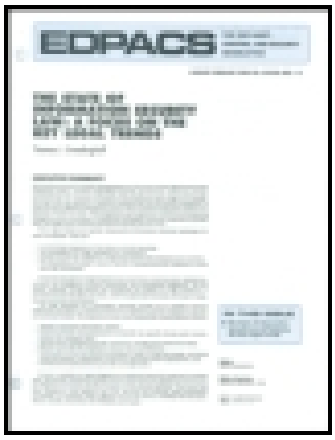


EDPACS: The EDP Audit, Control, and Security Newsletter

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uedp20

IPSec Solution

Derek Street

Published online: 20 Jan 2009.

To cite this article: Derek Street (2008) IPSec Solution, EDPACS: The EDP Audit, Control, and Security Newsletter, 38:5, 6-17, DOI: 10.1080/07366980802379871

To link to this article: http://dx.doi.org/10.1080/07366980802379871

EDPACS
THE EDP AUDIT, CONTROL, AND SECURITY NEWSLETTER

NOVEMBER 2008 VOL. XXXVIII, NO. 5

IPSec SOLUTION

DEREK STREET

THE IPSec ARCHITECTURE

Background

Confidential and integral communications are the basis on which e-commerce and distributed solutions are based. Within a Windows environment, the only communications that are inherently secured are with the Domain Controller. The communications to establish the domain logon are protected, but all other communications are not secured. As a result an e-mail that was carefully encrypted by the sender and only decrypted by the recipient on their desktop is sent over the network in plain text when the recipient sends it to the printer, which largely defeats the benefit of encrypting the e-mail from end-to-end. Additional measures are required to secure other communications in the network.

Currently Secure Socket Layer (SSL) and Virtual Private Networks (VPNs) are used to secure communications only where a risk-to-cost-to-benefit evaluation justifies the implementation of security technologies. As a result the vast majority of network communications within an organization are not protected in this manner, as the cost, in terms of capital outlay and human resources, is prohibitive. However, a risk assessment of an organization's network would likely identify that a VPN/SSL-like safeguard is desirable for the majority of network traffic as it would mitigate a large portion of the risk from the network-level elements of Threat and Risk Assessments (TRAs). Appendix A – SSL and VPN Issues provides more detail on the challenges these technologies face in trying to implement a similar architecture. This document explains the types of solutions that can be developed with IPSec. The details of how it works[1] and how to deploy and manage it[2] are subjects for separate documents.

IPSec can be used to protect some, most, or all of an organization's network communications. IPSec is a standard-based solution (standards listed in Appendix B – IPSec RFC) that provides encryption, integrity, and authentication to protect network traffic as well as port, protocol, and address filtering to protect network hosts. IPSec is cost effective and flexible enough to include the range of technical solutions currently deployed within an organization's network.

The IPSec Architecture creates a "hard boiled egg." The analogy is that the information flows within the "egg" (IPSec-protected object) are rigidly regulated and enforced and access to the contents of the

IN THIS ISSUE

Taylor & Francis
Taylor & Francis Group

"egg" from the outside is prevented. It is important to understand that with the IPSec Architecture, it is **impossible**[3] to connect to any IPSec-protected object without prior authorization, or view the contents of the protected object's network communications. Information flows into and out of the egg can be reduced to tightly regulated portals.

An organization that adheres to the Prevent, Detect, React, and Recover[4] approach to network breaches would benefit in each area:

- ☐ Prevent: No system can communicate with the IPSec-protected object (application, system, or network) without prior authorization.
- ☐ Detect: Any system failing to establish an IPSec connection to a protected object is unauthorized.
- ☐ React: Rectify security procedures relevant to source of intrusion.
- ☐ Recover: None required as the intruder never established communication.

In a typical network environment, this methodology results in significant effort being applied to detecting, reacting, and recovering from network breaches. Creating a secure network environment will reduce the effort applied to reacting to security breaches. The IPSec Architecture is a proactive approach that prevents security incidents rather than reacting to them after they have occurred.

KNOWN NETWORK SECURITY CHALLENGES

Implementing an IPSec Architecture in an organization provides a secure environment in which users can operate, while being scalable and manageable to an enterprise level by using exiting Identification & Authentication mechanisms (Kerberos and X.509). The IPSec Network Architecture will enable an organization to improve the security posture of the network by addressing the following challenges.

Unauthorized Access to the Network

Currently, considerable effort is spent trying to detect unauthorized access to the network and mitigate the impact of unauthorized access. With an IPSec Architecture unauthorized access to the protected object and related network communications is prevented. Implemented at the network level IPSec virtually eliminates the threat. An intruder may gain physical access to the network but they would not succeed in accessing any systems or deciphering network traffic.

Transmission of Sensitive Information

An organization's networks are in place to perform the "Business of the Organization." This business often includes information that is highly sensitive, may have legal requirements regarding its protection, and commonly is of tactical interest to other parties. The security of any organization's business practices would be increased and simplified by the implantation of an IPSec Architecture as it encrypts the communication for confidentiality.

Trusted Communications

To be able to trust the network and the applications that are available on it, the users must be sure they are communicating to the identity (server or user) that they believe they are communicating with. The network users must also be confident that the information they receive and send is not modified in transit. The IPSec Architecture requires authentication based on a mutually trusted source and verifies the integrity of the communication.

Verifiable Network Identities

To create a trusted environment, all communication must be from sources that can be reliably identified. The ability of users and systems on a network to identify each other (i.e., via Kerberos) provides the ability to log and audit activity, as well as the ability to reject communications based on the identity of the source. An IPSec Architecture can use Kerberos or X.509 Certificates to identify both users and systems on the network.

Tamper-Evident Communications

To trust the communication received over the network, a mechanism must exist to verify that the received message is identical to the one sent. Due to the open nature of networks, it is impossible to prevent the modification of information in transit, so detection of modification is required. The IPSec Architecture rejects (at the network level) all communications that fail verification.

Confidentiality

The confidentiality of the network ensures the participants in a communication that the information being passed over the network is not viewable other than by the participants in the communication. There are two elements to this layer of protection.

Protecting network traffic from viewing by unauthorized users (Outsiders) prevents information from being exposed to external entities. This type of protection is typically performed at the boundaries of the organization to protect communications to legitimate external partners. Often nothing is done to prevent viewing of data WITHIN the organization by external entities.

Protecting network traffic from being viewed by privileged internal entities (Insiders—Network Administrators for example) prevents them from being able to use their special access to the network to view the information traversing the network. There are many situations where the misuse (or even legitimate use) of privileges will inappropriately expose data on the network. Provision of true confidentiality requires that privileged users have no access to the data in transit over the network. An IPSec Network Architecture encrypts the data for the participants, so the communication is protected in transit.

THE IPSec EFFECT

The result of an organization adopting an IPSec Architecture is to create a secure environment for the IPSec-protected object (application, system, or network). As more and more enterprise business processes are incorporating distributed (networked) solutions the security (integrity and confidentiality) of an organization's network infrastructure will be a key factor in the success of these initiatives. By producing the following results the IPSec Architecture will provide a secure environment in which to deploy federated and e-business solutions.

1. Enforce that only authorized people and systems can connect to the IPSec- protected object.
2. Enforce that all communications within the IPSec-protected object are confidential to the participating parties.
3. Enforce that all communications within the IPSec-protected object have integrity.
4. Utilize the existing trust infrastructure (i.e., Windows logon) to enable secure communications within the IPSec-protected object.
5. Enforce tight restrictions to the IPSec-protected object providing at well-defined interface points.
6. Monitor IPSec-protected object communications with external entities and enforce policy.

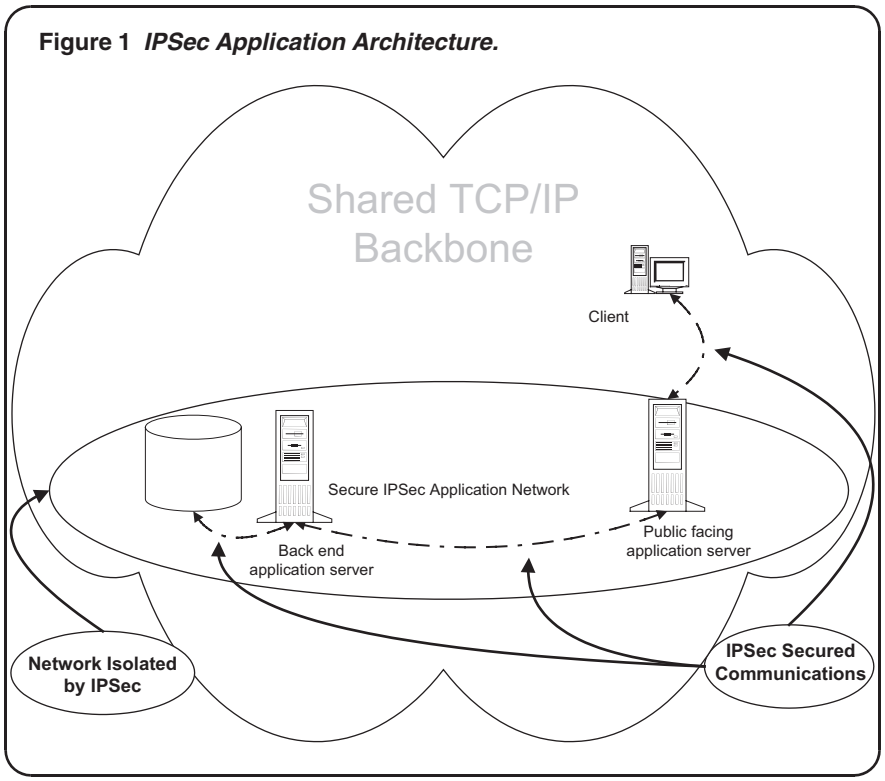
It is important to note that the IPSec Architecture is a powerful addition to the existing IT protection strategies that deal with unauthorized access to the network and the security of the information traversing it, which can be characterized as "outsider" (penetration) types of attack. IPSec does not eliminate the need to protect systems from authorized users attempting to perform unauthorized activities, which are considered "insider" attacks (vulnerabilities). It does provide for traffic filtering based on port, protocol, and address, which significantly reduces the exposure of the system on the network.

IPSec Application Architecture

The VPN-like aspects of the IPSec Application Architecture provide the capability of transmitting data securely over any network. The network traffic of the trust community has integrity as a whole, not just for the individual packets. As a result, the servers involved in the application delivery exist in a "separate" network that can only be accessed via authentication.

In the IPSec application architecture (Figure 1) the servers that provide the application are isolated from the general computing environment by IPSec. A public-facing server accepts the user requests (communications protected by IPSec) and relays them to the application server, which only accepts authenticated, encrypted, and signed communications from the public-facing server. No other system can communicate with it. This IPSec implementation authenticates, encrypts, and signs all application-related traffic (client to public server, public server to application server). This architecture forces application access to be channeled through the public-facing server, which can sanitize the traffic, request additional authentication if required, and prevent direct

Figure 1 ***IPSec Application Architecture.***



access to the back end application from any system other than the designated public-facing server.

IPSec Server Farm Architecture

The VPN-like aspects of the IPSec Application Architecture are expanded in the IPSec Server Farm Architecture to provide the secure communications capability to the servers providing essential cooperate services. The network traffic of the trust community has integrity as a whole, not just for the individual packets. As a result, the servers involved in the delivery of the essential corporate services exist in a "separate" network that can only be accessed via authentication.

The IPSec server farm architecture (Figure 2) provides authenticated access to public facing components that can employ digital signatures and encryption for integrity and confidentiality of the communications. The front end servers can inspect the incoming and outgoing traffic and can request additional authentication if required. The architecture secures and isolates the back end component traffic and systems from the rest of the network.

IPSec Network Architecture

Taken to its logical conclusion, an IPSec-protected object can encompass the entire network, providing integrity to the network as a whole. In this configuration an intruder would not be able to

Figure 2 ***IPSec Server Farm Architecture.***

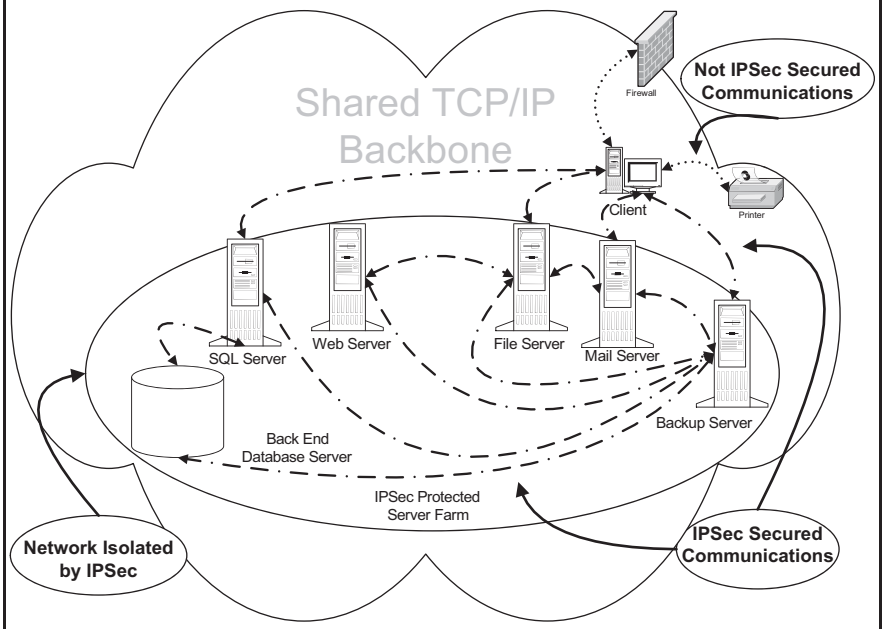
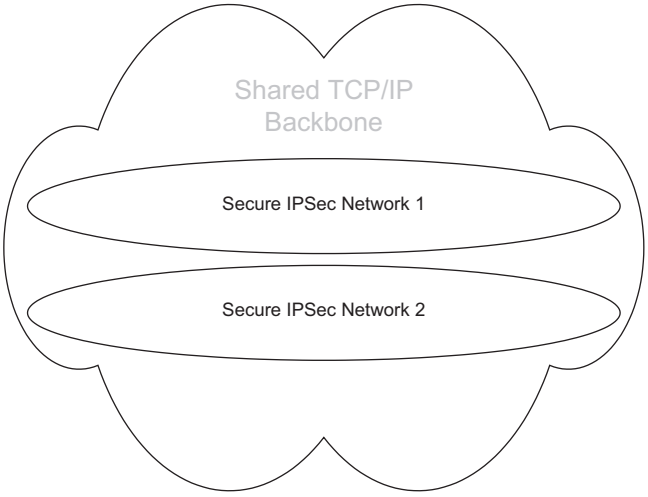


Figure 3 ***Two networks sharing one hardware environment.***



communicate with any system and would only be able to observe encrypted traffic on the network.

In Figure 3, the two networks share a hardware environment. The systems in each network are logically separated from each other by the IPSec requirement for authentication credentials and digital signatures to enable communications. The result is that the systems in the two networks cannot initiate communications because they lack the proper credentials. The information from the

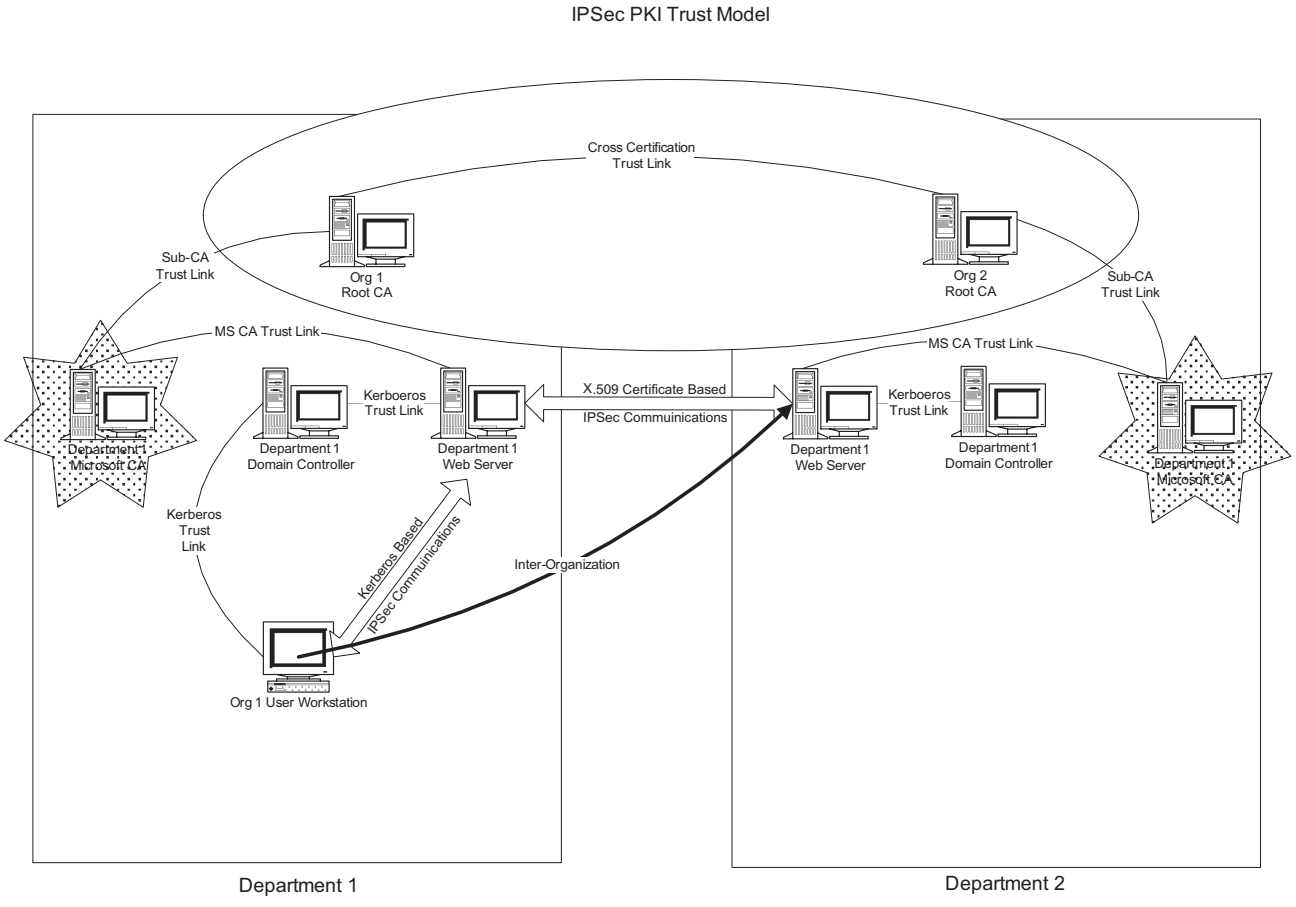
two logical IPSec networks is traversing the single physical network in an encrypted format, which maintains the logical isolation of the two networks.

IPSec Global Architecture

The use of X.509 Certificates allows trust to exist beyond the boundaries of an organization. Through the use of Certificate Trust Lists or Cross Certification in the IPSec Architecture an organization can authenticate and protect communication to another organization as seamlessly as it protects the internal communications (Figure 4).

The IPSec Global architecture is an extension of the IPSec Network architecture in that the separate isolated IPSec networks are configured to have an X.509 certificate– based trust relationship that allows the systems (when appropriately configured) to permit network traffic from the other trusted domain. The trusted communication path must be explicitly configured as the trust link makes the communication possible but does not enable specific communications paths between the domains. In this manner specific portals can be created to enable trusted communications between the separate IPSec- protected networks.

Figure 4 ***IPSec Global Architecture.***



SUMMARY

An IPSec Architecture will provide a secure environment for the network objects used for the business of the enterprise using existing I&A credentials. The IPSec Architecture has benefits that address the significant security challenges outlined in the earlier section, Known Network Security Challenges. The following list details how the IPSec Network Solution addresses identifiable business needs:

- ☐ *Prevent Unauthorized Access to Network*. Prevent unauthorized access to the network is written into virtually every security policy. In practice networks do very little to prevent unauthorized access. The network intruder can initiate communications with systems to gather information or launch attacks. IPSec requires credentials, issued by the systems owners, to be presented to initiate communication with systems under its protection. As a result, IPSec will prevent unauthorized (those without credentials) communications in the network.
- ☐ *Prevent Unauthorized Egress from the Network*. The systems in the IPSec network require authentication with specific credentials to communicate. Within the environment edge systems are configured to communicate internally with IPSec and externally without IPSec. As a result only the specially configured edge systems can communicate to an external system. This makes them the only way for the internal IPSec-only systems to access external systems. The edge system can perform the required access controls for outbound network traffic.
- ☐ *Certifiable to Transmit Sensitive Data*. The IPSec solution uses cryptography that is approved for Protected-B information in the Canadian context. Unauthorized disclosure of Protected-B information could reasonably be expected to cause serious injury to an individual, organization, or government. IPSec encrypts the network traffic from "end-to-end," providing security for the network packet payload from source to destination without exposing the contents at any point in between.
- ☐ *Leading Edge Technology for Significant Return on Investment*. IPSec is widely used in tunnel mode to secure communication between sites. The use of IPSec in transport mode to secure communications at the system level is an emerging approach that leverages the known security capabilities of IPSec, which are built into systems and devices already deployed within an organization.
- ☐ *Creates Trusted Communications*. IPSec provides the ability to authenticate the parties involved in a communication to ensure the participants that the other parties are indeed who they claim to be. Additionally, IPSec digitally signs the communications, which ensures the integrity of the communication. Trusted communications are supported by IPSec through identifying the participants and ensuring the integrity of the communications.

Currently the most common use of IPSec is for Virtual Private Networks (IPSec in Tunnel Mode) and most reference material for IPSec is on this subject. Additional reference reading is identified in Appendix C – Reference Reading that addresses IPSec on TRANSPORT mode as used in this architecture.

APPENDIX A—SSL AND VPN ISSUES

Virtual Private Networks

The VPN technology is used to secure communications between two well-defined end points. The result is all communication between the end points that is secure, as it has been encrypted for confidentiality, signed for integrity and authentication, and time stamped for anti-replay defense. A VPN is very effective at securing communications between sites.

Although the VPN provides the desired results between sites, to mimic the IPSec solution it would be labor intensive to set up, and must be defined in advance, prior to use with any given end point. Even if every system was configured to communicate with every other system with a VPN, it would not provide the same security posture as provided by IPSec because there is no port-blocking capability within the VPN. The VPN creates a secure communication link to the other system; it does not provide the ability to restrict communications to the other system to specific ports. The system is vulnerable to attacks over the VPN via ports that were enabled as a result of the VPN set-up, but may not be required for application functionality.

The addition of a system into a network that has VPN connections everywhere would require the configuration of a VPN to every other system in the network. The maintenance of such a solution, assuming you could initially configure it, would be unmanageable.

Secure Socket Layer

The SSL technology is used to protect specific communication protocols. A handful of protocols (HTTPs for example) natively support SSL. All other protocols need to be redirected to a secured port in what is called "tunnel mode." SSL is effective in scenarios where network connectivity is restricted to well-defined ports and protocols.

Although the SSL provides the desired results for limited communications, to mimic the IPSec solution it would be labor intensive to set up. Even if every required port on every system was configured to use SSL it would not provide the same security posture as provided by IPSec because there is no port-blocking capability within SSL. Setting up SSL for one protocol does not prevent (or block) the use of other protocols on the system. Setting up SSL to protect FTP (port 21) will secure communications for that protocol and port, but it will not block or secure traffic for Telnet (port 25).

The addition of a system into a network that is has SSL connections everywhere would require the configuration of SSL for every required port on the system. Maintenance of such a solution, assuming you could initially configure it, would be unmanageable.

APPENDIX B—IPSec RFC

RFC 2367
PF_KEY Interface
RFC 2401
Security Architecture for the Internet Protocol (IPsec overview)

RFC 2403
The Use of HMAC-MD5–96 within ESP and AH
RFC 2404
The Use of HMAC-SHA-1–96 within ESP and AH
RFC 2405
The ESP DES-CBC Cipher Algorithm With Explicit IV
RFC 2410
The NULL Encryption Algorithm and Its Use With IPsec
RFC 2411
IP Security Document Roadmap
RFC 2412
The OAKLEY Key Determination Protocol
RFC 2451
The ESP CBC-Mode Cipher Algorithms
RFC 2857
The Use of HMAC-RIPEMD-160-96 within ESP and AH
RFC 3526
More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
RFC 3706
A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers
RFC 3715
IPsec-Network Address Translation (NAT) Compatibility Requirements
RFC 3947
Negotiation of NAT-Traversal in the IKE
RFC 3948
UDP Encapsulation of IPsec ESP Packets
RFC 4106
The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
RFC 4301
Security Architecture for the Internet Protocol
RFC 4302
IP Authentication Header
RFC 4303
IP Encapsulating Security Payload
RFC 4304
Extended Sequence Number (ESN) Addendum to IPSec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP)
RFC 4307
Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
RFC 4308
Cryptographic Suites for IPSec
RFC 4309
Using Advanced Encryption Standard (AES) CCM Mode with IPSec Encapsulating Security Payload (ESP)
RFC 4478
Repeated Authentication in Internet Key Exchange (IKEv2) Protocol

RFC 4543
The Use of Galois Message Authentication Code (GMAC) in IPSec ESP and AH
RFC 4555
IKEv2 Mobility and Multi-homing Protocol (MOBIKE)
RFC 4621
Design of the IKEv2 Mobility and Multihoming (MOBIKE) Protocol
RFC 4718
IKEv2 Clarifications and Implementation Guidelines
RFC 4806
Online Certificate Status Protocol (OCSP) Extensions to IKEv2
RFC 4809
Requirements for an IPsec Certificate Management Profile
RFC 4945
The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2, and PKIX

APPENDIX C—REFERENCE READING

Virtually all literature on IPSec deals with the deployment of VPNs. Very little is currently available in regard to IPSec used on a host in TRANSPORT mode as described in this article.

The following book has references to the technology: Doraswamy, N., & Harkins, D. (2003). *IPSec: The New Security Standard for the Inter- net, Intranets, and Virtual Private Networks*. Prentice Hall.

The following websites have information on IPSec in TRANSPORT mode:

http://www.tcpipguide.com/free/t_IPSecModesTransportandTunnel.htm
http://search.technet.microsoft.com (enter IPSec as search string)
http://www.freeswan.org/freeswan_snaps/CURRENT-SNAP/doc/ipsec.html

Notes

1. Detailed Architecture Report.
2. IPSec Build Document.
3. Barring implementation or configuration errors.
4. PDRR is a Canadian Treasury Board Secretariat methodology.

Derek Street has 26 years of experience in the IT industry covering a range of disciplines such as operating system and application development, operations, customer support, system integration / testing and security architecture development. Derek has spent the last 12 years in the security realm. During this time he developed 1st High Availability solution for Entrust Certification Authority, deployed and accredited the initial Government of Canada PKI, was a System and Security Engineer for deployment and certification of the Government On-Line PKI (Canadian), developed the Windows 2003 Server hardening guidance on Communication Security Establishment Canada's web site and developed "state-of-the-art" IPSec security architecture while under contract for the Communication Security Establishment Canada.