC-2817.

5.2.2 Secure Shell (SSH)

Implementing SSH shall be done in accordance with the Internet draft “SSH Transport Layer Protocol,” draft-ietf-secsh-transport-17.txt.

5.2.3 Secure Socket Layer (SSL)

Implementation of SSLv3.0 shall be done in accordance with Internet draft “The SSL Protocol,” draft-freier-ssl-version3-02.txt.

5.3 DETAILED REQUIREMENTS FOR NETWORK LAYER

This section describes security protocols and mechanisms used to provide secure data communication at the network (i.e., IP) layer.

[1] NIST Special Publication 800-49: Federal S/MIME V3 Client Profile, November 2002.

[2] The RFC-3546 updates RFC-2246, The TLS Protocol version 1.0, and it is backward compatible with TLS v 1.0.

5.3.1 IP Security (IPSec)

IPSec implementation shall be done in accordance RFCs related to AH, ESP, and IKE, and RFC-2401.

5.3.1.1 Authentication Header (AH)

Implementation of the AH shall be done in accordance with the RFC-2402.

5.3.1.2 Encapsulating Security Payload (ESP)

The Encapsulating Security Payload shall be implemented in accordance with RFC-2406.

Programs using CBC-mode cipher algorithms with the IPSec ESP Protocol shall be in accordance with RFC-2451.

5.3.1.3 Combining IPSec protocols

Combinations of IPSec SAs for specific data streams (e.g., multiple security protocols) shall be effected by the two strategies identified in RFC-2401:

- **Transport adjacency,** which applies both AH and ESP to the same IP packet for end-to-end security.
- **Iterated tunneling,** where multiple SAs are each applied to individually nested IP tunnels. Capability shall be provided to configure the end points of such tunnels independently of each other.

These strategies may be aggregated at the discretion of project IRDs and ICDs. However, a minimum set of basic combinations of these strategies shall be supported in accordance with RFC-2401, as described below:

Case 1: End-to-end security

This is a case where a host is connecting to another host through the unsecured Internet. The end-to-end security is illustrated in Figure 3. One or more of the following combinations shall be supported for this implementation:

- Transport Mode: AH alone, ESP alone, AH applied after ESP
- Tunnel Mode: AH alone, ESP alone

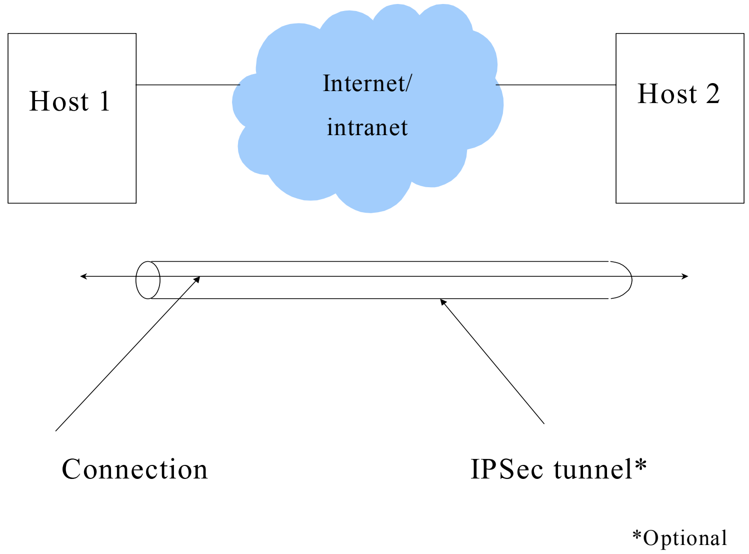


Figure 3 End-to-end security

Case 2: Basic VPN support

Basic VPN configuration is illustrated in Figure 4. Two hosts, each within a separate private network, are connecting to each other through Internet gateways. Both Internet gateways support IPSec, while the hosts do not. In this case, the gateways create an IPSec tunnel between them over the unsecured Internet. These gateways are required to support ESP and AH tunnels.

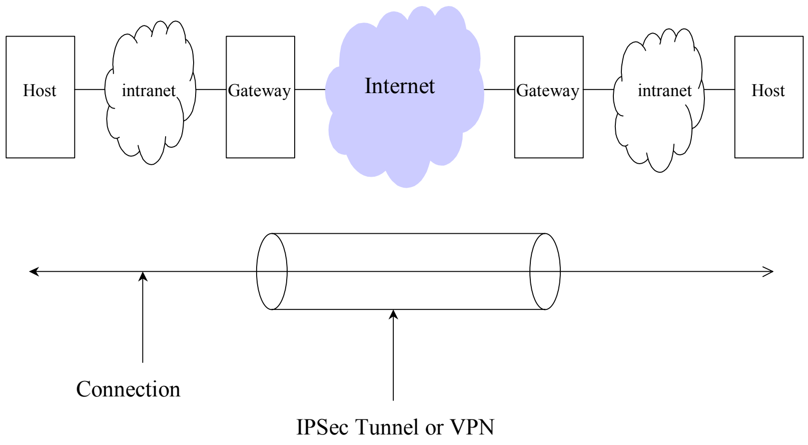


Figure 4 Basic VPN support

Case 3: End-to-end security with VPN support

End-to-end security with VPN support uses a combination of case 1 and case 2, as shown in Figure 5. It imposes no new requirements on the hosts or security gateways, other than a requirement for a security gateway to be configurable to pass IPSec traffic (including ISAKMP traffic) for hosts behind it.

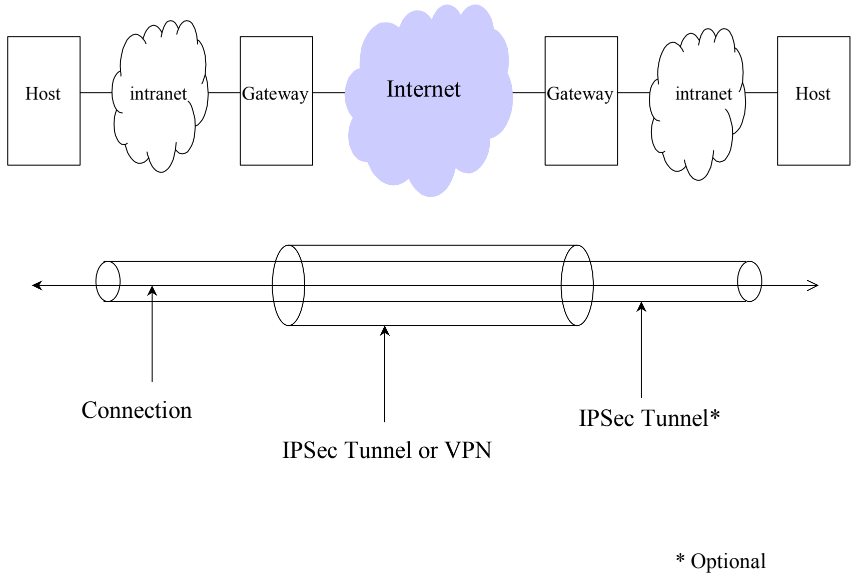


Figure 5 End-to-end security with VPN support

Case 4: Remote access

A remote system is using the unsecured Internet to reach the destination host, which is in the private network protected by a firewall/gateway, as shown in Figure 6. The remote host uses a serial IP protocol (e.g., PPP) to establish a session with the firewall/gateway. The remote host and the Internet gateway must support AH and ESP tunneling modes to support this session.

Either tunneling or transport adjacency may be enacted between the hosts. If transport adjacency is enabled, the transport header must be applied to the packets prior to the tunnel header.

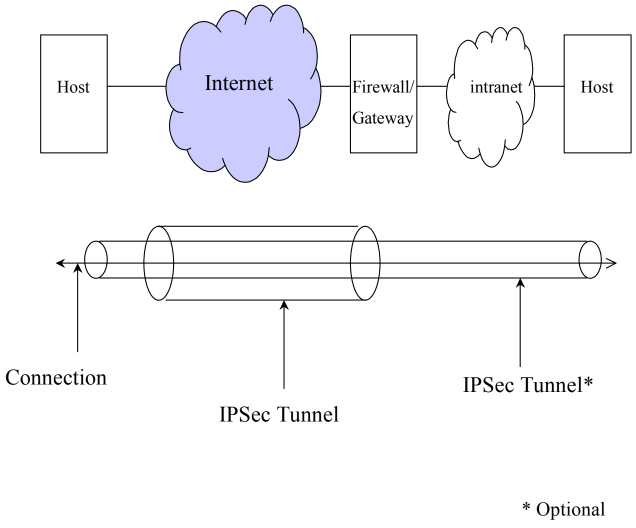


Figure 6 Remote access security

5.3.1.4 Internet Key Exchange (IKE) Protocol

The Internet Key Exchange (IKE) Protocol is part of the IPSec protocol that is implemented at the application layer. For information on IKE, refer to section 5.1.2.

5.3.2 Network Address Translation (NAT)

Network address translation shall be implemented in accordance with RFC-3022.

***Note**: Implementations of IPSec do not support NAT. IPSec has all the security features of NAT and shall not be implemented in conjunction with NAT.*

5.4 DETAILED REQUIREMENTS FOR LINK LAYER

This section describes security protocols and mechanisms used to provide secure data communication at the link layer.

5.4.1 MPLS

The MultiProtocol Label Switching (MPLS) allows for secure transfer of data at the link layer for diverse platforms such as Frame Relay (FR), FDDI, ATM, and PPP. Security at the link layer shall be implemented with MPLS protocol, which is detailed in the RFC-3031.

5.4.2 L2TP

L2TP facilitates the tunneling of PPP packets across an intervening network in a way that is as transparent as possible to both end-users and applications. Implementation shall be in accordance with RFC-2661 and RFC-3437.

5.5 DETAILED REQUIREMENTS FOR PHYSICAL LAYER

This document does not deal specifically with security at the physical layer. Physical security should follow the guidelines set forth in the project IRDs and ICDs.

6 NOTES

6.1 FIREWALLS

There are infinitely many possible firewall configurations used for protection of private networks, but most of them can be classified into four categories. These categories are: Packet-Filtering Firewall, Dual-Homed Gateway Firewall, Screened Host Firewall, and Screened Subnet Firewall (DMZ). The choice of which firewall configuration to use should be done depending on the security requirements defined in the project IRDs and ICDs.

For more information on firewalls and firewall policies see NIST Special Publication 800-41.

6.1.1 Packet–Filtering Firewall

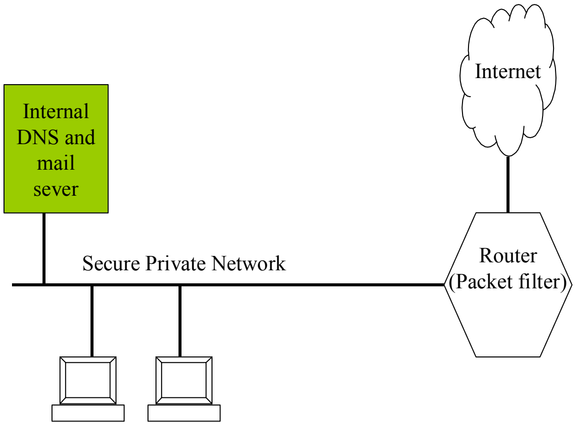


Figure 7 Packet-Filtering Firewall

Firewall in this case is just a router sitting between the untrusted network (such as Internet) and trusted network filtering packet according to some preset filtering rules, as shown in Figure 7.

6.1.2 Dual-Homed Gateway Firewall

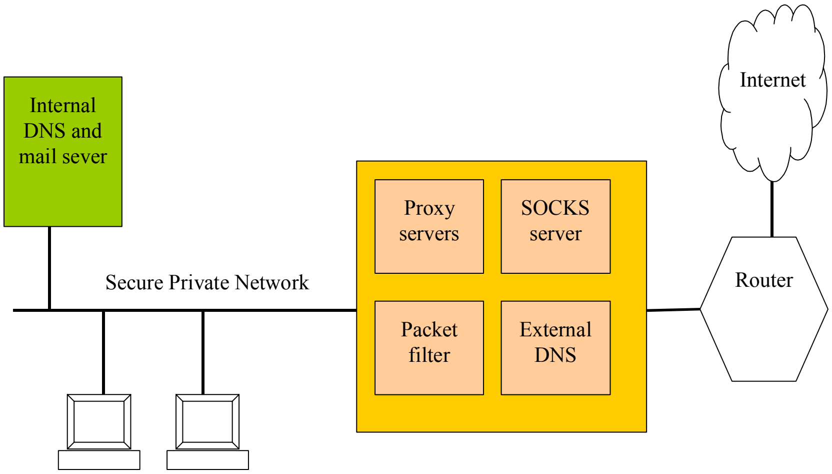


Figure 8 Dual-Homed Firewall

A dual-homed firewall has two or more network interfaces, as shown in Figure 8. It does not forward any packets, and the only way for a packet go from one end of the firewall to the other is by using SOCKS or proxy servers.

6.1.3 Screened Host Firewall

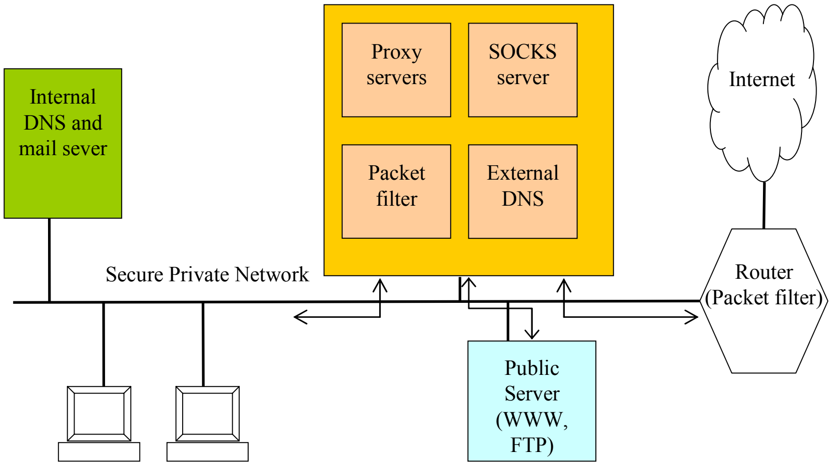


Figure 9 Screened Host Firewall

This type of firewall uses both packet filtering and application layer gateways to provide security to the private networks, as shown in Figure 9. Packet filtering is done in the router, as is the case in the packet-filtering firewall. The application layer gateway is implemented by using dual-homed firewall.

6.1.4 Screened Subnet Firewall (DMZ)

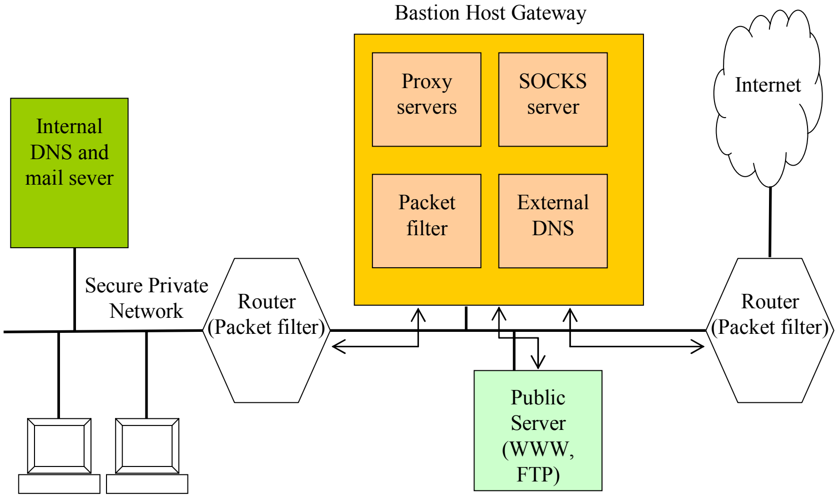


Figure 10 Screened Host Firewall (DMZ)

The screened subnet firewall (DMZ) consists of two packet-filtering routers, one at each end of a bastion host, and a bastion host, as shown in Figure 10. This type of firewall provides for the highest level of security.

6.2 TRANSPORT MODE vs. TUNNEL MODE

	Advantages	Disadvantages
Transport Mode	• Provides End-to-End Security • Lower overhead than tunnel mode • Larger Maximum Transmission Unit (MTU) • Negotiation of connection-specific selectors is common practice	• Requires IPSec to be implemented on the IPS entities • Greater difficulties with NAT traversal (TCP checksum invalidation)
Tunnel Mode	• More compatible with existing VPN gateways • Don’t have to implement IPSec on the IPS entity • Easier to traverse NATs	• More overhead • Smaller MTU • Secure operation with IPS scenarios would require negotiation of connection-specific selectors – not current practice • For hosts with dynamically assigned addresses, interoperability is poor

6.3 ENCRYPTION, CRYPTOGRAPHIC MODULES, and HASH ALGORITHMS

6.3.1 Encryption

The encryption standards for the secure data communication should be in accordance with the FIPS PUB 197. The DES or 3DES encryption standards, which are described in RFC-2405 and NIST FIPS 46-3, should NOT be used in any new FAA systems, since they are not an approved encryption standards. It should be noted that there are restrictions on what encryption standards can be implemented outside the United States.

6.3.2 Cryptographic algorithms

Common cryptographic modules for IPSec should follow the guidelines set forth by the NIST FIPS 140-2.

6.3.3 Hashing algorithms

The secure hashing algorithms should be in accordance with FIPS PUB 180-2, and FIPS PUB 198. IPSec implementation of hashing algorithms should be done in accordance with RFC-2404, which uses an approved hashing algorithm. Only legacy systems should continue to support MD5-96 hashing algorithm, described in RFC-2403, since MD5-96 is not approved algorithm by NIST FIPS 180-2.

6.4 SECURE TRANSITION FROM IPv4 TO IPv6 NETWORKS

Secure transition from IPSec on IPv4 to IPv6 NAS system should be done in accordance with the model in Figure 11. For more information on the model and on transition, refer to "Securely Transitioning Mixed IPv4/IPv6 Networks Configured for IPSec" document, prepared by ACB-250 for ASD-130.

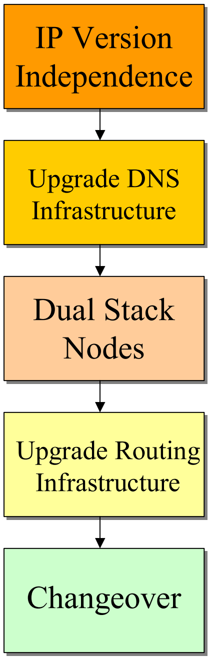


Figure 11 Proposed Migration Path[1]

[1] "Securely Transitioning Mixed IPv4/IPv6 Networks Configured for IPSec."