Ipsec research paper examples

Sociology, Communication

Internet Protocol Security

IPsec is the short abbreviation for Internet Protocol Security which is referred to as the protocol suite used in securing the Internet Protocol (IP) network communications through encrypting and validating each IP packet (data sent over the internet) of a communication session. Internet Protocol security comprises procedures and protocols used in establishing a reciprocated authentication or verification procedure between artificially intelligent agents at the commencement of the interconnection period and the intercession of cryptographic keys to be used by the network user during the given time lease period (Black, 2000).

Internet Protocol security can be used in guarding data and information that flows between a pair of hosts (host-to-host data communication) within a given network. The information between a security gateway and a host within a network also need protection against phishing or malicious internet hackers who pick up information from (network-to-host). The technique can be sued to protect data between a pair of security gateways, also referred to as (network-to-network) communication. This can either include a LAN (Local Area Network) or a WAN (Wide Area Network). These optional network configurations can usually be conducted on the network router interface.

In this case scenario the implementation of the IPsec will be on the network configuration of a network linkage between a numbers of hospitals. There are number of networking platforms that can be used to protect the hospitals network system from malicious attacks and unauthorized intrusive material, entities and agents (Rhee, 2003). One of the advisable protocols over the internet that can be used includes the IPv4 (Internet Protocol version four)

and the IPv6 (Internet Protocol version six). These protocols are the most operational with IPv4 being the most commonly used, while the IPv6 is currently being introduced into different technological and networking platforms.

The end-to-end security system functioning is in the Internet Layer of the Internet Protocol Suite, while some other Internet safety schemes in widespread use such as Secure Shell (SSH), Transport Layer Security (TLS) and Secure Sockets Layer (SSL), function in the higher layers of the TCP/IP model of networking. Therefore, IPsec safeguards any application traffic across an Internet Protocol network. The applications do not need to be precisely developed to use IPsec. Minus IPsec, the use of TLS/SSL had to be developed into an application system to safeguard the application protocols (Tan, 2003).

Use of tunneling and VPN for Data Communication

Tunneling provides a way to encapsulate subjective packets inside a transport protocol layer. Tunnels are usually applied as a virtual interface to offer a modest interface for alignment. The tunnel interface is usually not tied to an exact " passenger" or " transport" protocols, but, rather, it entails an architecture that is developed to deliver the services essential to implement any normal point-to-point encapsulation system.

Below is an exemplified diagram of the Internet Protocol Security Tunneling technique that is portrayed in a network connection.

The given scenario for implementing the network tunneling for the hospital is aimed at creating a secure network configuration that protects the data that

the client accesses when they make a request or submit a prerequisite appeal for information from the server. The diagram highlighted displays hoe one can make an information request for data forma server via an internet protocol which has a secured tunnel to protect their information from eavesdropping by unwanted and unauthorized personnel (Tan, 2003).

The VPN (Virtual Private Network) allows the remote access and the amount of contact the client has to the information. The Internet Protocol security provides the secure tunnels between the two peers, that is, can be the client and the server. These can usually be two routers that connect the two different networks that are being used to communicate (Loshin, 2000).

In a Virtual Privet Network (VPN), the workstations at both ends of the channel encrypt the data incoming into the tunnel and decrypt it at the other end. Though, a Virtual Private Network (VPN) requires more than just a couple of keys to deploy or apply an encryption. Thus, that is where the protocols come in. For instance, a site-to-site Virtual Private Network (VPN) could use either the generic routing encapsulation (GRE) or Internet protocol security protocol (IPsec). The generic routing encapsulation GRE offers the outline for how to suite the passenger protocol for transportation over the Internet protocol (IP).

This framework includes data on what type of packet one is encapsulating, in this case scenario the patient confidential records. Hence, subsequently the connection between sender and receiver are put under surveillance with the aim of establishing appropriate security measures (Black, 2000).

Types of Virtual Private Network (VPN) Tunneling

In a remote- access VPN, tunneling classically depends on a Point-to-point Protocol (PPP) tunneling which is a portion of the built-in protocols utilized by the Internet. For more accurately access to information, for example, the remote-access Virtual Private Networks (VPNs) use at least one of these three protocols based on Point-to-point Protocol (PPP) tunneling:

- The L2TP (Layer 2 Tunneling Protocol) - Associates structural features of PPTP and L2F and entirely supports the Internet Protocol Security (IPsec). This is also appropriate in a site-to-site Virtual Private Network (VPNs).
- The PPTP (Point-to-point Tunneling Protocol) – This networking communication method approach uses and implements a 40-bit and 128-bit encryption and every other verification system maintained by the PPP (Point-to-point Tunneling Protocol).
- The L2F (Layer 2 Forwarding) – This internet network communication was established by the Cisco Inc. It utilizes every certification system endorsed by the supported by PPP

The beneficial approach of tunneling in the scenario for use in a hospital is essentially aimed at ensuring data security. The subsequent circumstances in which tunneling or encapsulating the data traffic are applicable ate in another protocol in which they are convenient to empower multiprotocol local network systems over the given single-protocol backbone (Black, 2000).

Another added advantage of using a Virtual Private Network (VPN) tunneling is to offer workarounds for internet connectivity networks that use procedures that possess partial hop counts within the network; for example.

The hospital needs to connect discontinuous sub networks hence the implementation of a tunneling system aids in this application. The technology also permits the virtual private networks across WANs (Wide Area Networks)

Encryption Methods to be used

The best and frequently used methods of encryption are public-key encryption or symmetric-key encryption. In public-key encryption method, each workstation (or computer system end user) has a possession and access to a public-private key pair. Here, one computer utilizes its private key to encode a communication message, and another computer on the receiving end for instance utilizes the conforming public key to decode that particular communicated message. In symmetric-key coding, all computers end users virtually share similar key utilized to both encode and decode the communicated a message (Doraswamy & Harkins, 2003).

The IPv4 and IPv6 Protocols with VPN

The benefits of working with Virtual Private Network are that they solve the need for movement to access a particular service from a given area locations. The remote access capabilities of Virtual Private Network (VPN) essentially operates efficiently with the internet protocol (IP) versions for the implementation of a viable network with secured communication between tunnels.

Using the Internet Protocol (IPv4) is acceptable and viable in the use of the Virtual Private Networks (VPNs). This is because Virtual Private Networking through the use of Internet Protocol Security (IPsec) allows the network

administrator to be able to extend a secure, private network over an existing public network. The Internet Protocol version 4 (IPv4) is advisable for use over the Internet Protocol version 6 (IPv6) since IPv6 is not supported by VPN (Doraswamy & Harkins, 2003).

In the given scenario, in case there will be need for implementing IPv6 for future compatibility in network tunneling. The protocol can then be tunneled through the IPv4 by utilizing an iSeries Virtual Private Network facility that is applied on the IPv4 communication data traffic. This in turn can transparently handle the IPv6 payloads.

Another feature that would make the IPv4 viable for use rather than the IPv6 is that the applications in the source address selection in a data communication session. An application may designate a source Internet Protocol through the use of a source chosen based on the route.

In the Virtual Private Networks tunneled through sockets and set ports, an API (Application Program Interface) uses the TCP/IP model. The abundant usage of IPv4 in most organizations worldwide argues the fact; applications that do not usually need the IPv6 are not quite often affected by the needed use of sockets and open ports for communication. On the other hand, the use of an IPv6 can be prove really advantageous in the use tunneling ports for the VPNs since it handles the enhancement of though it is expensive to acquire the technology needed to support this platform (Kaufman & Newman, 1999).

In the Virtual Private Network (VPN), the Network Address Translation (NAT) for any data communicated between open port routes within a network usually has the basic functionalities set in place for an IPv4 network. This

comprise of the firewall functions and intrusion detection systems that are integrated on the TCP/IP model and configured using iSeries Navigator. Fortunately, the Network Address Translation (NAT) command is not required on the IPv6 since the expanded address space for the IPv6 eliminates the address shortage problem experienced by the IPv4. This allows easier renumbering of the network addresses and subnet masking. The online shortcoming for this improvised feature is that currently VPN does not support IPv6 (Kaufman & Newman, 1999).

The Basic High Level Topology view

The network topology that I would advise for used by the hospital is expected to be of a high level view which allocates room for network integration. A high level topology features the use multi-user web access. The benefit of this is the nature of its accuracy and affordable network maintenance.

Use of AES (Advanced Encryption Standard)

The AES (Advanced Encryption Standard) is the block cipher with usually a block length of 128 bits. The added advantage of AES (Advanced Encryption Standard) allows for the use of three different key lengths: 128, 192, or 256 bits which offer strong encryption for the data communicated over the network through a tunneled Virtual Privet Network. It is mainly used to secure wireless Virtual Private Networks with strong password encryptions. It consists of the first round which entails encryption session then the second round which entails the decryption process session through the use of a set algorithm on the network interface cards of the connecting device nodes

within the network. In other words, each round of processing works on the input state array and produces an output state array as highlighted in the diagram below. This can be implemented to help doctors access the hospital network remotely.

The use MD5 (Message-Digest Algorithm)

The Message-Digest Algorithm is a widely used cryptographic hash function that produces 128-bit (16-byte) hash values. A hash function is the algorithm that takes a block of data and creates a string of data, referred to as the hash function. It is of a fixed length and is usually run to aid in decryption of received data within the network. The nature of the MD5 offers a great extent of data accuracy in that it is difficult to find different messages with the same hash (Rhee, 2003).

The use of SHA-1 Encryption Technology

Like MD5, SHA-l processes input data in 512-bit blocks. SHA-l is a revised version of SHA designed by and the National Security Agency (NSA) and NIST (National Institute of Standards and Technology). The process is used to send a non-secret but signed message from sender to receiver. In such a case following steps are followed:

- Sender inputs a plaintext memo into SHA-l algorithm and gets a 160-bit SHA-l hash.
- Sender then ciphers the hash with his RSA private key and refers to both the plaintext memo and the signed hash to the recipient.
- After receiving the message, the recipient calculates the SHA-l hash

himself/herself and also applies the sender's public key to the signed hash to obtain the original hash H.

The use of SHA-2 Encryption Technology

This is an alternative technology for encryption of the passwords through the use of a set algorithmic code that encourages the strong coding of information. The disadvantage of this technique is that it is time consuming when using this technique for encryption purposes.

Security Protocols

The beneficial use of operating a Virtual Private Networking is Internet Protocol Security (IPsec) is the network system layer security processes which entail a number of components vital to successive encryption and decryption of data sent over the internet. These include two security protocols.

The Authentication Header (AH)

The first one is the Authentication Header (AH). AH can provide integrity protection for packet headers and data, but it cannot encrypt them. It can also protect the uppermost outermost IP header.

The Encapsulating Security Payload (ESP)

The other one is referred to as the Encapsulating Security Payload (ESP). ESP can deliver encryption and integrity protection for packets, but it cannot protect the outermost IP header, as AH can. However, this protection is not needed in most cases. Accordingly, ESP is used much more frequently than AH because of its encryption capabilities (Doraswamy & Harkins, 2003). In a

Virtual Private Network (VPN), which requires private transport network, then the ESP is the likely decision.

The use of Internet Key Exchange (IKE) protocol

IPsec uses IKE to transfer an IPsec connection setting(s); negotiate secret keys; describe the security limits of the IPsec-protected networks; validate communication endpoints to each other; and manage, update, and delete IPsec-protected internet communication network channels (Rhee, 2003).

References

Black, U. (2000). Internet security protocols: Protecting IP traffic. Englewood Cliffs, NJ [u. a.: Prentice Hall PTR.

Kaufman, E., & Newman, A. (1999). Implementing IPsec: Making security work on VPNs, intranets and extranets. New York [u. a.: Wiley.

Doraswamy, N., & Harkins, D. (2003). IPSec: The new security standard for the internet, intranets, and virtual private networks. Upper Saddle River, N. J: Prentice Hall PTR.

Tan, N.-K. (2003). Building VPNs with IPSec and MPLS. New York, NY [u. a.: McGraw-Hill.

Rhee, M. Y. (2003). Internet Security: Cryptographic Principles, Algorithms and Protocols. Chichester: John Wiley & Sons.

Loshin, P. (2000). Big book of IPsec RFCs. San Diego: Morgan Kaufmann.