EVALUATING THE PERFORMANCE OVERHEADS OF IPSEC PROTOCOL

B.Someshwar Reddy
B.Tech, Department of ECE, Sreenidhi Institute of Science and Technology, Village Yamnampet, Mandal Ghatkesar, Dist Ranga Reddy, Telangana, India.

ABSTRACT: A popular and widely deployed use of IPsec is in establishing Virtual Private Networks (VPNs). Through the use of cryptographic primitives, VPNs allow off-site personnel to access organizational resources over the public Internet as if they were on-site. Internet Protocol Security (IPsec) is a protocol suite for securing the Internet Protocol (IP) communications by means of the authentication and encryption of each IP packet transmission of a data stream. The IPsec personal network layer safety and it is extra appropriate for VPN technology. This paper evaluates the performance overheads associated with IPsec.

Keywords: IPsec Protocol, Virtual Private Networks

I. INTRODUCTION

VPNs securely join far remote customers and offices in a corporate network. The goal of a Virtual Private Network is to add a stage of security to the change of records. Even when an organization is the usage of a leased line, they could install a VPN network to shield their statistics. It is a virtual network; due to the relationship between any nodes of the entire VPN isn't a physical hyperlink which essentially private network makes use of. Instead, it builds up a logic network on top of the platform which an Internet Service Provider offers, as an instance, Internet, Asynchronous Transmission Mode (ATM), and Frame Relay (FR) and so on. And the user facts are transmitted within the logical link. VPN makes use of the tunneling generation, encryption and decryption process, and key management, person and tool identity authentication technologies. It covers the bundle across the shared or public networks, the encryption and authentication validation link, extension of the personal network.

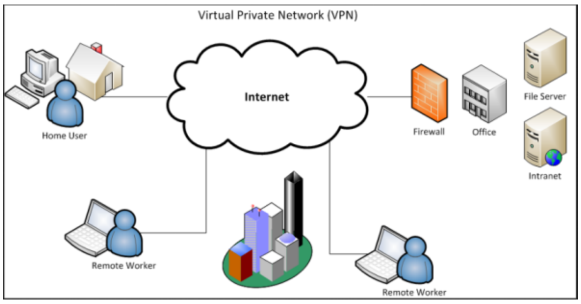

Fig1. Example for VPN

VPN (Virtual Private Network) generation offers a way of shielding statistics being transmitted over the Internet, by using allowing customers to set up a virtual private “tunnel” to safely input an inner network, having access to sources, data and communications through an insecure network consisting of the Internet.

IPsec is designed to offer interoperable, high nice, cryptographically-based completely safety for Ipv4 and Ipv6. The set of safety offerings provided includes get proper of entry to manipulate, connectionless integrity, records starting location authentication, safety against replays (a shape of partial collection integrity), confidentiality (encryption), and restricted traffic go together with the flow confidentiality. These services are furnished on the IP layer, providing protection for IP and/or higher layer protocols. These objectives are met thru the use of two traffic safety protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP), and through the use of cryptographic key management procedures and protocols. The set of IPsec protocols hired in any context, and the methods in which they’re employed, can be decided through the safety and gadget requirements of customers, applications, and/or web web sites/companies. When those mechanisms are efficiently carried out and deployed, they ought no longer to adversely have an impact on customers, hosts, and special Internet components that don’t rent those safety mechanisms for protection of their site visitors. These mechanisms also are designed to be set of guidelines-independent. This modularity allows desire of various sets of algorithms without affecting the other components of the implementation. For instance, unique individual organizations may choose special sets of algorithms (developing cliques) if required. A famous set of default algorithms is unique to facilitate interoperability in the global Internet. The use of those algorithms, along with IPsec visitors safety as well as key management protocols, is meant to permit device and application builders to set up high nice, Internet layer, cryptographic security technology.

The IPsec protocol is broadly used to put in force protection in pc networks and Internet. However, the introduction in the mobile access networks, more exactly in LTE, is current and has challenges unusual in conventional constant IP networks. LTE goals are to provide broadband offerings and actual-time offerings. Currently Release eight gives 300Mbps downlink and75Mbps uplink throughput rates, supports voice (VoLTE), Video (Interactive, Streaming and Broadcasting) and Interactive online games. To provide offerings differentiation, LTE implements Quality of Service (QoS) policies based totally in facts switch potential, latency, latency version (jitter) and transmission mistakes admitted in every carrier. With IPsec creation is theoretically expected lower community efficiency because of protocol overhead and higher latencies due to the use of pretty processing disturbing algorithms for records authentication as well as encryption.

II. RELATED WORK

The massive problem with the authentic IP version (IPv4) is the pending exhaustion of its cope with space. This scenario arose because of the speedy growth of the Internet beyond everybody's expectancies when IPv4 become developed. This same mismatch between how the Internet became whilst Ipv4 changed into created and how its miles now has brought about another most important hassle with IP: the shortage of a definitive manner of making sure security on IP internetworks.

RC6 and MARS do not have on-the-fly key schedules, raising cost and lowering performance, calling into question their suitability for certain high-performance IPsec hardware environments. If all the AES candidates had such limitations, it could per-haps be argued that the associated additional cost and complexity involved in using these algorithms in such systems is justifiable. However, Rijndael, Ser-pent, and Two fish all have on-the-fly key schedules that work very well in such environments, fitting easily into existing architectures without significantly affecting cost or performance. In existing, when IPsec was used over a wireless medium, the network load and number of transactions were the same as in a wireline environment. The transfer time increased, since more time was required to send the additional overhead due to IPsec over the wireless link. It was also shown that it is possible to predict the increase in the transfer time due to IPsec by comparing the transfer time for different network topologies, as long as the number of transactions and the network load used for a specific encryption scenario remain approximately the same. This research did not consider the processing overhead for compressing files before sending them. NewerFrees "IPsec implementations can be used to measure the impact on the network overhead when both compression and security are used.

III. OVERVIEW OF IPsec PROTOCOL

IPsec integrates safety on the IP layer. In order to provide better layer offerings, it defines new protocols, Encapsulating Security Payload (ESP) and Authentication Header (AH). Both ESP and AH protocols encapsulate IP packets using ESP and AH headers respectively.

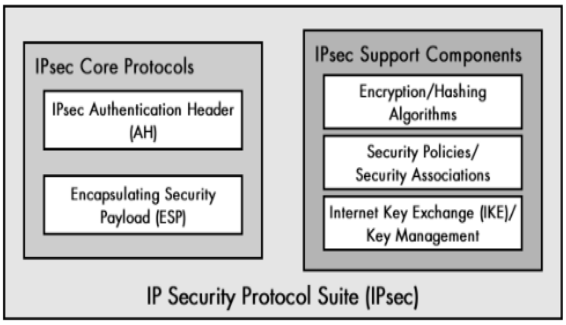
IPsec Core Protocols
IPsec Authentication Header (AH)
Encapsulating Security Payload (ESP)
IPsec Support Components
Encryption/Hashing Algorithms
Security Policies/ Security Associations
Internet Key Exchange (IKE)/ Key Management
IP Security Protocol Suite (IPsec)

Fig2. IPsec Protocols and Components

IPsec Authentication Header (AH)

This protocol gives authentication services for IPsec. It lets in the recipient of a message to affirm that the supposed originator of a message became truely fact the one that despatched it. It also permits the recipient to verify that intermediate devices en route haven't modified any of the information within the data-gram. It additionally gives safety in opposition to so-referred to as replay assaults, wherein a message is captured through an unauthorized user and resent.

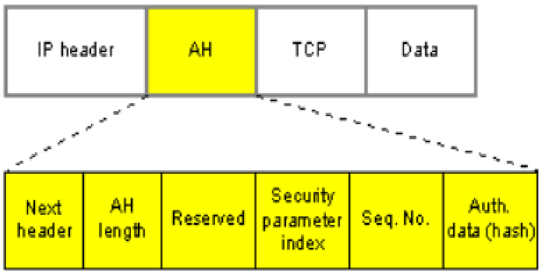

Fig3. IPsec Authentication Header

Encapsulating Security Payload (ESP)

AH ensures the integrity of the statistics in datagram, however not its privacy. When the data in a datagram is "in your eyes best," it could be further included the usage of ESP, which encrypts the payload of the IP datagram.

Both ESP and AH protocols may be utilized in both tunnel or in shipping mode. The shipping mode leaves the unique IP header untouched and is used to defend only the upper-layer protocols. As an end result, it may simplest be used between two cease-hosts which can be additionally cryptographic cease points. The tunnel mode protects the complete IP datagram by use of encapsulation and can be used to protect traffic between two cease-hosts, or gateways (e.g. Routers, firewalls), or among an end-host and a gateway.

Performance Overheads of IPsec

IPsec incurs 3 sets of overheads such as,

- Startup Overhead
- Wire Protocol overheads
- Speed of Encryption overheads

IV. PERFORMANCE ANALYSIS OF IPsec-BASED VPN SERVERS

We focused on the overheads for individual security operations for IPsec protocols in a single client setting. We utilized two methods to analyze the performance impact of the ESP protocol, the IKE protocol, various encryption algorithms, and various cryptographic key sizes.

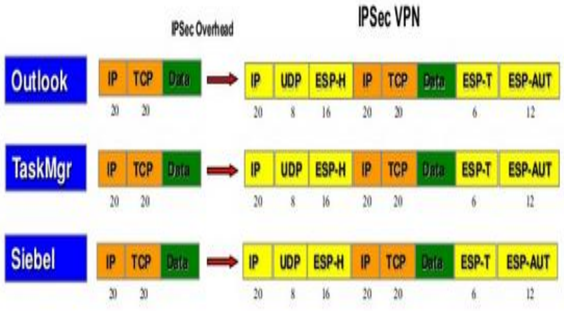

Fig4. IPsec VPN overheads

Here,

- IPsec adds 62 bytes of overhead to every packet
- Overhead mounts with multiple applications
- IPsec is not designed for wireless data─tunnel

"breaks" on roam or loss of coverage

- IPsec VPNs are very complex and cumbersome to maintain

The goal was to compare the difference between a native TCP/IP implementation and when IPsec is in use. We measured how the file transfer time changed as the number of concurrent VPN client connections increased from one to six.

IKE Protocol:

The goal of the IKE protocol is to establish and maintain shared security parameters and authenticated keys between the two IPsec end points. It uses a series of messages contained in UDP datagram's, typically directed to port 500.The IKE protocol consists of two distinct phases. The first phase establishes a symmetric IKE key between the initiator (typically, VPN client) and the responder (typically, VPN server). This key is used within the 2nd phase to establish asymmetric IPsec key to be used all through ESP or AH encapsulation. The IKE Security Association (SA) defines the way in which two quit factors communicate; as an instance, this includes agreeing at the set of rules used to encrypt visitors, the hash algorithm, and the mechanism to authenticate the alternative endpoint. IKE defines 3 categories of authentication strategies (with four man or woman strategies) for phase one: the first method uses pre-shared keys, the subsequent approach makes use of virtual signatures (the usage of RSA or other virtual signatures algorithms), and the last two methods use public key encryption. In both levels, the Diffie-Hellman protocol is completed on the way to alternate the keys. For better protection at some stage in longer VPN periods, IPsec provides a mechanism to periodically refresh each IKE and IPsec keys. Refreshing the IKE key entails running each IKE phases but clean the IPsec key best calls for going for walks the second one phase once more.

Advantages of IPsec Protocol:

- In a firewall/router, IPsec provides strong security to all traffic entering the network.
- IPsec protocol is below transport layer so, transparent to applications
- No need to upgrade applications when IPsec is used, if IPsec is implemented & configured in user machines

V. CONCLUSION

In this paper, we evaluated the performance of IPsec-based VPN servers in a multiple client setting as well as we found that IPsec does not scale as well as the native TCP/IP implementations. This analysis makes a strong case for performance optimization. Since IKE overheads can be a significant percentage of the overheads, especially for the VPN connections that last for a short duration, we focus on optimizing IKE in this paper.

REFERENCES

[1] G. Apostolopoulos, V. Peris, and D. Saha. Transport LayerSecurity: How much does it really cost? In IEEE INFOCOM, June 1999.

[2] C. Coarfa, P. Druschel, and D. Wallach. Performance analysis of TLS Web servers. In NDSS, February 2002.

[3] X. Corporation. Openswan Web-site, 2004. http://www.openswan.org/.

[4] Debian Linux Web-site. http://www.debian.org/.

[5] N. Doraswamy and D. Harkins. IPsec: the new securitystandard for the Internet, intranets, and virtual private networks. Prentice Hall, 1st edition, 1993.

[6] G. C. Hadjichristophi, N. J. Davis IV, and S. F. Midkiff.IPsec overhead in wireline and wireless networks for weband email applications. In 22nd IEEE IPCCC, April 2003.

[7] D. Harkins and D. Carrel. The Internet Key Exchange (IKE).RFC 2409 (Proposed Standard), Nov. 1998.

[8] S. Kent and R. Atkinson. IP authentication header. RFC2402 (Proposed Standard), Nov. 1998.

[9] S. Kent and R. Atkinson. IP encapsulating security payload.RFC 2406 (Proposed Standard), Nov. 1998.

[10] S. Kent and R. Atkinson. Security architecture for the internet protocol. RFC 2401 (Proposed Standard), Nov. 1998.Updated by RFC 3168.