IPSec Overhead in Wireline and Wireless Networks for Web and Email Applications

George C. Hadjichristofi

Thesis submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Master of Science
in
Computer Engineering

Dr. Nathaniel J. Davis, IV,Chair

Dr. Scott F. Midkiff,

Dr. John K. Shaw

November 29, 2001
Blacksburg, Virginia

Keywords: IP Security, 3DES, MD5, SHA1, ESP, AH

IPSec Overhead in Wireline and Wireless Networks for Web and Email Applications

George C. Hadjichristofi

Dr. Nathaniel J. Davis,IV, Chair
Computer Engineering

(ABSTRACT)

This research focuses on developing a set of secure communication network testbeds and using them to measure the overhead of IP Security (IPSec) for email and web applications. The network testbeds are implemented using both wireline and wireless technologies. The testing involves a combination of authentication algorithms such as Hashed Message Authentication Code-Message Digest 5 (HMAC-MD5) and Hashed Message Authentication Code-Secure Hash Algorithm 1 (HMAC-SHA1), implemented through different authentication protocols such as ESP and AH, and used in conjunction with the Triple Digital Encryption Standard (3DES). The research examines the overhead using no encryption and no authentication, authentication and no encryption, and authentication and encryption. A variety of different sizes of compressed and uncompressed files, are considered when measuring the overhead.

The testbed realizes security using IPSec to secure the connection between different nodes. The email protocol that is used is the Simple Mail Transfer Protocol (SMTP) and the web protocol considered is the Hyper Text Transfer Protocol (HTTP). The key metrics considered are the network load in bytes, the number of packets, and the transfer time.

This research emphasizes the importance of using HTTP to access files than using SMTP. Use of HTTP requires fewer packets, lower network loads, and lower transfer times than SMTP. It is demonstrated that this difference, which occurs regardless of security, is magnified by the use of authentication and encryption. The results also indicate the value of using compressed files for file transfers. Compressed and uncompressed files require the same transfer time, network load and number of packets since FreeS/WAN IPSec does not carry any form of compression on the data before passing it to the data link layer. Both authentication algorithms, HMAC-MD5 and HMAC- SHA1, result in about the same network load and number of packets. However, HMAC-SHA1 results in a higher transfer time than HMAC-MD5 because of SHA1's higher computational requirements. ESP authentication and ESP encryption reduce the network load for small files only, compared to ESP encryption and AH authentication. ESP authentication could not be compared with AH authentication, since the FreeS/WAN IPSec implementation used in the study does not support ESP authentication without using encryption. In a wireless environment, using IPSec does not increase the network load and the number of transactions, when compared to a wireline environment. Also, the effect of security on transfer time is higher compared to a wireline environment, even though that increase is overshadowed by the high transfer time percentage increase due to the wireless medium.

Acknowledgments

I would like to thank my advisor, Dr. Nathaniel Davis, who gave me the opportunity to carry out this research, and get involved in an area that greatly interests me. The benefits I received as a graduate research assistant made my graduate studies possible. I would also like to thank him for guiding me throughout my graduate studies and taking time out of his busy schedule to advise me, whenever I would get desperate. I would like to thank Dr. Scott Midkiff for originally getting me interested in this research and helping me whenever I needed extra advice at the different stages of my research. I would like to thank the third member of my advisory committee, Dr. John Shaw for his gracious service. I would also like to thank all the friends that helped me, especially Erik Hia and Adel Alfahad. I greatly appreciate their assistance.

This work was supported in part by the Office of Naval Research through the Navy Collaborative Integrated Information Technology Initiative. This support is gratefully acknowledged.

Table of Contents

List of Figures

List of Tables

Chapter 1. Introduction

1.1 Background

Since the beginning of time, people have always had the natural desire to keep secrets [9]. Some of the secrets they kept for themselves but some they communicated with others. The desire to communicate secrets with more people gave rise to the need for some sort of encryption, since it became more difficult to keep a secret, a secret. Another concern that developed was authentication. People could not decipher whether a certain document was from the original author or if it was just forged. Even though communication technology has developed from papyrus to the telegram, telephone, fax, and email, the issues of encryption and authentication still constitute a major concern.

Nowadays, the Internet connects millions of people and allows them to communicate via data, voice, and video. In this way, lots of messages can be sent cheaply and reliably from one party to others. Sometimes sensitive information is transmitted, that requires security. The security mechanism has to keep this information private and one way to achieve this goal is by securing the medium over which the information travels. Information on the Internet is carried using the Internet Protocol (IP), which does not provide any privacy or other security. As a result Internet Protocol Security (IPSec) was implemented to integrate security into IP.

The IPSec protocol, and its sub-protocols, ESP and AH, were developed by the Internet Engineering Task Force (IETF) and it is being widely implemented for IPv4. It will also be required as part of IPv6 [5]. IPSec is an ever growing standard for providing secure communication over IP. It uses authentication to ensure that packets are from the indicated sender and have not been altered in transit, and encryption to prevent unauthorized reading of packet contents. It is an extensible and complete network security solution. It uses two groups of traffic security protocols, the Authentication Header (AH) and the Encapsulating Security Payload (ESP). The IPSec protocol allows implementation of the preceding two groups in different ways and permits use of different concurrent combinations. These combinations provide a set of security services such as access control, connectionless integrity, data origin authentication, protection against replays, (confidentiality) encryption, and a limited traffic flow confidentiality.

Currently, IPSec is the only protocol that can secure any and all Internet traffic. It enables end-to-end security so that every piece of information sent to or from a computer can be secured. It can protect any protocol that runs on top of IP such as TCP, UDP, and ICMP. It reduces the need to implement security protocols at higher layers, and allows per flow or per connection security, enabling fine-grained security control. In addition, the overhead of key negotiation decreases considerably as multiple transport protocols and applications can share the key management infrastructure provided by the network layer.

There are limitations, however. IPSec is a point-to-point protocol and, thus, cannot be used for multicasting. In multicasting, there are many recipients for a single packet and often many senders to a particular (single) multicast address. The Internet Key Exchange (IKE) will not work, as there must be a shared group key.

1.2. Research Goals

This research evolved from work on the Navy Collaborative Integrated Information Technology Initiative (NAVCIITI) project sponsored by the Office of Naval Research. The "Network Protocol Interoperability" task, Task 3.1 of the NAVCIITI project, investigates network infrastructure for the Virtual Operations Network (VON), which is a rapidly-deployable internetwork of naval vessels at sea [12]. The computer network security area of this task focuses on the problem of enabling interoperability between heterogeneous networks that may belong to and be managed by different allies and coalition partners. This research addresses the security aspects for establishing a VON. A VON requires the creation of tunnels to send data packets securely over the Internet, or in the case of the Navy, to different coalition partners. Since IPSec is at the network layer, it provides subnet-based security. Everything passing through the untrusted network is encrypted by the IPSec gateway and decrypted by the gateway at the other end. This way, IPSec establishes the secure tunnel and connects two distinct and disparate networks that form a VON.

A reasonable network security solution must provide message authentication, integrity, and confidentiality. Furthermore the solution must be cost effective and promote interoperability, by using standard, commercial, off-the-shelf components. Therefore, it is important to understand the functionality and "cost" of using IPSec in different environments.

This research focuses on the overhead introduced by IPSec for web and email applications. The important questions to be answered can be posed as follows.

1) *What is the percentage increase in overhead when using no authentication and no encryption, versus using authentication and no encryption or using both authentication and encryption?* Different configurations pose different constraints on a network depending on the network load, number of transactions, and transfer time.

2) *Does ESP encryption and authentication induce more overhead versus ESP encryption and AH authentication?* AH may have higher overhead than using authentication in ESP, but it provides better check of integrity. Depending on the overhead induced by each method, a network operator may choose to sacrifice some integrity checking to enable better bandwidth utilization.

3) *Does ESP for authentication require more overhead than AH for authentication?* A network operator may want to use authentication without encryption where the data is

public but wants to be sure that the data is unaltered and from the indicated source, where strong encryption is provided at the link level, or where strong encryption is provided in other protocols above IP. Unlike AH authentication, ESP authentication does not authenticate the outer IP header when used in tunnel mode.

4) *Which algorithm requires more overhead, HMAC-MD5 or HMAC-SHA1?* Different authentication algorithms have different overhead. A network operator can select the algorithm to used based on the overhead.

5) *What is the network overhead for security for compressed and uncompressed files?* The secure transfer of different file types, such as compressed or uncompressed files, may require different system resources and network bandwidth. Depending on the overhead difference, a network operator may have to manage the number of compressed or uncompressed sent at different intervals and from different servers.

6) *What is the security overhead for HTTP and SMTP?* Different protocols have different overhead for sending files over the Internet. A network operator may have to decide whether it is better to use E-mail to send files to users versus letting them access the files via HTTP or vice versa.

7) *What is the overhead imposed when IPSec is used over wireless?* Securing traffic over wireless instead of wireline links may increase the overhead of IPSec. It is important to know the amount of extra overhead induced by wireless before deploying a secure wireless network.

The principle metrics of interest for evaluating the overhead are the network load, the number of packets, and the transfer time. The answers to the questions above have been realized by first implementing a simple network running IPSec, as explained in Chapter 3, and looking at its impact on the network. The simple network was then expanded by integrating 802.11 wireless and looking at the resulting impact on the overhead. Finally, both the first and second testbeds were configured so that Testbed 2 used only a wireline medium and Testbed 1 used only a wireless medium to transfer data (Section 3.2.1). Thus, transferring the same data through different media provided a means of further analyzing the impact of each medium.

The remainder of this thesis describes in detail how a solution to this problem was developed and how the solution was obtained.

1.3. Document Overview

This chapter introduced a brief history of IPSec to illustrate the origin of the problem that is addressed by this research. It also explained the goals of this research and gave a brief description of the solution. Chapter 2 presents an overview of IPSec, ESP, AH, 3DES, MD5, SHA1, and IKE. Chapter 3 presents the methodology employed to meet the research objectives. Different assumptions and limitations are also discussed. The

process of developing solutions to the research questions was decomposed into four steps: (i) testing IPSec over wireline connections using Testbed 1, (ii) testing IPSec over wireline and wireless connections using Testbed 2, (iii) repeating tests with Testbed 1 with a wireless connection, and (iv) repeating tests with Testbed 2 with a wireline connection. The results from each step were brought together to give an overall solution. Chapter 4 contains the experimental results and discussion of the results. Chapter 5 draws conclusions based on the results of this research and offers recommendations for further work.

Appendices A through N contain the data and statistics of all experiments. Appendices O through Q contain the information about the hardware and software configuration of the different testbeds.

Chapter 2. Background

This chapter gives a brief overview of the IPSec protocol and presents issues related to implementing a secure network using IPSec. Section 2.1 presents an overview of IPSec, its purpose, its advantages, and its disadvantages at the network layer. Section 2.2 describes the IPSec architecture. Section 2.3 describes the two protocols used to implement IPSec in greater detail. Their similarities and differences are discussed and compared. Section 2.4 gives a brief overview of MD5 and SHA1, the authentication algorithms used in IPSec. Section 2.5 describes the encryption algorithms, DES and 3DES, that are proposed for IPSec. Section 2.6 explains the operation of the IKE protocol. Finally, Section 2.7 briefly describes the Identification protocol.

2.1 IPSec Overview

IPSec is a way of protecting IP datagrams. It provides connectionless data integrity authentication, data confidentiality, anti-replay protection, data origin authentication, and limited traffic flow confidentiality [10, RFC 2401]. IPSec is chosen for this research because it is implemented at the network layer. At the network layer, IPSec can provide subnet base security and create virtual private networks (VPNs). Another advantage is that IPSec decreases the overall key negotiation overhead since any transport protocols and applications working above the network layer can share the key management infrastructure. Also, IPSec avoids the explosion of complexity in the implementation of security at higher layers, since the security implementation at higher layers tends to be more complicated than at lower layers [9]. Finally, using IPSec removes the need to implement security separately in every application since it can protect any protocol or application data using the network layer.

However, when implementing security at the network layer, it is much more difficult to handle issues such as the user-based security control on a multi-user system. Despite this weakness, it is assumed that, within a subnet, other mechanisms can be used to control users by securing appropriate higher protocol layers.

To protect IP datagrams, the IPSec protocol suite provides security by defining header extensions to standard IP [1]. The header extensions support two protocols, the AH protocol and the ESP protocol. AH provides data integrity, proof of data origin, and anti-replay protection. However, ESP provides everything that AH provides, as well as data confidentiality and limited traffic flow control. The security of AH and ESP is dependent on the cryptographic algorithms used, such as MD5 and DES. These services require shared keys, which can either be negotiated manually or automatically. Manual keying scales poorly, so a dynamic way of negotiating security and generating shared keys, defined by the Internet Key Exchange protocol (IKE), is typically used.

2.2 IPSec Architecture

As mentioned above, IPSec is a suite of protocols including AH, ESP, IKE, ISAKMP/Oakley and various transforms [9]. IPSec defines how these different components interact with each other to implement the required functionality. Figure 2.1 shows how the different components in IPSec are linked. The ESP and AH documents define the protocols, the header formats, the packet processing rules and the various services that can be provided. However, they do not describe the transforms used to provide these capabilities. The different authentication algorithms, such as MD5, and encryption algorithms, such as DES, are used to authenticate and encrypt the data. The parameters used for encryption and authentication are defined in the Domain of Interpretation. The Security Policy (SP) is also an important part of a network. It determines which transforms two entities should use to communicate with each other. Based on the security policy, the key management generates and manages a key by using IKE. All of the parameters used by the negotiating entities are defined in the Domain of Interpretation.

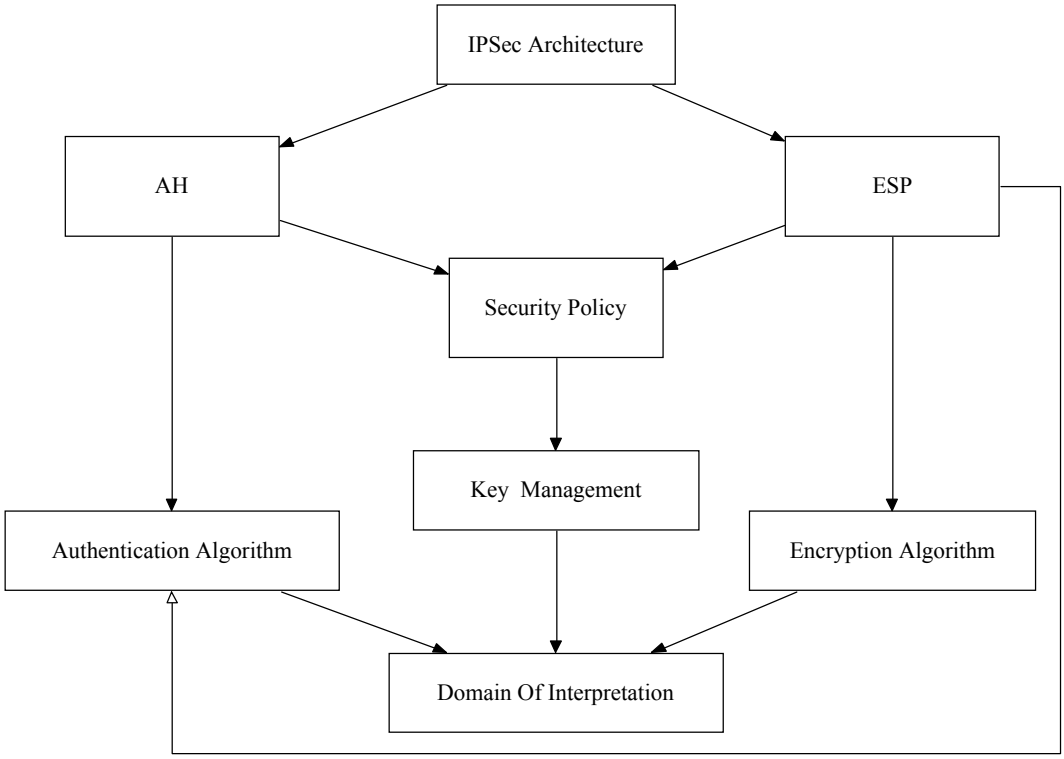


Figure 2.1. IPSec components and their relationship [10].

2.2.1 IPSec Implementation

IPSec can be implemented in end hosts and/or gateways. In end hosts, IPSec provides end-to-end security and per flow security and can authenticate a user when establishing

an IPSec connection. In gateways, IPSec is used to secure packets flowing between two networks when going through the Internet and to authorize and authenticate users that enter a VPN.

Implementations in end hosts can be classified into two schemes.

1) *Operating system integrated.* IPSec is integrated into the operating system. The advantages of this scheme are that it:
   - makes security on a per flow basis easier since IPSec and the network layer are joined together,
   - can take advantage of services provided at the network layer such as fragmentation, and
   - can support both IPSec modes (see Section 2.2.2).

2) *Bump In The Stack (BITS).* IPSec is implemented as a layer between the data link and the network layer. The advantage of this implementation is that it is independent of the features of the operating system used and it can provide more advance solutions. The disadvantage is that it has to implement all the features of the network layer, as it becomes more difficult to handle issues such as fragmentation [9].

Implementations in gateways can also be classified into two schemes.

1) The *Native Implementation* scheme, which is similar to the operating system integrated scheme described above.

2) The *Bump In The Wire* (BITW) scheme, which is similar to the BITS scheme described above. It is implemented on a device used specifically to secure packets and is attached to the physical layer. BITW is not considered a good solution since it is impractical to attach devices to every interface of a gateway.

2.2.2 IPSec Modes

IPSec can either be implemented in the transport mode or the tunnel mode. If the different protocols, such as AH and ESP, are considered, then there are actually four different combinations that can exist.

1) AH in transport mode
2) ESP in transport mode
3) AH in tunnel mode
4) ESP in tunnel mode

The transport mode in AH and ESP protects the IP payload, whereas the tunnel mode protects the full IP packet. The transport mode is used when the desired security is end-to-end. Figure 2.2 shows the format of packets for the transport mode.

IP header	Authentication Or Encryption Protocol	IP Payload (TCP+ Data)

Figure 2.2. Transport mode packet format.

The tunnel mode is used when the final destination of packet can be different from the security end point. Figure 2.3 shows the packet format for the tunnel mode. This research focuses on tunnel mode since it can be used to provide subnet-based security, creating VPNs for different parties.

Outer IP header	Authentication Or Encryption Protocol	IP Packet (Inner IP+ TCP+ Data)

Figure 2.3. Tunnel mode packet format.

2.2.3 Security Associations (SA)

Security associations are the contract between two communicating entities to provide inherent security features. They define the IPSec protocols, the transforms, the keys, and the key management used. An SA is unidirectional, meaning that different SAs are kept for inbound and outbound processing. All SAs are stored in the SA database (SADB), which works in conjunction with the Security Policy Database (SPD) (see Section 2.2.5).

2.2.4 SA Management

SAs can be created and deleted either manually or automatically. With manual keying, two parties agree on the parameters of an SA offline. The negotiation of all the parameters required for IPSec is done manually. Manual keying is usually used on a small scale or for testing. It is usually considered less secure and prone to errors. Automatic keying is done through an Internet standard key management protocol such as IKE. The IPSec kernel calls IKE when there is a need to establish a secure connection. The IKE negotiates the SA with the desired destination, and creates the SA depending on the policy used [9].

2.2.5 Security Policy (SP)

The SP determines the kind of services that can be used for a packet. It defines how IP packets are treated, which protocols to use, in which modes, and with which transforms. The SP can be different for inbound and outbound packets. Its management is usually

done by modifying the SPD, which is stored in the kernel. The IPSec implementation provides an interface to manipulate the SP.

2.3 IPSec Protocols

2.3.1 ESP

The Encapsulating Security Payload is a protocol header that goes into an IP datagram to secure the datagram. The set of services provided depends on the options chosen at the time of the configuration. As mentioned above, ESP can be chosen to provide confidentiality, data origin authentication, integrity, anti-replay protection, and limited traffic flow confidentiality. Confidentiality is usually applied with authentication and integrity so that the traffic is not vulnerable to certain type of attacks, such as reading encrypted data and hijacking sessions, as described by Bellovin [11]. The anti-replay service is only effective if the receiver checks the sequence number. To obtain traffic flow confidentiality, the tunnel mode must be used and implemented at the gateways, where it is possible to mask the true source and destination addresses.

2.3.1.1 ESP Header

The format of the ESP header is shown below in Figure 2.4. The protocol header immediately preceding the ESP header contains the value of 50 in the protocol field of the IPv4 header to indicate that an ESP header comes after it.

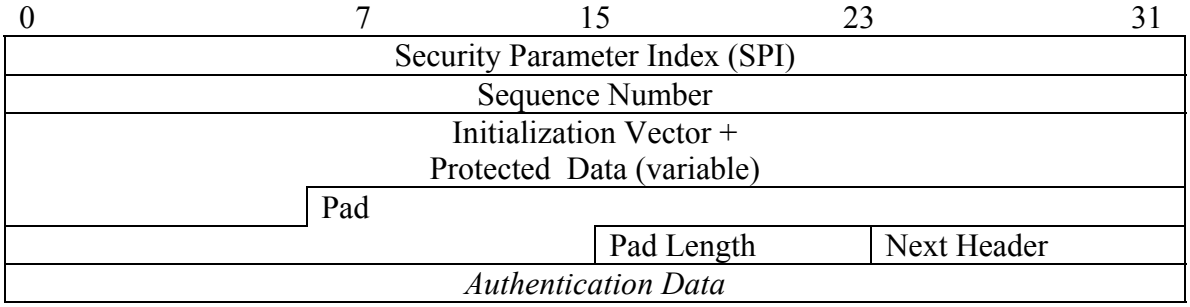


Figure 2.4. The ESP header and trailer.

The *Security Parameter Index* in Figure 2.4 is an arbitrary number obtained during the key exchange by the destination. It is only authenticated and it is used together with the protocol and destination fields in the preceding IP header to identify the SA to be used for the packet. The *Sequence Number* is authenticated but not encrypted since it does not expose any secrets. It provides anti-replay services to the ESP. The protected data has variable length and it also contains the *Initialization Vector* required by the encryption algorithm. The encryption algorithm usually used is the Data Encryption Standard in Cipher Block Chained mode (DES-CBC). The *Pad* is used to maintain data boundaries since some modes of encryption algorithms require that the input to the cipher be a

multiple of its block size. The *Pad Length* indicates how much pad has been added. The *Next Header* states the kind of data contained in the payload. The data usually depends on the mode used. If it is the transport mode, then the value is 6 denoting TCP. If tunnel mode is used, then the value is 4, indicating IP-in-IP encapsulation. The *Authentication Data* field holds the result of the data integrity check.

2.3.1.2 ESP Modes

ESP can be employed in the transport mode or the tunnel mode. The transport mode provides protection to the upper layer protocols, but no protection for the IP header. The tunnel mode provides protection for the entire IP Packet and is useful for creating VPNs. The general layout of the ESP positioning for both the transport and tunnel mode is shown below in Figure 2.5. The ESP authentication field is not used when there is no authentication. The ESP trailer encompasses the padding, pad length, and the next header fields.

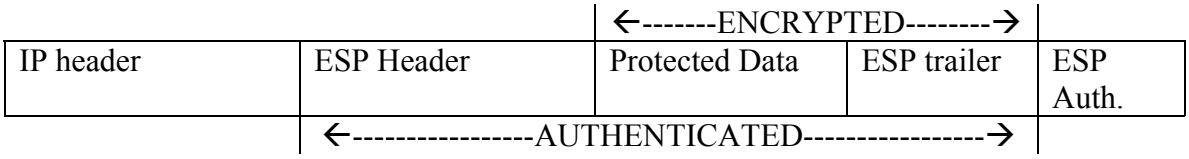


Figure 2.5. Packet layout using ESP.

This research focuses on the tunnel mode implementation of ESP as the focus is on VPNs. Therefore, the transport mode is not analyzed further. Figure 2.6 shows the ESP packet layout in tunnel mode. It is important to note that, in the tunnel mode, the entire IP packet is encrypted. ESP's authentication protects only the encrypted payload and not the IP header. If the IP header needs authentication, then AH should be deployed with ESP.

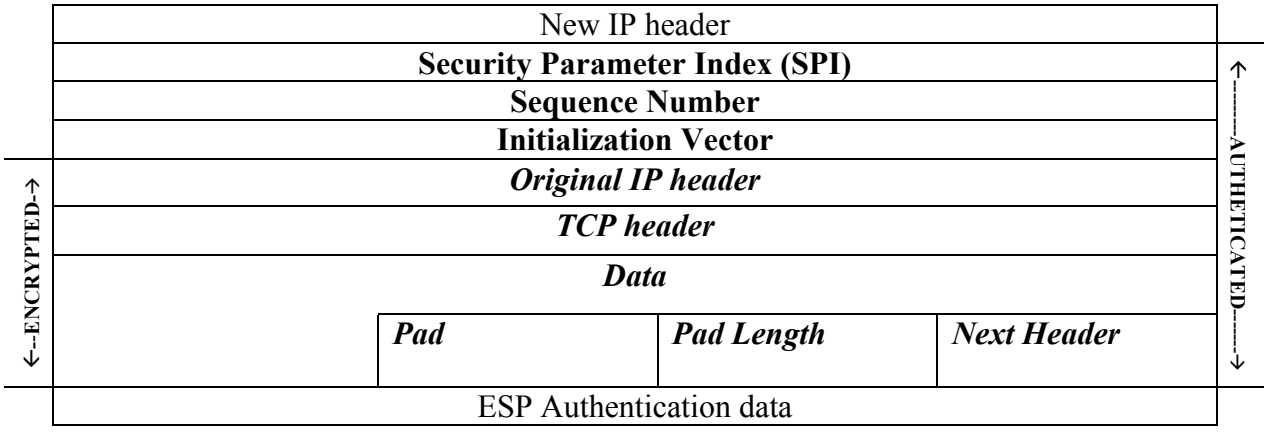


Figure 2.6. IP packet ESP authentication and encryption in tunnel mode.

2.3.2. AH

The Authentication Header is used to provide data origin authentication, connectionless data integrity, and protection against replays [10]. As was discussed for ESP, protection against replays is used if the receiver checks the sequence number. AH provides protection for upper layer protocols as well as the immutable fields of IP. This is because some fields may change when traveling from the sender to the receiver. Since the values of those fields cannot be predicted, the protection of AH in the IP outer header is partial.

A typical AH is shown in Figure 2.7. The *Next Header* field identifies the type of the next payload after the Authentication Header. The *Payload Length* specifies the length of the AH. The *Reserved* field is reserved for future use. It is usually set to zero. The *Security Parameter Index* is an arbitrary value that is used together with the destination IP address and security protocol to identify the Security Association for this datagram. The *Sequence Number* is a monotonically increasing number and it is always used even if the user chooses not to use anti-replay protection. The *Authentication Data* is a variable-length field that contains the integrity check value (ICV) for a packet.

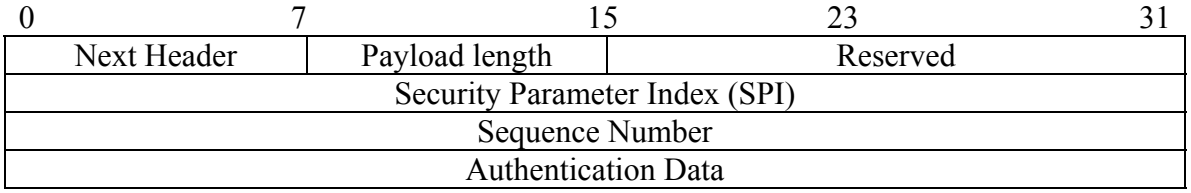


Figure 2.7. The AH.

2.3.2.1. AH Modes

Like ESP, AH may be employed in either transport or tunnel mode. The general layout of an IP datagram incorporating AH for both the transport mode and the tunnel mode, is shown in Figure 2.8. This research focuses on the tunnel mode implementation of AH as the focus is on VPNs. The packet layout for tunnel mode is shown in Figure 2.9.

Figure 2.8 Packet layout using AH.

New IP header	↑-------AUTHETICATED------→
Security Parameter Index (SPI)	
Sequence Number	
Initialization Vector	
Authentication Data	
Original IP header	
TCP header Data	

Authentication Data is not authenticated

Figure 2.9. Packet layout using AH for tunnel mode.

2.3.3 Overview of AH versus ESP

AH is used to provide data integrity, data origin authentication, and optional limited anti-replay services to IP. Unlike ESP, AH cannot be used to provide any encryption. In an IPSec implementation, if a network needs to use both authentication and encryption it can either use ESP to do both, or use AH for authentication and ESP for encryption (see Figures 2.5 and 2.8). The primary difference between AH and ESP authentication is the extent of coverage [10]. In the tunnel mode, ESP does not authenticate any IP header fields of the outer IP header. AH can provide a better check of integrity, if required, since it extends its protection to predictable fields of the outer IP header (see Figure 2.10). In this way, AH can authenticate the IPSec gateways that establish the IPSec tunnel.

0 7 15 23 31

Version	Payload Length	*Type of Service(*)*	Total Length
Identification			*Flags(*)* | *Fragment offset (*)*
Time to Live(*)		IP Protocol	*Header Checksum (*)*
Source IP Address			
Destination IP Address			

(*)=> Unprotected fields

Figure 2.10. IPv4 outer header fields protected by AH.

If AH authentication is used instead of ESP authentication, the AH header is inserted after the ESP header (see Figure 2.11). Even though this method expands the range of integrity check by authenticating the outer IP header fields on the packet, as described above, it has the disadvantage of introducing extra overhead. Therefore, depending on the need to authenticate the IPSec gateways, a network may choose whether to forgo the use of AH authentication.

IP Header	AH header	ESP header	Protected Data

Figure 2.11. AH and ESP packet format.

2.4 Authentication Algorithms

This research focuses on point-to-point communication. The authentication algorithm used for the ICV is usually specified by the SAs. Two parties that share a secret key may use Message Authentication Codes (MACs) to validate messages sent between them. Suitable authentication algorithms include Keyed-Hashing Message Authentication Codes (HMAC) based on symmetric encryption algorithms. HMAC provides a framework to incorporate any cryptographic hash function such as MD5 and SHA1. The cryptographic strength of the HMAC mechanism depends on the security provided by the underlying hash function [10-RFC 2104]. Even though MD5 has been found to be vulnerable to some attacks such as the collision search attack [14], the use of MD5 with HMAC is not compromised. SHA1 is a cryptographically stronger function since it produces a larger message digest than MD5, but takes a longer computational time [26].

The goal of HMAC is to use the available cryptographic hash functions without modifications and without degrading their performance. This allows for the ability to easily replace the functions in case they are not seen as secure at some point [26]. The two most widely used realizations of HMAC, when MD5 and SHA1 are used in IPSec, are denoted by HMAC-MD5-96 and HMAC-SHA1-96. The number "96" denotes the number of bits at which the output is truncated. After the message digest value is truncated to 96 bits, it is compared with the value in the authentication data field [25]. Truncating the output has the disadvantage of having fewer bits for the attacker to predict, but the advantage of giving less information about the hash result.

2.4.1 MD5

MD5 was developed by Rivest in 1991 [18]. It was designed as an extension to MD4. It is supposed to be slower than MD4 and more "conservative," thus providing more security. MD5 does not require a large substitution table and is relatively fast on 32-bit processors. The MD5 algorithm takes as input a message of any length and produces as an output a 128-bit "message digest" of the input. The conjecture is that it is computationally impossible to produce the same message digest from two different messages [27].

2.4.2 SHA1

SHA1 is a secret key authentication algorithm. SHA1 is a revision to SHA that was published in 1994 and corrects an unpublished flaw in SHA [17]. Its design is similar to the MD4 family of hash functions. The algorithm takes a message smaller than 2^{64} bits in length and produces a 160-bit authenticator value**.**

2.5 Encryption Algorithms

Encryption provides data confidentiality and limited traffic flow confidentiality. Two algorithms, DES and 3DES were originally used for securing Internet traffic, though the former is not preferred anymore, as discussed below.

2.5.1 DES

DES was first proposed in 1970. The cryptographic community considers DES insecure because its 56-bit key can now be discovered by a brute-force exhaustive attack in a relatively short period of time [16]. Therefore, DES is not sufficient for many security applications and is no longer used by the US government.

2.5.2 3DES

Triple-DES or 3DES has been used to replace DES. 3DES encrypts each 64-bit block of a message three times instead of one. The operations may involve two or three different keys. ANSI X9.52 defines a variety of ways of doing this encryption [15]. 3DES uses a key size of 112 bits in applications, as opposed to 56 bits for DES. The disadvantage of 3DES is that the encryption and decryption time per block is three times that of DES. However, 3DES is more secure to brute force attacks than DES.

2.6 IKE

IKE is a hybrid protocol for creating SAs dynamically and populating the SADB. It is based on the Internet Security Association and Key Management Protocol (ISAKMP) and implements part of the Oakley and SKEME key management protocols [9]. It uses the foundation of ISAKMP, the keying techniques of SKEME, and the modes of Oakley. As mentioned earlier, IKE is usually used in automatic keying of IPSec. IKE uses the two phases of ISAKMP. Phase 1 establishes an IKE SA and Phase 2 uses that SA to negotiate SAs for other protocols, such as IPSec. IKE has two Phase 1 exchanges, one Phase 2 exchange and two extra exchanges.

The two Phase 1 exchanges are the *main mode* and the *aggressive mode* and are used to create an IKE SA. The main mode uses six messages [9]. These include three messages for SA negotiation, a Diffie-Hellman exchange, a nonce exchange and the authentication of a user. The characteristic of main mode is identity protection by utilizing ISAKMP's negotiation capabilities.

The aggressive mode requires half the number of exchanges of the main mode. In the first exchange, the user sends his Diffie-Hellman public value, his nonce, his identity and his

list of protection suites. The negotiation party replies with his Diffie-Hellman public value, his nonce, his identity, his authentication payload, and his selected protection suite. Finally, the initiator then replies with his authentication data.

The aggressive mode limits the rich negotiation capabilities of IKE, such as not being able to offer different Diffie-Hellman groups in different protection suites. However, it can be used in cases where the two parties know each other's policy and want to create an IKE SA more quickly.

The Phase 2 exchange uses the *quick mode* to generate other SAs for other protocols such as IPSec. A quick mode negotiation uses three exchanges. The main reason for these transactions is to provide a liveness test similar to the three-way handshake of TCP. The optional and required attributes that IKE uses to negotiate in a Phase 2 exchange are defined in the DOI.

Thus far, the Phase 1 exchanges create the IKE SAs, and the Phase 2 exchanges create the IPSec SAs. IKE also offers two extra exchanges. The first extra exchange allows communicating parties to send information related error messages and SA status. The second extra exchange defines a new group exchange and allows communication entities to negotiate private groups and group identifiers for their own use [9].

2.7 The Identification Protocol

Sendmail uses an Identification protocol at the beginning of an email transfer [22]. The Identification Protocol, also known as Ident or the Ident Protocol, is used to determine the identity of a user of a TCP connection. It takes a TCP port number pair and it returns a character string, which identifies the owner of the connection on the server. A server listens for TCP connections on port 113. As soon as the connection is established, the server reads the data to determine the connection of interest. A system dependent user identifier for the connection of interest is sent as the reply. The server may continue to read/respond to multiple queries or shut down the connection [19].

2.8 Summary

This chapter gave a brief overview of IPSec, its protocols, and its authentication and encryption algorithms. The differences between AH and ESP were discussed and the advantages related to each choice were analyzed. A brief history of the hash functions and the encryption algorithms was also given, and the major differences between them were briefly mentioned. Finally, an overview of the IKE and Identification protocols was presented.

Chapter 3 presents the methodology that was employed to meet the research objectives. Different assumptions and limitations are discussed. The principle problem is

decomposed into four steps and the solutions of each step are brought together to give an overall solution.

Chapter 3. Designing and Developing the Methodology

3.1 Introduction

This chapter describes the methodology that was employed to measure the overhead of using IPSec with email and web protocols. It gives an overview of the testbed layouts, software and hardware considerations, and the data collection procedure.

3.2 Overview of the Methodology

The principal problem for investigating the overhead of IPSec was decomposed into six steps: (i) deciding what and how many testbed layouts should be used; (ii) deciding what software to install for each testbed; (iii) deciding any special hardware needed for each testbed, (iv) deciding what and how data should be recorded; (v) deploying the first testbed according to the previous steps analysis, getting some preliminary data and making required adjustments; (vi) adjusting any configuration after deploying all testbeds and obtaining the data sets. The data obtained from each testbed were then aggregated and used to calculate the IPSec overhead relative to the research goals, as specified in Section 1.2. The results or decisions taken in each step were applied in the next step.

3.2.1 Step 1: Testbed Layouts

A simple wireline testbed with two computers can be used to determine the relationship between the different algorithms, different protocols, and file types (see Figure 3.1). A 10-Mbps Ethernet local area network is used to connect the two hosts. The data was obtained by using a third computer, "Sniffer." Computers "West" (client) and "East" (server) were connected by an IPSec tunnel and a client server configuration was used between them.

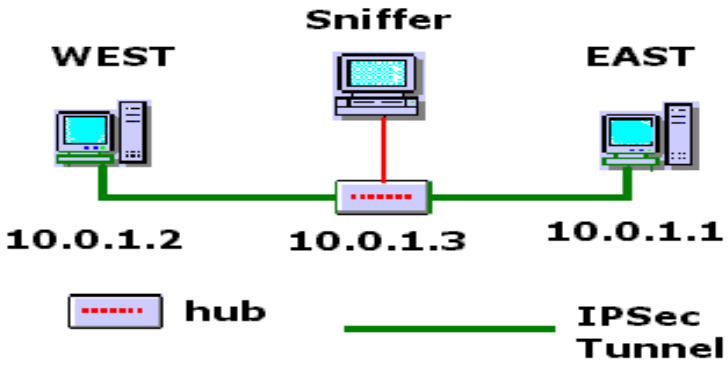


Figure 3.1. Testbed 1.

To examine the effect of a wireless link on IPSec overhead, Testbed 1 was expanded by adding a wireless node to form Testbed 2, as shown in Figure 3.2, and repeating the measurements done on Testbed 1. In this way, the effects of a heterogeneous configuration of wireline and wireless could be observed. The client for Testbed 2 was "Dusk," the wireless node, and the server was "East," as in Testbed 1. An IEEE 802.11 wireless local area network operating at 2 Mbps was used to connect Dusk to the wired network. The access point was connected to the wireless node instead of being connected to West due to the wireless card hardware incompatibility with Dusk. To provide a wireless link the wireless card was installed in West instead of Dusk. Even though, this configuration deviated from a typical wireless configuration where the access point is connected to the wired network, the hardware were not adjusted, since this configuration would not have impacted the measurements. The acquired data was secured in both the wireless and wireline media using IPSec.

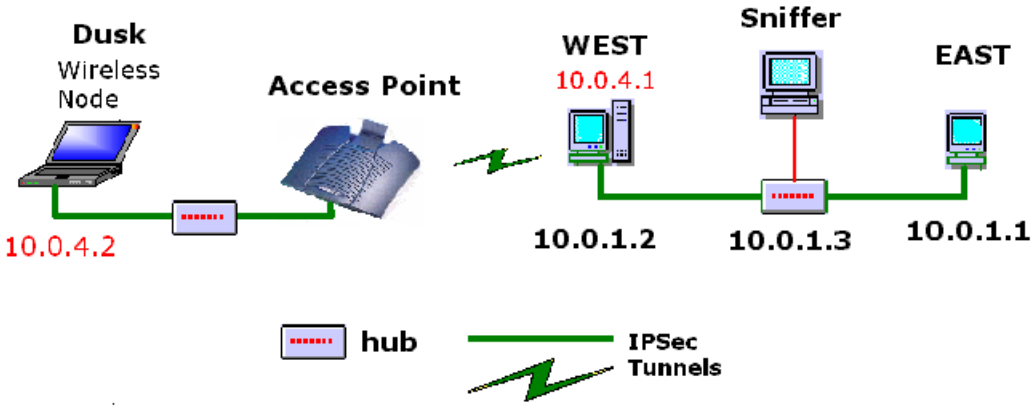


Figure 3.2. Testbed 2.

Since Testbed 2 was a combination of wireless and wireline media, the data obtained could not be compared with Testbed 1 because the client nodes, West for Testbed 1 and

Dusk for Testbed 2, were different. Therefore, an additional testbed was needed, Testbed 3. Testbed 3 extended Testbed 2 by connecting Dusk and West over a wireline network, as shown in Figure 3.3.

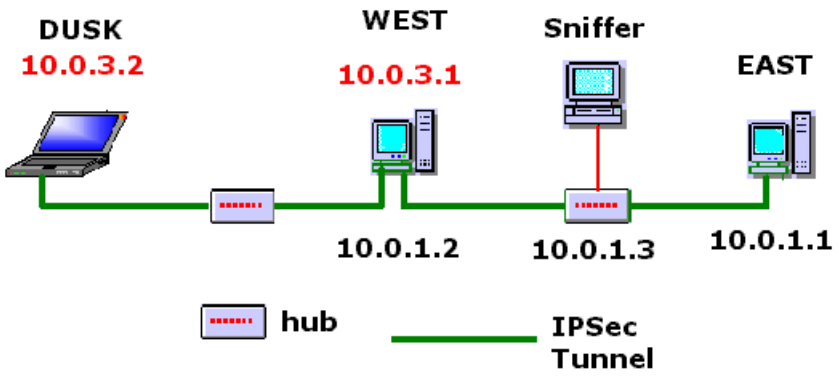


Figure 3.3. Testbed 3.

Another concern was that Testbeds 2 and 3 were a combination of wireline and wireless media. To observe IPSec overhead over *only* a wireless link, Testbed 1 was configured by using a wireless link between West and East as shown in Figure 3.4. The wireline medium between East and the access point provides a connection point for the Sniffer. Therefore, it was not counted as a wireline medium.

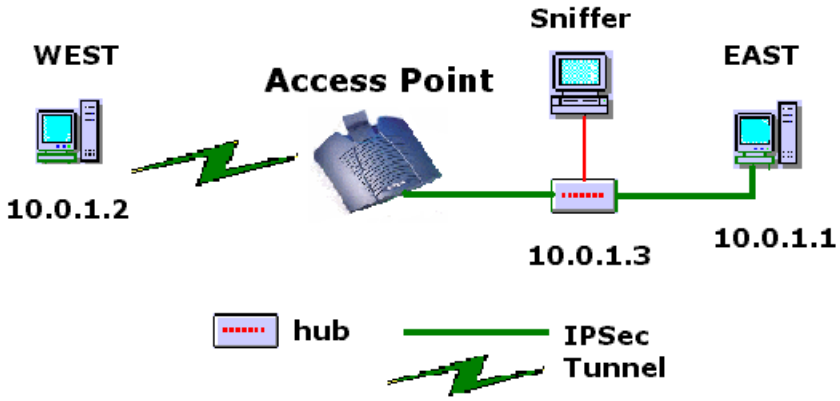


Figure 3.4. Testbed 4.

East was the server for all four testbeds. West was the client for Testbeds 1 and 4 and Dusk was the client for testbed 2, and 3. In this way, data from Testbed 1 could be compared to data from Testbed 4 and data from Testbed 2 could be compared to data from Testbed 3.

3.2.2 Step 2: Hardware

Step 2 involved the determination of the hardware needed for each testbed. The three computers of Testbed 1 each required an Ethernet card. Also a hub was required to connect them together. Testbed 2 required a wireless card that was installed on West and an access point (see Appendix O for details). The access point was connected to Dusk's Ethernet card using another hub. Testbed 3 required the installation of an additional Ethernet card into West to enable the wireline connection with Dusk. Finally, Testbed 4 did not require any additional hardware.

3.2.3 Step 3: Software

Step 3 involved the determination of the software needed for each testbed. Red Hat Linux was used for all testbeds. The freeware tool Ethereal was installed on host Sniffer. Ethereal was used as a network protocol analyzer to analyze the packets sniffed on the secure tunnels [8].

FreeS/WAN was chosen to provide Internet protocol security since it was freeware and it could run on Linux. FreeS/WAN is an implementation of IPSec and IKE. Several companies co-operate in the Secure Wide Area Network (S/WAN) project to ensure product interoperation. They make IPSec widespread by providing freely available source code, which can run on a range of machines [7]. FreeS/WAN IPSec was compiled and integrated into the operating system (Section 2.2.1). FreeS/WAN was installed on all computers except Sniffer.

3.2.4 Step 4: Data Acquisition

Step 4 was used to determine the scenarios, metrics, files and protocols to be used for the data acquisition. In order to be able to provide a solution for all the goals stated in Section 1.2, different combinations of protocols, algorithms were simulated on the testbeds as shown in Table 3.1. The Scenarios were determined by expanding on the different variations that existed with regards to the IPSec sub-protocols, ESP and AH, the authenticationa algorithms, MD5 and SHA1, and the encryption algorithm 3DES. The Internet Protocol version used for all scenarios was version 4.

The metrics that were to be recorded in each scenario were the network load in bytes per second, the number of transactions and the transfer time in seconds required to transfer a file from the server to the client. The network load and number of transactions were separated into the client to server and server to the client traffic. The number of transactions is the number of The file types that were used were "Zip" for compressed files, and "Doc" for uncompressed files. "Zip" files were created using Winzip and the "Doc" files using Microsoft Word. The files sizes for file transfers were 1KB, 10 KB,

100KB, 1MB and 10 MB. A table of the file sizes that were created is shown below (see Table 3.2).

Table 3.1. Scenarios for testing.

	IPv4	ESP authentication (No AH)		AH Authentication		ESP Encryption 3DES
		MD5	SHA1	MD5	SHA1	
Scenario 1	X					
Scenario 2	X			X		
Scenario 3	X				X	
Scenario 4	X	X				X
Scenario 5	X		X			X
Scenario 6	X			X		X
Scenario 7	X				X	X
Scenario 8	X	X				
Scenario 9	X		X			

The files were created so that the percentage difference between the actual size was small. The files were transferred using two protocols, SMTP and HTTP. The HTTP protocol was implemented by requesting a file from the Apache server running on East (see Appendix O). The SMTP protocol was implemented by sending an email from the server to the client using Netscape Communicator.

Table 3.2. File sizes and percentage differences.

		Uncompressed Files (.doc)		Compressed Files (.zip)	
File Size	Bytes	Size Used	Difference from actual Size /%	Size Used	Difference from actual Size /%
1 KB	1024	1024	0	1020	-0.391
10 KB	10240	10237	-0.029	10247	0.068
100 KB	102400	102400	0	102546	0.143
1000 KB	1048576	1049088	0.049	1049915	0.128
10 MB	10485760	10490368	0.044	10484820	-0.009

3.2.5 Step 5: Preliminary Data Collection And Adjustments

This step involved the deployment of Testbed 1 to check for any software limitations, get some preliminary data, and adjust the methods/scenarios for future data collections.

3.2.5.1 FreeS/WAN IPSec limitation

Testbed 1 was setup as shown in Figure 3.1. IPSec was run on East and West using both manual keying (Table 3.3) and automatic keying (Table 3.4) to determine the restrictions provided by the software. It was found that authentication or null encryption could only be used in manual mode. An automatically-keyed connection in Linux FreeS/WAN *always* used ESP encryption. This was preset and could not be turned off in the configuration file (Appendix P). The fact is that both encryption and some type of authentication in automatic mode *must* be used, in order to provide adequate security in every available configuration.

Furthermore, in the automatic mode, the authentication algorithm could not be specified every time. By default, a machine would ask to authenticate using MD5 first and then SHA1. So it was more likely for two machines to use MD5 than SHA1, unless one machine asked for SHA1 first. Therefore, manual keying was used to obtain the data, since it allowed for a finer granularity in the options and removed the need to filter the key negotiation overhead from the sniffed packets.

The comparison between AH authentication and ESP authentication was not run (Scenariors 8 and 9), since FreeS/WAN did not allow the use of ESP authentication without encryption. Only the first seven scenarios listed in Table 3.5 were simulated. The letters "M" and "A" signify which scenario was used in manual and automatic modes.

Table 3.3. Scenarios for Manual Keying.

Manual Keying			
	IPSec.conf Parameter	IPSec.secrets Parameter	WORKS
Scenario 1	NA	NA	✓
Scenario 2	Ah=hmac-md5-96	NA	✓
Scenario 3	Ah=hmac-sha1-96	NA	✓
Scenario 4	Esp= 3des-md5-96	NA	✓
Scenario 5	Esp=3des-sha1-96	NA	✓
Scenario 6	Esp=3des Ah=hmac-md5-96	NA	✓
Scenario 7	Esp=3des Ah=hmac-md5-96	NA	✓
Scenario 8	NA	NA	✗, null encryption disabled for ESP
Scenario 9	NA	NA	✗, null encryption disabled for ESP

Table 3.4. Scenarios for Automatic Keying.

Automatic keying			WORKS
	IPSec.conf	IPSec.secrets	
Scenario 1	NA	NA	NA
Scenario 2	NA	NA	✗, encryption must be used
Scenario 3	NA	NA	✗, encryption must be used
Scenario 4	Auth=esp	No change	✓, usually md5
Scenario 5	Auth=esp	No change	✓, usually md5
Scenario 6	Auth=ah	No change	✓, usually md5
Scenario 7	Auth=ah	No change	✓, usually md5
Scenario 8	NA	NA	✗ , encryption must be used
Scenario 9	NA	NA	✗ , encryption must be used

Table 3.5. Notation for the scenarios used.

Scenario 1	**➔1-[null]-[null]**
Scenario 2	**➔2M-[AH-MD5]-[null]**
Scenario 3	**➔3M-[AH-SHA1]-[null]**
Scenario 4	**➔4MA-[ESP-MD5]-[ESP-3DES]**
Scenario 5	**➔5MA-[ESP-SHA1]-[ESP-3DES]**
Scenario 6	**➔6MA-[AH-MD5]-[ESP-3DES]**
Scenario 7	**➔7MA-[AH-SHA1]-[ESP-3DES]**
M=offered in Manual Keying	*A= offered in Automatic Keying*

3.2.5.2 Data collection

Once the limitations of FreeS/WAN were assessed, different combinations of scenarios were simulated to investigate the network behavior and make any required adjustments. Two sets of data were collected: the first one by varying the IPSec virtual interface Maximum Transmission Unit (MTU) size and the second one with a fixed MTU size. MTU is the size of the largest packet that can be sent over a network interface.

3.2.5.2.1 Various MTU sizes.

The reason for varying the MTU sizes was to determine how the MTU size affects the overhead and what MTU should be used for the rest of the data collection. The MTU sizes decided upon were 600, 1500, 8000 and 16260 (default) bytes. These values were chosen by picking a value in between the default Ethernet interface MTU size (1500 bytes) and the default IPSec interface MTU size (16260 bytes), and a value smaller than the Ethernet interface MTU (1500 bytes). The combinations of scenarios that were used are shown in Figure 3.5. The variables of the protocol size and file type were fixed to avoid redundancy in the data collected.

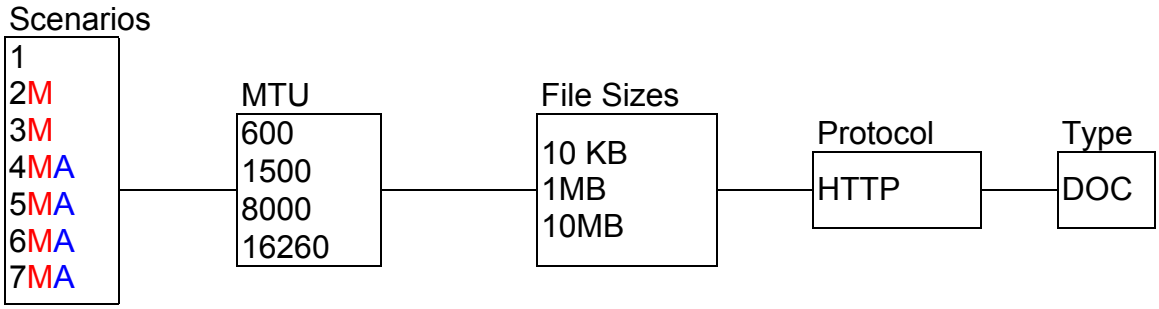


Figure 3.5. Various MTU data collection scenario combinations.

Initially, every combination of scenarios, MTU sizes, file sizes, protocol and file type was run 2 times to determine the load time and the number of transactions. The load and transactions were filtered to isolate the overhead from the client to server and vice versa. Since the transfer time was more likely to fluctuate, each scenario was run 2 more times to obtain more transfer time readings.

Once the data for various MTU sizes was obtained (Appendix A) the following observations were made:

- There was more fragmentation with MTUs of size 8000 and 16260 bytes than using an MTU of 1500 bytes. The IPSec MTU of 1500 caused an IPSec packet to be broken into 2 Ethernet packets.

- There were approximately 16 seconds TCP delay in closing transactions. Also, additional transactions from previous file retrievals were carried to the next file transfer. This was because the connection was kept alive by the server. The server configuration file had to be altered so that a connection was closed immediately after sending the data (Appendix O).

- An MTU size of 8000 bytes gave the fastest transfer time, the least network load in bytes, and the least number of transactions.

In order to determine whether the rest of the data should be recorded with an MTU size of 8000 bytes, the 8000 MTU size data was compared with the “ideal” MTU size data. The “ideal” MTU size was the maximum MTU size that caused no fragmentation. The “ideal” MTU size for the IPSec interface was found for all scenarios (Table 3.6). The lowest MTU size of 1438 bytes from all scenarios was used for the rest of the data collection, since it did not fragment for scenarios 2M-7MA.

Table 3.6. "Ideal" MTU size for IPSec Interface.

SCENARIOS	IPSec MTU
1-[null]-[null]	NA
2M-[AH-MD5]-[null]	1456
3M-[AH-SHA1]-[null]	1456
4MA-[ESP-MD5]-[ESP-3DES]	1446
5MA-[ESP-SHA1]-[ESP-3DES]	1446
6MA-[AH-MD5]-[ESP-3DES]	1438
7MA-[AH-SHA1]-[ESP-3DES]	1438
Ethernet MTU size =>1500	

After the combinations shown in Figure 3.5 were simulated again, the data was compared with the 8000 MTU size data (Appendix C). It was determined that the total network load and number of transactions of the 8000 MTU size was less than the "ideal" MTU (Table 3.7). The transfer time for the 1 MB and 10 MB files was approximately 15% less. This was mainly attributed to the Client to Server (CtoS) acknowledgments (ACKs). The client acknowledged every approximately 8KB instead of approximately 3KB. In addition, the server to client (StoC) load was up to 5% less due to a decrease in the per-packet header overhead. A fragmented packet carried only the IP header overhead of 20 bytes whereas the non-fragmented carried an IPSec header overhead of up to 62 bytes (1500-1438). Even though the 8000 MTU had a better performance, the ideal MTU was a better solution. In a larger network the CtoS ACKs are more likely to fluctuate. The server to client overhead is a better indication than the CtoS traffic. The ideal MTU size StoC transactions were lower. In addition, fragmentation caused by the 8000 MTU gave a higher transfer time. This can be seen in the transfer time of the 10 KB file, where the effect of the decreased CtoS ACKs was less.

Table 3.7. Percentage difference of 8000 MTU vs. "Ideal" MTU size data.

Scenario 7MA-[AH-SHA1]-[ESP-3DES]							
File Size	**Transactions/%**			**Network Load /%**			**Transfer Time/%**
	C to S	**S to C**	**Total**	**C to S**	**S to C**	**Total**	
10 KB	-33.33	9.09	-10	-25.62	-3.6	-6.09	16.67
1 MB	-77.90	4.59	-27.35	-77.67	-4.95	-8.71	-14.87
10 MB	-79.77	4.64	-27.08	-79.15	-4.95	-8.64	-15.47
(+) sign => 8000 MTU size data has a ***higher*** value than the "ideal" MTU size data (-) sign => 8000 MTU size data has a ***lower*** value than the "ideal" MTU size data							

3.2.5.2.2 Fixed MTU

The fixed MTU size for the IPSec interface was chosen to be the same as the Ethernet interface (1500 bytes). The combinations were simulated as shown in Figure 3.6. The purpose of this data set collection was to observe the behavior of the network and make

any adjustments possible. Each combination was repeated the same way as described in Section 3.2.5.2.1.

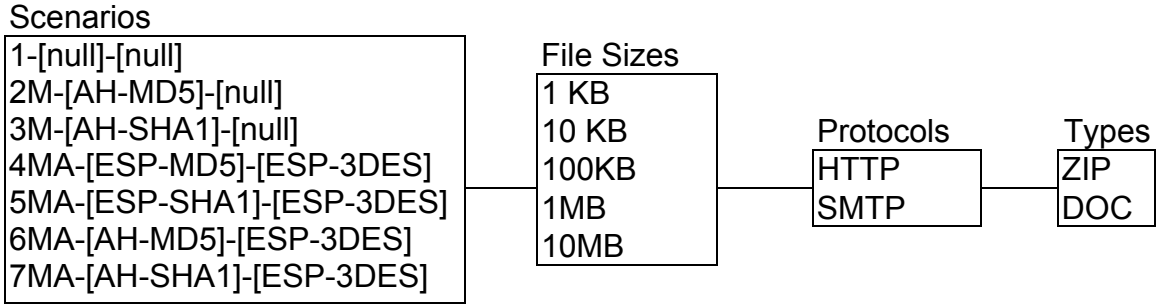


Figure 3.6. Combinations used for Fixed MTU data set collection.

The following observations were made:

- The transfer time of smaller files had a higher standard deviation and therefore required more than four readings.

- The last 2 transactions for the 1 KB file had a transfer time of 2-3 times longer than the actual time taken to send the rest of the packets. This delay occurred even after the connection was selected to shut down, as discussed in Section 3.2.5.2.1. These last 2 additional transactions were FIN-ACK packets from the CtoS to close the connection. The delay was because it took longer to execute the application that the Netscape Communicator software at the client had associated with the particular file type, than to transfer the file. Even when a NO-OP application like "cd" was associated with both file types, it was not fast enough to finish execution before the file was transferred. Since bigger files took longer to transfer, the last 2 transactions did not exist. Therefore, the last two transactions were not used in the transfer time data for the 1KB files.

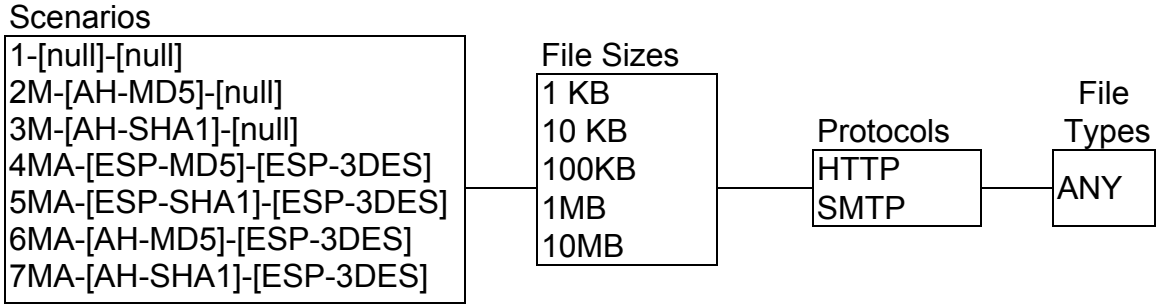
- The identification protocol overhead used by Sendmail at the beginning of an email transfer, affected the overall IPSec overhead for smaller files. Therefore the Ident data was isolated on the rest of the data inquiries to observe the overhead of IPSec with and/or without Ident.

- Compressed and Uncompressed files incurred the same amount of IPSec overhead.

As a result, the remaining data was taken using either "Doc" or "Zip" file types.

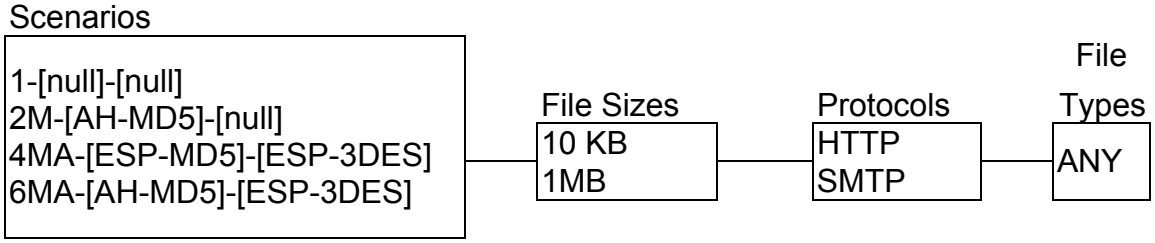
- The number of transactions and the network load in scenarios [2,3],[4,5] and [6,7] were approximately the same. Thus, this data was only recorded in Testbed 1. In Testbeds 2,3,4 the network load and transactions were only recorded for scenarios 2,4, and 6. Furthermore only two file sizes were used in Testbeds 2, and 3 to avoid data redundancy.

Therefore, Testbeds 1,2,3,4 were simulated using the combinations of scenarios, file sizes, protocols and file types shown in Figure 3.7 and Figure 3.8.



Scenarios 3M,5MA,7MA measurements for load and transactions skipped for Testbed 2

Figure 3.7. Combinations for Testbed 1,2.



Scenarios 3M,5MA,7MA measurements were skipped

Figure 3.8. Combinations for Testbeds 3,4.

3.2.6 Step 6: Final Adjustments

This step involved making any final adjustments after deploying all testbeds. The first significant behavior that was noticed was with regards to wireline Testbed 1 and wireless Testbed 4. More specifically, when transferring the 1MB and 10 MB files, West would generate more transactions from the CtoS. This was attributed to the fact that it was slow to handle the load from the server. As a result, it sent ACKs advertising a smaller window size. In order to provide a solution with a faster configuration, Dusk was used in place of West and the 1 MB and 10 MB sets of data of Testbed 1 were retaken (see Appendix H).

The second adjustment was with regards to the MTU for wireless Testbeds 2,4. The connection stalled with an Ethernet MTU size of 1500 bytes. To solve this problem, both the Ethernet MTU and the IPSec MTU were decreased by 8 bytes - 1492 bytes for the Ethernet interface and 1430 bytes for the IPSec MTU.

3.3 Conclusion

This chapter gave an overview of the 6 steps used to investigate the performance of IPSec. Step 1 covered the testbed layouts that were used to investigate the IPSec

overhead. Step 2 and Step 3 covered the hardware and software that were used on the testbeds described on Step1. Step 4 covered the scenarios required for testing, the files, and protocols used. Step 5 expanded on the previous steps, by deploying the first testbed, checking for software limitations, and making any adjustments needed for the rest of the data. Finally, Step 6 involved deploying all testbeds getting all the data and making final adjustments.

It was shown that an IPSec MTU size higher than the Ethernet MTU size caused more fragmentation but decreased the number of ACKs from the CtoS. It also decreased the network load by approximately 5 % due to the difference of the header overhead between the fragmented and non-fragmented packets. In addition, using an IPSec MTU size bigger than the Ethernet interface MTU size increased the transfer time.

The limitation of FreeS/WAN IPSec did not allow the collection of data for ESP authentication in order to be compared to AH authentication (see Section 3.2.5.1). Furthermore, the data collection was modified so that the Ident protocol was recorded as it impacted the overhead of smaller files (Section 4.6). The file type used was either compressed or uncompressed since it did not affect the IPSec overhead (Section 4.5). Also, the network load and number of transactions did not vary with the algorithm so the data for scenarios 3M, 5MA and 7MA were not collected (see Section 3.2.5.2.2 , Section 4.4). Testbed 1 data measurements for bigger file sizes were repeated with a faster configuration because West, the slower computer, sent extra ACKs decreasing the packet flow. Finally, a wireless medium required a lower MTU than the Ethernet MTU because the connection stalled.

Chapter 4 describes the methods used to analyze the data, with respect to the goals specified (Section 1.2). The data of all the testbeds was aggregated to evaluate the behavior of the IPSec with respect to the protocols, algorithms, file sizes and file types used.

Chapter 4 Discussion of Data Analysis

This chapter analyses the data acquired from each testbed. The data for the testbeds was aggregated to evaluate the behavior of the IPSec with respect to the protocols, algorithms, file sizes and file types used. The different behavior evaluations were carried out by presenting the variations on the metrics of network load, number of transactions and transfer time with regards to the goals specified in Section 2.1. The results were presented with the ident protocol overhead included or excluded from the measurements in order to examine the percentage increase in the IPSec overhead if the protocol was used or not used accordingly (see Section 2.7).

4.1 Overhead of Authentication with/without Encryption

This section investigates the overhead of using no authentication and no encryption, versus using authentication and no encryption or versus using both authentication and encryption. The data used to find the overhead change between no authentication and no encryption and only authentication or both authentication and encryption were primarily from Testbed 1. Testbed 1 had two sets of data: one using the client to be a slower computer, West, (see Appendix D) and one data set from the faster computer, Dusk (see Appendix H). The data from Testbed 1's fast configuration is referred to as "Testbed1 Extra" data since they were taken to account for the increase in overhead due to the Client ACKs for the 1 MB and 10 MB files (see Section 3.2.6). The percentage increase in overhead for securing data was calculated by finding the percentage increase in the network load, number of transactions and transfer time of each scenario compared to the no encryption and no authentication scenario (see Appendix I).

4.1.1 Number of Transactions

The percentage increase in the number or transactions for 1KB and 10 KB files was negligible (see Figure 4.1). For bigger file sizes, the percentage increased to approximately 5% for scenarios 2M and 7M. However, for the slow configuration and scenarios 4MA to 7MA, the percentage increase was 10% instead of 5%. This additional percentage increase was due to the increase in the number of CtoS ACKs from the slower computer, West, to slow down the server. This observation can be verified with the analysis of the faster computer data, using Dusk, in Testbed 1. Dusk was fast enough to process the packets received from the server and did not sent additional ACKs to slow down the server. Therefore, the percentage increase in the total transactions in the faster configuration stayed close to 5% for scenarios 4M to 7MA (see Appendix I).

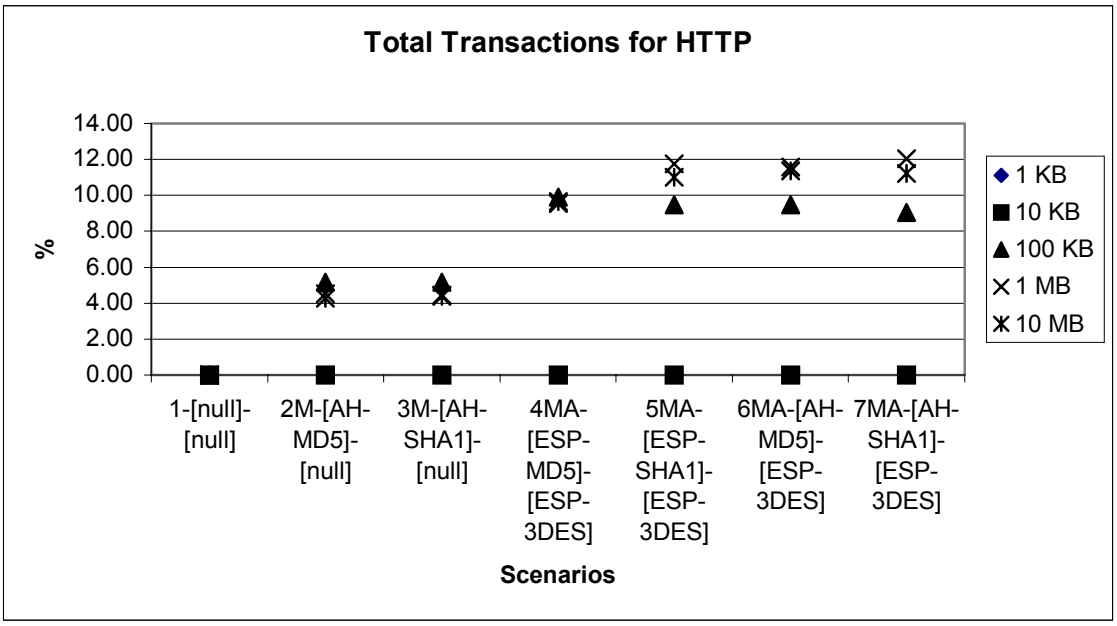


Figure 4.1. Total Transactions for HTTP for Testbed 1 (slow configuration).

The behavior of SMTP was similar to that of HTTP. For small file sizes, the number of transactions stayed the same regardless of the scenario used. For bigger file sizes, the percentage increase was again approximately 5% for scenarios 2M and 7M. However, the percentage increase in the number of transactions for the slow configuration increased from 5% to 20% for scenarios 4MA to 7MA (see Figure 4.2). This additional increase was again due to the CtoS ACKs to control the packet flow from the server. The reason for being 20% for SMTP, compared to the 10% of HTTP, was that SMTP had higher computational requirements than HTTP. These higher computational requirements slowed down West even further, decreasing its processing rate of the packets received from the server. As a result, more ACKs were required with SMTP than with HTTP to control the packet flow. This additional increase from 5% to 20% could not be verified with the faster configuration of Testbed 1, as done for HTTP above. The faster configuration did not give an overall percentage increase close to 5% (like HTTP) due to the 4k observation (see Section 4.8.1). According to the 4k observation, the packets sent from the StoC, followed a continuous pattern of two MTU-sized packets and a third one of smaller size. These three packets added to 4 KB chunks when considering the TCP packet for each one. Additional packets were not required when shifting from scenario 1 to 7MA because the extra load that was required for IPSec just filled the third smaller packet and generated a closer to full-size MTU packet. This resulted in the transactions for all file sizes and scenarios to fluctuate close to 0%. In a bigger network, it would be the case that Sendmail would prepare packets faster than the network would send them out and this observation would not exist. Therefore, the result of 0% increase in transactions for the faster configuration of Testbed 1 was ignored. The Ident protocol did not affect the percentage increase in the number of transactions when using encryption and/or authentication for both the fast and slow configurations (see Table 4.1).

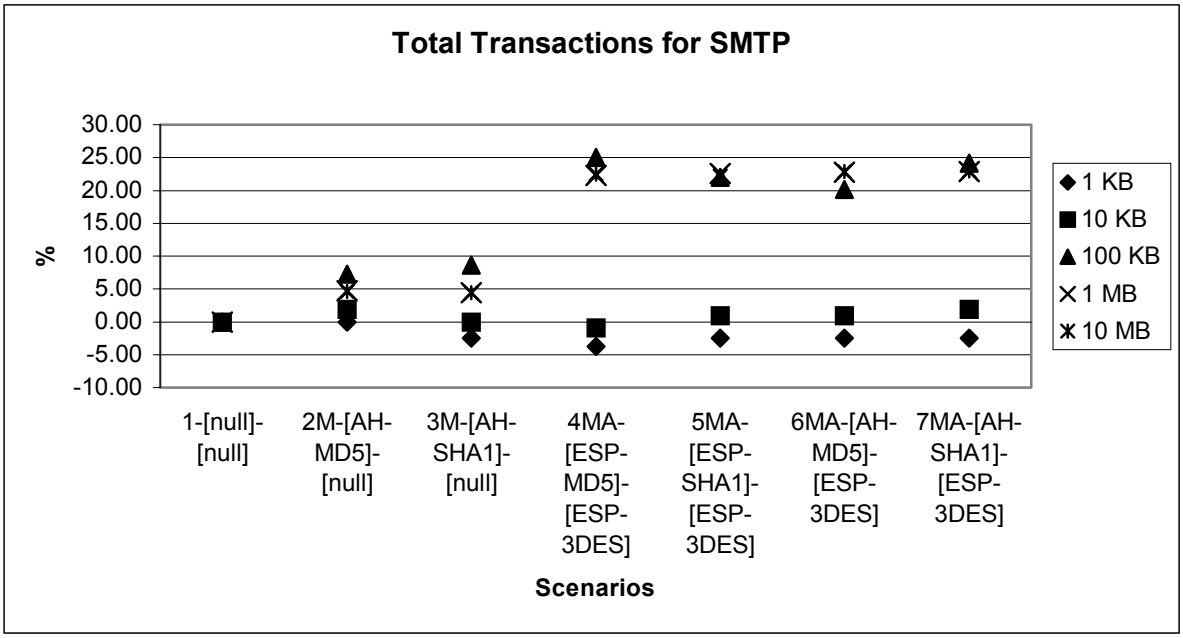


Figure 4.2. Total Transactions for SMTP for Testbed 1.

Table 4.1. Percentage difference of Ident for SMTP Transaction.

Slow Configuration Transactions = %SMTP Ident –% SMTP without Ident					
Scenarios	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	0.00	-0.53	-0.46	-0.03	0.00
3M-[AH-SHA1]-[null]	0.95	0.00	-0.54	-0.02	0.00
4MA-[ESP-MD5]-[ESP-3DES]	1.42	0.26	-1.57	-0.12	-0.01
5MA-[ESP-SHA1]-[ESP-3DES]	0.95	-0.26	-1.39	-0.13	-0.01
6MA-[AH-MD5]-[ESP-3DES]	0.95	-0.26	-1.27	-0.13	-0.01
7MA-[AH-SHA1]-[ESP-3DES]	0.95	-0.53	-1.52	-0.13	-0.01

4.1.2 Network Load

The trend of the percentage change in the network load from the CtoS and StoC, for different file sizes and different scenarios is shown below in Figure 4.3. The percentage of network load from the CtoS load increased due to the increase in the number of ACKs to control the traffic flow. The scenario of 2M had the minimum increase in the network load and the scenario of 7MA had the highest increase in the network load.

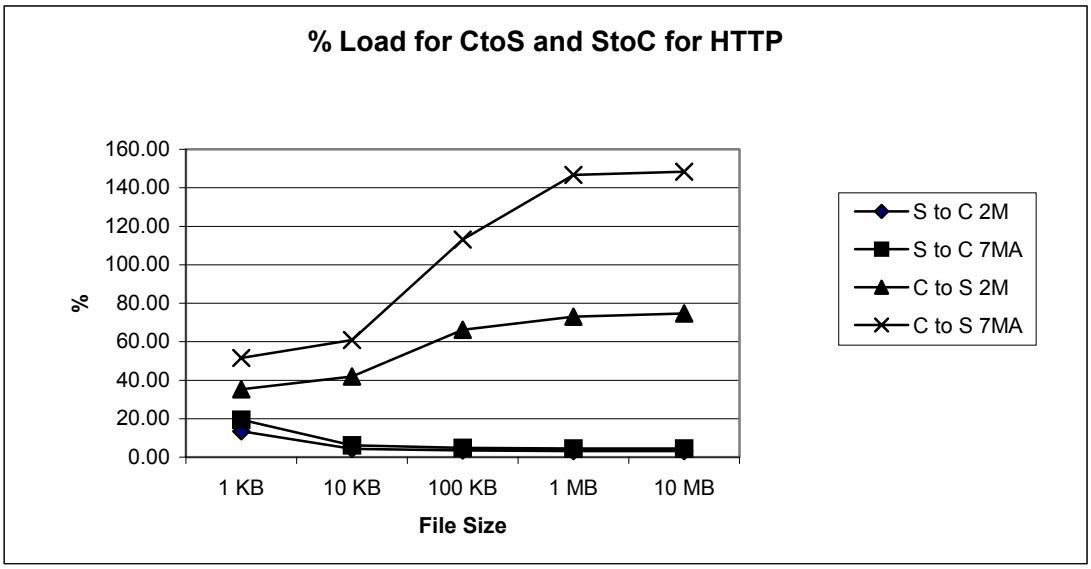


Figure 4.3. Percentage load increase for HTTP.

The load from the server to the client, for both the 2M and the 7MA scenarios, decreased as the file size increased. This was because the IPSec overhead took a smaller percentage of the overall load as the file size that was transferred increased. The general pattern for the percentage increase in network load with respect to all scenarios for different file sizes is shown in Figures 4.4 and 4.5. HTTP and SMTP demonstrated a similar pattern. The 1 KB and 10 KB files had a higher percentage of network load than bigger file sizes.

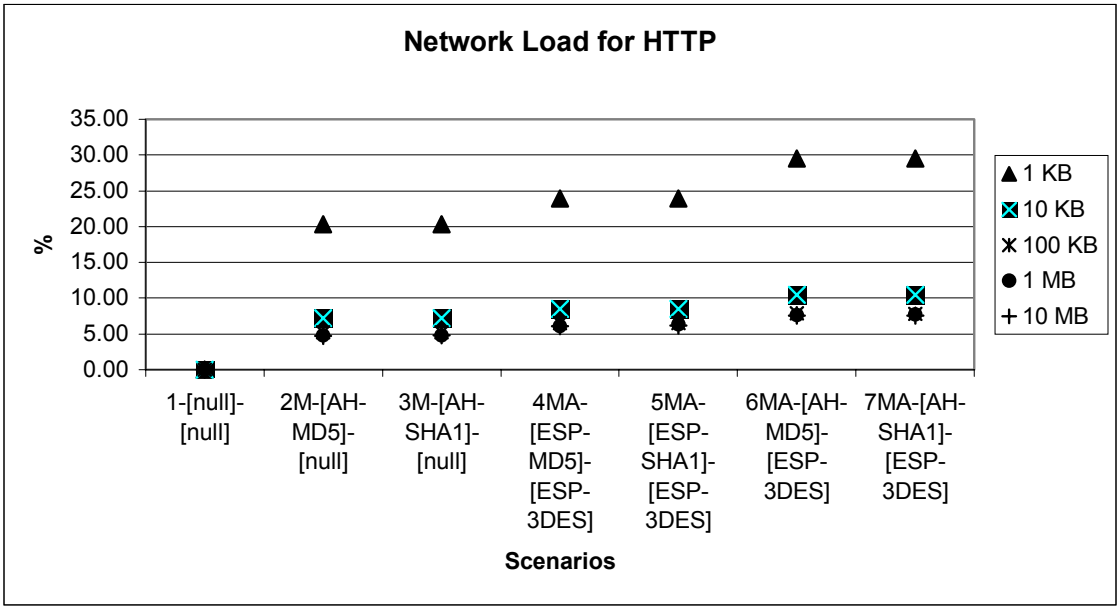


Figure 4.4. Percentage load increase for HTTP.

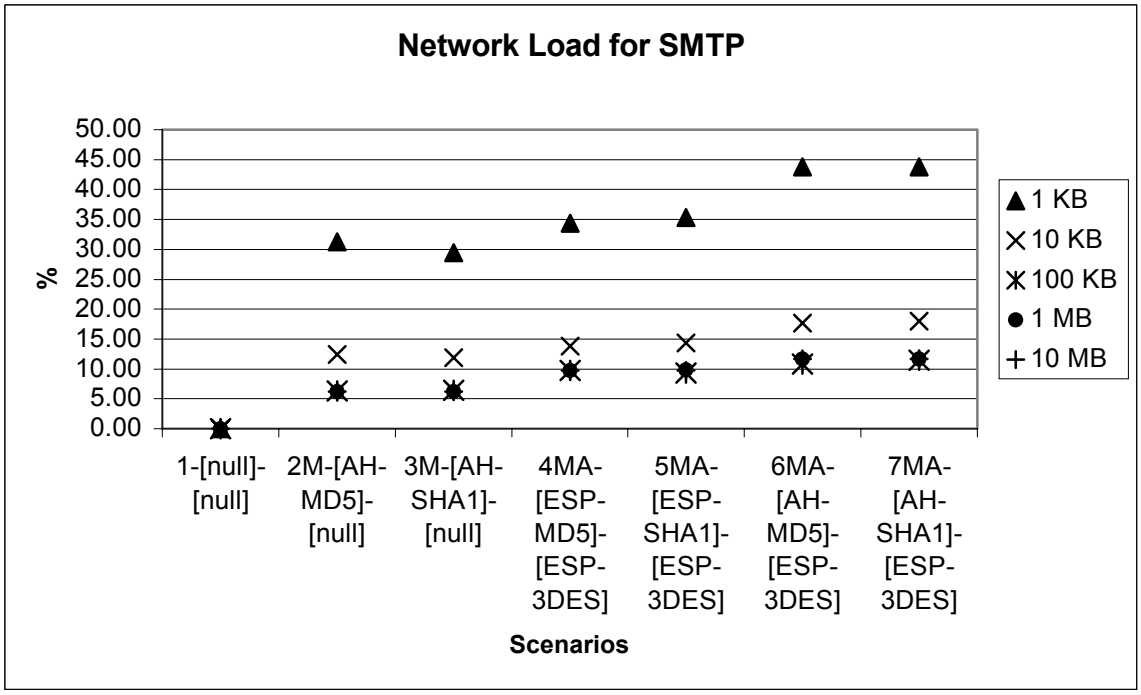


Figure 4.5. Percentage load increase for SMTP.

Bigger file sizes had approximately the same increase in the network load. However, SMTP had a higher percentage network load than HTTP. The ranges for the lowest and highest percentage load increase for both configurations of Testbed 1 are shown in Table 4.2. The faster Testbed 1 configuration gave a lower percentage for the 10 MB file mainly due to the decrease in the CtoS ACKs as mentioned above (see Section 4.1.1). When taking into consideration the Ident protocol, the percentage load due to IPSec increased by a maximum value of approximately 5% for small files (1 KB and 10 KB) and by a negligible percentage for bigger files.

Table 4.2. Maximum and Minimum Percentage Increase in Network Load.

Network load ranges	**1 KB**		**10 MB**	
	Lowest % (2M)	**Highest % (7MA)**	**Lowest % (2M)**	**Highest % (7MA)**
Slow-HTTP	20.31	29.50	4.75	7.53
Fast -HTTP (Extra)	**SASC**	**SASC**	3.24	4.53
Slow –SMTP with Ident	31.31	43.74	6.20	11.72
Slow –SMTP without Ident	26.36	36.30	6.20	11.71
Fast – SMTP with Ident (Extra)	**SASC**	**SASC**	4.45	6.17
SASC => Same As Slow Configuration				

4.1.3 Transfer Time

The graph of transfer time in Figure 4.6 shows how the transfer time for each file size varied with each scenario. The basic relationship for the percentage increase between the various algorithms can be ordered as:

1 < 2M < 3M < 4MA < 6MA < 5MA < 7MA

Authentication incurred a higher transfer time than no authentication but was lower than when using both authentication and encryption. SHA1 scenarios gave a higher percentage increase in transfer time than MD5 scenarios, since SHA1 required a higher computation overhead for authentication (see Section 2.5.2).

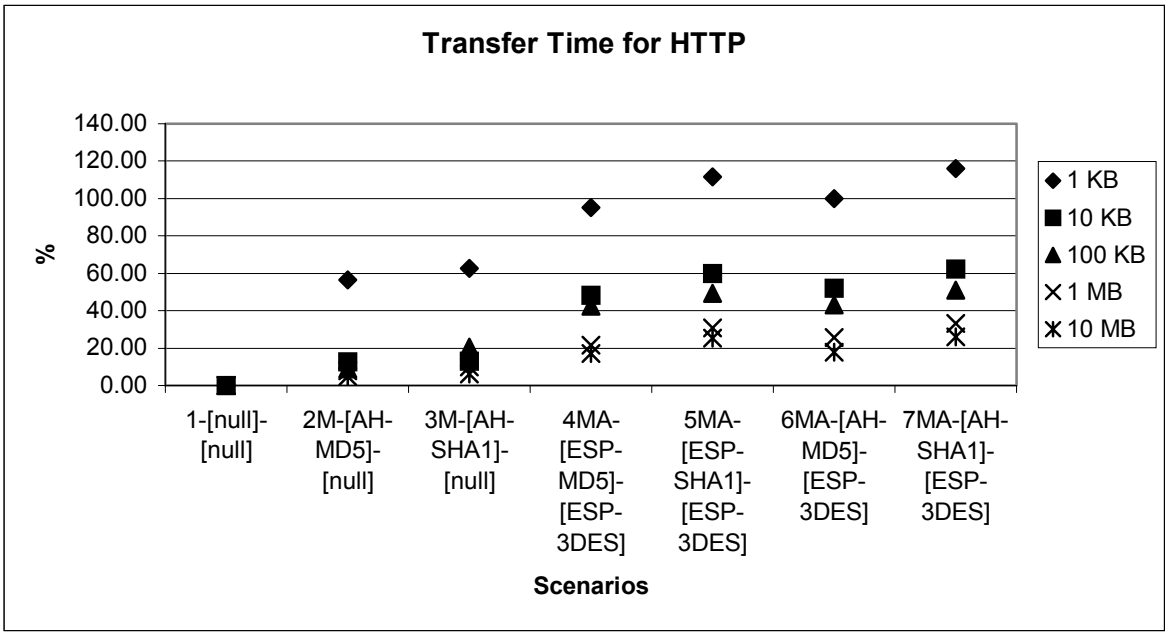


Figure 4.6. Percentage increase of Transfer Time.

The following observations were made for the transfer time.

i. For HTTP and both the slow and fast configurations of Testbed 1, the 1 KB file had the highest percentage increase in the transfer time and the 10 MB file had the lowest one (see Table 4.3). However, the percentage increase of transfer time was overall smaller for all the files of the faster configuration of Testbed 1 when compared to the slower configuration.

ii. The percentage increase in the transfer time for HTTP using the 10 MB file was higher (11.06%) than for SMTP (0.96%) because HTTP took less time to transfer the file, which caused the percentage increase to be more responsive to changes in time when using different scenarios.

iii. For the slower configuration, the percentage increase in the transfer time for SMTP was due to the extra number of ACKs from the CtoS to slow down the traffic flow of packets from the server (see Section 3.2.6).

iv. The Ident protocol did not affect the percentage increase in the transfer time for the 10 MB file since the protocol constituted a very small number of packets, compared to the total number transmitted, which took a relatively shorter transfer time. However, the Ident transfer time constituted a greater percentage of the total transfer time for the 1 KB file. Therefore, when the Ident time was deducted, the percentage difference in the transfer time due to IPSec increased to approximately 4% (see Section 4.1.4).

v. The faster computer configuration gave a higher percentage increase for SMTP since the machines involved in the configuration had higher computational capabilities giving a smaller transfer time. Thus, the overhead of each scenario constituted a higher percentage of the total transfer time, giving a higher percentage increase for the transfer time. This pattern was also shown with the Ident protocol. When the Ident protocol transfer time deducted there was a percentage increase in transfer time of 17% that was a lot higher compared to the slow configuration (4%).

vi. In the faster configuration, when using the 10 MB file, a percentage increase in transfer time of 6.34% for the authentication scenario (2M) was obtained instead of a lower value than the 0.96% of scenario 7MA. This was due to the higher number of CtoS ACKs. With authentication, the client would acknowledge approximately every two packets instead of every three packets.

Table 4.3. Maximum and Minimum Percentage Increase in Transfer Time.

	1 KB		10 MB	
	Lowest % (2M)	Highest % (7MA)	Lowest % (2M)	Highest % (7MA)
Slow-HTTP	56.38	115.98	4.64	26.17
Fast –HTTP (Extra)	17.82	52.02	2.79	11.06 *(ii)*
Slow- SMTP with Ident	9.21	25.46 (iv)	***13.69 (iii)***	***64.77 (iii)***
Slow-SMTP without Ident	10.32	29.78 (iv)	***13.71 (iii)***	***64.88 (iii)***
Fast –SMTP with Ident (Extra)	29.26	39.52 (v)	6.34 (vi)	0.96 *(ii)*
Fast –SMTP without Ident (Extra)	43.63	56.38 (v)	6.34 (vi)	0.96
Roman numeral entries refer to the bullets explained above				

4.1.4 The Ident protocol Percentages

The Ident protocol overhead as a percentage of the total metrics of transactions, network load and transfer time are shown in Figure 4.7. The data used to calculate these percentages was from Testbed 1. All three metrics followed similar patterns. The Ident

protocol took a greater percentage of the metrics for smaller files, and a negligible percentage for smaller files. The maximum and minimum percentage values for the Ident protocol overhead were tabulated in Table 4.4.

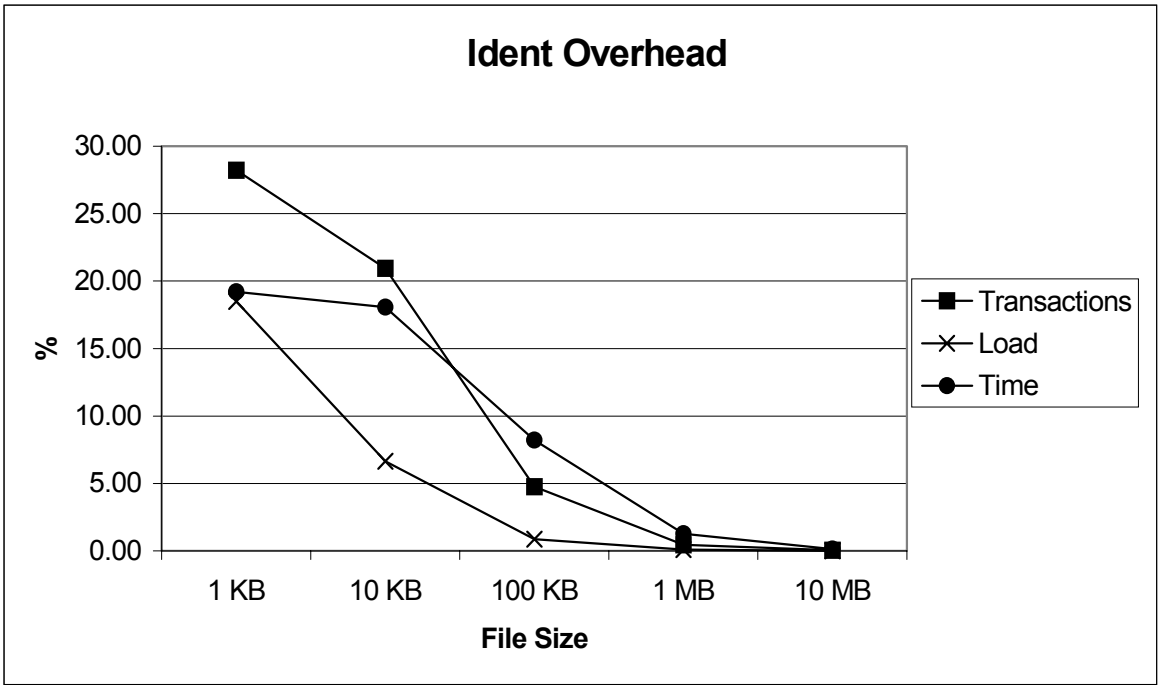


Figure 4.7. Ident overhead as a percentage of the metrics used.

Table 4.4. Percentage of Ident Overhead over Total Metric (Wireline).

Transactions	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	27.50	21.36	5.91	*0.55*	*0.06*
7MA-[AH-SHA1]-[ESP-3DES]	28.21	20.95	4.76	*0.45*	*0.05*
Network Load					
1-[null]-[null]	14.04	4.14	*0.51*	*0.05*	*0.01*
7MA-[AH-SHA1]-[ESP-3DES]	18.49	6.64	*0.87*	*0.08*	*0.01*
Transfer Time					
1-[null]-[null]	21.89	19.61	10.05	*1.77*	*0.21*
7MA-[AH-SHA1]-[ESP-3DES]	19.20	18.07	8.22	*1.27*	*0.14*

4.1.5 Summary of Authentication with/without Encryption

This section has demonstrated the following.

- For small files the **number of transactions** is the same for all scenarios giving a 0% increase in transactions. For bigger files, the number of transactions for both HTTP and SMTP increased by 5% for scenarios 2M-7MA. However, this increase was even higher for the slow configuration for scenarios 4MA-7MA (10% for HTTP and 20% for SMTP). This increase was due to the CtoS ACKs to slow down the packet flow

from the server. The SMTP protocol had higher computational requirements than the HTTP protocol thus slowing down the nodes more and requiring more CtoS ACKs than HTTP.

- The percentage increase in the **network load** for small files was higher than bigger files. Bigger files had approximately the same percentage increase in the network load. However, the HTTP protocol gave a lower network load increase than the SMTP protocol. The ranges of the network load percentage increase are shown in Table 4.2.

- The percentage increase in the **transfer time** for small files was higher than bigger files. For the SMTP protocol the total transfer time for a file was higher than the HTTP protocol thus giving a smaller percentage increase in the transfer time for each scenario (see Table 4.3). The transfer time was affected by:
  - the increase in the CtoS ACKs due to the slow computer West, and
  - acknowledging after receiving different loads of traffic.
- The basic relationship for the percentage increase in transfer time between the various scenarios and algorithms was:

  1 < 2M < 3M < 4MA < 6MA < 5MA < 7MA

  The ranges of the transfer time are shown in Table 4.3.

- The **Ident** protocol overhead took a greater percentage of the total metrics involved for small files and a negligible percentage for bigger files. The percentages are shown in Table 4.4.
  When the Ident protocol was considered/(included) the following results were shown.
  - It did not affect the percentage increase in the number of transactions,
  - The percentage network load increased by a maximum value of approximately 5% for small files (1 KB and 10 KB) and by a negligible percentage for bigger files.
  - The percentage transfer time decreased since the ident transfer time constituted a large percentage of the overall transfer time. For the slow configuration, the percentage decrease in transfer time was approximately 4% for small files (1KB). The faster computer configuration gave a higher percentage decrease of 17% for the small files. The percentage decrease in transfer time for bigger files for both the slow and fast configurations was negligible.

4.2 Overhead of ESP vs. AH (with 3DES)

This section investigates the overhead of using ESP encryption and authentication versus ESP encryption and AH authentication. The analysis was done by comparing the scenarios shown below in Table 4.5, using Testbed 1 data. The algorithms were kept the same to provide valid criteria for the analysis.

Table 4.5. Comparison AH authentication Vs ESP authentication.

Comparison 1	4MA-[ESP-MD5]-[ESP-3DES] ➔6MA-[AH-MD5]-[ESP-3DES]
Comparison 2	5MA-[ESP-SHA1]-[ESP-3DES] ➔7MA-[AH-SHA1]-[ESP-3DES]

The results of the calculations were tabulated in Appendix N. The percentage increase in the number of transactions was negligible when using AH or ESP for authentication (see Table 4.6). The percentage increase in the network load mostly affected the 1 KB file and, to a lesser extent the 10 KB file. The deviation due to the Ident protocol was negligible.

Table 4.6. ESP vs. AH authentication (with 3DES).

	1 KB		**10 KB**		**10 MB**	
Transactions	**% for 6MA**	**% for 7MA**	**% for 6MA**	**% for 7MA**	**% for 6MA**	**% for 7MA**
Slow-HTTP	0.00	0.00	0.00	0.00	1.57	0.16
Slow-SMTP with Ident	1.30	0.00	1.96	0.96	0.39	0.64
Slow-SMTP without Ident	1.82	0.00	2.5	1.22	0.39	0.64
Fast-HTTP (EXTRA)	SAA	SAA	SAA	SAA	0.16	0.18
Fast-SMTP with Ident(EXTRA)	SAA	SAA	SAA	SAA	0.4	0.99
Network load						
Slow-HTTP	**4.47**	**4.47**	1.81	1.81	1.42	1.25
Slow-SMTP with Ident	**7.02**	**6.18**	3.42	3.14	1.76	1.8
Slow-SMTP without Ident	**6.42**	**5.41**	2.99	2.7	1.76	1.8
Fast-HTTP (EXTRA)	SAA	SAA	SAA	SAA	0.4	0.99
Fast-SMTP with Ident(EXTRA)	SAA	SAA	SAA	SAA	0.83	0.83
Transfer time	**1 KB**	**10 KB**	**100 KB**	**1MB**	**10 MB**	
Slow-HTTP	2.33	2.07	0.70	2.56	0.59	
Slow-SMTP with Ident	0.89	0.52	0.37	1.02	1.62	
Slow-SMTP without Ident	0.94	0.49	0.35	1.02	1.62	
Fast-HTTP (EXTRA)	1.50	0.63	0.87	1.96	2.39	
Fast-SMTP with Ident(EXTRA)	2.26	1.53	0.73	1.06	0.24	
Fast-SMTP without Ident(EXTRA)	**3.11**	1.91	0.77	SAA	SAA	
SAA= Same As Above						

The transfer time was obtained by averaging the percentage increase of scenarios 6MA and 7MA for each file size (average of the sum of comparison 1and 2). The average maximum increase in the percentage of transfer time was approximately 3%, which was insignificant. Therefore, switching from ESP for authentication and encryption, to AH for authentication and encryption depends on the number of small size files sent on a network, and on the bandwidth of the medium over which the data is sent. That is, if the percentage of smaller files sent over a network is significant, and the network has a limited bandwidth, then it would be better to use ESP to provide authentication. However, this decision will also depend on the security policy of the network and whether it is allowed to forgo the extra authentication coverage provided by AH (see Section 2.3.3).

Summarizing, switching from ESP to AH authentication (with 3DES):

- Did not affect the number of transactions,
- Increased the network load by around 5% for the 1 KB file and by a negligible percentage for bigger files,
- Did not affect the transfer time.

4.3 ESP vs. AH Authentication

The goal of this section was to look at the overhead of using ESP for authentication versus AH. This aspect could not be explored due to the FreeS/WAN limitation that did not allow for null encryption when using ESP (see Section 3.2.5.1). Null encryption is the ability to use ESP authentication without encryption. Therefore, if only authentication was required, it had to be done in manual keying using only AH.

4.4 HMAC-MD5 vs. HMAC-SHA1

This section addresses the overhead of MD5 versus SHA1. The overhead difference between the MD5 and SHA1 was calculated by comparing the data combinations for the same protocols and file sizes, but different algorithms (see Table 4.7). The data used was from Testbed 1 and the analysis results were tabulated in Appendix L.

Table 4.7. Comparison Criteria.

Comparison 1	2M-[AH-MD5]-[null] ➔3M-[AH-SHA1]-[null]
Comparison 2	4MA-[ESP-MD5]-[ESP-3DES] ➔5MA-[ESP-SHA1]-[ESP-3DES]
Comparison 3	6MA-[AH-MD5]-[ESP-3DES] ➔7MA-[AH-SHA1]-[ESP-3DES]

The percentage increase in the network load and the number of transactions was the same regardless of the algorithm used. However, it always required a greater amount of transfer time to send the files using SHA1 due to its higher computational requirements (see Table 4.8). The average percentage increase in the transfer time for 100 KB, 1 MB and 10 MB files in the slow configuration was higher. West had lower computational capabilities to process the data received so it sent more ACKs to decrease the flow of packets from the server, which caused the increase in the transfer time. Unlike the slow configuration, extra ACKs were not sent in the faster configuration of Testbed 1. Therefore, the percentage increase in transfer time for switching from MD5 to SHA1 decreased with the size of the file.

Summarizing, switching from MD5 to SHA1:

- Did not affect the number of transactions.
- Did not affect the network load.

- Increased the transfer time by a value depending on the computational capabilities of the nodes involved. Computers with faster computational capabilities gave a smaller percentage increase (see Table 4.8).

Table 4.8. Transfer time percentage increase.

	1 KB	**10 KB**	**100 KB**	**1 MB**	**10 MB**
HTTP	6.81	4.98	7.01	5.16	5.32
SMTP With Ident	4.82	2.34	9.07	2.50	5.62
SMTP Without Ident	5.55	2.42	9.79	2.51	5.62
AVERAGE For Testbed 1 (slow)	**5.73**	**3.25**	***8.62***	***3.39***	***5.52***
HTTP (Extra)	4.96	2.21	1.95	1.77	1.78
SMTP With Ident(Extra)	2.20	4.21	1.54	1.81	0.27
SMTP Without Ident(Extra)	4.21	4.21	4.21	1.81	0.27
AVERAGE For Faster Configuration	**3.79**	**3.55**	**2.56**	**1.80**	**0.77**

4.5 Compressed vs. Uncompressed files

This section investigates the IPSec overhead for transmitting compressed versus uncompressed files. In order to determine the difference in overhead between compressed and uncompressed files, the percentage difference between the same file sizes of "Zip" and "Doc" file types were calculated. The data that was used for comparing "Zip "and "Doc" file types was the 1500 MTU data (see Appendix A). The comparison was done by fixing the protocol, algorithm, and file size variables and calculating the percentage difference. The percentage file size difference was also calculated and it is shown in Table 4.9. The difference was negligible and it was not taken into account when analyzing the data.

Table 4.9. File Sizes and percentage differences.

		Uncompressed Files (.doc)	Compressed Files (.zip)	Comparing doc/zip file sizes
File Size	Bytes	Size Used	Size Used	(zip-doc)/zip*100
1 KB	1024	1024	1020	0.391
10 KB	10240	10237	10247	-0.098
100 KB	102400	102400	102546	-0.143
1000 KB	1048576	1049088	1049915	-0.079
10 MB	10485760	10490368	10484820	0.053

For all protocols and algorithms, there was no trend that compressed or uncompressed files required more overhead (see Appendix M). The percentage change deviated in both directions resulting to an average value close to 0%. However, the percentage difference for the HTTP protocol (see Figure 4.8) was found to be closer to 0% than SMTP, for all metrics of transactions, network load, and transfer time. Furthermore, the percentage difference of the transfer time deviated more for small size files. This deviation was

because the short transfer time interval of the small files was more prone to be affected by other processes running on a system (see Figure 4.9).

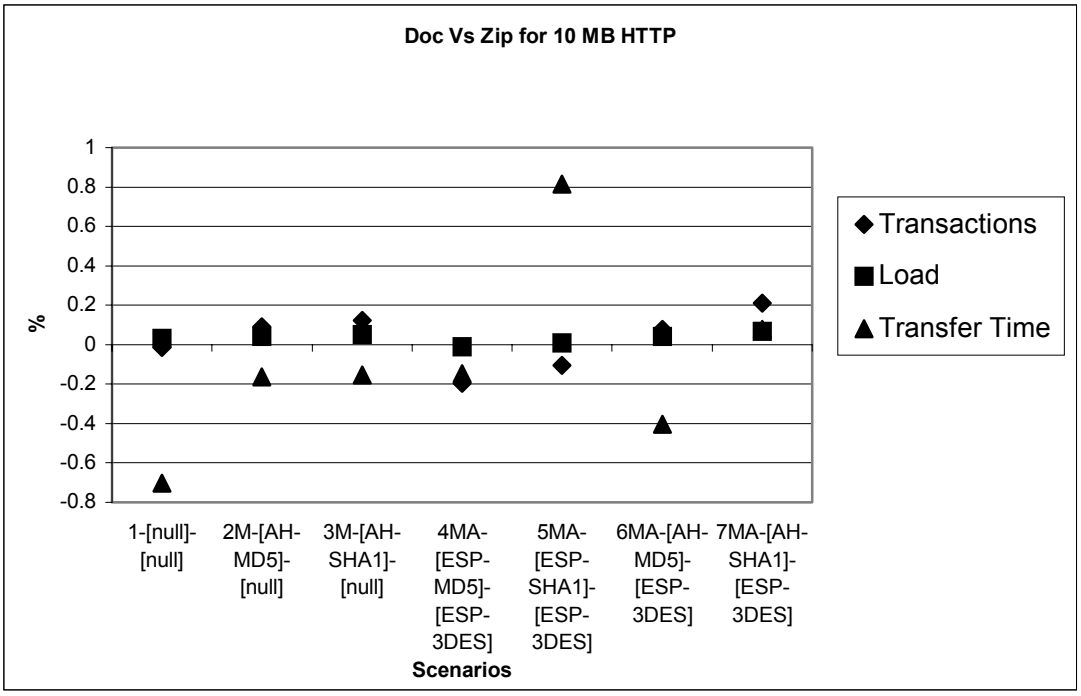


Figure 4.8. Doc vs. Zip for 10 MB HTTP.

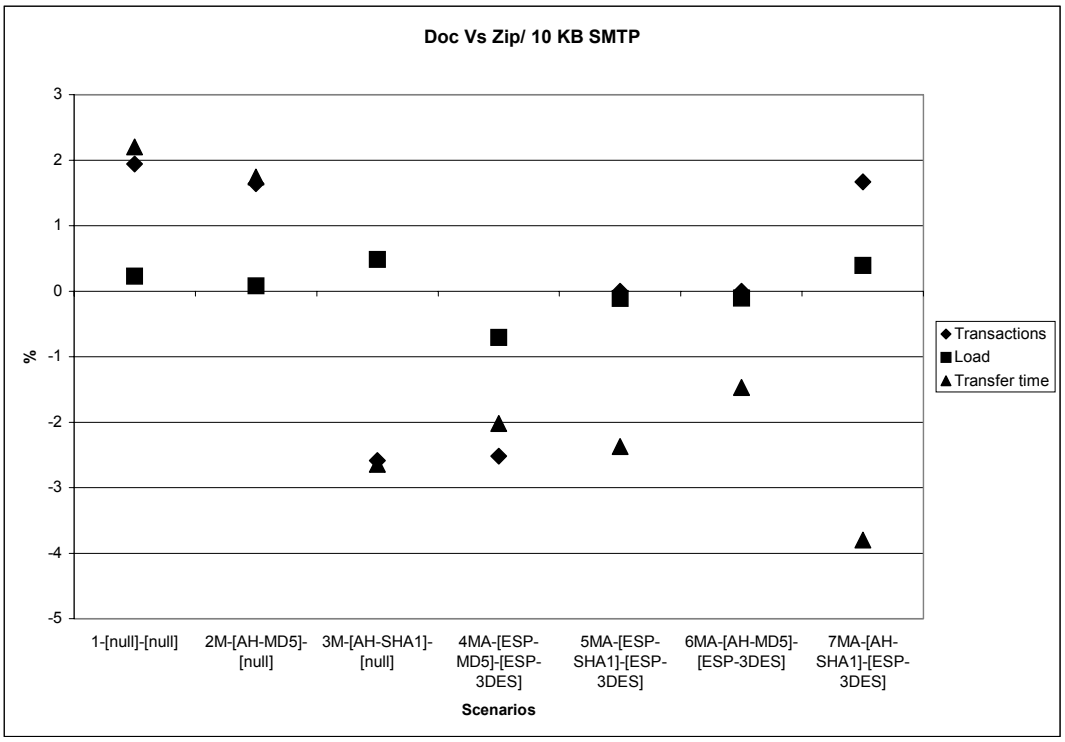


Figure 4.9. Doc vs. zip for 10 KB file SMTP.

Summarizing, switching form "Doc" file types to "Zip" file types:

- did not change the number of transactions,
- did not change the network load, and
- did not change the transfer time.

The IPSec overhead of both file types remained the same because the FreeS/Wan IPSec did not carry any form of compression before passing the data to the link layer.

4.6 HTTP vs. SMTP

This section investigates the overhead of sending files using HTTP (web-based) versus sending files with SMTP (email-based). The analysis was done by comparing the different combinations of scenarios, algorithms and file types of HTTP with SMTP transfers. The data used was from Testbed 1. Appendix J shows the tabulated data from the calculations. A summary of the percentage ranges for the increase in overhead due to IPSec between HTTP and SMTP is shown in Table 4.10.

Table 4.10. Range of the percentage increase of overhead with SMTP

	1 KB		10 MB	
Transactions	**Scenario 1/%**	**Scenario 7MA/%**	**Scenario 1/%**	**Scenario 7MA/%**
HTTP vs. SMTP with Ident	263.64	254.55	79.54	96.93
HTTP vs. SMTP without Ident	163.64	154.55	80.58	99.77
HTTP (Extra) versus SMTP with Ident	SAA	SAA	33.71	29.16
Network load				
HTTP vs. SMTP with Ident	134.66	160.47	39.85	45.29
HTTP vs. SMTP without Ident	101.72	112.31	39.84	45.28
HTTP (Extra) versus SMTP with Ident	SAA	SAA	36.83	36.11
Transfer time				
HTTP vs. SMTP with Ident	5126.18	2935.76	115.34	181.24
HTTP vs. SMTP without Ident	3982.25	2353.00	114.90	180.85
HTTP (Extra) versus SMTP with Ident	1416.43	1291.77	53.08	39.15
HTTP (Extra) versus SMTP without Ident	864.02	891.62	SAA	SAA
SAA =Same As Above				

SMTP required a higher overhead than HTTP when considering all three metrics of transactions, network load and transfer time. However, the percentage increase in overheads tended to be higher for small size files than bigger file sizes. The impact of the Ident protocol was also more significant especially for the smaller files. The highest percentage increase in the overhead from all three metrics was the transfer time, especially for the 1KB file, for the slow configuration (see Figure 4.10). The faster configuration of Testbed 1 decreased this high percentage increase of the transfer time for the 1KB file, because it had faster hardware to handle the higher computational requirements of SMTP. The speedup in transfer time with the faster configuration was 3.6 times [$\frac{5126.18\%}{1416.43\%} = 3.6$]. Even though this decrease in transfer time by the faster configuration testbed was significant, the percentage increase of 1416% with Ident was still very high.

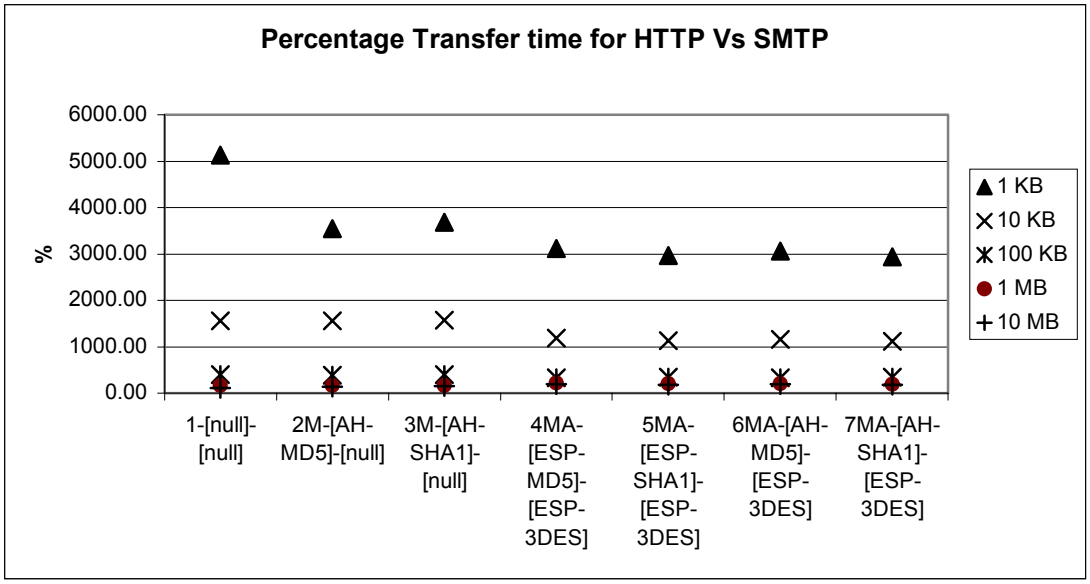


Figure 4.10. Percentage increase of Transfer time.

Summarizing, switching from HTTP to SMTP:

- Increased the number of transactions by a value between 30-264%.
- Increased the network load by a value between 36-135%.
- Increased the transfer load by a value between 40-5126%.

This variation was depended on the scenario used, file size used, testbed configuration and whether the Ident protocol was included. Scenario 1 had the lowest percentage increase and Scenario 7MA the highest one. The bigger files had a smaller percentage increase than the smaller files and the faster testbed configuration had a smaller percentage increase than the slower configuration. The higher percentages were obtained when considering the Ident protocol overhead in the comparisons.
Finally, using IPSec magnified the percentage increase in overhead (see Table 4.10).

4.7 IPSec Overhead over Wireless Transmission Links

This section investigates the impact of wireless links on the overhead of IPSec. Section 4.7.1 analyzes the data of Testbeds 2 and 4 and looks at the patterns of overhead with regards to the scenarios used. Section 4.7.2 analyzes the data of Testbed 1 (slow configuration) versus Testbed 4 and the data of Testbed 2 versus Testbed 3 by comparing the wireless and wireline data sets.

4.7.1 Scenario Comparison

The analysis for comparing the scenario overhead was done following the same approach used in Section 4.1. The no authentication and no encryption scenarios were compared to the ones that used just authentication or both authentication and encryption (see

Appendix K). The results from both Testbed 2 and 4 showed that the patterns of overhead for wireless and wireline links were similar to those in Section 4.1, except for the transfer time percentage increase. The percentage difference between scenarios 2M and 6MA was smaller because the wireless medium became the bottleneck of the network (see Table 4.11). The network nodes could process and get the data ready faster than it could be sent out. Furthermore, the Ident protocol slowed down the connection, taking approximately 3 seconds to authenticate the users. The Ident time was a lot bigger than the time to transfer the whole file. As a result, there was almost a 10% increase in the transfer time percentage for the 1KB file, when the Ident time was removed (compared to 4% for the wireline medium).

Table 4.11. Ranges of Percentage Increase of Metrics Used.

Testbed 2				
	1 KB		10 MB	
Transactions	**Scenario 2MA/%**	**Scenario 6MA/%**	**Scenario 2MA/%**	**Scenario 6MA/%**
HTTP	0	0	4.94	4.88
SMTP with Ident	1.37	1.37	3.91	4.73
SMTP without Ident	1.96	1.96	3.92	4.73
Network load				
HTTP	20.23	29.85	5.29	7.22
SMTP with Ident	29.69	41.85	4.8	7.45
SMTP without Ident	27.73	39.03	4.8	7.44
Transfer time				
HTTP	30.22	29.62	4.29	6.74
SMTP with Ident	0.53	1.01	4.31	6.82
SMTP without Ident	10.85	12.33	4.15	7.04
Scenario 7MA was not used to avoid redundancy.				

4.7.2 Protocol Comparison

This analysis investigated the impact of using wireless links, by comparing the data using the same protocols, algorithms, and file sizes, over wireless and wireline links. Testbed 1 data (slow configuration) was compared to Testbed 4 data, and Testbed 2 data was compared to Testbed 3 data (see Appendix K). The reason for using only the slow configuration data of Testbed 1 was because the comparison could only be valid if both Testbeds used the same computers. The fast configuration of Testbed 1 used a faster computer Dusk which was not used in the wireless Testbed 4 (see Section 3.2.1 and Section 3.2.6).

For HTTP and the Testbed 2 and 3 comparison, there was an increase in the percentage increase of transactions for bigger files due to the extra number of ACKs from the CtoS to control the traffic flow over the wireless link (see Table 4.12). This increase was negative or negligible for Testbeds 1 and 4 comparison. This was because the number of CtoS ACKs sent by “West,” the slow computer, to decrease the packet flow in Testbed 1,

were equal or greater than the CtoS ACKs sent by West in Testbed 4 to control the traffic flow over the wireless link. In Testbed 4, the wireless link became the bottleneck, slowing down the transfer of packets and giving more time to the client to process the packets received. As a result, less ACKs than in Testbed 1, were required to control the packet flow down the server. The network load for both wireless and wireline testbeds was approximately the same. The percentage increase in transfer time over wireless varied from 400% to 700%. Testbeds 2 and 3 comparison gave a higher percentage for the 10 K file since the computers involved had higher processing capabilities, giving a shorter transfer time, which fluctuated more to changes in transfer time.

Table 4.12. HTTP wireless vs. HTTP wireline.

	Testbed 1 vs. Testbed 4		**Testbed 2 vs. Testbed 3**	
Transactions	10 KB	1 MB	10 KB	1 MB
1-[null]-[null]	0.00	0.81 (*)	0.00	4.09 (**)
6MA-[AH-MD5]-[ESP-3DES]	0.00	-5.23 (*)	0.00	5.19 (**)
Network load	10 KB	1 MB	10 KB	1 MB
1-[null]-[null]	0.18	0.15	0.36	0.57
6MA-[AH-MD5]-[ESP-3DES]	0.15	-0.52	0.33	1.01
Transfer Time	10 KB	1 MB	10 KB	1 MB
1-[null]-[null]	509.25	449.00	**723.63**	**434.33**
6MA-[AH-MD5]-[ESP-3DES]	412.93	363.49	756.45	414.50
Average	438.26	406.15	739.01	428.39
(*) due to more CtoS ACKs to slow down the server in Testbed 1 (**)due to CtoS ACKs to control packet flow in the wireless link of Testbed 2				

For SMTP, the pattern for the three metrics was similar to that of HTTP. The percentage increase in transactions was negligible for small files and increased by approximately 5% for bigger files for Testbeds 2 and 3 comparison (see Table 4.13). This increase was again due to the extra number of ACKs from the CtoS to control the traffic flow over the wireless link. Similar to HTTP, the reason for getting a negative increase in percentage for the number transactions in Testbeds 1 and 4 comparison, was due to the slower configuration of Testbed 1. West, the client, was sending more ACKs to slow down the traffic from East, the server (see Table 4.14) when a wireless link was not used. The network load increase was insignificant. The transfer time increase in percentage was a lot higher due to the 3 seconds constant time required by Ident over wireless, as mentioned in Section 4.7.1. This can also be seen in Table 4.15 where the Ident protocol transfer time constituted up to 95% of the total transfer time for the 1 KB file. Even though the Ident protocol increased the percentage of the transfer time over wireless links, it did not affect the number of transactions and network load.

Table 4.13. SMTP wireless vs. SMTP wireline.

	10 KB		1 MB	
Transactions	**Scenario 1**	**Scenario 6MA**	**Scenario 1**	**Scenario 6MA**
T1-4 with Ident	0	0.96	**-21.84 ***	**-33.63 ***
T1-4 without Ident	0	1.22	**-21.96 ***	**-33.78 ***
T2-3 with Ident	-2.88	-2.88	6.09 **	6.2 **
T2-3 without Ident	-3.66	-3.66	6.14 **	6.24 **
Network load				
T1-4 with Ident	2.22	1.42	**-1.68***	**-5.94***
T1-4 without Ident	2.18	1.41	**-1.68***	**-5.94***
T2-3 with Ident	0.64	-0.32	0.72	1.04
T2-3 without Ident	2.79	3.38	0.74	1.09
Transfer time				
T1-4 with Ident	1225.74***	1069.58***	307.24	186.49
T1-4 without Ident	139.97	132.09	210.27	121.04
T2-3 with Ident	4211.09***	3666.33***	564.25	549.45
T2-3 without Ident	369.79	316.88	409.16	402.20
T1-4=> Testbed 1 vs. Testbed 4			**T2-3=>** Testbed 2 vs. Testbed 3	
(+) wireless metric > wireline metric **(-)** wireless metric < wireline metric				
(*) CtoS ACKs to slow down server in Testbed 1 (**)CtoS ACKs to control traffic flow due to wireless in Testbed 2 (***) high percentage due to 3 seconds delay for the Ident protocol				

Table 4.14. Transactions for 1 MB, Scenario 6MA.

SMTP with Ident			
Testbeds	Link	**Cto S**	**Sto C**
Testbed 1 (Slow)	Wireline	1379.5 (*)	1056
Testbed 1 Extra (Fast)	Wireline	468.5	1099(**)
Testbed 4	Wireless	554	1062.5
(*)increased CtoS ACKs sent by West to slow the server			
(**) increased StoC transactions due to the “4k Observation”			

Table 4.15. Percentage of Ident Overhead over Total Metric (Wireless-Testbed 2).					
Transactions	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	30.14	21.78	5.82	*0.69*	*0.07*
6MA-[AH-MD5]-[ESP-3DES]	29.73	21.78	5.71	*0.67*	*0.07*
Network Load					
1-[null]-[null]	14.51	4.20	*0.52*	*0.05*	*0.01*
6MA-[AH-MD5]-[ESP-3DES]	19.1	6.76	*0.90*	*0.09*	*0.01*
Transfer Time					
1-[null]-[null]	94.75	92.63	71.92	23.51	3.27
6MA-[AH-MD5]-[ESP-3DES]	94.09	91.40	71.33	23.14	3.09

Summarizing, switching from wireline to wireless links gave a similar pattern for the scenarios used. The Ident time to authenticate was a lot higher since it took approximately 3 seconds to authenticate the users.

Furthermore, using wireless links:

- Increased the number of transactions by a negligible amount for small files and by 5% for bigger files due to the CtoS ACKs to control the traffic on the wireless link. (Negative percentages were due to the slow computer sending more ACKs over the wireline links of Testbed 1). This change percentage increase was not due to IPSec.
- Did not change the network load by a significant amount.
- Increased the transfer time by a range of 400-700% for HTTP and a range between 120-4210% for SMTP. As mentioned above, these percentages were dependent on on the hardware processing capabilities of the nodes involved, the Ident protocol, the scenario and the file size used. The faster nodes gave smaller transfer times and therefore higher percentages. The increase in the Ident protocol transfer time in Testbeds 2 and 4, increased the percentage in the total transfer time. Furthermore, scenario 1 required a higher transfer time than scenario 7MA. Finally, big files had an overall lower percentage increase in transfer time than small files.

4.8 "4 KB" Data Chunks in the Faster Configuration of Testbed 1

This section covers a specific observation that affected the increase in the number of StoC transactions on the fast configuration of Testbed 1. Testbed 1's faster configuration was used to get extra data since the client, "West," was slower and generated more ACKs to control the data flow (see Table 4.16).

The faster configuration gave a continuous pattern of two MTU-sized packets and a third one of smaller size when sending 1MB and 10 MB files via SMTP. When adding the IP payload of these three packets, it summed to 4 KB. This pattern of 4KB chunks stopped temporarily after the client acknowledged giving 5-6 MTU-sized packets. Altering the send buffer size (SndbufSize) in the Sendmail configuration file did not give MTU- sized packets for all transactions (see Appedix O). The reason for this pattern was that SMTP protocol required more processing time than HTTP. Sendmail took longer to fill a stdio buffer than HTTP, and created a third packet that was less than the MTU-sized packet. This pattern affected the network load and the number of transactions from StoC since the system did not consistently send smaller path-MTU-sized packets during data. However, if the data were being sent on a larger network with more transfer delays, then Sendmail would have more time to combine the new blocks of data with previous data that still had not been sent over the Internet. This pattern would therefore not exist, deeming this observation somewhat insignificant, but worth mentioning.

Table 4.16. Transactions for Testbed 1 (slow) and Testbed 1 Extra (fast).

Scenario 7MA Protocol SMTP						
	Testbed 1 Transactions		**Testbed 1 Extra Transactions**		**% difference Slow vs. Fast conf.**	
	C to S	S to C	C to S	S to C	C to S	S to C
1 MB	1381	1056	459	1098	**200.87(*)**	**-3.83 (**)**
10 MB	13946	10391.5	3981	10812.5	**250.31 (*)**	**-3.89 (**)**
(+) slow trans. > fast trans. configuration (-) slow trans. < fast trans. Configuration (*) Due to CtoS ACKs sent by West to slow the server (**) 4KB chunks Observation						

4.9 Conclusion

This chapter covered the mathematical analysis of the data measured from all testbeds, and gave the general pattern of the overhead of IPSec. It was shown how the IPSec overhead varies with respect to the different protocols, algorithms and file sizes. The metrics used to analyze the data were the network load, the number of transactions and the transfer time.

The analysis was broken into seven major sections:

1) Overhead of Authentication with/without Encryption
2) ESP vs. AH (with 3DES) Overhead
3) ESP vs. AH Authentication Overhead
4) HMAC-MD5 vs. HMAC-SHA1 Overhead
5) Compressed vs. Uncompressed files Overhead
6) HTTP vs. SMTP Overhead
7) IPSec Overhead over Wireless Transmission Links

It was found that:

1) When securing a connection using Authentication with/without Encryption, small files had a higher percentage increase in the network load and transfer time than bigger files. However, the number of transactions for small files was the same for all scenarios giving no percentage increase. For bigger files, the number of transactions, network load, and the transfer time was affected by CtoS ACKs due to the slow computer West and due to sending ACKs after receiving different loads of traffic. The basic relationship for the percentage increase in transfer time between the various scenarios and algorithms was:

   1 < 2M < 3M < 4MA < 6MA < 5MA < 7MA

   The Ident protocol overhead took a greater percentage of the total metrics involved for small files and a negligible percentage for bigger files. When the Ident protocol was considered it did not affect the percentage increase in the number of transactions. However, for small files only, it increased the percentage of the total network load by a maximum value of 5% and decreased the percentage of the total transfer time by 4% for the slow configuration and 17% for the fast one.

2) Using AH instead of ESP authentication (with 3DES) did not affect the number of transactions and transfer time, but increased the network load by around 5% for the 1KB file only.

3) ESP vs. AH Authentication could not be explored due to the FreeS/WAN limitation. Authentication without encryption can only be done in manual keying using AH.

4) Using MD5 vs. SHA1 did not affect the number of transactions, and the network load but increased the transfer time for SHA1 by a value depending on the computational capabilities of the nodes involved. Faster nodes gave a faster transfer time.

5) Using Compressed vs. Uncompressed files took the same number of transactions, network load, and the transfer time. FreeS/WAN IPSec did not carry any form of compression on the files.

6) SMTP took a greater number of transactions, a higher network load and transfer time than HTTP with the use of IPSec. This variation was depended on the scenario used, file size used, testbed configuration and whether the Ident protocol was included.

7) Switching from wireline to wireless links gave a similar pattern with regards to the scenarios used but with smaller percentages increases when comparing scenarios 1-6MA (see Table 4.11). The Ident time to authenticate was a lot higher due to approximately 3 seconds taken to authenticate the users. Overall, using IPSec with a wireless link instead of a wireline link, did not affect the network load and number of transactions percentage increase. Even though, the transfer time increase was higher than in a wireline environment, it was overshadowed by the overall percentage increase due to the slower link of the wireless medium.

Chapter 5 gives a summary of the thesis and describes the conclusion derived according to the analysis of the data of this Chapter. It also gives recommendations for the deploying security in networks and suggests how to extend or improve this thesis according to the results obtained.

Chapter 5 Conclusion

This chapter summarizes the research, provides conclusions, and offers suggestions for future work.

5.1 Summary and Conclusions

This research was dedicated to developing testbed(s) for investigating the overhead of IPSec over wireline and wireless links, securing the connection between the nodes of the testbeds with IPSec, and measuring the overhead of IPSec. The data were transferred over SMTP, an email-based protocol, and HTTP, a Web-based protocol. The testing involved a combination of authentication algorithms, MD5 and SHA1, implemented through different authentication protocols such as ESP and AH, and used in conjunction with 3DES. A variety of different sizes of compressed and uncompressed files were transferred, in order to assess the IPSec overhead.

The goals of the research were to examine the IPSec overhead when using:

- no authentication and no encryption versus using just authentication for both HTTP and SMTP,
- no authentication and no encryption versus using both authentication and encryption for both HTTP and SMTP,
- ESP encryption and authentication versus using ESP encryption and AH authentication,
- MD5 versus SHA1 for authentication,
- compressed versus uncompressed files to transfer data,
- HTTP versus SMTP protocol,
- wireless versus wireline media, and
- ESP for authentication versus AH for authentication.

The research was conducted in six steps. The goal of the first step was deciding the wireline and/or wireless configurations of all the testbeds. In Step 2, the hardware needed for the testbeds was selected. Step 3 investigated the software needed for the operating system to build the IPSec tunnels and to "sniff" the packets. In Step 4, the different scenarios required for the testing were decided based on the protocols and on the authentication and encryption algorithms. Different file sizes of compressed and uncompressed file types were also created. In Step 5, Testbed 1 was setup, software limitations were assessed, and preliminary data was taken. The key metrics that were recorded were the network load in bytes, the number of packets transmitted, and the transfer time. Based on the results of the preliminary data, adjustments were made that were used in Step 6. In this step, all testbeds were deployed and further adjustments in the data collection and the configurations were made.

It was found that authentication takes less overhead than both authentication and encryption. However, authentication can only be used in manual keying, which is less secure and scales poorly since it is more prone to errors [23]. ESP authentication and

encryption had a lower network load for only small files, when compared to ESP encryption and AH authentication. Authentication algorithms, MD5 and SHA1, required approximately the same network load and number of packets. However, SHA1 took a larger transfer time than MD5, because of its higher computational requirements.

In addition, both compressed files and uncompressed file types required the same transfer time, network load and number of packets. Therefore, it is recommended that the frequently used files be compressed before sent on the network. This way, more data would be sent over the same period of time, utilizing less network bandwidth.

Furthermore, the overhead of HTTP versus SMTP was a lot higher when IPSec was used. HTTP required a lower number of packets, a lower network load, and a lower transfer time than SMTP. Based on these results users should access files through web transfers, rather than via email.

The IPSec overhead of using a wireless medium for the number of transactions and the network load was insignificant. Due to the wireless medium being the bottleneck of the network, the percentage increase in the transfer time between no encryption and no authentication to both encryption and authentication, was higher compared to the wireline configuration. However, this percentage increase was significantly smaller compared to the overall percentage increase in transfer time when using a wireless link.

Finally, ESP authentication was not compared with AH authentication, since FreeS/WAN IPSec did not support ESP authentication without using encryption. If authentication is required, it can only be implemented using the AH protocol.

5.2 Recommendations

Based on this research the following recommendations are made for a network operator.

- If the network needs to provide just authentication, it can only be done in manual keying with the AH protocol. Manual keying should only be used on a small scale and it is more prone to errors. There is also a need to secure the keys on every gateway that implements IPSec.

- If the network needs to provide authentication with encryption, it has higher overhead than using just authentication. However, the key negotiation can be done automatically, which is much more secure and can be used on a larger scale. The disadvantage of automatic keying is that the network operator will not be able to specify the algorithm that is going to be used. If a connecting gateway uses only SHA1, then that would be the default authentication algorithm. However, if the connecting node does not specifically ask for SHA1, then MD5 will be used by default.

- The network operator can use either MD5 or SHA1 when the major concern in a network is the network load and the number of transactions. This is because SHA1 and MD5 had the same number of transactions and network load. However, if the transfer time is an issue, then MD5 should be used since it has lower computational requirements than SHA1, and it will give faster transfer times.

- The network operator may use the AH authentication protocol instead of the ESP authentication (with 3DES) since AH just increased the network load by around 5% for the 1 KB file only. AH provides better authentication coverage by authenticating the outer IP Header.

- Network users should compress frequently accessed files since they take the same overhead as uncompressed files. The reason for not suggesting to compress all files sent is because this research did not account for the processing required to compress the files before sending them. It is also better to avoid sending a lot of small files, since with bigger files IPSec constitutes a smaller percentage of the overall network load.

- It is also recommended to use HTTP (web-based) than SMTP (email-based). SMTP is a slower protocol, requiring more processing and taking a lot more transactions and network load, and a higher transfer time.

- If the network operator switches from wireline to wireless links IPSec has no significant impact on the overhead except the transfer time. However, the increase in transfer time due to IPSec is overshadowed by the lower bandwidth of the link. Therefore, the major issue with regards to using wireless instead of wireline links would be the security of the underlying system. For example, how fast keys are negotiated in wireless networks and whether there is a risk that an attacker can obtain those keys.

5.3 Future Work

Future work on this system should focus on two fronts. First, a method should be found for measuring the processing overhead for compressing files. This research did not consider the processing overhead for compressing files before sending them on the network. The files were created before testing. This thesis could be extended by using IPSec implementations that compress files before sending them. Compression in the FreeS/WAN IPSec used in the testbeds, did not work properly, however. The second front that should be pursued regards the use of alternative key management protocols. The current IPSec data could then be compared with the alternative key management protocols for suitability for the network studied in the NAVCIITI project and other networks.

References

[1] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, The Internet Society, November 1998.

[2] S. Kent, R. Atkinson, "IP Authentication Header," RFC 2402, The Internet Society, November 1998.

[3] S. Kent, R. Atkinson, "IP Encapsulating Security Payload (ESP)," RFC 2406, The Internet Society, November 1998.

[4] Harkins, D. and D. Carrel, "The Internet Key Exchange (IKE)," RFC 2409. Internet Engineering Task Force, November 1998.

[5] "Linux FreeS/WAN Overview," http://www.freeswan.org/freeswan_trees/ freeswan-1.7/doc/overview.html,available June 27, 2000.

[6] C. Madson and N. Doraswamy, "The ESP DES-CBC Cipher Algorithm with Explicit IV," RFC 2405, The Internet Society, November 1998.

[7] Linux FreeS/WAN, http://www.freeswan.org, available February 10, 2001.

[8] Ethereal, http://www.zing.org, available February 10, 2001.

[9] Naganand Doraswamy, Dan Harkins, IPSec The New Security Standard for the Internet,Intranets, and Virtual Private Networks, Prentice Hall PTR, Upper Saddle River, NJ 07458,1999.

[10] Pete Loshin, Big Book of IPSec RFCs, Academic Press, San Diego, CA 92101, 2000.

[11] Steven M. Bellovin, *Problem areas for the IP Security Protocols*, Proceedings of the Sixth Usenix Unix Security Symposium, July,1996.

[12] Casey Wilson, Peter Doak, Creating and Implementing Virtual Private Networks, Coriolis Group, Arizona 85260, 2000.

[13] *Information Technology Interoperability*, Naval Research Advisory Committee Report, NRAC 98-2, November 1998.

[14] H. Dobbertin, *The Status of MD5 After Recent Attack*, RSA Labs' *CryptoBytes*, Vol. 2 No 2, Summer 1996.

[15] "What is triple-DES?," http://www.rsasecurity.com/rsalabs/faq/3-2-6.html /, available May 10,2001.

[16] "Has DES been broken?," http://www.rsasecurity.com/rsalabs/faq/3-2-2.html, available May 11,2001.

[17] "What are SHA and SHA-1?," http://www.rsasecurity.com/rsalabs/faq/3-6-5.html available May 11,2001.

[18] "What are MD2, MD4, and MD5?," http://www.rsasecurity.com/rsalabs/faq/3-6-6.html, available May 11, 2001.

[19] "RFC 1413," http://www.faqs.org/rfcs/rfc1413.html, available May23, 2001.

[20] "Performance tuning and troubleshooting," http://www.linux.org/docs/ldp/howto/DSL-HOWTO / tuning.html, available February 10, 2001.

[21] "Raylink," http://www.raylink.com/, available June 4, 2001

[22] "E-mail Explained," http://www.sendmail.org/email-explained.html, available June 4, 2001

[23] "Using manual keying in production," http://www.freeswan.org/freeswan_trees/freeswan-1.9/doc/config.html#prodman, available June 3, 2001

[25] C. Madson, R. Glenn, "The Use of HMAC-MD5-96 within ESP and AH," RFC 2403, The Internet Society, November 1998.

[26] H. Krawczyk, M. Bellare, R. Canetti, "HMAC: Keyed-Hashing for Message Authentication," RFC 2104, February 1997.

[27] Rivest, R., "The MD5 Message-Digest Algorithm," RFC 1321, RSA Data Security, Inc., April 1992.

Appendices

A Various MTU Average data

B 1500 MTU Average data

C Ideal MTU versus Various MTU

D Testbed 1 Average data

E Testbed 2 Average data

F Testbed 3 Average data

G Testbed 4 Average data

H Extra Data for Testbed 1 (Dusk->West)

I All Scenarios versus No authentication and No Encryption

J SMTP Vs HTTP

K Wireless Vs Wireline

L MD5 VS SHA

M Compressed Vs Uncompressed Files

N AH Vs ESP authentication with 3DES

O HARDWARE and SOFTWARE Information

P IPSEC.conf file

Q FREESWAN VERSIONS

Appendix A - Various MTU Data
Average data

FILE TYPE =>doc	FILE SIZE =>10 KB			PROTOCOL =>HTTP MTU=> 600->1500			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	0	0	0	0	0	0	0.0000
2M-[AH-MD5]-[null]	15	23	38	2002	13051	15053	0.0237
3M-[AH-SHA1]-[null]	15	23	38	2002	13051	15053	0.0218
4MA-[ESP-MD5]-[ESP-3DES]	15	23	38	2122	13314	15436	0.0271
5MA-[ESP-SHA1]-[ESP-3DES]	15	23	38	2122	13314	15436	0.0299
6MA-[AH-MD5]-[ESP-3DES]	15	23	38	2302	13590	15892	0.0278
7MA-[AH-SHA1]-[ESP-3DES]	15	23	38	2302	13590	15892	0.0311

FILE TYPE =>doc	FILE SIZE =>1 MB			PROTOCOL =>HTTP MTU=> 600->1500			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	0	0	0	0	0	0	0.0000
2M-[AH-MD5]-[null]	968	1922	2890	107174	1260810	1367984	1.6852
3M-[AH-SHA1]-[null]	968	1922	2890	107174	1260810	1367984	1.7060
4MA-[ESP-MD5]-[ESP-3DES]	1043.5	1919	2962.5	123829	1283498	1407327	1.7428
5MA-[ESP-SHA1]-[ESP-3DES]	1052.5	1920	2972.5	124891	1283616	1408507	1.9496
6MA-[AH-MD5]-[ESP-3DES]	1046	1919	2965	136676	1306526	1443202	1.8395
7MA-[AH-SHA1]-[ESP-3DES]	1052	1919	2971	137456	1306526	1443982	2.0129

FILE TYPE =>doc	FILE SIZE =>10 MB			PROTOCOL =>HTTP MTU=> 600->1500			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	0	0	0	0	0	0	0.0000
2M-[AH-MD5]-[null]	9468	19211	28679	1042076	12601737	13643813	17.0488
3M-[AH-SHA1]-[null]	9484.5	19210	28694.5	1043947	12601677	13645624	17.1589
4MA-[ESP-MD5]-[ESP-3DES]	10361.5	19149.5	29511	1223353	12824814	14048167	17.4851
5MA-[ESP-SHA1]-[ESP-3DES]	10486	19146.5	29632.5	1238044	12824476	14062520	19.2248
6MA-[AH-MD5]-[ESP-3DES]	10433	19147.5	29580.5	1356986	13054360	14411346	17.9621
7MA-[AH-SHA1]-[ESP-3DES]	10490	19146	29636	1364396	13054172	14418568	20.0834

FILE TYPE => Doc	FILE SIZE =>10 KB			PROTOCOL =>HTTP MTU=> 1438->1500			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	9	11	20	946	11247	12193	0.0165
2M-[AH-MD5]-[null]	9	11	20	1342	11731	13073	0.0186
3M-[AH-SHA1]-[null]	9	11	20	1342	11731	13073	0.0186
4MA-[ESP-MD5]-[ESP-3DES]	9	11	20	1414	11810	13224	0.0244
5MA-[ESP-SHA1]-[ESP-3DES]	9	11	20	1414	11810	13224	0.0264
6MA-[AH-MD5]-[ESP-3DES]	9	11	20	1522	11942	13464	0.0251
7MA-[AH-SHA1]-[ESP-3DES]	9	11	20	1522	11942	13464	0.0268

FILE TYPE => Doc	FILE SIZE => 1MB			PROTOCOL =>HTTP MTU=> 1438->1500			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	373.5	731	1104.5	25345	1097648	1122993	1.1621
2M-[AH-MD5]-[null]	392.5	762	1154.5	43869	1133210	1177079	1.2519
3M-[AH-SHA1]-[null]	391.5	762	1153.5	43759	1133210	1176969	1.2763
4MA-[ESP-MD5]-[ESP-3DES]	448	762	1210	53560	1137804	1191364	1.4121
5MA-[ESP-SHA1]-[ESP-3DES]	472.5	762	1234.5	56274	1137804	1194078	1.5191
6MA-[AH-MD5]-[ESP-3DES]	470.5	762	1232.5	61861	1146948	1208809	1.4592
7MA-[AH-SHA1]-[ESP-3DES]	475.5	762	1237.5	62511	1146948	1209459	1.5463

FILE TYPE =>Doc	FILE SIZE => 10 MB			PROTOCOL =>HTTP MTU=> 1438->1500			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	3639.5	7310.5	10950	241377	10971128	11212505	12.0117
2M-[AH-MD5]-[null]	3826	7592	11418	421556	11323743	11745299	12.5692
3M-[AH-SHA1]-[null]	3834	7597	11431	422436	11324293	11746729	12.7595
4MA-[ESP-MD5]-[ESP-3DES]	4433	7573.5	12006.5	523790	11367185	11890975	14.0507
5MA-[ESP-SHA1]-[ESP-3DES]	4585	7572	12157	541726	11366992	11908718	15.0714
6MA-[AH-MD5]-[ESP-3DES]	4622.5	7572	12194.5	601621	11457856	12059477	14.1398
7MA-[AH-SHA1]-[ESP-3DES]	4605	7572	12177	599346	11457856	12057202	15.1546

FILE TYPE =>Doc	FILE SIZE =>10 KB			PROTOCOL =>HTTP MTU=> 1500->1500			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	0	0	0	0	0	0	0.0000
2M-[AH-MD5]-[null]	9	18	27	1342	11969	13311	0.0214
3M-[AH-SHA1]-[null]	9	18	27	1342	11969	13311	0.0218
4MA-[ESP-MD5]-[ESP-3DES]	9	18	27	1414	12056	13470	0.0247
5MA-[ESP-SHA1]-[ESP-3DES]	9	18	27	1414	12056	13470	0.0265
6MA-[AH-MD5]-[ESP-3DES]	9	18	27	1522	12188	13710	0.0253
7MA-[AH-SHA1]-[ESP-3DES]	9	18	27	1522	12188	13710	0.0272

FILE TYPE =>Doc	FILE SIZE =>1 MB			PROTOCOL =>HTTP MTU=> 1500->1500			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	373.5	731	1104.5	25345	1097648	1122993	1.1728
2M-[AH-MD5]-[null]	378	1454.5	1832.5	42274	1154399	1196673	1.3880
3M-[AH-SHA1]-[null]	378.5	1455	1833.5	42455	1154438	1196893	1.4386
4MA-[ESP-MD5]-[ESP-3DES]	451	1454	1905	53914	1160156	1214070	1.4419
5MA-[ESP-SHA1]-[ESP-3DES]	456	1454	1910	54504	1160156	1214660	1.5462
6MA-[AH-MD5]-[ESP-3DES]	465.5	1454	1919.5	61211	1168916	1230127	1.4553
7MA-[AH-SHA1]-[ESP-3DES]	476	1454	1930	62576	1168916	1231492	1.5615

FILE TYPE =>Doc	FILE SIZE =>10 MB			PROTOCOL =>HTTP MTU=> 1500->1500			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	0	0	0	0	0	0	0.0000
2M-[AH-MD5]-[null]	3662	14482	18144	403769	11534047	11937816	13.9788
3M-[AH-SHA1]-[null]	3671	14489	18160	404834	11535080	11939914	14.1643
4MA-[ESP-MD5]-[ESP-3DES]	4405	14493.5	18898.5	520080	11590337	12110417	14.2856
5MA-[ESP-SHA1]-[ESP-3DES]	4490	14492	18982	530458	11590218	12120676	15.2090
6MA-[AH-MD5]-[ESP-3DES]	4419	14490.5	18909.5	574885	11676968	12251853	14.3392
7MA-[AH-SHA1]-[ESP-3DES]	4494.5	14492	18986.5	584911	11677194	12262105	15.3385

FILE TYPE =>Doc	**FILE SIZE =>10 KB**			**PROTOCOL =>HTTP MTU=> 8000->1500**			
	Average # of Trans.			Average Network Load			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	0	0	0	0	0	0	0.0000
2M-[AH-MD5]-[null]	6	12	18	1022	11385	12407	0.0208
3M-[AH-SHA1]-[null]	6	12	18	1022	11385	12407	0.0212
4MA-[ESP-MD5]-[ESP-3DES]	6	12	18	1060	11440	12500	0.0289
5MA-[ESP-SHA1]-[ESP-3DES]	6	12	18	1060	11440	12500	0.0308
6MA-[AH-MD5]-[ESP-3DES]	6	12	18	1132	11512	12644	0.0300
7MA-[AH-SHA1]-[ESP-3DES]	6	12	18	1132	11512	12644	0.0313

FILE TYPE =>Doc	**FILE SIZE =>1MB**			**PROTOCOL =>HTTP MTU=> 8000->1500**			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	0	0	0	0	0	0	0.0000
2M-[AH-MD5]-[null]	99.5	796.5	896	11639	1086851	1098490	1.0225
3M-[AH-SHA1]-[null]	96	797	893	11254	1086900	1098154	1.0263
4MA-[ESP-MD5]-[ESP-3DES]	101.5	797	898.5	12673	1088534	1101207	1.2519
5MA-[ESP-SHA1]-[ESP-3DES]	105.5	797	902.5	13145	1088534	1101679	1.3111
6MA-[AH-MD5]-[ESP-3DES]	104	797	901	14216	1090178	1104394	1.2950
7MA-[AH-SHA1]-[ESP-3DES]	102	797	899	13956	1090178	1104134	1.3163

FILE TYPE =>Doc	**FILE SIZE =>10 MB**			**PROTOCOL =>HTTP MTU=> 8000->1500**			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	0	0	0	0	0	0	0.0000
2M-[AH-MD5]-[null]	896.5	7924.5	8821	99261	10858820	10958081	10.2689
3M-[AH-SHA1]-[null]	895.5	7923.5	8819	99201	10858760	10957961	10.3151
4MA-[ESP-MD5]-[ESP-3DES]	912.5	7923	8835.5	108371	10874594	10982965	12.1333
5MA-[ESP-SHA1]-[ESP-3DES]	967	7923	8890	114802	10874594	10989396	12.8822
6MA-[AH-MD5]-[ESP-3DES]	935	7923	8858	122246	10890494	11012740	12.2335
7MA-[AH-SHA1]-[ESP-3DES]	956	7923	8879	124976	10890494	11015470	12.8096

FILE TYPE =>Doc	FILE SIZE =>10 KB			PROTOCOL =>HTTP MTU=> 16260->1500			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	0	0	0	0	0	0	0.0000
2M-[AH-MD5]-[null]	6	12	18	1012	11309	12321	0.0220
3M-[AH-SHA1]-[null]	6	12	18	1012	11309	12321	0.0231
4MA-[ESP-MD5]-[ESP-3DES]	6	12	18	1060	11348	12408	0.0316
5MA-[ESP-SHA1]-[ESP-3DES]	6	12	18	1060	11348	12408	0.0328
6MA-[AH-MD5]-[ESP-3DES]	6	12	18	1132	11408	12540	0.0312
7MA-[AH-SHA1]-[ESP-3DES]	6	12	18	1132	11408	12540	0.0334

FILE TYPE =>Doc	FILE SIZE =>1 MB			PROTOCOL =>HTTP MTU=> 16260->1500			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	0	0	0	0	0	0	0.0000
2M-[AH-MD5]-[null]	71	781	852	8504	1082596	1091100	1.0165
3M-[AH-SHA1]-[null]	71	781	852	8504	1082596	1091100	1.0191
4MA-[ESP-MD5]-[ESP-3DES]	71	781	852	9074	1082646	1091720	1.6139
5MA-[ESP-SHA1]-[ESP-3DES]	71	781	852	9074	1082646	1091720	1.6436
6MA-[AH-MD5]-[ESP-3DES]	71	781	852	9926	1082706	1092632	1.6269
7MA-[AH-SHA1]-[ESP-3DES]	71	781	852	9926	1082706	1092632	1.6399

FILE TYPE =>Doc	FILE SIZE =>10 MB			PROTOCOL =>HTTP MTU=> 16260->1500			
Scenario	**Average # of Trans.**			**Average Network Load**			0.0000
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	0	0	0	0	0	0	0.0000
2M-[AH-MD5]-[null]	655.5	7772	8427.5	72701	10816763	10889464	9.8658
3M-[AH-SHA1]-[null]	654.5	7770	8424.5	72691	10816643	10889334	9.9001
4MA-[ESP-MD5]-[ESP-3DES]	654.5	7770.5	8425	77927	10816767	10894694	16.1823
5MA-[ESP-SHA1]-[ESP-3DES]	505	7771	8276	77986	10816826	10894812	16.5245
6MA-[AH-MD5]-[ESP-3DES]	654.5	7770	8424.5	85781	10816792	10902573	16.2326
7MA-[AH-SHA1]-[ESP-3DES]	654.5	7770	8424.5	85781	10816792	10902573	16.5865

Appendix B - Fixed MTU (1500)

Average Data

FILE TYPE =>Doc		FILE SIZE =>1 KB			PROTOCOL =>HTTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	6	5	11	747	1636	2383	0.0045
2M-[AH-MD5]-[null]	6	5	11	1011	1856	2867	0.0071
3M-[AH-SHA1]-[null]	6	5	11	1011	1856	2867	0.0077
4MA-[ESP-MD5]-[ESP-3DES]	6	5	11	1060	1894	2954	0.0092
5MA-[ESP-SHA1]-[ESP-3DES]	6	5	11	1060	1894	2954	0.0099
6MA-[AH-MD5]-[ESP-3DES]	6	5	11	1132	1954	3086	0.0094
7MA-[AH-SHA1]-[ESP-3DES]	6	5	11	1132	1954	3086	0.0101

FILE TYPE =>Doc		FILE SIZE =>10k			PROTOCOL =>HTTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	9	11	20	946	11247	12193	0.0175
2M-[AH-MD5]-[null]	9	18	27	1342	11969	13311	0.0214
3M-[AH-SHA1]-[null]	9	18	27	1342	11969	13311	0.0218
4MA-[ESP-MD5]-[ESP-3DES]	9	18	27	1414	12056	13470	0.0247
5MA-[ESP-SHA1]-[ESP-3DES]	9	18	27	1414	12056	13470	0.0265
6MA-[AH-MD5]-[ESP-3DES]	9	18	27	1522	12188	13710	0.0253
7MA-[AH-SHA1]-[ESP-3DES]	9	18	27	1522	12188	13710	0.0272

FILE TYPE =>doc		FILE SIZE =>100k			PROTOCOL =>HTTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	42	74	116	3125	107570	110695	0.1037
2M-[AH-MD5]-[null]	42	144	186	4973	113206	118179	0.1244
3M-[AH-SHA1]-[null]	42	144	186	4973	113206	118179	0.1304
4MA-[ESP-MD5]-[ESP-3DES]	44.5	144	188.5	5603	113800	119403	0.1548
5MA-[ESP-SHA1]-[ESP-3DES]	44.5	144	188.5	5603	113800	119403	0.1650
6MA-[AH-MD5]-[ESP-3DES]	47.5	144	191.5	6527	114688	121215	0.1565
7MA-[AH-SHA1]-[ESP-3DES]	47.5	144	191.5	6527	114688	121215	0.1670

FILE TYPE => Doc		FILE SIZE => 1MB		PROTOCOL => HTTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	373.5	731	1104.5	25345	1097648	1122993	1.1728
2M-[AH-MD5]-[null]	378	1454.5	1832.5	42274	1154399	1196673	1.3880
3M-[AH-SHA1]-[null]	378.5	1455	1833.5	42455	1154438	1196893	1.4386
4MA-[ESP-MD5]-[ESP-3DES]	451	1454	1905	53914	1160156	1214070	1.4419
5MA-[ESP-SHA1]-[ESP-3DES]	456	1454	1910	54504	1160156	1214660	1.5462
6MA-[AH-MD5]-[ESP-3DES]	465.5	1454	1919.5	61211	1168916	1230127	1.4553
7MA-[AH-SHA1]-[ESP-3DES]	476	1454	1930	62576	1168916	1231492	1.5615

FILE TYPE =>Doc		FILE SIZE =>10 MB		PROTOCOL =>HTTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	3639.5	7310.5	10950	241377	1.1E+07	1.1E+07	11.9904
2M-[AH-MD5]-[null]	3662	14482	18144	403769	1.2E+07	1.2E+07	13.9788
3M-[AH-SHA1]-[null]	3671	14489	18160	404834	1.2E+07	1.2E+07	14.1643
4MA-[ESP-MD5]-[ESP-3DES]	4405	14493.5	18898.5	520080	1.2E+07	1.2E+07	14.2856
5MA-[ESP-SHA1]-[ESP-3DES]	4490	14492	18982	530458	1.2E+07	1.2E+07	15.2090
6MA-[AH-MD5]-[ESP-3DES]	4419	14490.5	18909.5	574885	1.2E+07	1.2E+07	14.3392
7MA-[AH-SHA1]-[ESP-3DES]	4494.5	14492	18986.5	584911	1.2E+07	1.2E+07	15.3385

FILE TYPE =>Zip		FILE SIZE =>1 KB		PROTOCOL => HTTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	6	5	11	743	1629	2372	0.0041
2M-[AH-MD5]-[null]	6	5	11	1007	1849	2856	0.0069
3M-[AH-SHA1]-[null]	6	5	11	1007	1849	2856	0.0079
4MA-[ESP-MD5]-[ESP-3DES]	6	5	11	1060	1894	2954	0.0091
5MA-[ESP-SHA1]-[ESP-3DES]	6	5	11	1060	1894	2954	0.0095
6MA-[AH-MD5]-[ESP-3DES]	6	5	11	1132	1954	3086	0.0091
7MA-[AH-SHA1]-[ESP-3DES]	6	5	11	1132	1954	3086	0.0098

FILE TYPE =>Zip		FILE SIZE =>10k			PROTOCOL =>HTTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	9	11	20	942	11254	12196	0.0180
2M-[AH-MD5]-[null]	9	18	27	1338	11976	13314	0.0215
3M-[AH-SHA1]-[null]	9	18	27	1338	11976	13314	0.0209
4MA-[ESP-MD5]-[ESP-3DES]	9	18	27	1414	12064	13478	0.0254
5MA-[ESP-SHA1]-[ESP-3DES]	9	18	27	1414	12064	13478	0.0265
6MA-[AH-MD5]-[ESP-3DES]	9	18	27	1522	12196	13718	0.0256
7MA-[AH-SHA1]-[ESP-3DES]	9	18	27	1522	12196	13718	0.0273

FILE TYPE => Zip		FILE SIZE =>100k			PROTOCOL =>HTTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	43	75	118	3187	107779	110966	0.1092
2M-[AH-MD5]-[null]	42	146	188	4969	113493	118462	0.1240
3M-[AH-SHA1]-[null]	42	146	188	4969	113493	118462	0.1370
4MA-[ESP-MD5]-[ESP-3DES]	46	146	192	5780	114096	119876	0.1553
5MA-[ESP-SHA1]-[ESP-3DES]	45.5	146	191.5	5721	114096	119817	0.1632
6MA-[AH-MD5]-[ESP-3DES]	48	146	194	6592	114996	121588	0.1565
7MA-[AH-SHA1]-[ESP-3DES]	48	146	194	6592	114996	121588	0.1684

FILE TYPE =>Zip		FILE SIZE => 1MB			PROTOCOL =>HTTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	372.5	733.5	1106	25271	1098637	1123908	1.2284
2M-[AH-MD5]-[null]	377	1456	1833	42156	1155274	1197430	1.3923
3M-[AH-SHA1]-[null]	378	1456.5	1834.5	42266	1155405	1197671	1.4144
4MA-[ESP-MD5]-[ESP-3DES]	448.5	1456	1904.5	53619	1161132	1214751	1.4400
5MA-[ESP-SHA1]-[ESP-3DES]	464	1456	1920	55448	1161132	1216580	1.5407
6MA-[AH-MD5]-[ESP-3DES]	468.5	1456	1924.5	61601	1169904	1231505	1.4772
7MA-[AH-SHA1]-[ESP-3DES]	463	1456	1919	60886	1169904	1230790	1.5640

FILE TYPE =>Zip		FILE SIZE =>10 MB		PROTOCOL =>HTTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	3590.5	7361	10951.5	237991	1.1E+07	1.1E+07	12.0748
2M-[AH-MD5]-[null]	3648	14479.5	18127.5	401994	1.2E+07	1.2E+07	14.0017
3M-[AH-SHA1]-[null]	3656.5	14481	18137.5	402923	1.2E+07	1.2E+07	14.1860
4MA-[ESP-MD5]-[ESP-3DES]	4447.5	14488	18935.5	525443	1.2E+07	1.2E+07	14.3065
5MA-[ESP-SHA1]-[ESP-3DES]	4513	14489	19002	533114	1.2E+07	1.2E+07	15.0852
6MA-[AH-MD5]-[ESP-3DES]	4407	14488	18895	573536	1.2E+07	1.2E+07	14.3972
7MA-[AH-SHA1]-[ESP-3DES]	4457	14489.5	18946.5	580073	1.2E+07	1.2E+07	15.3266

FILE TYPE =>Doc		FILE SIZE =>1 KB		PROTOCOL =>SMTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	20.5	19.5	40	1882	3710	5592	0.2442
2M-[AH-MD5]-[null]	20	20	40	2729	4544	7273	0.2632
3M-[AH-SHA1]-[null]	19.5	20	39.5	2674	4544	7218	0.2665
4MA-[ESP-MD5]-[ESP-3DES]	20	20	40	2888	4716	7604	0.2706
5MA-[ESP-SHA1]-[ESP-3DES]	20	20	40	2888	4716	7604	0.2816
6MA-[AH-MD5]-[ESP-3DES]	20	20	40	3128	4944	8072	0.2763
7MA-[AH-SHA1]-[ESP-3DES]	20.5	20.5	41	3193	5005	8198	0.2956

FILE TYPE =>Doc		FILE SIZE =>10 KB		PROTOCOL =>SMTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	23.5	28	51.5	2080	16902	18982	0.2726
2M-[AH-MD5]-[null]	24	37	61	3169	18434	21603	0.2752
3M-[AH-SHA1]-[null]	21	37	58	3169	18466	21635	0.2779
4MA-[ESP-MD5]-[ESP-3DES]	23	36.5	59.5	3242	18703	21945	0.2976
5MA-[ESP-SHA1]-[ESP-3DES]	23	36	59	3242	18648	21890	0.3087
6MA-[AH-MD5]-[ESP-3DES]	23.5	36.5	60	3583	18997	22580	0.3008
7MA-[AH-SHA1]-[ESP-3DES]	23.5	36.5	60	3583	18997	22580	0.3119

FILE TYPE =>Doc		FILE SIZE =>100 KB			PROTOCOL =>SMTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	66.5	119.5	186	4918	149238	154156	0.5318
2M-[AH-MD5]-[null]	85.5	208	293.5	9934	157261	167195	0.5764
3M-[AH-SHA1]-[null]	90.5	206.5	297	10484	157369	167853	0.6091
4MA-[ESP-MD5]-[ESP-3DES]	101	203	304	12446	158146	170592	0.6864
5MA-[ESP-SHA1]-[ESP-3DES]	90.5	204.5	295	11207	158248	169455	0.7331
6MA-[AH-MD5]-[ESP-3DES]	88	210	298	11968	159696	171664	0.7219
7MA-[AH-SHA1]-[ESP-3DES]	97	205	302	13138	159610	172748	0.7557

FILE TYPE =>Doc		FILE SIZE =>1MB			PROTOCOL =>SMTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	969.5	1013.5	1983	64506	1505551	1570057	3.0136
2M-[AH-MD5]-[null]	1341.5	1998.5	3340	148069	1583566	1731635	3.3877
3M-[AH-SHA1]-[null]	1352	2000	3352	149249	1583604	1732853	3.5629
4MA-[ESP-MD5]-[ESP-3DES]	1371	1997	3368	162306	1591702	1754008	4.3650
5MA-[ESP-SHA1]-[ESP-3DES]	1345	1999.5	3344.5	159238	1591775	1751013	4.4402
6MA-[AH-MD5]-[ESP-3DES]	990.5	1999.5	2990	129293	1603879	1733172	4.4214
7MA-[AH-SHA1]-[ESP-3DES]	990	2000.5	2990.5	129228	1603913	1733141	4.5314

FILE TYPE =>Doc		FILE SIZE =>10 MB			PROTOCOL => SMTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	9837.5	9946.5	19784	649839	1.5E+07	1.6E+07	25.8324
2M-[AH-MD5]-[null]	13466.5	19723.5	33190	1481793	1.6E+07	1.7E+07	31.6045
3M-[AH-SHA1]-[null]	13868	19866.5	33734.5	1525958	1.6E+07	1.7E+07	32.2174
4MA-[ESP-MD5]-[ESP-3DES]	13786.5	19866	33652.5	1627219	1.6E+07	1.8E+07	40.4770
5MA-[ESP-SHA1]-[ESP-3DES]	13843	19861.5	33704.5	1633886	1.6E+07	1.8E+07	42.6632
6MA-[AH-MD5]-[ESP-3DES]	8477.5	19860	28337.5	522463	1.6E+07	1.7E+07	40.6603
7MA-[AH-SHA1]-[ESP-3DES]	8439	19865.5	28304.5	1097528	1.6E+07	1.7E+07	42.3445

FILE TYPE =>Zip		**FILE SIZE =>1 KB**		**PROTOCOL =>SMTP**			
	Average # of Trans.			Average Network Load			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	20.5	19.5	40	1882	3712	5594	0.2588
2M-[AH-MD5]-[null]	20	20.5	40.5	2729	4595	7324	0.2748
3M-[AH-SHA1]-[null]	20.5	20	40.5	2784	4546	7330	0.2770
4MA-[ESP-MD5]-[ESP-3DES]	20.5	20.5	41	2947	4771	7718	0.2895
5MA-[ESP-SHA1]-[ESP-3DES]	20.5	20.5	41	2947	4771	7718	0.3027
6MA-[AH-MD5]-[ESP-3DES]	21	21	42	3223	5035	8258	0.2914
7MA-[AH-SHA1]-[ESP-3DES]	20	20.5	40.5	3128	5005	8133	0.3036

FILE TYPE =>Zip		**FILE SIZE =>10 KB**		**PROTOCOL =>SMTP**			
	Average # of Trans.			Average Network Load			
	C to S	S to C	Total Trans.	C to S	S to C	Total Load	Average Transfer Time/sec
1-[null]-[null]	23	27.5	50.5	2047	16891	18938	0.2666
2M-[AH-MD5]-[null]	23.5	36.5	60	3114	18471	21585	0.2704
3M-[AH-SHA1]-[null]	23	36.5	59.5	3059	18471	21530	0.2853
4MA-[ESP-MD5]-[ESP-3DES]	24	37	61	3360	18740	22100	0.3036
5MA-[ESP-SHA1]-[ESP-3DES]	23	36	59	3242	18672	21914	0.3161
6MA-[AH-MD5]-[ESP-3DES]	23.5	36.5	60	3583	19021	22604	0.3052
7MA-[AH-SHA1]-[ESP-3DES]	22.5	36.5	59	3453	19038	22491	0.3238

FILE TYPE =>Zip		**FILE SIZE => 100 KB**		**PROTOCOL =>SMTP**			
	Average # of Trans.			Average Network Load			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	76.5	117.5	194	5578	149314	154892	0.5290
2M-[AH-MD5]-[null]	82	205	287	9549	157488	167037	0.5662
3M-[AH-SHA1]-[null]	92	206	298	10649	157414	168063	0.5998
4MA-[ESP-MD5]-[ESP-3DES]	110	210	320	13508	158418	171926	0.6659
5MA-[ESP-SHA1]-[ESP-3DES]	102	205	307	12564	158586	171150	0.6948
6MA-[AH-MD5]-[ESP-3DES]	96	205.5	301.5	11773	159931	171704	0.7032
7MA-[AH-SHA1]-[ESP-3DES]	96.5	205.5	302	13073	159935	173008	0.7472

FILE TYPE =>Zip		FILE SIZE =>1MB			PROTOCOL =>SMTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	971.5	1015	1986.5	64648	1506794	1571442	3.0151
2M-[AH-MD5]-[null]	1348	2002	3350	148809	1584778	1733587	3.5433
3M-[AH-SHA1]-[null]	1350	1999.5	3349.5	149029	1584807	1733836	3.7340
4MA-[ESP-MD5]-[ESP-3DES]	1375.5	2002	3377.5	162837	1593042	1755879	4.4425
5MA-[ESP-SHA1]-[ESP-3DES]	1371.5	2000.5	3372	162365	1593037	1755402	4.5714
6MA-[AH-MD5]-[ESP-3DES]	989.5	2001	2990.5	129163	1605118	1734281	4.5130
7MA-[AH-SHA1]-[ESP-3DES]	995	2000.5	2995.5	129878	1605209	1735087	4.6609

FILE TYPE =>Zip		FILE SIZE => 10 MB			PROTOCOL =>SMTP		
Scenario							
							Average Transfer Time/sec
1-[null]-[null]	ZIP SAME AS DOC						27.4703
2M-[AH-MD5]-[null]							30.0978
3M-[AH-SHA1]-[null]							34.2381
4MA-[ESP-MD5]-[ESP-3DES]							40.1549
5MA-[ESP-SHA1]-[ESP-3DES]							41.9065
6MA-[AH-MD5]-[ESP-3DES]							40.2049
7MA-[AH-SHA1]-[ESP-3DES]							41.9412

Appendix C - Various MTU Compared To The Ideal MTU

{[Various MTU]-[ideal MTU]}/[ideal MTU]*100

Transfer Time

MTU =>600	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	27.13	34.61	35.64
3M-[AH-SHA1]-[null]	17.03	33.67	34.48
4MA-[ESP-MD5]-[ESP-3DES]	10.82	23.42	24.44
5MA-[ESP-SHA1]-[ESP-3DES]	13.25	28.34	27.56
6MA-[AH-MD5]-[ESP-3DES]	11.00	26.06	27.03
7MA-[AH-SHA1]-[ESP-3DES]	16.25	30.18	32.52
MTU =>1500	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	15.20	10.87	11.21
3M-[AH-SHA1]-[null]	16.80	12.72	11.01
4MA-[ESP-MD5]-[ESP-3DES]	1.07	2.10	1.67
5MA-[ESP-SHA1]-[ESP-3DES]	0.51	1.78	0.91
6MA-[AH-MD5]-[ESP-3DES]	0.85	-0.27	1.41
7MA-[AH-SHA1]-[ESP-3DES]	1.61	0.98	1.21
MTU =>8000	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	11.65	-18.32	-18.30
3M-[AH-SHA1]-[null]	13.63	-19.58	-19.16
4MA-[ESP-MD5]-[ESP-3DES]	18.13	-11.35	-13.65
5MA-[ESP-SHA1]-[ESP-3DES]	16.60	-13.69	-14.53
6MA-[AH-MD5]-[ESP-3DES]	19.50	-11.25	-13.48
7MA-[AH-SHA1]-[ESP-3DES]	16.67	-14.87	-15.47
MTU =>16260	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	18.04	-18.81	-21.51
3M-[AH-SHA1]-[null]	24.07	-20.15	-22.41
4MA-[ESP-MD5]-[ESP-3DES]	29.18	14.29	15.17
5MA-[ESP-SHA1]-[ESP-3DES]	24.44	8.19	9.64
6MA-[AH-MD5]-[ESP-3DES]	24.28	11.49	14.80
7MA-[AH-SHA1]-[ESP-3DES]	24.53	6.05	9.45

Network Load

Total Load MTU=> 600	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	15.15	16.22	16.16
3M-[AH-SHA1]-[null]	15.15	16.23	16.17
4MA-[ESP-MD5]-[ESP-3DES]	16.73	18.13	18.14
5MA-[ESP-SHA1]-[ESP-3DES]	16.73	17.96	18.09
6MA-[AH-MD5]-[ESP-3DES]	18.03	19.39	19.50
7MA-[AH-SHA1]-[ESP-3DES]	18.03	19.39	19.58
S to C	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	11.25	11.26	11.29
3M-[AH-SHA1]-[null]	11.25	11.26	11.28
4MA-[ESP-MD5]-[ESP-3DES]	12.73	12.80	12.82
5MA-[ESP-SHA1]-[ESP-3DES]	12.73	12.82	12.82
6MA-[AH-MD5]-[ESP-3DES]	13.80	13.91	13.93
7MA-[AH-SHA1]-[ESP-3DES]	13.80	13.91	13.93
C to S	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	49.18	144.30	147.20
3M-[AH-SHA1]-[null]	49.18	144.92	147.13
4MA-[ESP-MD5]-[ESP-3DES]	50.07	131.20	133.56
5MA-[ESP-SHA1]-[ESP-3DES]	50.07	121.93	128.54
6MA-[AH-MD5]-[ESP-3DES]	51.25	120.94	125.55
7MA-[AH-SHA1]-[ESP-3DES]	51.25	119.89	127.65
Total Load MTU=>1500	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	1.82	1.66	1.64
3M-[AH-SHA1]-[null]	1.82	1.69	1.64
4MA-[ESP-MD5]-[ESP-3DES]	1.86	1.91	1.85
5MA-[ESP-SHA1]-[ESP-3DES]	1.86	1.72	1.78
6MA-[AH-MD5]-[ESP-3DES]	1.83	1.76	1.60
7MA-[AH-SHA1]-[ESP-3DES]	1.83	1.82	1.70
S to C	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	2.03	1.87	1.86
3M-[AH-SHA1]-[null]	2.03	1.87	1.86
4MA-[ESP-MD5]-[ESP-3DES]	2.08	1.96	1.96
5MA-[ESP-SHA1]-[ESP-3DES]	2.08	1.96	1.96
6MA-[AH-MD5]-[ESP-3DES]	2.06	1.92	1.91
7MA-[AH-SHA1]-[ESP-3DES]	2.06	1.92	1.91
C to S	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	-3.64	-4.22
3M-[AH-SHA1]-[null]	0.00	-2.98	-4.17
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.66	-0.71
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	-3.15	-2.08
6MA-[AH-MD5]-[ESP-3DES]	0.00	-1.05	-4.44
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.10	-2.41

Total Load MTU=>8000	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	-5.09	-6.68	-6.70
3M-[AH-SHA1]-[null]	-5.09	-6.70	-6.71
4MA-[ESP-MD5]-[ESP-3DES]	-5.47	-7.57	-7.64
5MA-[ESP-SHA1]-[ESP-3DES]	-5.47	-7.74	-7.72
6MA-[AH-MD5]-[ESP-3DES]	-6.09	-8.64	-8.68
7MA-[AH-SHA1]-[ESP-3DES]	-6.09	-8.71	-8.64
S to C	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	-2.95	-4.09	-4.11
3M-[AH-SHA1]-[null]	-2.95	-4.09	-4.11
4MA-[ESP-MD5]-[ESP-3DES]	-3.13	-4.33	-4.33
5MA-[ESP-SHA1]-[ESP-3DES]	-3.13	-4.33	-4.33
6MA-[AH-MD5]-[ESP-3DES]	-3.60	-4.95	-4.95
7MA-[AH-SHA1]-[ESP-3DES]	-3.60	-4.95	-4.95
C to S	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	-23.85	-73.47	-76.45
3M-[AH-SHA1]-[null]	-23.85	-74.28	-76.52
4MA-[ESP-MD5]-[ESP-3DES]	-25.04	-76.34	-79.31
5MA-[ESP-SHA1]-[ESP-3DES]	-25.04	-76.64	-78.81
6MA-[AH-MD5]-[ESP-3DES]	-25.62	-77.02	-79.68
7MA-[AH-SHA1]-[ESP-3DES]	-25.62	-77.67	-79.15
Total Load MTU=>16260	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	-5.75	-7.30	-7.29
3M-[AH-SHA1]-[null]	-5.75	-7.30	-7.30
4MA-[ESP-MD5]-[ESP-3DES]	-6.17	-8.36	-8.38
5MA-[ESP-SHA1]-[ESP-3DES]	-6.17	-8.57	-8.51
6MA-[AH-MD5]-[ESP-3DES]	-6.86	-9.61	-9.59
7MA-[AH-SHA1]-[ESP-3DES]	-6.86	-9.66	-9.58
S to C	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	-3.60	-4.47	-4.48
3M-[AH-SHA1]-[null]	-3.60	-4.47	-4.48
4MA-[ESP-MD5]-[ESP-3DES]	-3.91	-4.85	-4.84
5MA-[ESP-SHA1]-[ESP-3DES]	-3.91	-4.85	-4.84
6MA-[AH-MD5]-[ESP-3DES]	-4.47	-5.60	-5.59
7MA-[AH-SHA1]-[ESP-3DES]	-4.47	-5.60	-5.59
C to S	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	-24.59	-80.62	-82.75
3M-[AH-SHA1]-[null]	-24.59	-80.57	-82.79
4MA-[ESP-MD5]-[ESP-3DES]	-25.04	-83.06	-85.12
5MA-[ESP-SHA1]-[ESP-3DES]	-25.04	-83.88	-85.60
6MA-[AH-MD5]-[ESP-3DES]	-25.62	-83.95	-85.74
7MA-[AH-SHA1]-[ESP-3DES]	-25.62	-84.12	-85.69

Number of Transactions

Total Trans. MTU=> 600	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	90.00	150.32	151.17
3M-[AH-SHA1]-[null]	90.00	150.54	151.02
4MA-[ESP-MD5]-[ESP-3DES]	90.00	144.83	145.79
5MA-[ESP-SHA1]-[ESP-3DES]	90.00	140.79	143.75
6MA-[AH-MD5]-[ESP-3DES]	90.00	140.57	142.57
7MA-[AH-SHA1]-[ESP-3DES]	90.00	140.08	143.38
S to C	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	109.09	152.23	153.04
3M-[AH-SHA1]-[null]	109.09	152.23	152.86
4MA-[ESP-MD5]-[ESP-3DES]	109.09	151.84	152.85
5MA-[ESP-SHA1]-[ESP-3DES]	109.09	151.97	152.86
6MA-[AH-MD5]-[ESP-3DES]	109.09	151.84	152.87
7MA-[AH-SHA1]-[ESP-3DES]	109.09	151.84	152.85
C to S	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	66.67	146.62	147.46
3M-[AH-SHA1]-[null]	66.67	147.25	147.38
4MA-[ESP-MD5]-[ESP-3DES]	66.67	132.92	133.74
5MA-[ESP-SHA1]-[ESP-3DES]	66.67	122.75	128.70
6MA-[AH-MD5]-[ESP-3DES]	66.67	122.32	125.70
7MA-[AH-SHA1]-[ESP-3DES]	66.67	121.24	127.80
Total Trans. MTU=> 1500	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	35.00	58.73	58.91
3M-[AH-SHA1]-[null]	35.00	58.95	58.87
4MA-[ESP-MD5]-[ESP-3DES]	35.00	57.44	57.40
5MA-[ESP-SHA1]-[ESP-3DES]	35.00	54.72	56.14
6MA-[AH-MD5]-[ESP-3DES]	35.00	55.74	55.07
7MA-[AH-SHA1]-[ESP-3DES]	35.00	55.96	55.92
S to C	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	63.64	90.88	90.75
3M-[AH-SHA1]-[null]	63.64	90.94	90.72
4MA-[ESP-MD5]-[ESP-3DES]	63.64	90.81	91.37
5MA-[ESP-SHA1]-[ESP-3DES]	63.64	90.81	91.39
6MA-[AH-MD5]-[ESP-3DES]	63.64	90.81	91.37
7MA-[AH-SHA1]-[ESP-3DES]	63.64	90.81	91.39
C to S	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	-3.69	-4.29
3M-[AH-SHA1]-[null]	0.00	-3.32	-4.25
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.67	-0.63
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	-3.49	-2.07
6MA-[AH-MD5]-[ESP-3DES]	0.00	-1.06	-4.40
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.11	-2.40

Total Trans. MTU=8000	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	-10.00	-22.39	-22.74
3M-[AH-SHA1]-[null]	-10.00	-22.58	-22.85
4MA-[ESP-MD5]-[ESP-3DES]	-10.00	-25.74	-26.41
5MA-[ESP-SHA1]-[ESP-3DES]	-10.00	-26.89	-26.87
6MA-[AH-MD5]-[ESP-3DES]	-10.00	-26.90	-27.36
7MA-[AH-SHA1]-[ESP-3DES]	-10.00	-27.35	-27.08
S to C	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	9.09	4.53	4.38
3M-[AH-SHA1]-[null]	9.09	4.59	4.30
4MA-[ESP-MD5]-[ESP-3DES]	9.09	4.59	4.61
5MA-[ESP-SHA1]-[ESP-3DES]	9.09	4.59	4.64
6MA-[AH-MD5]-[ESP-3DES]	9.09	4.59	4.64
7MA-[AH-SHA1]-[ESP-3DES]	9.09	4.59	4.64
C to S	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	-33.33	-74.65	-76.57
3M-[AH-SHA1]-[null]	-33.33	-75.48	-76.64
4MA-[ESP-MD5]-[ESP-3DES]	-33.33	-77.34	-79.42
5MA-[ESP-SHA1]-[ESP-3DES]	-33.33	-77.67	-78.91
6MA-[AH-MD5]-[ESP-3DES]	-33.33	-77.90	-79.77
7MA-[AH-SHA1]-[ESP-3DES]	-33.33	-78.55	-79.24
Total Trans. MTU=>16260	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	-10.00	-26.20	-26.19
3M-[AH-SHA1]-[null]	-10.00	-26.14	-26.30
4MA-[ESP-MD5]-[ESP-3DES]	-10.00	-29.59	-29.83
5MA-[ESP-SHA1]-[ESP-3DES]	-10.00	-30.98	-31.92
6MA-[AH-MD5]-[ESP-3DES]	-10.00	-30.87	-30.92
7MA-[AH-SHA1]-[ESP-3DES]	-10.00	-31.15	-30.82
S to C	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	9.09	2.49	2.37
3M-[AH-SHA1]-[null]	9.09	2.49	2.28
4MA-[ESP-MD5]-[ESP-3DES]	9.09	2.49	2.60
5MA-[ESP-SHA1]-[ESP-3DES]	9.09	2.49	2.63
6MA-[AH-MD5]-[ESP-3DES]	9.09	2.49	2.61
7MA-[AH-SHA1]-[ESP-3DES]	9.09	2.49	2.61
C to S	**10 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	-33.33	-81.91	-82.87
3M-[AH-SHA1]-[null]	-33.33	-81.86	-82.93
4MA-[ESP-MD5]-[ESP-3DES]	-33.33	-84.15	-85.24
5MA-[ESP-SHA1]-[ESP-3DES]	-33.33	-84.97	-88.99
6MA-[AH-MD5]-[ESP-3DES]	-33.33	-84.91	-85.84
7MA-[AH-SHA1]-[ESP-3DES]	-33.33	-85.07	-85.79

Appendix D - Testbed 1 Average Data

FILE TYPE =>Doc	FILE SIZE =>1 KB			PROTOCOL =>HTTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	6	5	11	747	1636	2383	0.0047
2M-[AH-MD5]-[null]	6	5	11	1011	1856	2867	0.0073
3M-[AH-SHA1]-[null]	6	5	11	1011	1856	2867	0.0076
4MA-[ESP-MD5]-[ESP-3DES]	6	5	11	1060	1894	2954	0.0091
5MA-[ESP-SHA1]-[ESP-3DES]	6	5	11	1060	1894	2954	0.0099
6MA-[AH-MD5]-[ESP-3DES]	6	5	11	1132	1954	3086	0.0093
7MA-[AH-SHA1]-[ESP-3DES]	6	5	11	1132	1954	3086	0.0101

FILE TYPE =>Doc	FILE SIZE =>10k			PROTOCOL =>HTTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	9	11	20	946	11247	12193	0.0165
2M-[AH-MD5]-[null]	9	11	20	1342	11731	13073	0.0186
3M-[AH-SHA1]-[null]	9	11	20	1342	11731	13073	0.0186
4MA-[ESP-MD5]-[ESP-3DES]	9	11	20	1414	11810	13224	0.0244
5MA-[ESP-SHA1]-[ESP-3DES]	9	11	20	1414	11810	13224	0.0264
6MA-[AH-MD5]-[ESP-3DES]	9	11	20	1522	11942	13464	0.0251

FILE TYPE =>Doc	FILE SIZE =>100k			PROTOCOL =>HTTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	42	74	116	3125	107570	110695	0.1074
2M-[AH-MD5]-[null]	44	78	122	5193	111266	116459	0.1170
3M-[AH-SHA1]-[null]	44	78	122	5193	111266	116459	0.1295
4MA-[ESP-MD5]-[ESP-3DES]	49.5	78	127.5	6193	111740	117933	0.1530
5MA-[ESP-SHA1]-[ESP-3DES]	49	78	127	6134	111740	117874	0.1604
6MA-[AH-MD5]-[ESP-3DES]	49	78	127	6722	112676	119398	0.1535
7MA-[AH-SHA1]-[ESP-3DES]	48.5	78	126.5	6657	112676	119333	0.1621

FILE TYPE =>Doc		FILE SIZE =>1MB		PROTOCOL =>HTTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	373.5	731	1104.5	25345	1097648	1122993	1.1621
2M-[AH-MD5]-[null]	392.5	762	1154.5	43869	1133210	1177079	1.2519
3M-[AH-SHA1]-[null]	391.5	762	1153.5	43759	1133210	1176969	1.2763
4MA-[ESP-MD5]-[ESP-3DES]	448	762	1210	53560	1137804	1191364	1.4121
5MA-[ESP-SHA1]-[ESP-3DES]	472.5	762	1234.5	56274	1137804	1194078	1.5191
6MA-[AH-MD5]-[ESP-3DES]	470.5	762	1232.5	61861	1146948	1208809	1.4592
7MA-[AH-SHA1]-[ESP-3DES]	475.5	762	1237.5	62511	1146948	1209459	1.5463
FILE TYPE =>Doc		**FILE SIZE =>10 MB**		**PROTOCOL =>HTTP**			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	3639.5	7310.5	10950	241377	10971128	11212505	12.0117
2M-[AH-MD5]-[null]	3826	7592	11418	421556	11323743	11745299	12.5692
3M-[AH-SHA1]-[null]	3834	7597	11431	422436	11324293	11746729	12.7595
4MA-[ESP-MD5]-[ESP-3DES]	4433	7573.5	12006.5	523790	11367185	11890975	14.0507
5MA-[ESP-SHA1]-[ESP-3DES]	4585	7572	12157	541726	11366992	11908718	15.0714
6MA-[AH-MD5]-[ESP-3DES]	4622.5	7572	12194.5	601621	11457856	12059477	14.1398
7MA-[AH-SHA1]-[ESP-3DES]	4605	7572	12177	599346	11457856	12057202	15.1546
FILE TYPE =>Doc		**FILE SIZE =>1 KB**		**PROTOCOL =>SMTP**			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	20.5	19.5	40	1882	3710	5592	0.2442
2M-[AH-MD5]-[null]	20.5	19.5	40	2784	4559	7343	0.2667
3M-[AH-SHA1]-[null]	20	19	39	2729	4510	7239	0.2874
4MA-[ESP-MD5]-[ESP-3DES]	19.5	19	38.5	2829	4682	7511	0.2938
5MA-[ESP-SHA1]-[ESP-3DES]	20	19	39	2888	4682	7570	0.3032
6MA-[AH-MD5]-[ESP-3DES]	20	19	39	3128	4910	8038	0.2960
7MA-[AH-SHA1]-[ESP-3DES]	20	19	39	3128	4910	8038	0.3064

FILE TYPE =>Doc		FILE SIZE =>10 KB		PROTOCOL =>SMTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	23.5	28	51.5	2080	16902	18982	0.2726
2M-[AH-MD5]-[null]	24	28.5	52.5	3169	18177	21346	0.3094
3M-[AH-SHA1]-[null]	23.5	28	51.5	3114	18128	21242	0.3110
4MA-[ESP-MD5]-[ESP-3DES]	23	28	51	3242	18352	21594	0.3135
5MA-[ESP-SHA1]-[ESP-3DES]	24	28	52	3360	18352	21712	0.3239
6MA-[AH-MD5]-[ESP-3DES]	23.5	28.5	52	3583	18749	22332	0.3153
7MA-[AH-SHA1]-[ESP-3DES]	23.5	29	52.5	3583	18810	22393	0.3254

FILE TYPE =>Doc		FILE SIZE =>100 KB		PROTOCOL =>SMTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	66.5	119.5	186	4918	149238	154156	0.5318
2M-[AH-MD5]-[null]	79.5	120	199.5	9274	154548	163822	0.5704
3M-[AH-SHA1]-[null]	82.5	119.5	202	9604	154493	164097	0.6421
4MA-[ESP-MD5]-[ESP-3DES]	112	120.5	232.5	13744	155370	169114	0.6642
5MA-[ESP-SHA1]-[ESP-3DES]	107	120	227	13154	155352	168506	0.7128
6MA-[AH-MD5]-[ESP-3DES]	103.5	120	223.5	13983	156792	170775	0.6667
7MA-[AH-SHA1]-[ESP-3DES]	111	120	231	14958	156792	171750	0.7155

FILE TYPE =>Doc		FILE SIZE =>1MB		PROTOCOL =>SMTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	969.5	1013.5	1983	64506	1505551	1570057	3.0136
2M-[AH-MD5]-[null]	1021	1056	2077	112839	1554808	1667647	3.3611
3M-[AH-SHA1]-[null]	1014.5	1057	2071.5	112124	1554924	1667048	3.4707
4MA-[ESP-MD5]-[ESP-3DES]	1369.5	1056.5	2426	162129	1561279	1723408	4.4918
5MA-[ESP-SHA1]-[ESP-3DES]	1374	1056.5	2430.5	162660	1561279	1723939	4.5757
6MA-[AH-MD5]-[ESP-3DES]	1379.5	1056	2435.5	179863	1573900	1753763	4.5259
7MA-[AH-SHA1]-[ESP-3DES]	1381	1056	2437	180058	1573884	1753942	4.6338

FILE TYPE =>Doc			FILE SIZE =>10 MB			PROTOCOL =>SMTP	
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	9838.5	9946.5	19785	649905	15030371	15680276	25.8666
2M-[AH-MD5]-[null]	10317.5	10390.5	20708	1135404	15516795	16652199	29.4084
3M-[AH-SHA1]-[null]	10262	10393	20655	1129349	15517813	16647162	32.0987
4MA-[ESP-MD5]-[ESP-3DES]	13834	10392	24226	1632940	15579472	17212412	40.3855
5MA-[ESP-SHA1]-[ESP-3DES]	13791.5	10391.5	24183	1627925	15579409	17207334	42.0157
6MA-[AH-MD5]-[ESP-3DES]	13930	10390.5	24320.5	1811433	15703973	17515406	41.1116
7MA-[AH-SHA1]-[ESP-3DES]	13946	10391.5	24337.5	1813508	15704103	17517611	42.6208

Ident Protocol data

The transfer time for the Identity protocol was found by subtracting the time to synchronize at the beginning of a connection from the end time of the Ident protocol.

Ident overhead	**Transactions**		**Load**		**Transfer time**
	C to S	**S to C**	**C to S**	**S to C**	
1-[null]-[null]	6	5	413	372	0.05345
2M-[AH-MD5]-[null]	6	5	677	592	0.05626
3M-[AH-SHA1]-[null]	6	5	677	592	0.05737
4MA-[ESP-MD5]-[ESP-3DES]	6	5	724	630	0.05726
5MA-[ESP-SHA1]-[ESP-3DES]	6	5	724	630	0.05827
6MA-[AH-MD5]-[ESP-3DES]	6	5	796	690	0.05752
7MA-[AH-SHA1]-[ESP-3DES]	6	5	796	690	0.05881

Percentage Ident Overhead

Equation used:(Ident metric/Total metric)*100

Transactions	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	27.50	21.36	5.91	0.55	0.06
2M-[AH-MD5]-[null]	27.50	20.95	5.51	0.53	0.05
3M-[AH-SHA1]-[null]	28.21	21.36	5.45	0.53	0.05
4MA-[ESP-MD5]-[ESP-3DES]	28.57	21.57	4.73	0.45	0.05
5MA-[ESP-SHA1]-[ESP-3DES]	28.21	21.15	4.85	0.45	0.05
6MA-[AH-MD5]-[ESP-3DES]	28.21	21.15	4.92	0.45	0.05
7MA-[AH-SHA1]-[ESP-3DES]	28.21	20.95	4.76	0.45	0.05

Network Load	1 KB	10 KB	100 KB	1 MB	10 MB
1-[null]-[null]	14.04	4.14	0.51	0.05	0.01
2M-[AH-MD5]-[null]	17.28	5.94	0.77	0.08	0.01
3M-[AH-SHA1]-[null]	17.53	5.97	0.77	0.08	0.01
4MA-[ESP-MD5]-[ESP-3DES]	18.03	6.27	0.80	0.08	0.01
5MA-[ESP-SHA1]-[ESP-3DES]	17.89	6.24	0.80	0.08	0.01
6MA-[AH-MD5]-[ESP-3DES]	18.49	6.65	0.87	0.08	0.01
7MA-[AH-SHA1]-[ESP-3DES]	18.49	6.64	0.87	0.08	0.01
Transfer Time	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	21.89	19.61	10.05	1.77	0.21
2M-[AH-MD5]-[null]	21.10	18.18	9.86	1.67	0.19
3M-[AH-SHA1]-[null]	19.96	18.45	8.93	1.65	0.18
4MA-[ESP-MD5]-[ESP-3DES]	19.49	18.26	8.62	1.27	0.14
5MA-[ESP-SHA1]-[ESP-3DES]	19.22	17.99	8.18	1.27	0.14
6MA-[AH-MD5]-[ESP-3DES]	19.43	18.24	8.63	1.27	0.14
7MA-[AH-SHA1]-[ESP-3DES]	19.20	18.07	8.22	1.27	0.14

SMTP without Ident

FILE TYPE =>Doc	FILE SIZE =>1 KB			PROTOCOL => SMTP			
Scenario	Average # of Trans.			Average Network Load			
	C to S	S to C	Total Trans.	C to S	S to C	Total Load	Average Transfer Time/sec
1-[null]-[null]	14.5	14.5	29	1469	3338	4807	0.1907
2M-[AH-MD5]-[null]	14.5	14.5	29	2107	3967	6074	0.2104
3M-[AH-SHA1]-[null]	14	14	28	2052	3918	5970	0.2301
4MA-[ESP-MD5]-[ESP-3DES]	13.5	14	27.5	2105	4052	6157	0.2366
5MA-[ESP-SHA1]-[ESP-3DES]	14	14	28	2164	4052	6216	0.2449
6MA-[AH-MD5]-[ESP-3DES]	14	14	28	2332	4220	6552	0.2385
7MA-[AH-SHA1]-[ESP-3DES]	14	14	28	2332	4220	6552	0.2475
FILE TYPE =>Doc	FILE SIZE =>10 KB			PROTOCOL =>SMTP			
Scenario	Average # of Trans.			Average Network Load			
	C to S	S to C	Total Trans.	C to S	S to C	Total Load	Average Transfer Time/sec
1-[null]-[null]	17.5	23	40.5	1667	16530	18197	0.2191
2M-[AH-MD5]-[null]	18	23.5	41.5	2492	17585	20077	0.2532
3M-[AH-SHA1]-[null]	17.5	23	40.5	2437	17536	19973	0.2536
4MA-[ESP-MD5]-[ESP-3DES]	17	23	40	2518	17722	20240	0.2562
5MA-[ESP-SHA1]-[ESP-3DES]	18	23	41	2636	17722	20358	0.2656
6MA-[AH-MD5]-[ESP-3DES]	17.5	23.5	41	2787	18059	20846	0.2578
7MA-[AH-SHA1]-[ESP-3DES]	17.5	24	41.5	2787	18120	20907	0.2666

FILE TYPE =>Doc		FILE SIZE =>100 KB		PROTOCOL =>SMTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	60.5	114.5	175	4505	148866	153371	0.4784
2M-[AH-MD5]-[null]	73.5	115	188.5	8597	153956	162553	0.5142
3M-[AH-SHA1]-[null]	76.5	114.5	191	8927	153901	162828	0.5847
4MA-[ESP-MD5]-[ESP-3DES]	106	115.5	221.5	13020	154740	167760	0.6070
5MA-[ESP-SHA1]-[ESP-3DES]	101	115	216	12430	154722	167152	0.6545
6MA-[AH-MD5]-[ESP-3DES]	97.5	115	212.5	13187	156102	169289	0.6091
7MA-[AH-SHA1]-[ESP-3DES]	105	115	220	14162	156102	170264	0.6567
FILE TYPE =>Doc		**FILE SIZE =>1MB**		**PROTOCOL =>SMTP**			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	963.5	1008.5	1972	64093	1505179	1569272	2.9601
2M-[AH-MD5]-[null]	1015	1051	2066	112162	1554216	1666378	3.3049
3M-[AH-SHA1]-[null]	1008.5	1052	2060.5	111447	1554332	1665779	3.4133
4MA-[ESP-MD5]-[ESP-3DES]	1363.5	1051.5	2415	161405	1560649	1722054	4.4345
5MA-[ESP-SHA1]-[ESP-3DES]	1368	1051.5	2419.5	161936	1560649	1722585	4.5174
6MA-[AH-MD5]-[ESP-3DES]	1373.5	1051	2424.5	179067	1573210	1752277	4.4684
7MA-[AH-SHA1]-[ESP-3DES]	1375	1051	2426	179262	1573194	1752456	4.5750
FILE TYPE =>Doc		**FILE SIZE =>10 MB**		**PROTOCOL =>SMTP**			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	9832.5	9941.5	19774	649492	15029999	15679491	25.8132
2M-[AH-MD5]-[null]	10311.5	10385.5	20697	1134727	15516203	16650930	29.3521
3M-[AH-SHA1]-[null]	10256	10388	20644	1128672	15517221	16645893	32.0413
4MA-[ESP-MD5]-[ESP-3DES]	13828	10387	24215	1632216	15578842	17211058	40.3283
5MA-[ESP-SHA1]-[ESP-3DES]	13785.5	10386.5	24172	1627201	15578779	17205980	41.9574
6MA-[AH-MD5]-[ESP-3DES]	13924	10385.5	24309.5	1810637	15703283	17513920	41.0540
7MA-[AH-SHA1]-[ESP-3DES]	13940	10386.5	24326.5	1812712	15703413	17516125	42.5620

Appendix E - Testbed 2 Average Data

The data for number of transactions and the network load for 3M,5MA and 7MA was not recorded because it is the same as 2M,4MA, and 6MA respectively.

FILE TYPE =>Zip	**FILE SIZE =>1 KB**			**PROTOCOL =>HTTP**			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	6	5	11	743	1649	2392	0.0432
2M-[AH-MD5]-[null]	6	5	11	1007	1869	2876	0.0563
3M-[AH-SHA1]-[null]							0.0568
4MA-[ESP-MD5]-[ESP-3DES]	6	5	11	1060	1914	2974	0.0566
5MA-[ESP-SHA1]-[ESP-3DES]							0.0562
6MA-[AH-MD5]-[ESP-3DES]	6	5	11	1132	1974	3106	0.0567
7MA-[AH-SHA1]-[ESP-3DES]							0.0560

FILE TYPE =>Zip	**FILE SIZE =>10k**			**PROTOCOL =>HTTP**			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	9	11	20	942	11298	12240	0.1330
2M-[AH-MD5]-[null]	9	11	20	1338	11782	13120	0.1596
3M-[AH-SHA1]-[null]							0.1626
4MA-[ESP-MD5]-[ESP-3DES]	9	11	20	1414	11854	13268	0.1654
5MA-[ESP-SHA1]-[ESP-3DES]							0.1705
6MA-[AH-MD5]-[ESP-3DES]	9	11	20	1522	11986	13508	0.1784
7MA-[AH-SHA1]-[ESP-3DES]							0.1787

FILE TYPE =>Zip	**FILE SIZE =>100k**			**PROTOCOL =>HTTP**			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	42	75	117	3121	108079	111200	0.7357
2M-[AH-MD5]-[null]	52	78.5	130.5	6176	111721	117897	0.7507
3M-[AH-SHA1]-[null]							0.7722
4MA-[ESP-MD5]-[ESP-3DES]	51	79	130	6718	112350	119068	0.7790
5MA-[ESP-SHA1]-[ESP-3DES]							0.7798
6MA-[AH-MD5]-[ESP-3DES]	50.5	79	129.5	7701	113298	120999	0.7740
7MA-[AH-SHA1]-[ESP-3DES]							0.7749

FILE TYPE =>Zip		FILE SIZE =>1MB		PROTOCOL =>HTTP			
Scenario	**Average # of Trans.**			**Average Network Load**			0.0000
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	412.5	733.5	1146	28193	1101577	1129770	6.7039
2M-[AH-MD5]-[null]	434	766	1200	49092	1137550	1186642	7.0698
3M-[AH-SHA1]-[null]							7.1386
4MA-[ESP-MD5]-[ESP-3DES]	442	766.5	1208.5	53578	1142217	1195795	7.1489
5MA-[ESP-SHA1]-[ESP-3DES]							7.1551
6MA-[AH-MD5]-[ESP-3DES]	449	766	1215	60378	1151348	1211726	7.1022
7MA-[AH-SHA1]-[ESP-3DES]							7.1389
FILE TYPE =>Zip		**FILE SIZE =>10 MB**		**PROTOCOL =>HTTP**			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	4066	7285.5	11351.5	275361	10995120	11270481	65.7311
2M-[AH-MD5]-[null]	4275.5	7636.5	11912	477813	11388765	11866578	68.5524
3M-[AH-SHA1]-[null]							68.6920
4MA-[ESP-MD5]-[ESP-3DES]	4264.5	7637	11901.5	512488	11436034	11948522	68.9636
5MA-[ESP-SHA1]-[ESP-3DES]							68.9914
6MA-[AH-MD5]-[ESP-3DES]	4268	7637	11905	564488	11519791	12084279	69.7627
7MA-[AH-SHA1]-[ESP-3DES]							70.1619
FILE TYPE =>Zip		**FILE SIZE =>1 KB**		**PROTOCOL =>SMTP**			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	18.5	18	36.5	1811	3737	5548	3.2263
2M-[AH-MD5]-[null]	18	19	37	2570	4625	7195	3.2436
3M-[AH-SHA1]-[null]							3.2519
4MA-[ESP-MD5]-[ESP-3DES]	19	19	38	2810	4734	7544	3.2564
5MA-[ESP-SHA1]-[ESP-3DES]							3.2578
6MA-[AH-MD5]-[ESP-3DES]	18	19	37	2908	4962	7870	3.2545
7MA-[AH-SHA1]-[ESP-3DES]							3.2588

FILE TYPE =>Zip		FILE SIZE =>10 KB		PROTOCOL =>SMTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	24	26.5	50.5	2174	16977	19151	3.3261
2M-[AH-MD5]-[null]	22.5	27	49.5	3065	18185	21250	3.3250
3M-[AH-SHA1]-[null]							3.3439
4MA-[ESP-MD5]-[ESP-3DES]	23	27	50	3282	18334	21616	3.3505
5MA-[ESP-SHA1]-[ESP-3DES]							3.3521
6MA-[AH-MD5]-[ESP-3DES]	23.5	27	50.5	3623	18658	22281	3.3505
7MA-[AH-SHA1]-[ESP-3DES]							3.3509

FILE TYPE =>Zip		FILE SIZE =>100 KB		PROTOCOL =>SMTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	74	115	189	5528	149655	155183	4.2328
2M-[AH-MD5]-[null]	72	118.5	190.5	8493	155108	163601	4.2659
3M-[AH-SHA1]-[null]							4.2886
4MA-[ESP-MD5]-[ESP-3DES]	73.5	119	192.5	9313	155862	165175	4.2969
5MA-[ESP-SHA1]-[ESP-3DES]							4.3002
6MA-[AH-MD5]-[ESP-3DES]	72.5	120	192.5	9923	157354	167277	4.2934
7MA-[AH-SHA1]-[ESP-3DES]							4.3001

FILE TYPE =>Zip		FILE SIZE =>1MB		PROTOCOL =>SMTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	576	1017	1593	39404	1511037	1550441	12.6604
2M-[AH-MD5]-[null]	593	1062.5	1655.5	66395	1560910	1627305	13.0574
3M-[AH-SHA1]-[null]							13.0716
4MA-[ESP-MD5]-[ESP-3DES]	601.5	1061.5	1663	72861	1567211	1640072	13.1174
5MA-[ESP-SHA1]-[ESP-3DES]							13.2582
6MA-[AH-MD5]-[ESP-3DES]	592.5	1061.5	1654	78563	1579945	1658508	13.2347
7MA-[AH-SHA1]-[ESP-3DES]							13.2767

FILE TYPE =>Zip		FILE SIZE =>10 MB		PROTOCOL =>SMTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	5648	10023.5	15671.5	383144	15100328	15483472	93.3820
2M-[AH-MD5]-[null]	5819	10466	16285	648600	15577853	16226453	97.4113
3M-[AH-SHA1]-[null]							97.8139
4MA-[ESP-MD5]-[ESP-3DES]	5837	10495.5	16332.5	699823	15687691	16387514	98.0897
5MA-[ESP-SHA1]-[ESP-3DES]							98.1599
6MA-[AH-MD5]-[ESP-3DES]	5884.5	10528.5	16413	775849	15860500	16636349	98.9644
7MA-[AH-SHA1]-[ESP-3DES]							99.7529

Ident Protocol data

The transfer time for the Identity protocol was found by subtracting the time to synchronize at the beginning of a connection from the end time of the Ident protocol.

Ident overhead	**Transactions**		**Load**		**Transfer time**
	C to S	S to C	C to S	S to C	
1-[null]-[null]	6	5	413	392	3.0568
2M-[AH-MD5]-[null]	6	5	677	612	3.0556
3M-[AH-SHA1]-[null]	6	5	677	612	3.0572
4MA-[ESP-MD5]-[ESP-3DES]	6	5	724	650	3.0503
5MA-[ESP-SHA1]-[ESP-3DES]	6	5	724	650	3.0571
6MA-[AH-MD5]-[ESP-3DES]	6	5	796	710	3.0623
7MA-[AH-SHA1]-[ESP-3DES]	6	5	796	710	3.0683

Ident Protocol Overhead Percentage

Transactions	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	30.14	21.78	5.82	0.69	0.07
2M-[AH-MD5]-[null]	29.73	22.22	5.77	0.66	0.07
4MA-[ESP-MD5]-[ESP-3DES]	28.95	22.00	5.71	0.66	0.07
6MA-[AH-MD5]-[ESP-3DES]	29.73	21.78	5.71	0.67	0.07
Network Load	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	14.51	4.20	0.52	0.05	0.01
2M-[AH-MD5]-[null]	17.92	6.07	0.79	0.08	0.01
4MA-[ESP-MD5]-[ESP-3DES]	18.21	6.36	0.83	0.08	0.01
6MA-[AH-MD5]-[ESP-3DES]	19.1	6.76	0.90	0.09	0.01
Transfer Time	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	94.75	92.63	71.92	23.51	3.27
2M-[AH-MD5]-[null]	94.20	91.90	71.63	23.40	3.14
4MA-[ESP-MD5]-[ESP-3DES]	93.67	91.04	70.99	23.25	3.11
6MA-[AH-MD5]-[ESP-3DES]	94.09	91.40	71.33	23.14	3.09

SMTP without Ident

FILE TYPE =>Zip		FILE SIZE =>1 KB		PROTOCOL =>SMTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	12.5	13	25.5	1805	3345	5150	0.1695
2M-[AH-MD5]-[null]	12	14	26	2565	4013	6578	0.1879
3M-[AH-SHA1]-[null]							0.1948
4MA-[ESP-MD5]-[ESP-3DES]	13	14	27	2810	4084	6894	0.2061
5MA-[ESP-SHA1]-[ESP-3DES]							0.2008
6MA-[AH-MD5]-[ESP-3DES]	12	14	26	2908	4252	7160	0.1921
7MA-[AH-SHA1]-[ESP-3DES]							0.1905

FILE TYPE =>Zip		FILE SIZE =>10 KB		PROTOCOL =>SMTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	18	21.5	39.5	2168	16585	18753	0.2693
2M-[AH-MD5]-[null]	16.5	22	38.5	3060	17573	20633	0.2694
3M-[AH-SHA1]-[null]							0.2868
4MA-[ESP-MD5]-[ESP-3DES]	17	22	39	3282	17684	20966	0.3002
5MA-[ESP-SHA1]-[ESP-3DES]							0.2951
6MA-[AH-MD5]-[ESP-3DES]	17.5	22	39.5	3623	17948	21571	0.2882
7MA-[AH-SHA1]-[ESP-3DES]							0.2826

FILE TYPE =>Zip		FILE SIZE =>100 KB		PROTOCOL =>SMTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	68	110	178	5522	149263	154785	1.1760!
2M-[AH-MD5]-[null]	66	113.5	179.5	8488	154496	162984	1.2102
3M-[AH-SHA1]-[null]							1.2314
4MA-[ESP-MD5]-[ESP-3DES]	67.5	114	181.5	9313	155212	164525	1.2466
5MA-[ESP-SHA1]-[ESP-3DES]							1.2431
6MA-[AH-MD5]-[ESP-3DES]	66.5	115	181.5	9923	156644	166567	1.2310
7MA-[AH-SHA1]-[ESP-3DES]							1.2318

FILE TYPE =>Zip		**FILE SIZE =>1MB**		**PROTOCOL =>SMTP**			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	570	1012	1582	39398	1510645	1550043	9.6036
2M-[AH-MD5]-[null]	587	1057.5	1644.5	66390	1560298	1626688	10.0018
3M-[AH-SHA1]-[null]							10.0145
4MA-[ESP-MD5]-[ESP-3DES]	595.5	1056.5	1652	72861	1566561	1639422	10.0671
5MA-[ESP-SHA1]-[ESP-3DES]							10.2011
6MA-[AH-MD5]-[ESP-3DES]	586.5	1056.5	1643	78563	1579235	1657798	10.1723
7MA-[AH-SHA1]-[ESP-3DES]							10.2084

FILE TYPE =>Zip		**FILE SIZE =>10 MB**		**PROTOCOL =>SMTP**			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	5642	10018.5	15660.5	383138	15099936	15483074	90.3252
2M-[AH-MD5]-[null]	5813	10461	16274	648595	15577241	16225836	94.3556
3M-[AH-SHA1]-[null]							94.7567
4MA-[ESP-MD5]-[ESP-3DES]	5831	10490.5	16321.5	699823	15687041	16386864	95.0394
5MA-[ESP-SHA1]-[ESP-3DES]							95.1028
6MA-[AH-MD5]-[ESP-3DES]	5878.5	10523.5	16402	775849	15859790	16635639	95.9020
7MA-[AH-SHA1]-[ESP-3DES]							96.6846

Appendix F - Testbed 3 Average Data

FILE TYPE =>Zip		FILE SIZE =>10 KB			PROTOCOL =>HTTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	9	11	20	942	11254	12196	0.0161
2M-[AH-MD5]-[null]	9	11	20	1338	11738	13076	0.0183
4MA-[ESP-MD5]-[ESP-3DES]	9	11	20	1414	11810	13224	0.0206
6MA-[AH-MD5]-[ESP-3DES]	9	11	20	1522	11942	13464	0.0208

FILE TYPE =>Zip		FILE SIZE =>1 MB			PROTOCOL =>HTTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	370.5	730.5	1101	24969.5	1098380	1123349.5	1.2546
2M-[AH-MD5]-[null]	390.5	762	1152.5	43641	1134034	1177675	1.3117
4MA-[ESP-MD5]-[ESP-3DES]	389.5	763.5	1153	46657	1138809	1185466	1.3597
6MA-[AH-MD5]-[ESP-3DES]	392.5	762.5	1155	51721	1147837	1199558	1.3804

FILE TYPE =>Zip		FILE SIZE =>10 KB			PROTOCOL =>SMTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	24	28	52	2121	16908	19029	0.0772
2M-[AH-MD5]-[null]	22	28	50	2957	18134	21091	0.0870
4MA-[ESP-MD5]-[ESP-3DES]	24	28.5	52.5	3376	18407	21783	0.0944
6MA-[AH-MD5]-[ESP-3DES]	24	28	52	3664	18688	22352	0.0990

FILE TYPE =>Zip		FILE SIZE =>1 MB			PROTOCOL =>SMTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	405	1096.5	1501.5	27267	1512157	1539424	1.9060
2M-[AH-MD5]-[null]	429.5	1097.5	1527	47782	1560507	1608289	1.9605
4MA-[ESP-MD5]-[ESP-3DES]	455.5	1098	1553.5	54293	1567924	1622217	2.0364
6MA-[AH-MD5]-[ESP-3DES]	459.5	1098	1557.5	60327	1581100	1641427	2.1230

Ident Protocol data

The transfer time for the Identity protocol was found by subtracting the time to synchronize at the beginning of a connection from the end time of the Ident protocol.

	Transactions		Load		Transfer time
Scenario	C to S	S to C	C to S	S to C	
1-[null]-[null]	6	5	413	372	0.0198
2M-[AH-MD5]-[null]	6	5	677	592	0.0212
4MA-[ESP-MD5]-[ESP-3DES]	6	5	724	630	0.0218
6MA-[AH-MD5]-[ESP-3DES]	6	5	796	690	0.0220

SMTP without Ident

FILE TYPE =>Zip		**FILE SIZE =>10 KB**			**PROTOCOL =>SMTP**		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	18	23	41	1708	16536	18244	0.0573
2M-[AH-MD5]-[null]	16	23	39	2280	17542	19822	0.0657
4MA-[ESP-MD5]-[ESP-3DES]	18	23.5	41.5	2652	17777	20429	0.0725
6MA-[AH-MD5]-[ESP-3DES]	18	23	41	2868	17998	20866	0.0770
FILE TYPE =>Zip		**FILE SIZE =>1 MB**			**PROTOCOL =>SMTP**		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	399	1091.5	1490.5	26854	1511785	1538639	1.8862
2M-[AH-MD5]-[null]	423.5	1092.5	1516	47105	1559915	1607020	1.9392
4MA-[ESP-MD5]-[ESP-3DES]	449.5	1093	1542.5	53569	1567294	1620863	2.0145
6MA-[AH-MD5]-[ESP-3DES]	453.5	1093	1546.5	59531	1580410	1639941	2.1010

Appendix G - Testbed 4 Average Data

FILE TYPE =>Doc	FILE SIZE =>10 KB				PROTOCOL =>HTTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	9	11	20	968	11247	12215	0.1005
2M-[AH-MD5]-[null]	9	11	20	1421	11731	13152	0.1066
4MA-[ESP-MD5]-[ESP-3DES]	10	11	21	1556	11810	13366	0.1120
6MA-[AH-MD5]-[ESP-3DES]	9	11	20	1542	11942	13484	0.1287

FILE TYPE =>Doc	FILE SIZE =>1 MB				PROTOCOL =>HTTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	381.5	732	1113.5	27042	1097688	1124730	6.3799
2M-[AH-MD5]-[null]	394	765.5	1159.5	43917.5	1133588	1177505.5	6.6751
4MA-[ESP-MD5]-[ESP-3DES]	402	765.5	1167.5	49556	1138873	1188429	6.7633
6MA-[AH-MD5]-[ESP-3DES]	402.5	765.5	1168	54447	1148059	1202506	6.7634

FILE TYPE =>Doc	FILE SIZE =>10 KB				PROTOCOL =>SMTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	24	27.5	51.5	2484	16919	19403	3.6139
2M-[AH-MD5]-[null]	24.5	28	52.5	3419	18169	21588	3.6484
4MA-[ESP-MD5]-[ESP-3DES]	24.5	27.5	52	3621	18337	21958	3.6562
6MA-[AH-MD5]-[ESP-3DES]	25	27.5	52.5	3982	18667	22649	3.6877

FILE TYPE =>Doc	FILE SIZE =>1MB				PROTOCOL =>SMTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	528.5	1021.5	1550	37621	1506132	1543753	12.2724
2M-[AH-MD5]-[null]	559.5	1062.5	1622	64541	1556264.5	1620805.5	12.5936
4MA-[ESP-MD5]-[ESP-3DES]	566	1064.5	1630.5	70020	1562951	1632971	12.7210
6MA-[AH-MD5]-[ESP-3DES]	554	1062.5	1616.5	74864	1574769	1649633	12.9664

Ident Protocol data

The transfer time for the Identity protocol was found by subtracting the time to synchronize at the beginning of a connection from the end time of the Ident protocol.

Ident overhead	**Transactions**		**Load**		**Transfer time**
	C to S	S to C	C to S	S to C	
1-[null]-[null]	6	5	372	437	3.0880
2M-[AH-MD5]-[null]	6	5	592	701	3.0931
4MA-[ESP-MD5]-[ESP-3DES]	6	5	630	748	3.0954
6MA-[AH-MD5]-[ESP-3DES]	6	5	690	820	3.0894

SMTP without Ident

FILE TYPE =>Doc	**FILE SIZE =>10 KB**			**PROTOCOL =>SMTP**			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	18	22.5	40.5	2047	16547	18594	0.5259
2M-[AH-MD5]-[null]	18.5	23	41.5	2718	17577	20295	0.5553
4MA-[ESP-MD5]-[ESP-3DES]	18.5	22.5	41	2873	17707	20580	0.5609
6MA-[AH-MD5]-[ESP-3DES]	19	22.5	41.5	3162	17977	21139	0.5983
FILE TYPE =>Doc	**FILE SIZE =>1MB**			**PROTOCOL =>SMTP**			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	522.5	1016.5	1539	37184	1505760	1542944	9.1844
2M-[AH-MD5]-[null]	553.5	1057.5	1611	63840	1555672.5	1619512.5	9.5004
4MA-[ESP-MD5]-[ESP-3DES]	560	1059.5	1619.5	69272	1562321	1631593	9.6257
6MA-[AH-MD5]-[ESP-3DES]	548	1057.5	1605.5	74044	1574079	1648123	9.8770

Appendix H-Testbed 1 Extra Data

Data for Faster Configuration of Testbed 1. Client was Dusk instead of West

FILE TYPE =>Doc	**FILE SIZE =>1 KB**			**PROTOCOL =>HTTP**			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]							0.0034
2M-[AH-MD5]-[null]							0.0040
3M-[AH-SHA1]-[null]							0.0042
4MA-[ESP-MD5]-[ESP-3DES]							0.0049
5MA-[ESP-SHA1]-[ESP-3DES]							0.0051
6MA-[AH-MD5]-[ESP-3DES]							0.0050
7MA-[AH-SHA1]-[ESP-3DES]							0.0052

FILE TYPE =>Doc	**FILE SIZE =>10k**			**PROTOCOL =>HTTP**			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]							0.0120
2M-[AH-MD5]-[null]							0.0135
3M-[AH-SHA1]-[null]							0.0139
4MA-[ESP-MD5]-[ESP-3DES]							0.0155
5MA-[ESP-SHA1]-[ESP-3DES]							0.0157
6MA-[AH-MD5]-[ESP-3DES]							0.0155
7MA-[AH-SHA1]-[ESP-3DES]							0.0159

FILE TYPE =>Doc	**FILE SIZE =>100k**			**PROTOCOL =>HTTP**			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	42	74	116	3125	107570	110695	0.1051
2M-[AH-MD5]-[null]	44	78	122	5193	111266	116459	0.1152
3M-[AH-SHA1]-[null]	44	78	122	5193	111266	116459	0.1165
4MA-[ESP-MD5]-[ESP-3DES]	44	78	122	5544	111740	117284	0.1235
5MA-[ESP-SHA1]-[ESP-3DES]	44	78	122	5544	111740	117284	0.1262
6MA-[AH-MD5]-[ESP-3DES]	45	78	123	6202	112676	118878	0.1244
7MA-[AH-SHA1]-[ESP-3DES]	45	78	123	6202	112676	118878	0.1275

FILE TYPE =>Doc		FILE SIZE =>1MB		PROTOCOL =>HTTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	369.5	729	1098.5	24738	1097490	1122228	1.2238
2M-[AH-MD5]-[null]	388.5	761	1149.5	43086	1133086	1176172	1.2713
3M-[AH-SHA1]-[null]	390.5	762	1152.5	43306	1131196	1174502	1.2758
4MA-[ESP-MD5]-[ESP-3DES]	389	762	1151	46254	1137788	1184042	1.3017
5MA-[ESP-SHA1]-[ESP-3DES]	388	762.5	1150.5	46136	1137839	1183975	1.3334
6MA-[AH-MD5]-[ESP-3DES]	386.5	762.5	1149	50562	1146958	1197520	1.3265
7MA-[AH-SHA1]-[ESP-3DES]	389	762.5	1151.5	50922	1146997	1197919	1.3601

FILE TYPE =>Doc		FILE SIZE =>10 MB		PROTOCOL =>HTTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	3586	7310	10896	237280	10971082	11208362	13.4787
2M-[AH-MD5]-[null]	3824.5	7615	11439.5	421169	11326159	11747328	13.8551
3M-[AH-SHA1]-[null]	3819	7620.5	11439.5	420342	11326764	11747106	13.9654
4MA-[ESP-MD5]-[ESP-3DES]	3788.5	7642	11430.5	447279	11375334	11822613	14.2975
5MA-[ESP-SHA1]-[ESP-3DES]	3775.5	7657.5	11433	445745	11377870	11823615	14.4811
6MA-[AH-MD5]-[ESP-3DES]	3807.5	7641	11448.5	495187	11466941	11962128	14.4987
7MA-[AH-SHA1]-[ESP-3DES]	3805	7648.5	11453.5	495038	11467865	11962903	14.9700

FILE TYPE =>Doc	FILE SIZE =>1 KB			PROTOCOL =>SMTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]							0.0521
2M-[AH-MD5]-[null]							0.0673
3M-[AH-SHA1]-[null]							0.0673
4MA-[ESP-MD5]-[ESP-3DES]							0.0688
5MA-[ESP-SHA1]-[ESP-3DES]							0.0703
6MA-[AH-MD5]-[ESP-3DES]							0.0695
7MA-[AH-SHA1]-[ESP-3DES]							0.0727

FILE TYPE =>Doc	FILE SIZE =>10 KB			PROTOCOL =>SMTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]							0.0776
2M-[AH-MD5]-[null]							0.0807
3M-[AH-SHA1]-[null]							0.0831
4MA-[ESP-MD5]-[ESP-3DES]							0.0890
5MA-[ESP-SHA1]-[ESP-3DES]							0.0936
6MA-[AH-MD5]-[ESP-3DES]							0.0906
7MA-[AH-SHA1]-[ESP-3DES]							0.0948

FILE TYPE =>Doc	FILE SIZE =>100 KB			PROTOCOL =>SMTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	63.5	122	185.5	4727	149338	154065	0.2504
2M-[AH-MD5]-[null]	63.5	123	186.5	7521	154813	162334	0.2647
3M-[AH-SHA1]-[null]	64.5	123.5	188	7631	154868	162499	0.2679
4MA-[ESP-MD5]-[ESP-3DES]	64.5	123.5	188	8155	155737	163892	0.2689
5MA-[ESP-SHA1]-[ESP-3DES]	63.5	123.5	187	8008	155733	163741	0.2737
6MA-[AH-MD5]-[ESP-3DES]	63.5	124.5	188	8799	157353	166152	0.2710
7MA-[AH-SHA1]-[ESP-3DES]	66.5	124.5	191	9178	157345	166523	0.2755

FILE TYPE =>Doc	FILE SIZE =>1MB			PROTOCOL =>SMTP			
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	427	1098	1525	28773	1511632	1540405	2.0514
2M-[AH-MD5]-[null]	426.5	1099.5	1526	47427	1559471.5	1606898.5	2.2390
3M-[AH-SHA1]-[null]	429	1096	1525	47677	1559124	1606801	2.2315
4MA-[ESP-MD5]-[ESP-3DES]	461.5	1098.5	1560	54972	1566770	1621742	2.0658
5MA-[ESP-SHA1]-[ESP-3DES]	459.5	1098.5	1558	54707	1566737	1621444	2.1076
6MA-[AH-MD5]-[ESP-3DES]	468.5	1099	1567.5	61414	1580007	1641421	2.0703
7MA-[AH-SHA1]-[ESP-3DES]	457.5	1099.5	1557	60008	1580084	1640092	2.1478

FILE TYPE =>Doc	FILE SIZE =>10 MB			PROTOCOL =>SMTP			
Scenario	**Average # of Trans.**			**Average Network Load**			**Average Transfer Time/sec**
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	
1-[null]-[null]	3749	10820	14569	247971	15087960	15335931	20.6326
2M-[AH-MD5]-[null]	4124	10803	14927	454197	15563447	16017644	21.9404
3M-[AH-SHA1]-[null]	4090	10803.5	14893.5	450337	15562122	16012459	21.9759
4MA-[ESP-MD5]-[ESP-3DES]	3752	10815	14567	443164	15635455	16078619	20.7144
5MA-[ESP-SHA1]-[ESP-3DES]	3830	10818	14648	452368	15635851	16088219	20.7740
6MA-[AH-MD5]-[ESP-3DES]	3812	10813.5	14625.5	496004	15765023	16261027	20.7580
7MA-[AH-SHA1]-[ESP-3DES]	3981	10812.5	14793.5	518055	15764861	16282916	20.8311

Ident Protocol data

The transfer time for the Identity protocol was found by subtracting the time to synchronize at the beginning of a connection from the end time of the Ident protocol.

Ident overhead	**Transactions**		**Network Load**		**Transfer Time**
	C to S	S to C	C to S	S to C	
1-[null]-[null]	6	5	413	372	0.0190
2M-[AH-MD5]-[null]	6	5	677	592	0.0198
3M-[AH-SHA1]-[null]	6	5	677	592	0.0203
4MA-[ESP-MD5]-[ESP-3DES]	6	5	724	630	0.0203
5MA-[ESP-SHA1]-[ESP-3DES]	6	5	724	630	0.0208
6MA-[AH-MD5]-[ESP-3DES]	6	5	796	690	0.0204
7MA-[AH-SHA1]-[ESP-3DES]	6	5	796	690	0.0209

SMTP without Ident

FILE TYPE =>Doc	**FILE SIZE =>1 KB**			**PROTOCOL =>SMTP**			
Scenario	**Average # of Trans.**			**Average Network Load**			**Average Transfer Time/sec**
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	
1-[null]-[null]							0.03310
2M-[AH-MD5]-[null]							0.04755
3M-[AH-SHA1]-[null]							0.04698
4MA-[ESP-MD5]-[ESP-3DES]							0.04844
5MA-[ESP-SHA1]-[ESP-3DES]							0.04943
6MA-[AH-MD5]-[ESP-3DES]							0.04917
7MA-[AH-SHA1]-[ESP-3DES]							0.05177
FILE TYPE =>Doc	**FILE SIZE =>10 KB**			**PROTOCOL =>**			**SMTP**
Scenario	**Average # of Trans.**			**Average Network Load**			**Average Transfer Time/sec**
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	
1-[null]-[null]							0.05864
2M-[AH-MD5]-[null]							0.06099
3M-[AH-SHA1]-[null]							0.06281
4MA-[ESP-MD5]-[ESP-3DES]							0.06871
5MA-[ESP-SHA1]-[ESP-3DES]							0.07272
6MA-[AH-MD5]-[ESP-3DES]							0.07022
7MA-[AH-SHA1]-[ESP-3DES]							0.07390

FILE TYPE =>Doc		**FILE SIZE =>100 KB**			**PROTOCOL =>SMTP**		
Scenario	**Average # of Trans.**			**Average Network Load**			**Average Transfer Time/sec**
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	
1-[null]-[null]	57.5	117	174.5	4314	148966	153280	0.23145
2M-[AH-MD5]-[null]	57.5	118	175.5	6844	154221	161065	0.24496
3M-[AH-SHA1]-[null]	58.5	118.5	177	6954	154276	161230	0.2476
4MA-[ESP-MD5]-[ESP-3DES]	58.5	118.5	177	7431	155107	162538	0.2486
5MA-[ESP-SHA1]-[ESP-3DES]	57.5	118.5	176	7284	155103	162387	0.2528
6MA-[AH-MD5]-[ESP-3DES]	57.5	119.5	177	8003	156663	164666	0.2506
7MA-[AH-SHA1]-[ESP-3DES]	60.5	119.5	180	8382	156655	165037	0.2547

Appendix I – Authentication with/without Encryption

All Scenarios versus No authentication and No Encryption (% comparison with scenario 1-[null]-[null])

Testbed 1

HTTP TRANSACTIONS					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	0.00	0.00	5.17	4.53	4.27
3M-[AH-SHA1]-[null]	0.00	0.00	5.17	4.44	4.39
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	9.91	9.55	9.65
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	9.48	11.77	11.02
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	9.48	11.59	11.37
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.00	9.05	12.04	11.21
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	0.00	0.00	5.41	4.24	3.85
3M-[AH-SHA1]-[null]	0.00	0.00	5.41	4.24	3.92
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	5.41	4.24	3.60
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	5.41	4.24	3.58
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	5.41	4.24	3.58
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.00	5.41	4.24	3.58
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	0.00	0.00	4.76	5.09	5.12
3M-[AH-SHA1]-[null]	0.00	0.00	4.76	4.82	5.34
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	17.86	19.95	21.80
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	16.67	26.51	25.98
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	16.67	25.97	27.01
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.00	15.48	27.31	26.53
HTTP LOAD					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	20.31	7.22	5.21	4.82	4.75
3M-[AH-SHA1]-[null]	20.31	7.22	5.21	4.81	4.76
4MA-[ESP-MD5]-[ESP-3DES]	23.96	8.46	6.54	6.09	6.05
5MA-[ESP-SHA1]-[ESP-3DES]	23.96	8.46	6.49	6.33	6.21
6MA-[AH-MD5]-[ESP-3DES]	29.50	10.42	7.86	7.64	7.55
7MA-[AH-SHA1]-[ESP-3DES]	29.50	10.42	7.80	7.70	7.53

S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	13.45	4.30	3.44	3.24	3.21
3M-[AH-SHA1]-[null]	13.45	4.30	3.44	3.24	3.22
4MA-[ESP-MD5]-[ESP-3DES]	15.77	5.01	3.88	3.66	3.61
5MA-[ESP-SHA1]-[ESP-3DES]	15.77	5.01	3.88	3.66	3.61
6MA-[AH-MD5]-[ESP-3DES]	19.44	6.18	4.75	4.49	4.44
7MA-[AH-SHA1]-[ESP-3DES]	19.44	6.18	4.75	4.49	4.44
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	35.34	41.86	66.18	73.09	74.65
3M-[AH-SHA1]-[null]	35.34	41.86	66.18	72.65	75.01
4MA-[ESP-MD5]-[ESP-3DES]	41.90	49.47	98.18	111.32	117.00
5MA-[ESP-SHA1]-[ESP-3DES]	41.90	49.47	96.29	122.03	124.43
6MA-[AH-MD5]-[ESP-3DES]	51.54	60.89	115.10	144.08	149.25
7MA-[AH-SHA1]-[ESP-3DES]	51.54	60.89	113.02	146.64	148.30
HTTP TIME					
	1 KB	10 KB	100 KB	1 MB	10 MB
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	56.38	12.81	8.96	7.73	4.64
3M-[AH-SHA1]-[null]	62.77	13.01	20.56	9.83	6.23
4MA-[ESP-MD5]-[ESP-3DES]	95.12	48.13	42.50	21.52	16.97
5MA-[ESP-SHA1]-[ESP-3DES]	111.44	59.96	49.36	30.72	25.47
6MA-[AH-MD5]-[ESP-3DES]	100.02	52.05	42.98	25.57	17.72
7MA-[AH-SHA1]-[ESP-3DES]	115.98	62.34	50.94	33.06	26.17
SMTP (WITH IDENT) TRANSACTIONS					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	0.00	1.94	7.26	4.74	4.67
3M-[AH-SHA1]-[null]	-2.50	0.00	8.60	4.46	4.40
4MA-[ESP-MD5]-[ESP-3DES]	-3.75	-0.97	25.00	22.34	22.45
5MA-[ESP-SHA1]-[ESP-3DES]	-2.50	0.97	22.04	22.57	22.23
6MA-[AH-MD5]-[ESP-3DES]	-2.50	0.97	20.16	22.82	22.92
7MA-[AH-SHA1]-[ESP-3DES]	-2.50	1.94	24.19	22.89	23.01
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	0.00	1.79	0.42	4.19	4.46
3M-[AH-SHA1]-[null]	-2.56	0.00	0.00	4.29	4.49
4MA-[ESP-MD5]-[ESP-3DES]	-2.56	0.00	0.84	4.24	4.48
5MA-[ESP-SHA1]-[ESP-3DES]	-2.56	0.00	0.42	4.24	4.47
6MA-[AH-MD5]-[ESP-3DES]	-2.56	1.79	0.42	4.19	4.46
7MA-[AH-SHA1]-[ESP-3DES]	-2.56	3.57	0.42	4.19	4.47

C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	0.00	2.13	19.55	19.55	4.87
3M-[AH-SHA1]-[null]	-2.44	0.00	24.06	24.06	4.30
4MA-[ESP-MD5]-[ESP-3DES]	-4.88	-2.13	68.42	68.42	40.61
5MA-[ESP-SHA1]-[ESP-3DES]	-2.44	2.13	60.90	60.90	40.18
6MA-[AH-MD5]-[ESP-3DES]	-2.44	0.00	55.64	55.64	41.59
7MA-[AH-SHA1]-[ESP-3DES]	-2.44	0.00	66.92	66.92	41.75
SMTP(WITH IDENT) LOAD					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	31.31	12.45	6.27	6.22	6.20
3M-[AH-SHA1]-[null]	29.45	11.91	6.45	6.18	6.17
4MA-[ESP-MD5]-[ESP-3DES]	34.32	13.76	9.70	9.77	9.77
5MA-[ESP-SHA1]-[ESP-3DES]	35.37	14.38	9.31	9.80	9.74
6MA-[AH-MD5]-[ESP-3DES]	43.74	17.65	10.78	11.70	11.70
7MA-[AH-SHA1]-[ESP-3DES]	43.74	17.97	11.41	11.71	11.72
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	22.88	7.54	3.56	3.27	3.24
3M-[AH-SHA1]-[null]	21.56	7.25	3.52	3.28	3.24
4MA-[ESP-MD5]-[ESP-3DES]	26.20	8.58	4.11	3.70	3.65
5MA-[ESP-SHA1]-[ESP-3DES]	26.20	8.58	4.10	3.70	3.65
6MA-[AH-MD5]-[ESP-3DES]	32.35	10.93	5.06	4.54	4.48
7MA-[AH-SHA1]-[ESP-3DES]	32.35	11.29	5.06	4.54	4.48
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	47.93	52.36	88.57	74.93	74.70
3M-[AH-SHA1]-[null]	45.01	49.71	95.28	73.82	73.77
4MA-[ESP-MD5]-[ESP-3DES]	50.32	55.87	179.46	151.34	151.26
5MA-[ESP-SHA1]-[ESP-3DES]	53.45	61.54	167.47	152.16	150.49
6MA-[AH-MD5]-[ESP-3DES]	66.21	72.26	184.32	178.83	178.72
7MA-[AH-SHA1]-[ESP-3DES]	66.21	72.26	204.15	179.13	179.04
SMTP (WITH IDENT) TIME					
	1 KB	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	9.21	13.51	7.25	11.53	13.69
3M-[AH-SHA1]-[null]	17.71	14.08	20.72	15.17	24.09
4MA-[ESP-MD5]-[ESP-3DES]	20.33	15.00	24.89	49.05	56.13
5MA-[ESP-SHA1]-[ESP-3DES]	24.15	18.82	34.02	51.84	62.43
6MA-[AH-MD5]-[ESP-3DES]	21.21	15.67	25.35	50.18	58.94
7MA-[AH-SHA1]-[ESP-3DES]	25.46	19.37	34.53	53.77	64.77

SMTP (WITHOUT IDENT) TRANSACTIONS					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	0.00	2.47	7.71	4.77	4.67
3M-[AH-SHA1]-[null]	-3.45	0.00	9.14	4.49	4.40
4MA-[ESP-MD5]-[ESP-3DES]	-5.17	-1.23	26.57	22.46	22.46
5MA-[ESP-SHA1]-[ESP-3DES]	-3.45	1.23	23.43	22.69	22.24
6MA-[AH-MD5]-[ESP-3DES]	-3.45	1.23	21.43	22.95	22.94
7MA-[AH-SHA1]-[ESP-3DES]	-3.45	2.47	25.71	23.02	23.02
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	0.00	2.17	0.44	4.21	4.47
3M-[AH-SHA1]-[null]	-3.45	0.00	0.00	4.31	4.49
4MA-[ESP-MD5]-[ESP-3DES]	-3.45	0.00	0.87	4.26	4.48
5MA-[ESP-SHA1]-[ESP-3DES]	-3.45	0.00	0.44	4.26	4.48
6MA-[AH-MD5]-[ESP-3DES]	-3.45	2.17	0.44	4.21	4.47
7MA-[AH-SHA1]-[ESP-3DES]	-3.45	4.35	0.44	4.21	4.48
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	0.00	2.86	21.49	21.49	4.87
3M-[AH-SHA1]-[null]	-3.45	0.00	26.45	26.45	4.31
4MA-[ESP-MD5]-[ESP-3DES]	-6.90	-2.86	75.21	75.21	40.64
5MA-[ESP-SHA1]-[ESP-3DES]	-3.45	2.86	66.94	66.94	40.20
6MA-[AH-MD5]-[ESP-3DES]	-3.45	0.00	61.16	61.16	41.61
7MA-[AH-SHA1]-[ESP-3DES]	-3.45	0.00	73.55	73.55	41.77
SMTP (WITHOUT IDENT) LOAD					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	26.36	10.33	5.99	6.19	6.20
3M-[AH-SHA1]-[null]	24.19	9.76	6.17	6.15	6.16
4MA-[ESP-MD5]-[ESP-3DES]	28.08	11.23	9.38	9.74	9.77
5MA-[ESP-SHA1]-[ESP-3DES]	29.31	11.88	8.99	9.77	9.74
6MA-[AH-MD5]-[ESP-3DES]	36.30	14.56	10.38	11.66	11.70
7MA-[AH-SHA1]-[ESP-3DES]	36.30	14.89	11.01	11.67	11.71
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	18.84	6.38	3.42	3.26	3.23
3M-[AH-SHA1]-[null]	17.38	6.09	3.38	3.27	3.24
4MA-[ESP-MD5]-[ESP-3DES]	21.39	7.21	3.95	3.69	3.65
5MA-[ESP-SHA1]-[ESP-3DES]	21.39	7.21	3.93	3.69	3.65
6MA-[AH-MD5]-[ESP-3DES]	26.42	9.25	4.86	4.52	4.48
7MA-[AH-SHA1]-[ESP-3DES]	26.42	9.62	4.86	4.52	4.48

C to S	1 KB	10 KB	100 KB	1 MB	10 MB
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	43.43	49.49	90.83	75.00	74.71
3M-[AH-SHA1]-[null]	39.69	46.19	98.16	73.88	73.78
4MA-[ESP-MD5]-[ESP-3DES]	43.29	51.05	189.01	151.83	151.31
5MA-[ESP-SHA1]-[ESP-3DES]	47.31	58.13	175.92	152.66	150.53
6MA-[AH-MD5]-[ESP-3DES]	58.75	67.19	192.72	179.39	178.78
7MA-[AH-SHA1]-[ESP-3DES]	58.75	67.19	214.36	179.69	179.10

SMTP (WITHOUT IDENT) TIME					
SMTP	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	10.32	15.52	7.48	11.65	13.71
3M-[AH-SHA1]-[null]	20.62	15.72	22.22	15.31	24.13
4MA-[ESP-MD5]-[ESP-3DES]	24.03	16.92	26.87	49.81	56.23
5MA-[ESP-SHA1]-[ESP-3DES]	28.39	21.21	36.81	52.61	62.54
6MA-[AH-MD5]-[ESP-3DES]	25.02	17.63	27.33	50.95	59.04
7MA-[AH-SHA1]-[ESP-3DES]	29.78	21.65	37.27	54.56	64.88

Extra data for Testbed 1

The data for the 1 KB and 10 KB files for the network load and the number of transactions was not recorded, since the measurements did not deviate from Testbed 1 data (slow configuration). SMTP without Ident was not shown for the1 MB and 10 MB files since its effect was negligible.

HTTP TRANSACTIONS			
TOTAL	100 KB	1 MB	10 MB
1-[null]-[null]	0.00	0.00	0.00
2M-[AH-MD5]-[null]	5.17	4.64	4.99
3M-[AH-SHA1]-[null]	5.17	4.92	4.99
4MA-[ESP-MD5]-[ESP-3DES]	5.17	4.78	4.91
5MA-[ESP-SHA1]-[ESP-3DES]	5.17	4.73	4.93
6MA-[ESP-SHA1]-[ESP-3DES]	6.03	4.60	5.07
7MA-[AH-SHA1]-[ESP-3DES]	6.03	4.82	5.12
S to C	100 KB	1 MB	10 MB
1-[null]-[null]	0.00	0.00	0.00
2M-[AH-MD5]-[null]	5.41	4.39	4.17
3M-[AH-SHA1]-[null]	5.41	4.53	4.25
4MA-[ESP-MD5]-[ESP-3DES]	5.41	4.53	4.54
5MA-[ESP-SHA1]-[ESP-3DES]	5.41	4.60	4.75
6MA-[ESP-SHA1]-[ESP-3DES]	5.41	4.60	4.53
7MA-[AH-SHA1]-[ESP-3DES]	5.41	4.60	4.63

C to S	100 KB	1 MB	10 MB
1-[null]-[null]	0.00	0.00	0.00
2M-[AH-MD5]-[null]	4.76	5.14	6.65
3M-[AH-SHA1]-[null]	4.76	5.68	6.50
4MA-[ESP-MD5]-[ESP-3DES]	4.76	5.28	5.65
5MA-[ESP-SHA1]-[ESP-3DES]	4.76	5.01	5.28
6MA-[ESP-SHA1]-[ESP-3DES]	7.14	4.60	6.18
7MA-[AH-SHA1]-[ESP-3DES]	7.14	5.28	6.11
HTTP LOAD			
TOTAL	100 KB	1 MB	10 MB
1-[null]-[null]	0.00	0.00	0.00
2M-[AH-MD5]-[null]	5.21	4.81	4.81
3M-[AH-SHA1]-[null]	5.21	4.66	4.81
4MA-[ESP-MD5]-[ESP-3DES]	5.95	5.51	5.48
5MA-[ESP-SHA1]-[ESP-3DES]	5.95	5.50	5.49
6MA-[ESP-SHA1]-[ESP-3DES]	7.39	6.71	6.73
7MA-[AH-SHA1]-[ESP-3DES]	7.39	6.74	6.73
	0.00		
S to C	100 KB	1 MB	10 MB
1-[null]-[null]	0.00	0.00	0.00
2M-[AH-MD5]-[null]	3.44	3.24	3.24
3M-[AH-SHA1]-[null]	3.44	3.07	3.24
4MA-[ESP-MD5]-[ESP-3DES]	3.88	3.67	3.68
5MA-[ESP-SHA1]-[ESP-3DES]	3.88	3.68	3.71
6MA-[ESP-SHA1]-[ESP-3DES]	4.75	4.51	4.52
7MA-[AH-SHA1]-[ESP-3DES]	4.75	4.51	4.53
	0.00		
C to S	100 KB	1 MB	10 MB
1-[null]-[null]	0.00	0.00	0.00
2M-[AH-MD5]-[null]	66.18	74.17	77.50
3M-[AH-SHA1]-[null]	66.18	75.06	77.15
4MA-[ESP-MD5]-[ESP-3DES]	77.41	86.98	88.50
5MA-[ESP-SHA1]-[ESP-3DES]	77.41	86.50	87.86
6MA-[ESP-SHA1]-[ESP-3DES]	98.46	104.39	108.69
7MA-[AH-SHA1]-[ESP-3DES]	98.46	105.85	108.63

HTTP TRANSFER TIME					
	1 KB	10 KB	100 KB	1 MB	10 MB
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	17.82	13.18	9.65	3.88	2.79
3M-[AH-SHA1]-[null]	23.24	16.20	10.89	4.25	3.61
4MA-[ESP-MD5]-[ESP-3DES]	42.45	29.29	17.58	6.37	6.07
5MA-[ESP-SHA1]-[ESP-3DES]	49.48	31.55	20.13	8.96	7.44
6MA-[ESP-SHA1]-[ESP-3DES]	44.29	29.80	18.39	8.39	7.57
7MA-[AH-SHA1]-[ESP-3DES]	52.02	32.68	21.39	11.14	11.06

SMTP TRANSACTIONS	SMTP (WITH IDENT)			SMTP (WITHOUT IDENT)
TOTAL	100 KB	1 MB	10 MB	100 KB
1-[null]-[null]	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	0.54	0.07	2.46	0.57
3M-[AH-SHA1]-[null]	1.35	0.00	2.23	1.43
4MA-[ESP-MD5]-[ESP-3DES]	1.35	2.30	-0.01	1.43
5MA-[ESP-SHA1]-[ESP-3DES]	0.81	2.16	0.54	0.86
6MA-[ESP-SHA1]-[ESP-3DES]	1.35	2.79	0.39	1.43
7MA-[AH-SHA1]-[ESP-3DES]	2.96	2.10	1.54	3.15
S to C	100 KB	1 MB	10 MB	100 KB
1-[null]-[null]	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	0.82	0.14	-0.16	0.85
3M-[AH-SHA1]-[null]	1.23	-0.18	-0.15	1.28
4MA-[ESP-MD5]-[ESP-3DES]	1.23	0.05	-0.05	1.28
5MA-[ESP-SHA1]-[ESP-3DES]	1.23	0.05	-0.02	1.28
6MA-[ESP-SHA1]-[ESP-3DES]	2.05	0.09	-0.06	2.14
7MA-[AH-SHA1]-[ESP-3DES]	2.05	0.14	-0.07	2.14
C to S	100 KB	1 MB	10 MB	100 KB
1-[null]-[null]	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	0.00	-0.12	10.00	0.00
3M-[AH-SHA1]-[null]	1.57	0.47	9.10	1.74
4MA-[ESP-MD5]-[ESP-3DES]	1.57	8.08	0.08	1.74
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	7.61	2.16	0.00
6MA-[ESP-SHA1]-[ESP-3DES]	0.00	9.72	1.68	0.00
7MA-[AH-SHA1]-[ESP-3DES]	4.72	7.14	6.19	5.22
SMTP LOAD				
TOTAL	100 KB	1 MB	10 MB	100 KB
1-[null]-[null]	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	5.37	4.32	4.45	5.08
3M-[AH-SHA1]-[null]	5.47	4.31	4.41	5.19
4MA-[ESP-MD5]-[ESP-3DES]	6.38	5.28	4.84	6.04
5MA-[ESP-SHA1]-[ESP-3DES]	6.28	5.26	4.91	5.94
6MA-[ESP-SHA1]-[ESP-3DES]	7.85	6.56	6.03	7.43
7MA-[AH-SHA1]-[ESP-3DES]	8.09	6.47	6.17	7.67
S to C	100 KB	1 MB	10 MB	100 KB
1-[null]-[null]	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	3.67	3.16	3.15	3.53
3M-[AH-SHA1]-[null]	3.70	3.14	3.14	3.56
4MA-[ESP-MD5]-[ESP-3DES]	4.28	3.65	3.63	4.12
5MA-[ESP-SHA1]-[ESP-3DES]	4.28	3.65	3.63	4.12
6MA-[ESP-SHA1]-[ESP-3DES]	5.37	4.52	4.49	5.17
7MA-[AH-SHA1]-[ESP-3DES]	5.36	4.53	4.49	5.16

C to S	100 KB	1 MB	10 MB	100 KB
1-[null]-[null]	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	59.11	64.83	83.17	58.65
3M-[AH-SHA1]-[null]	61.43	65.70	81.61	61.20
4MA-[ESP-MD5]-[ESP-3DES]	72.52	91.05	78.72	72.25
5MA-[ESP-SHA1]-[ESP-3DES]	69.41	90.13	82.43	68.85
6MA-[ESP-SHA1]-[ESP-3DES]	86.14	113.44	100.03	85.51
7MA-[AH-SHA1]-[ESP-3DES]	94.16	108.56	108.92	94.30

TRANSFER TIME					
SMTP (WITH IDENT)	1 KB	10 KB	100 KB	1 MB	10 MB
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	29.26	4.04	5.71	9.15	6.34
3M-[AH-SHA1]-[null]	29.16	7.06	6.96	8.78	6.51
4MA-[ESP-MD5]-[ESP-3DES]	32.04	14.71	7.40	0.70	0.40
5MA-[ESP-SHA1]-[ESP-3DES]	34.96	20.56	9.28	2.74	0.69
6MA-[ESP-SHA1]-[ESP-3DES]	33.55	16.73	8.22	0.93	0.61
7MA-[AH-SHA1]-[ESP-3DES]	39.52	22.13	10.03	4.70	0.96
SMTP (WITHOUT IDENT)	1 KB	10 KB	100 KB		
1-[null]-[null]	0.00	0.00	0.00		
2M-[AH-MD5]-[null]	43.63	4.00	5.84		
3M-[AH-SHA1]-[null]	41.90	7.11	6.97		
4MA-[ESP-MD5]-[ESP-3DES]	46.33	17.16	7.42		
5MA-[ESP-SHA1]-[ESP-3DES]	49.32	24.02	9.23		
6MA-[ESP-SHA1]-[ESP-3DES]	48.54	19.75	8.29		
7MA-[AH-SHA1]-[ESP-3DES]	56.37	26.02	10.03		

Appendix J - Protocol comparison

(% comparison(SMTP-HTTP)/HTTP)

HTTP Vs SMTP(WITH IDENT) TRANSACTIONS					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	263.64	157.50	60.34	79.54	80.68
2M-[AH-MD5]-[null]	263.64	162.50	63.52	79.90	81.36
3MA-[AH-SHA1]-[null]	254.55	157.50	65.57	79.58	80.69
4MA-[ESP-MD5]-[ESP-3DES]	250.00	155.00	82.35	100.50	101.77
5MA-[ESP-SHA1]-[ESP-3DES]	254.55	160.00	78.74	96.88	98.92
6MA-[ESP-SHA1]-[ESP-3DES]	254.55	160.00	75.98	97.61	99.44
7MA-[AH-SHA1]-[ESP-3DES]	254.55	162.50	82.61	96.93	99.86
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	290.00	154.55	61.49	38.65	36.06
2M-[AH-MD5]-[null]	290.00	159.09	53.85	38.58	36.86
3MA-[AH-SHA1]-[null]	280.00	154.55	53.21	38.71	36.80
4MA-[ESP-MD5]-[ESP-3DES]	280.00	154.55	54.49	38.65	37.22
5MA-[ESP-SHA1]-[ESP-3DES]	280.00	154.55	53.85	38.65	37.24
6MA-[ESP-SHA1]-[ESP-3DES]	280.00	159.09	53.85	38.58	37.22
7MA-[AH-SHA1]-[ESP-3DES]	280.00	163.64	53.85	38.58	37.24
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	241.67	161.11	58.33	58.33	170.33
2M-[AH-MD5]-[null]	241.67	166.67	80.68	80.68	169.67
3MA-[AH-SHA1]-[null]	233.33	161.11	87.50	87.50	167.66
4MA-[ESP-MD5]-[ESP-3DES]	225.00	155.56	126.26	126.26	212.07
5MA-[ESP-SHA1]-[ESP-3DES]	233.33	166.67	118.37	118.37	200.80
6MA-[ESP-SHA1]-[ESP-3DES]	233.33	161.11	111.22	111.22	201.35
7MA-[AH-SHA1]-[ESP-3DES]	233.33	161.11	128.87	128.87	202.84
HTTP Vs SMTP (WITH IDENT) LOAD					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	134.66	55.68	39.26	39.81	39.85
2M-[AH-MD5]-[null]	156.12	63.28	40.67	41.68	41.78
3MA-[AH-SHA1]-[null]	152.49	62.49	40.91	41.64	41.72
4MA-[ESP-MD5]-[ESP-3DES]	154.27	63.29	43.40	44.66	44.75
5MA-[ESP-SHA1]-[ESP-3DES]	156.26	64.19	42.95	44.37	44.49
6MA-[ESP-SHA1]-[ESP-3DES]	160.47	65.86	43.03	45.08	45.24
7MA-[AH-SHA1]-[ESP-3DES]	160.47	66.32	43.92	45.02	45.29

S to C	1 KB	10 KB	100 KB	1 MB	10 MB
1-[null]-[null]	126.77	50.28	38.74	37.16	37.00
2M-[AH-MD5]-[null]	145.64	54.95	38.90	37.20	37.03
3MA-[AH-SHA1]-[null]	143.00	54.53	38.85	37.21	37.03
4MA-[ESP-MD5]-[ESP-3DES]	147.20	55.39	39.05	37.22	37.06
5MA-[ESP-SHA1]-[ESP-3DES]	147.20	55.39	39.03	37.22	37.06
6MA-[ESP-SHA1]-[ESP-3DES]	151.28	57.00	39.15	37.23	37.06
7MA-[AH-SHA1]-[ESP-3DES]	151.28	57.51	39.15	37.22	37.06
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	151.94	119.87	57.38	154.51	169.25
2M-[AH-MD5]-[null]	175.37	136.14	78.59	157.22	169.34
3MA-[AH-SHA1]-[null]	169.93	132.04	84.94	156.23	167.34
4MA-[ESP-MD5]-[ESP-3DES]	166.89	129.28	121.93	202.71	211.75
5MA-[ESP-SHA1]-[ESP-3DES]	172.45	137.62	114.44	189.05	200.51
6MA-[ESP-SHA1]-[ESP-3DES]	176.33	135.41	108.02	190.75	201.09
7MA-[AH-SHA1]-[ESP-3DES]	176.33	135.41	124.70	188.04	202.58
HTTP Vs SMTP (WITH IDENT) TIME					
	1 KB	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	5126.18	1552.02	395.27	159.32	115.34
2M-[AH-MD5]-[null]	3549.91	1562.36	387.53	168.47	133.97
3M-[AH-SHA1]-[null]	3679.32	1567.58	395.94	171.94	151.57
4MA-[ESP-MD5]-[ESP-3DES]	3123.03	1182.56	334.07	218.08	187.43
5MA-[ESP-SHA1]-[ESP-3DES]	2968.59	1127.15	344.40	201.21	178.78
6MA-[AH-MD5]-[ESP-3DES]	3066.84	1156.75	334.18	210.16	190.75
7MA-[AH-SHA1]-[ESP-3DES]	2935.76	1114.75	341.44	199.67	181.24

HTTP Vs SMTP (WITHOUT IDENT) TRANSACTIONS					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	163.64	102.50	50.86	78.54	80.58
2M-[AH-MD5]-[null]	163.64	107.50	54.51	78.95	81.27
3M-[AH-SHA1]-[null]	154.55	102.50	56.56	78.63	80.60
4MA-[ESP-MD5]-[ESP-3DES]	150.00	100.00	73.73	99.59	101.68
5MA-[ESP-SHA1]-[ESP-3DES]	154.55	105.00	70.08	95.99	98.83
6MA-[AH-MD5]-[ESP-3DES]	154.55	105.00	67.32	96.71	99.35
7MA-[AH-SHA1]-[ESP-3DES]	154.55	107.50	73.91	96.04	99.77
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	190.00	109.09	54.73	37.96	35.99
2M-[AH-MD5]-[null]	190.00	113.64	47.44	37.93	36.80
3M-[AH-SHA1]-[null]	180.00	109.09	46.79	38.06	36.74
4MA-[ESP-MD5]-[ESP-3DES]	180.00	109.09	48.08	37.99	37.15
5MA-[ESP-SHA1]-[ESP-3DES]	180.00	109.09	47.44	37.99	37.17
6MA-[AH-MD5]-[ESP-3DES]	180.00	113.64	47.44	37.93	37.16
7MA-[AH-SHA1]-[ESP-3DES]	180.00	118.18	47.44	37.93	37.17

C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	141.67	94.44	44.05	44.05	170.16
2M-[AH-MD5]-[null]	141.67	100.00	67.05	67.05	169.51
3M-[AH-SHA1]-[null]	133.33	94.44	73.86	73.86	167.50
4MA-[ESP-MD5]-[ESP-3DES]	125.00	88.89	114.14	114.14	211.93
5MA-[ESP-SHA1]-[ESP-3DES]	133.33	100.00	106.12	106.12	200.67
6MA-[AH-MD5]-[ESP-3DES]	133.33	94.44	98.98	98.98	201.22
7MA-[AH-SHA1]-[ESP-3DES]	133.33	94.44	116.49	116.49	202.71
HTTP Vs SMTP (WITHOUT IDENT) LOAD					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	101.72	49.24	38.55	39.74	39.84
2M-[AH-MD5]-[null]	111.86	53.58	39.58	41.57	41.77
3M-[AH-SHA1]-[null]	108.23	52.78	39.82	41.53	41.71
4MA-[ESP-MD5]-[ESP-3DES]	108.43	53.06	42.25	44.54	44.74
5MA-[ESP-SHA1]-[ESP-3DES]	110.43	53.95	41.81	44.26	44.48
6MA-[AH-MD5]-[ESP-3DES]	112.31	54.83	41.79	44.96	45.23
7MA-[AH-SHA1]-[ESP-3DES]	112.31	55.28	42.68	44.90	45.28
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	104.03	46.97	38.39	37.13	37.00
2M-[AH-MD5]-[null]	113.74	49.90	38.37	37.15	37.02
3M-[AH-SHA1]-[null]	111.10	49.48	38.32	37.16	37.03
4MA-[ESP-MD5]-[ESP-3DES]	113.94	50.06	38.48	37.16	37.05
5MA-[ESP-SHA1]-[ESP-3DES]	113.94	50.06	38.47	37.16	37.05
6MA-[AH-MD5]-[ESP-3DES]	115.97	51.22	38.54	37.16	37.05
7MA-[AH-SHA1]-[ESP-3DES]	115.97	51.73	38.54	37.16	37.05
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	96.65	76.22	44.16	152.88	169.08
2M-[AH-MD5]-[null]	108.41	85.69	65.55	155.67	169.18
3M-[AH-SHA1]-[null]	102.97	81.59	71.90	154.68	167.18
4MA-[ESP-MD5]-[ESP-3DES]	98.58	78.08	110.24	201.35	211.62
5MA-[ESP-SHA1]-[ESP-3DES]	104.15	86.42	102.64	187.76	200.37
6MA-[AH-MD5]-[ESP-3DES]	106.01	83.11	96.18	189.47	200.96
7MA-[AH-SHA1]-[ESP-3DES]	106.01	83.11	112.74	186.77	202.45
HTTP Vs SMTP (WITHOUT IDENT) TIME					
	1 KB	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	3982.25	1228.09	345.49	154.72	114.90
2M-[AH-MD5]-[null]	2779.88	1260.09	339.45	163.98	133.52
3M-[AH-SHA1]-[null]	2925.02	1259.94	351.63	167.45	151.12
4MA-[ESP-MD5]-[ESP-3DES]	2495.01	948.30	296.66	214.03	187.02
5MA-[ESP-SHA1]-[ESP-3DES]	2378.75	906.37	308.07	197.37	178.39
6MA-[AH-MD5]-[ESP-3DES]	2451.45	927.50	296.72	206.21	190.34
7MA-[AH-SHA1]-[ESP-3DES]	2353.00	895.21	305.16	195.87	180.85

Testbed 1 Extra Data

The data for the 1 KB and 10 KB files for the network load and the number of transactions was not recorded, since the measurements did not deviate from Testbed 1 data (slow configuration). SMTP without Ident was not shown for the1 MB and 10 MB files since its effect was negligible.

TRANSACTIONS	**HTTP VS SMTP (WITH IDENT)**			**HTTP VS SMTP(WITHOUT IDENT)**
TOTAL	100 KB	1 MB	10 MB	100 KB
1-[null]-[null]	59.91	38.83	33.71	50.43
2M-[AH-MD5]-[null]	52.87	32.75	30.49	43.85
3MA-[AH-SHA1]-[null]	54.10	32.32	30.19	45.08
4MA-[ESP-MD5]-[ESP-3DES]	54.10	35.53	27.44	45.08
5MA-[ESP-SHA1]-[ESP-3DES]	53.28	35.42	28.12	44.26
6MA-[ESP-SHA1]-[ESP-3DES]	52.85	36.42	27.75	43.90
7MA-[AH-SHA1]-[ESP-3DES]	55.28	35.21	29.16	46.34
S to C	100 KB	1 MB	10 MB	100 KB
1-[null]-[null]	64.86	50.62	48.02	58.11
2M-[AH-MD5]-[null]	57.69	44.48	41.86	51.28
3MA-[AH-SHA1]-[null]	58.33	43.83	41.77	51.92
4MA-[ESP-MD5]-[ESP-3DES]	58.33	44.16	41.52	51.92
5MA-[ESP-SHA1]-[ESP-3DES]	58.33	44.07	41.27	51.92
6MA-[ESP-SHA1]-[ESP-3DES]	59.62	44.13	41.52	53.21
7MA-[AH-SHA1]-[ESP-3DES]	59.62	44.20	41.37	53.21
C to S	100 KB	1 MB	10 MB	100 KB
1-[null]-[null]	51.19	15.56	4.55	36.90
2M-[AH-MD5]-[null]	44.32	9.78	7.83	30.68
3MA-[AH-SHA1]-[null]	46.59	9.86	7.10	32.95
4MA-[ESP-MD5]-[ESP-3DES]	46.59	18.64	-0.96	32.95
5MA-[ESP-SHA1]-[ESP-3DES]	44.32	18.43	1.44	30.68
6MA-[ESP-SHA1]-[ESP-3DES]	41.11	21.22	0.12	27.78
7MA-[AH-SHA1]-[ESP-3DES]	47.78	17.61	4.63	34.44
LOAD				
TOTAL	100 KB	1 MB	10 MB	100 KB
1-[null]-[null]	39.18	37.26	36.83	38.47
2M-[AH-MD5]-[null]	39.39	36.62	36.35	38.30
3MA-[AH-SHA1]-[null]	39.53	36.81	36.31	38.44
4MA-[ESP-MD5]-[ESP-3DES]	39.74	36.97	36.00	38.58
5MA-[ESP-SHA1]-[ESP-3DES]	39.61	36.95	36.07	38.46
6MA-[ESP-SHA1]-[ESP-3DES]	39.77	37.07	35.94	38.52
7MA-[AH-SHA1]-[ESP-3DES]	40.08	36.91	36.11	38.83

S to C	100 KB	1 MB	10 MB	100 KB
1-[null]-[null]	38.83	37.74	37.52	38.48
2M-[AH-MD5]-[null]	39.14	37.63	37.41	38.61
3MA-[AH-SHA1]-[null]	39.19	37.83	37.39	38.66
4MA-[ESP-MD5]-[ESP-3DES]	39.37	37.70	37.45	38.81
5MA-[ESP-SHA1]-[ESP-3DES]	39.37	37.69	37.42	38.81
6MA-[ESP-SHA1]-[ESP-3DES]	39.65	37.76	37.48	39.04
7MA-[AH-SHA1]-[ESP-3DES]	39.64	37.76	37.47	39.03
C to S	100 KB	1 MB	10 MB	100 KB
1-[null]-[null]	51.26	16.31	4.51	38.05
2M-[AH-MD5]-[null]	44.83	10.08	7.84	31.79
3MA-[AH-SHA1]-[null]	46.95	10.09	7.14	33.91
4MA-[ESP-MD5]-[ESP-3DES]	47.10	18.85	-0.92	34.04
5MA-[ESP-SHA1]-[ESP-3DES]	44.44	18.58	1.49	31.39
6MA-[ESP-SHA1]-[ESP-3DES]	41.87	21.46	0.16	29.04
7MA-[AH-SHA1]-[ESP-3DES]	47.98	17.84	4.65	35.15

TRANSFER TIME **HTTP VS SMTP (WITH IDENT)**					
SMTP	1 KB	10 KB	100 KB	1 MB	10 MB
1-[null]-[null]	1416.43	548.98	138.35	67.63	53.08
2M-[AH-MD5]-[null]	1563.59	496.59	129.80	76.12	58.36
3MA-[AH-SHA1]-[null]	1489.24	497.97	129.90	74.91	57.36
4MA-[ESP-MD5]-[ESP-3DES]	1305.63	475.80	117.70	58.70	44.88
5MA-[ESP-SHA1]-[ESP-3DES]	1269.13	494.76	116.82	58.06	43.46
6MA-[ESP-SHA1]-[ESP-3DES]	1303.55	483.65	117.87	56.08	43.17
7MA-[AH-SHA1]-[ESP-3DES]	1291.77	497.38	116.04	57.91	39.15
HTTP VS SMTP (WITHOUT IDENT)	1 KB	10 KB	100 KB		
1-[null]-[null]	864.02	390.36	2176.34		
2M-[AH-MD5]-[null]	1075.21	350.60	2097.31		
3MA-[AH-SHA1]-[null]	1009.99	352.02	2095.75		
4MA-[ESP-MD5]-[ESP-3DES]	890.28	344.38	1979.67		
5MA-[ESP-SHA1]-[ESP-3DES]	863.02	362.26	1969.84		
6MA-[ESP-SHA1]-[ESP-3DES]	892.37	352.39	1982.05		
7MA-[AH-SHA1]-[ESP-3DES]	891.62	365.74	1963.19		

Appendix K - Wireless Vs Wireline mediums

Scenario Comparison
Testbed 2 Data

HTTP TRANSACTIONS					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	0.00	0.00	11.54	4.71	4.94
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	11.11	5.45	4.85
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	10.68	6.02	4.88
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	0.00	0.00	4.67	4.43	4.94
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	5.33	4.50	4.85
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	5.33	4.43	4.88
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	0.00	0.00	23.81	5.21	5.15
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	21.43	7.15	4.88
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	20.24	8.85	4.97
HTTP LOAD					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	20.23	7.19	6.02	5.03	5.29
4MA-[ESP-MD5]-[ESP-3DES]	24.33	8.40	7.08	5.84	6.02
6MA-[AH-MD5]-[ESP-3DES]	29.85	10.36	8.81	7.25	7.22
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	13.34	4.28	3.37	3.27	3.58
4MA-[ESP-MD5]-[ESP-3DES]	16.07	4.92	3.95	3.69	4.01
6MA-[AH-MD5]-[ESP-3DES]	19.71	6.09	4.83	4.52	4.77
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	35.53	42.04	97.89	74.13	73.52
4MA-[ESP-MD5]-[ESP-3DES]	42.66	50.11	115.25	90.04	86.11
6MA-[AH-MD5]-[ESP-3DES]	52.36	61.57	146.75	114.16	105.00

HTTP TIME					
	1 KB	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	30.22	20.00	2.04	5.46	4.29
3M-[AH-SHA1]-[null]	31.26	22.27	4.95	6.48	4.50
4MA-[ESP-MD5]-[ESP-3DES]	30.88	24.36	5.89	6.64	4.92
5MA-[ESP-SHA1]-[ESP-3DES]	30.06	28.22	5.99	6.73	4.96
6MA-[AH-MD5]-[ESP-3DES]	31.04	34.11	5.21	5.94	6.13
7MA-[AH-SHA1]-[ESP-3DES]	29.62	34.38	5.33	6.49	6.74
SMTP (WITH IDENT) TRANSACTIONS					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	1.37	-1.98	0.79	3.92	3.91
4MA-[ESP-MD5]-[ESP-3DES]	4.11	-0.99	1.85	4.39	4.22
6MA-[AH-MD5]-[ESP-3DES]	1.37	0.00	1.85	3.83	4.73
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	5.56	1.89	3.04	4.47	4.41
4MA-[ESP-MD5]-[ESP-3DES]	5.56	1.89	3.48	4.38	4.71
6MA-[AH-MD5]-[ESP-3DES]	5.56	1.89	4.35	4.38	5.04
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	-2.70	-6.25	-2.70	2.95	3.03
4MA-[ESP-MD5]-[ESP-3DES]	2.70	-4.17	-0.68	4.43	3.35
6MA-[AH-MD5]-[ESP-3DES]	-2.70	-2.08	-2.03	2.86	4.19
SMTP (WITH IDENT) LOAD					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	29.69	10.96	5.42	4.96	4.80
4MA-[ESP-MD5]-[ESP-3DES]	35.98	12.87	6.44	5.78	5.84
6MA-[AH-MD5]-[ESP-3DES]	41.85	16.34	7.79	6.97	7.45
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	23.76	7.12	3.64	3.30	3.16
4MA-[ESP-MD5]-[ESP-3DES]	26.68	7.99	4.15	3.72	3.89
6MA-[AH-MD5]-[ESP-3DES]	32.78	9.90	5.14	4.56	5.03
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	41.91	40.98	53.64	68.50	69.28
4MA-[ESP-MD5]-[ESP-3DES]	55.16	50.97	68.47	84.91	82.65
6MA-[AH-MD5]-[ESP-3DES]	60.57	66.65	79.50	99.38	102.50

SMTP(WITH IDENT) TIME					
	1 KB	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	0.53	-0.03	0.78	3.14	4.31
3M-[AH-SHA1]-[null]	0.79	0.53	1.32	3.25	4.75
4MA-[ESP-MD5]-[ESP-3DES]	0.93	0.73	1.52	3.61	5.04
5MA-[ESP-SHA1]-[ESP-3DES]	0.98	0.78	1.59	4.72	5.12
6MA-[AH-MD5]-[ESP-3DES]	0.87	0.73	1.43	4.54	5.98
7MA-[AH-SHA1]-[ESP-3DES]	1.01	0.75	1.59	4.87	6.82
SMTP(WITHOUT IDENT) TRANSACTIONS					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	1.96	-2.53	0.84	3.95	3.92
4MA-[ESP-MD5]-[ESP-3DES]	5.88	-1.27	1.97	4.42	4.22
6MA-[AH-MD5]-[ESP-3DES]	1.96	0.00	1.97	3.86	4.73
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	7.69	2.33	3.18	4.50	4.42
4MA-[ESP-MD5]-[ESP-3DES]	7.69	2.33	3.64	4.40	4.71
6MA-[AH-MD5]-[ESP-3DES]	7.69	2.33	4.55	4.40	5.04
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	-4.00	-8.33	-2.94	2.98	3.03
4MA-[ESP-MD5]-[ESP-3DES]	4.00	-5.56	-0.74	4.47	3.35
6MA-[AH-MD5]-[ESP-3DES]	-4.00	-2.78	-2.21	2.89	4.19
SMTP(WITHOUT IDENT) LOAD					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	27.73	10.03	5.30	4.94	4.80
4MA-[ESP-MD5]-[ESP-3DES]	33.86	11.80	6.29	5.77	5.84
6MA-[AH-MD5]-[ESP-3DES]	39.03	15.03	7.61	6.95	7.44
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	19.97	5.96	3.51	3.29	3.16
4MA-[ESP-MD5]-[ESP-3DES]	22.09	6.63	3.99	3.70	3.89
6MA-[AH-MD5]-[ESP-3DES]	27.12	8.22	4.94	4.54	5.03
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	42.11	41.14	53.71	68.51	69.28
4MA-[ESP-MD5]-[ESP-3DES]	55.68	51.38	68.65	84.94	82.66
6MA-[AH-MD5]-[ESP-3DES]	61.11	67.11	79.70	99.41	102.50

SMTP(WITHOUT IDENT) TIME					
	1 KB	**10 KB**	**100 KB**	**1 MB**	**10 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	10.85	0.01	2.91	4.15	4.46
3M-[AH-SHA1]-[null]	14.88	6.47	4.72	4.28	4.91
4MA-[ESP-MD5]-[ESP-3DES]	21.54	11.48	6.01	4.83	5.22
5MA-[ESP-SHA1]-[ESP-3DES]	18.41	9.56	5.71	6.22	5.29
6MA-[AH-MD5]-[ESP-3DES]	13.32	7.01	4.68	5.92	6.17
7MA-[AH-SHA1]-[ESP-3DES]	12.33	4.93	4.75	6.30	7.04

Testbed 4

HTTP TRANSACTIONS		
TOTAL	**10 KB**	**1 MB**
1-[null]-[null]	0.00	0.00
2M-[AH-MD5]-[null]	0.00	4.13
4MA-[ESP-MD5]-[ESP-3DES]	5.00	4.85
6MA-[AH-MD5]-[ESP-3DES]	0.00	4.89
S to C	**10 KB**	**1 MB**
1-[null]-[null]	0.00	0.00
2M-[AH-MD5]-[null]	4.58	4.58
4MA-[ESP-MD5]-[ESP-3DES]	4.58	4.58
6MA-[AH-MD5]-[ESP-3DES]	4.58	4.58
C to S	**10 KB**	**1 MB**
1-[null]-[null]	0.00	0.00
2M-[AH-MD5]-[null]	3.28	3.28
4MA-[ESP-MD5]-[ESP-3DES]	5.37	5.37
6MA-[AH-MD5]-[ESP-3DES]	5.50	5.50
HTTP LOAD		
TOTAL	**10 KB**	**1 MB**
1-[null]-[null]	0.00	0.00
2M-[AH-MD5]-[null]	7.67	4.69
4MA-[ESP-MD5]-[ESP-3DES]	9.42	5.66
6MA-[AH-MD5]-[ESP-3DES]	10.39	6.92
S to C	**10 KB**	**1 MB**
1-[null]-[null]	0.00	0.00
2M-[AH-MD5]-[null]	4.30	3.27
4MA-[ESP-MD5]-[ESP-3DES]	5.01	3.75
6MA-[AH-MD5]-[ESP-3DES]	6.18	4.59
C to S	**10 KB**	**1 MB**
1-[null]-[null]	0.00	0.00
2M-[AH-MD5]-[null]	46.80	62.40
4MA-[ESP-MD5]-[ESP-3DES]	60.74	83.26

6MA-[AH-MD5]-[ESP-3DES]	59.30	101.34		
HTTP TIME				
	1 KB	**10 KB**		
1-[null]-[null]	0.00	0.00		
2M-[AH-MD5]-[null]	6.05	4.63		
4MA-[ESP-MD5]-[ESP-3DES]	11.38	6.01		
6MA-[AH-MD5]-[ESP-3DES]	28.01	6.01		
TRANSACTIONS	**SMTP(WITH IDENT)**		**SMTP(WITHOUT IDENT)**	
TOTAL	**1 MB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	1.94	4.65	2.47	4.68
4MA-[ESP-MD5]-[ESP-3DES]	0.97	5.19	1.23	5.23
6MA-[AH-MD5]-[ESP-3DES]	1.94	4.29	2.47	4.32
S to C	**1 MB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	1.82	4.01	2.22	4.03
4MA-[ESP-MD5]-[ESP-3DES]	0.00	4.21	0.00	4.23
6MA-[AH-MD5]-[ESP-3DES]	0.00	4.01	0.00	4.03
C to S	**1 MB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	2.08	5.87	2.78	5.93
4MA-[ESP-MD5]-[ESP-3DES]	2.08	7.10	2.78	7.18
6MA-[AH-MD5]-[ESP-3DES]	4.17	4.82	5.56	4.88
LOAD	**SMTP(WITH IDENT)**		**SMTP(WITHOUT IDENT)**	
TOTAL	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	11.26	4.99	9.15	4.96
4MA-[ESP-MD5]-[ESP-3DES]	13.17	5.78	10.68	5.75
6MA-[AH-MD5]-[ESP-3DES]	16.73	6.86	13.69	6.82
S to C	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	7.39	3.33	6.22	3.31
4MA-[ESP-MD5]-[ESP-3DES]	8.38	3.77	7.01	3.76
6MA-[AH-MD5]-[ESP-3DES]	10.33	4.56	8.64	4.54
C to S	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	37.64	71.56	32.78	71.69
4MA-[ESP-MD5]-[ESP-3DES]	45.77	86.12	40.35	86.30
6MA-[AH-MD5]-[ESP-3DES]	60.31	99.00	54.47	99.13

TIME	SMTP(WITH IDENT)		SMTP(WITHOUT IDENT)	
SMTP	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	0.00	0.00	0.00	0.00
2M-[AH-MD5]-[null]	0.95	2.62	5.59	3.44
4MA-[ESP-MD5]-[ESP-3DES]	1.17	3.66	6.65	4.80
6MA-[AH-MD5]-[ESP-3DES]	2.04	5.66	13.77	7.54

Protocol comparison

HTTP wireless vs. HTTP wireline

TRANSACTIONS	Testbed 1 vs. Testbed 4		Testbed 2 vs. Testbed 3	
TOTAL	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	0.00	0.81	0.00	4.09
2M-[AH-MD5]-[null]	2.50	0.43	0.00	4.12
4MA-[ESP-MD5]-[ESP-3DES]	5.00	-3.51	0.00	4.81
6MA-[AH-MD5]-[ESP-3DES]	0.00	-5.23	0.00	5.19
S to C	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	0.00	0.14	0.00	0.41
2M-[AH-MD5]-[null]	0.00	0.46	0.00	0.52
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.46	0.00	0.39
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.46	0.00	0.46
C to S	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	0.00	2.14	0.00	11.34
2M-[AH-MD5]-[null]	5.56	0.38	0.00	11.14
4MA-[ESP-MD5]-[ESP-3DES]	11.11	-10.27	0.00	13.48
6MA-[AH-MD5]-[ESP-3DES]	0.00	-14.45	0.00	14.39
LOAD	**Testbed 1 vs. Testbed 4**		**Testbed 2 vs. Testbed 3**	
TOTAL	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	0.18	0.15	0.36	0.57
2M-[AH-MD5]-[null]	0.60	0.04	0.34	0.76
4MA-[ESP-MD5]-[ESP-3DES]	1.07	-0.25	0.33	0.87
6MA-[AH-MD5]-[ESP-3DES]	0.15	-0.52	0.33	1.01
S to C	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	0.00	0.00	0.39	0.29
2M-[AH-MD5]-[null]	0.00	0.03	0.37	0.31
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.09	0.37	0.30
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.10	0.37	0.31

C to S	10 KB	1 MB	10 KB	1 MB
1-[null]-[null]	2.33	6.70	0.00	12.91
2M-[AH-MD5]-[null]	5.89	0.11	0.00	12.49
4MA-[ESP-MD5]-[ESP-3DES]	10.04	-7.48	0.00	14.83
6MA-[AH-MD5]-[ESP-3DES]	1.31	-11.98	0.00	16.74
TIME	**Testbed 1 vs. Testbed 4**		**Testbed 2 vs. Testbed 3**	
	10 KB	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	509.25	449.00	723.63	434.33
2M-[AH-MD5]-[null]	472.75	433.17	771.28	438.99
4MA-[ESP-MD5]-[ESP-3DES]	358.11	378.94	704.66	425.75
6MA-[AH-MD5]-[ESP-3DES]	412.93	363.49	756.45	414.50
Average	438.26	406.15	739.01	428.39

Testbed 1 vs. Testbed 4

SMTP wireless vs. SMTP wireline

TRANSACTIONS	SMTP (WITH IDENT)		SMTP (WITHOUT IDENT)	
TOTAL	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	0.00	-21.84	0.00	-21.96
2M-[AH-MD5]-[null]	0.00	-21.91	0.00	-22.02
4MA-[ESP-MD5]-[ESP-3DES]	1.96	-32.79	2.50	-32.94
6MA-[AH-MD5]-[ESP-3DES]	0.96	-33.63	1.22	-33.78
S to C	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	-1.79	0.79	-2.17	0.79
2M-[AH-MD5]-[null]	-1.75	0.62	-2.13	0.62
4MA-[ESP-MD5]-[ESP-3DES]	-1.79	0.76	-2.17	0.76
6MA-[AH-MD5]-[ESP-3DES]	-3.51	0.62	-4.26	0.62
C to S	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	2.13	5.36	2.86	-45.77
2M-[AH-MD5]-[null]	2.08	4.06	2.78	-45.47
4MA-[ESP-MD5]-[ESP-3DES]	6.52	-22.27	8.82	-58.93
6MA-[AH-MD5]-[ESP-3DES]	6.38	-22.98	8.57	-60.10
LOAD	**SMTP (WITH IDENT)**		**SMTP (WITHOUT IDENT)**	
TOTAL	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	2.22	-1.68	2.18	-1.68
2M-[AH-MD5]-[null]	1.13	-2.81	1.09	-2.81
4MA-[ESP-MD5]-[ESP-3DES]	1.69	-5.25	1.68	-5.25
6MA-[AH-MD5]-[ESP-3DES]	1.42	-5.94	1.41	-5.94

S to C	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	0.10	0.04	0.10	0.04
2M-[AH-MD5]-[null]	-0.04	0.09	-0.05	0.09
4MA-[ESP-MD5]-[ESP-3DES]	-0.08	0.11	-0.08	0.11
6MA-[AH-MD5]-[ESP-3DES]	-0.44	0.06	-0.45	0.06
C to S	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	19.42	-41.68	22.08	-41.98
2M-[AH-MD5]-[null]	7.89	-42.80	9.07	-43.08
4MA-[ESP-MD5]-[ESP-3DES]	11.69	-56.81	14.10	-57.08
6MA-[AH-MD5]-[ESP-3DES]	11.14	-58.38	13.46	-58.65
TIME	**SMTP (WITH IDENT)**		**SMTP (WITHOUT IDENT)**	
SMTP	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	1225.74	307.24	139.97	210.27
2M-[AH-MD5]-[null]	1079.08	274.68	119.32	187.47
4MA-[ESP-MD5]-[ESP-3DES]	1066.34	183.21	118.90	117.06
6MA-[AH-MD5]-[ESP-3DES]	1069.58	186.49	132.09	121.04

Testbed 2 vs. Testbed 3

SMTP wireless vs. SMTP wireline

TRANSACTIONS	**SMTP (WITH IDENT)**		**SMTP (WITHOUT IDENT)**	
TOTAL	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	-2.88	6.09	-3.66	6.14
2M-[AH-MD5]-[null]	-1.00	8.42	-1.28	8.48
4MA-[ESP-MD5]-[ESP-3DES]	-4.76	7.05	-6.02	7.10
6MA-[AH-MD5]-[ESP-3DES]	-2.88	6.20	-3.66	6.24
S to C	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	-5.36	-7.25	-6.52	-7.28
2M-[AH-MD5]-[null]	-3.57	-3.19	-4.35	-3.20
4MA-[ESP-MD5]-[ESP-3DES]	-5.26	-3.32	-6.38	-3.34
6MA-[AH-MD5]-[ESP-3DES]	-3.57	-3.32	-4.35	-3.34
C to S	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	0.00	42.22	0.00	42.86
2M-[AH-MD5]-[null]	2.27	38.07	3.13	38.61
4MA-[ESP-MD5]-[ESP-3DES]	-4.17	32.05	-5.56	32.48
6MA-[AH-MD5]-[ESP-3DES]	-2.08	28.94	-2.78	29.33

LOAD	**SMTP (WITH IDENT)**		**SMTP (WITHOUT IDENT)**	
TOTAL	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	0.64	0.72	2.79	0.74
2M-[AH-MD5]-[null]	0.75	1.18	4.09	1.22
4MA-[ESP-MD5]-[ESP-3DES]	-0.77	1.10	2.63	1.15
6MA-[AH-MD5]-[ESP-3DES]	-0.32	1.04	3.38	1.09
S to C	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	0.41	-0.07	0.30	-0.08
2M-[AH-MD5]-[null]	0.28	0.03	0.18	0.02
4MA-[ESP-MD5]-[ESP-3DES]	-0.40	-0.05	-0.52	-0.05
6MA-[AH-MD5]-[ESP-3DES]	-0.16	-0.07	-0.28	-0.07
C to S	**10 KB**	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	2.50	44.51	26.93	46.71
2M-[AH-MD5]-[null]	3.65	38.95	34.21	40.94
4MA-[ESP-MD5]-[ESP-3DES]	-2.78	34.20	23.76	36.01
6MA-[AH-MD5]-[ESP-3DES]	-1.12	30.23	26.32	31.97
TIME	**SMTP (WITH IDENT)**		**SMTP (WITHOUT IDENT)**	
	10 KB	**1 MB**	**10 KB**	**1 MB**
1-[null]-[null]	4211.09	564.25	369.79	409.16
2M-[AH-MD5]-[null]	3722.11	566.03	309.77	415.76
4MA-[ESP-MD5]-[ESP-3DES]	3449.09	544.15	313.88	399.72
6MA-[AH-MD5]-[ESP-3DES]	3283.05	523.38	274.10	384.16
Average	3666.33	549.45	316.88	402.20

Appendix L - MD5 vs. SHA1

Testbed 1

HTTP TRANSACTIONS					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	0.00	0.00	0.00	-0.09	0.11
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	-0.39	2.02	1.25
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.00	-0.39	0.41	-0.14
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	0.00	0.00	0.00	0.00	0.07
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	-0.02
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	0.00	0.00	0.00	-0.25	0.21
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	-1.01	5.47	3.43
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.00	-1.02	1.06	-0.38
HTTP LOAD					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	0.00	0.00	0.00	-0.01	0.01
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	-0.05	0.23	0.15
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.00	-0.05	0.05	-0.02
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	0.00	0.00	0.00	0.00	0.00
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00

C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	0.00	0.00	0.00	-0.25	0.21
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	-0.95	5.07	3.42
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.00	-0.97	1.05	-0.38
HTTP TIME					
	1 KB	10 KB	100 KB	1 MB	10 MB
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	4.09	0.18	10.65	1.94	1.51
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	8.37	7.99	4.82	7.58	7.26
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	7.98	6.77	5.56	5.97	7.18
Average	6.81	4.98	7.01	5.16	5.32
SMTP(WITH IDENT) TRANSACTIONS					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	-2.50	-1.90	1.25	-0.26	-0.26
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	1.30	1.96	-2.37	0.19	-0.18
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.96	3.36	0.06	0.07
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	-2.56	-1.75	-0.42	0.09	0.02
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	-0.41	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	0.00	1.75	0.00	0.00	0.01
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	-2.44	-2.08	3.77	3.77	-0.54
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	2.56	4.35	-4.46	-4.46	-0.31
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.00	7.25	7.25	0.11

SMTP(WITH IDENT) LOAD					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	-1.42	-0.49	0.17	-0.04	-0.03
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.79	0.55	-0.36	0.03	-0.03
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.27	0.57	0.01	0.01
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	-1.07	-0.27	-0.04	0.01	0.01
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	-0.01	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.33	0.00	0.00	0.00
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	-1.98	-1.74	3.56	-0.63	-0.53
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	2.09	3.64	-4.29	0.33	-0.31
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.00	6.97	0.11	0.11
SMTP(WITH IDENT) TIME					
	1 KB	**10 KB**	**100 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	7.78	0.50	12.56	3.26	9.15
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	3.17	3.32	7.31	1.87	4.04
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	3.51	3.20	7.33	2.38	3.67
Average	4.82	2.34	9.07	2.50	5.62

SMTP(WITHOUT IDENT) TRANSACTIONS					
TOTAL	1 KB	10 KB	100 KB	1 MB	10 MB
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	-3.45	-2.41	1.33	-0.27	-0.26
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	1.82	2.50	-2.48	0.19	-0.18
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	0.00	1.22	3.53	0.06	0.07
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	-3.45	-2.13	-0.43	0.10	0.02
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	-0.43	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	0.00	2.13	0.00	0.00	0.01
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	-3.45	-2.78	4.08	4.08	-0.54
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	3.70	5.88	-4.72	-4.72	-0.31
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.00	7.69	7.69	0.11
SMTP(WITHOUT IDENT) LOAD					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	-1.71	-0.52	0.17	-0.04	-0.03
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.96	0.58	-0.36	0.03	-0.03
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.29	0.58	0.01	0.01
	0.00	0.00	0.00	0.00	0.00
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	-1.24	-0.28	-0.04	0.01	0.01
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	-0.01	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.34	0.00	0.00	0.00

C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	-2.61	-2.21	3.84	-0.64	-0.53
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	2.80	4.69	-4.53	0.33	-0.31
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.00	7.39	0.11	0.11
SMTP(WITHOUT IDENT) TIME					
	1 KB	**10 KB**	**100 KB**	**1 MB**	**10 MB**
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	9.33	0.17	13.72	3.28	9.16
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	3.51	3.67	7.83	1.87	4.04
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	3.81	3.42	7.81	2.39	3.67
Average	5.55	2.42	9.79	2.51	5.62

Testbed 1 EXTRA data

The data for the 1 KB and 10 KB files for the network load and the number of transactions was not recorded, since the measurements did not deviate from Testbed 1 data (slow configuration). SMTP without Ident was not shown for the1 MB and 10 MB files since its effect was negligible.

HTTP TRANSFER TIME					
	1 KB	10 KB	100 KB	1 MB	10 MB
	0.00	0.00	0.00		
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	4.60	2.67	1.14	0.35	0.80
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	4.93	1.75	2.16	2.44	1.28
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	5.35	2.22	2.53	2.54	3.25
Average	4.96	2.21	1.95	1.77	1.78

SMTP(WITH IDENT) TRANSFER TIME					
	1 KB	10 KB	100 KB	1 MB	10 MB
	0.00	0.00	0.00		
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.00	0.00
3M-[AH-SHA1]-[null]	-0.08	2.91	1.18	-0.34	0.16
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	2.21	5.11	1.75	2.02	0.29
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
7MA-[AH-SHA1]-[ESP-3DES]	4.47	4.63	1.68	3.74	0.35
Average	2.20	4.21	1.54	1.81	0.27
SMTP (WITHOUT IDENT)	1 KB	10 KB	100 KB		
1-[null]-[null]	0.00	0.00	0.00		
2M-[AH-MD5]-[null]	0.00	0.00	0.00		
3M-[AH-SHA1]-[null]	2.91	2.91	2.91		
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00		
5MA-[ESP-SHA1]-[ESP-3DES]	5.11	5.11	5.11		
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00		
7MA-[AH-SHA1]-[ESP-3DES]	4.63	4.63	4.63		
Average	4.21	4.21	4.21		

Appendix M – Zip vs. Doc File Type Comparison

Comparison Between Zip and Doc file types from 1500 MTU data

Equation used: ((doc –zip) /doc *100)

	FILE SIZE =>1 KB				**PROTOCOL =>HTTP**		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	0.00	0.00	0.00	0.54	0.43	0.46	9.10
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.40	0.38	0.38	2.47
3M-[AH-SHA1]-[null]	0.00	0.00	0.00	0.40	0.38	0.38	-2.36
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00	0.00	0.68
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00	0.00	4.74
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00	0.00	3.24
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00	0.00	2.68
	FILE SIZE => 10 KB				**PROTOCOL =>** HTTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	0.00	0.00	0.00	0.42	-0.06	-0.02	-2.72
2M-[AH-MD5]-[null]	0.00	0.00	0.00	0.30	-0.06	-0.02	-0.26
3M-[AH-SHA1]-[null]	0.00	0.00	0.00	0.30	-0.06	-0.02	4.00
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	-0.07	-0.06	-2.99
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	-0.07	-0.06	-0.01
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	-0.07	-0.06	-1.07
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	-0.07	-0.06	-0.34
	FILE SIZE => 100 KB				**PROTOCOL =>** HTTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	-2.38	-1.35	-1.72	-1.98	-0.19	-0.24	-5.29
2M-[AH-MD5]-[null]	0.00	-1.39	-1.08	0.08	-0.25	-0.24	0.37
3M-[AH-SHA1]-[null]	0.00	-1.39	-1.08	0.08	-0.25	-0.24	-5.05
4MA-[ESP-MD5]-[ESP-3DES]	-3.37	-1.39	-1.86	-3.16	-0.26	-0.40	-0.27
5MA-[ESP-SHA1]-[ESP-3DES]	-2.25	-1.39	-1.59	-2.11	-0.26	-0.35	1.09
6MA-[AH-MD5]-[ESP-3DES]	-1.05	-1.39	-1.31	-1.00	-0.27	-0.31	-0.01
7MA-[AH-SHA1]-[ESP-3DES]	-1.05	-1.39	-1.31	-1.00	-0.27	-0.31	-0.84

	FILE SIZE => 1 MB				**PROTOCOL =>** HTTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	0.27	-0.34	-0.14	0.29	-0.09	-0.08	-4.75
2M-[AH-MD5]-[null]	0.26	-0.10	-0.03	0.28	-0.08	-0.06	-0.31
3M-[AH-SHA1]-[null]	0.13	-0.10	-0.05	0.45	-0.08	-0.07	1.68
4MA-[ESP-MD5]-[ESP-3DES]	0.55	-0.14	0.03	0.55	-0.08	-0.06	0.13
5MA-[ESP-SHA1]-[ESP-3DES]	-1.75	-0.14	-0.52	-1.73	-0.08	-0.16	0.35
6MA-[AH-MD5]-[ESP-3DES]	-0.64	-0.14	-0.26	-0.64	-0.08	-0.11	-1.51
7MA-[AH-SHA1]-[ESP-3DES]	2.73	-0.14	0.57	2.70	-0.08	0.06	-0.16
	FILE SIZE =>10 MB				**PROTOCOL =>HTTP**		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	1.35	-0.69	-0.01	1.40	0.00	0.03	-0.70
2M-[AH-MD5]-[null]	0.38	0.02	0.09	0.44	0.03	0.04	-0.16
3M-[AH-SHA1]-[null]	0.39	0.06	0.12	0.47	0.04	0.05	-0.15
4MA-[ESP-MD5]-[ESP-3DES]	-0.96	0.04	-0.20	-1.03	0.03	-0.01	-0.15
5MA-[ESP-SHA1]-[ESP-3DES]	-0.51	0.02	-0.11	-0.50	0.03	0.01	0.81
6MA-[AH-MD5]-[ESP-3DES]	0.27	0.02	0.08	0.23	0.03	0.04	-0.40
7MA-[AH-SHA1]-[ESP-3DES]	0.83	0.02	0.21	0.83	0.03	0.07	0.08
	FILE SIZE =>1 KB				**PROTOCOL =>**SMTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	0.00	0.00	0.00	0.00	-0.05	-0.04	-5.99
2M-[AH-MD5]-[null]	0.00	-2.50	-1.25	0.00	-1.12	-0.70	-4.42
3M-[AH-SHA1]-[null]	-5.13	0.00	-2.53	-4.11	-0.04	-1.55	-3.93
4MA-[ESP-MD5]-[ESP-3DES]	-2.50	-2.50	-2.50	-2.04	-1.17	-1.50	-6.96
5MA-[ESP-SHA1]-[ESP-3DES]	-2.50	-2.50	-2.50	-2.04	-1.17	-1.50	-7.51
6MA-[AH-MD5]-[ESP-3DES]	-5.00	-5.00	-5.00	-3.04	-1.84	-2.30	-5.45
7MA-[AH-SHA1]-[ESP-3DES]	2.44	0.00	1.22	2.04	0.00	0.79	-2.72
	FILE SIZE => 10 KB				**PROTOCOL =>** SMTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	2.13	1.79	1.94	1.59	0.07	0.23	2.20
2M-[AH-MD5]-[null]	2.08	1.35	1.64	1.74	-0.20	0.08	1.74
3M-[AH-SHA1]-[null]	-9.52	1.35	-2.59	3.47	-0.03	0.49	-2.64
4MA-[ESP-MD5]-[ESP-3DES]	-4.35	-1.37	-2.52	-3.64	-0.20	-0.71	-2.02
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	-0.13	-0.11	-2.37
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	-0.13	-0.11	-1.47
7MA-[AH-SHA1]-[ESP-3DES]	4.26	0.00	1.67	3.63	-0.22	0.39	-3.80

	FILE SIZE =>100 KB				**PROTOCOL** =>SMTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	-15.04	1.67	-4.30	-13.42	-0.05	-0.48	0.54
2M-[AH-MD5]-[null]	4.09	1.44	2.21	3.88	-0.14	0.09	1.77
3M-[AH-SHA1]-[null]	-1.66	0.24	-0.34	-1.57	-0.03	-0.12	1.52
4MA-[ESP-MD5]-[ESP-3DES]	-8.91	-3.45	-5.26	-8.53	-0.17	-0.78	2.98
5MA-[ESP-SHA1]-[ESP-3DES]	-12.71	-0.24	-4.07	-12.11	-0.21	-1.00	5.22
6MA-[AH-MD5]-[ESP-3DES]	-9.09	2.14	-1.17	1.63	-0.15	-0.02	2.59
7MA-[AH-SHA1]-[ESP-3DES]	0.52	-0.24	0.00	0.49	-0.20	-0.15	1.12
	FILE SIZE =>1 MB				**PROTOCOL** =>SMTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	-0.21	-0.15	-0.18	-0.22	-0.08	-0.09	-0.05
2M-[AH-MD5]-[null]	-0.48	-0.18	-0.30	-0.50	-0.08	-0.11	-4.59
3M-[AH-SHA1]-[null]	0.15	0.03	0.07	0.15	-0.08	-0.06	-4.80
4MA-[ESP-MD5]-[ESP-3DES]	-0.33	-0.25	-0.28	-0.33	-0.08	-0.11	-1.78
5MA-[ESP-SHA1]-[ESP-3DES]	-1.97	-0.05	-0.82	-1.96	-0.08	-0.25	-2.96
6MA-[AH-MD5]-[ESP-3DES]	0.10	-0.08	-0.02	0.10	-0.08	-0.06	-2.07
7MA-[AH-SHA1]-[ESP-3DES]	-0.51	0.00	-0.17	-0.50	-0.08	-0.11	-2.86
		FILE SIZE =>10 MB			**PROTOCOL** =>SMTP		
Scenario	**Average # of Trans.**			**Average Network Load**			
	C to S	S to C	**Total Trans.**	C to S	S to C	Total Load	**Average Transfer Time/sec**
1-[null]-[null]	NA						-6.34
2M-[AH-MD5]-[null]							4.77
3M-[AH-SHA1]-[null]							-6.27
4MA-[ESP-MD5]-[ESP-3DES]							0.80
5MA-[ESP-SHA1]-[ESP-3DES]							1.77
6MA-[AH-MD5]-[ESP-3DES]							1.12
7MA-[AH-SHA1]-[ESP-3DES]							0.95

Appendix N - AH Vs ESP Authentication (with 3DES)

Testbed 1

HTTP TRANSACTIONS					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	-0.39	1.86	1.57
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.00	-0.39	0.24	0.16
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	-0.02
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.00	-1.01	5.02	4.27
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.00	-1.02	0.63	0.44
HTTP LOAD					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	4.47	1.81	1.24	1.46	1.42
7MA-[AH-SHA1]-[ESP-3DES]	4.47	1.81	1.24	1.29	1.25
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	3.17	1.12	0.84	0.80	0.80
7MA-[AH-SHA1]-[ESP-3DES]	3.17	1.12	0.84	0.80	0.80
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	6.79	7.64	8.54	15.50	14.86
7MA-[AH-SHA1]-[ESP-3DES]	6.79	7.64	8.53	11.08	10.64
HTTP TIME					
	1 KB	10 KB	100 KB	1 MB	10 MB
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	2.51	2.65	0.34	3.34	0.63
7MA-[AH-SHA1]-[ESP-3DES]	2.15	1.49	1.06	1.79	0.55
Average	2.33	2.07	0.70	2.56	0.59

SMTP(WITH IDENT) TRANSACTIONS					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	1.30	1.96	-3.87	0.39	0.39
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.96	1.76	0.27	0.64
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	0.00	1.79	-0.41	-0.05	-0.01
7MA-[AH-SHA1]-[ESP-3DES]	0.00	3.57	0.00	-0.05	0.00
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	2.56	2.17	-7.59	-7.59	0.69
7MA-[AH-SHA1]-[ESP-3DES]	0.00	-2.08	3.74	3.74	1.12
SMTP (WITH IDENT) LOAD					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	7.02	3.42	0.98	1.76	1.76
7MA-[AH-SHA1]-[ESP-3DES]	6.18	3.14	1.93	1.74	1.80
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	4.87	2.16	0.92	0.81	0.80
7MA-[AH-SHA1]-[ESP-3DES]	4.87	2.50	0.93	0.81	0.80
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	10.57	10.52	1.74	10.94	10.93
7MA-[AH-SHA1]-[ESP-3DES]	8.31	6.64	13.71	10.70	11.40
SMTP (WITH IDENT) TIME					
	1 KB	**10 KB**	**100 KB**	**1 MB**	**10 MB**
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	0.73	0.58	0.37	0.76	1.80
7MA-[AH-SHA1]-[ESP-3DES]	1.05	0.47	0.38	1.27	1.44
Average	0.89	0.52	0.37	1.02	1.62

SMTP (WITHOUT IDENT) TRANSACTIONS					
TOTAL	1 KB	10 KB	100 KB	1 MB	10 MB
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	1.82	2.50	-4.06	0.39	0.39
7MA-[AH-SHA1]-[ESP-3DES]	0.00	1.22	1.85	0.27	0.64
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	0.00	2.17	-0.43	-0.05	-0.01
7MA-[AH-SHA1]-[ESP-3DES]	0.00	4.35	0.00	-0.05	0.00
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	3.70	2.94	-8.02	-8.02	0.69
7MA-[AH-SHA1]-[ESP-3DES]	0.00	-2.78	3.96	3.96	1.12
SMTP (WITHOUT IDENT) LOAD					
TOTAL	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	6.42	2.99	0.91	1.76	1.76
7MA-[AH-SHA1]-[ESP-3DES]	5.41	2.70	1.86	1.73	1.80
S to C	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	4.15	1.90	0.88	0.80	0.80
7MA-[AH-SHA1]-[ESP-3DES]	4.15	2.25	0.89	0.80	0.80
	0.00	0.00	0.00	0.00	0.00
C to S	**1 KB**	**10 KB**	**100 KB**	**1 MB**	**10 MB**
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	10.78	10.68	1.28	10.94	10.93
7MA-[AH-SHA1]-[ESP-3DES]	7.76	5.73	13.93	10.70	11.40
SMTP (WITHOUT IDENT) TIME					
	1 KB	**10 KB**	**100 KB**	**1 MB**	**10 MB**
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	0.79	0.61	0.36	0.76	1.80
7MA-[AH-SHA1]-[ESP-3DES]	1.08	0.37	0.34	1.28	1.44
Average	0.94	0.49	0.35	1.02	1.62

Testbed 1 Extra Data

HTTP TRANSACTIONS			
TOTAL	100 KB	1 MB	10 MB
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	0.82	-0.17	0.16
7MA-[AH-SHA1]-[ESP-3DES]	0.82	0.09	0.18
S to C	100 KB	1 MB	10 MB
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.07	-0.01
7MA-[AH-SHA1]-[ESP-3DES]	0.00	0.00	-0.12
C to S	100 KB	1 MB	10 MB
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	2.27	-0.64	0.50
7MA-[AH-SHA1]-[ESP-3DES]	2.27	0.26	0.78
HTTP LOAD			
TOTAL	100 KB	1 MB	10 MB
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	1.36	1.14	1.18
7MA-[AH-SHA1]-[ESP-3DES]	1.36	1.18	1.18
HTTP 1 TO 2	100 KB	1 MB	10 MB
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	0.84	0.81	0.81
7MA-[AH-SHA1]-[ESP-3DES]	0.84	0.80	0.79
HTTP 2 TO 1	100 KB	1 MB	10 MB
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	11.87	9.31	10.71
7MA-[AH-SHA1]-[ESP-3DES]	11.87	10.37	11.06

HTTP TRANSFER TIME					
	1 KB	10 KB	100 KB	1 MB	10 MB
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	1.29	0.40	0.69	1.90	1.41
7MA-[AH-SHA1]-[ESP-3DES]	1.70	0.86	1.05	2.01	3.38
Average	1.50	0.63	0.87	1.96	2.39

SMTP TRANSACTIONS	SMTP (WITH IDENT)			SMTP (WITHOUT IDENT)
TOTAL	100 KB	1 MB	10 MB	100 KB
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	0.00	0.48	0.40	0.00
7MA-[AH-SHA1]-[ESP-3DES]	2.14	-0.06	0.99	2.27
	0			
S to C	100 KB	1 MB	10 MB	100 KB
4MA-[ESP-MD5]-[ESP-3DES]	0	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	0.81	0.05	-0.01	0.84
7MA-[AH-SHA1]-[ESP-3DES]	0.81	0.09	-0.05	0.84
	0.00			
C to S	100 KB	1 MB	10 MB	100 KB
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	-2.27	1.52	1.60	-2.27
7MA-[AH-SHA1]-[ESP-3DES]	6.82	-0.44	3.94	6.82
SMTP LOAD				
TOTAL	100 KB	1 MB	10 MB	100 KB
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	1.38	1.21	1.13	1.31
7MA-[AH-SHA1]-[ESP-3DES]	1.70	1.15	1.21	1.63
	0			
S to C	100 KB	1 MB	10 MB	100 KB
4MA-[ESP-MD5]-[ESP-3DES]	0	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	1.04	0.84	0.83	1.00
7MA-[AH-SHA1]-[ESP-3DES]	1.04	0.85	0.83	1.00
	0			
C to S	100 KB	1 MB	10 MB	100 KB
4MA-[ESP-MD5]-[ESP-3DES]	0	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	11.62	11.72	11.92	10.32
7MA-[AH-SHA1]-[ESP-3DES]	21.10	9.69	14.52	19.81

SMTP(WITH IDENT)					
TRANSFER TIME	1 KB	10 KB	100 KB	1 MB	10 MB
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	1.14	1.77	0.76	0.22	0.21
7MA-[AH-SHA1]-[ESP-3DES]	3.38	1.30	0.69	1.91	0.28
Average	2.26	1.53	0.73	1.06	0.24

SMTP (WITHOUT IDENT) TRANSFER TIME	1 KB	10 KB	100 KB
4MA-[ESP-MD5]-[ESP-3DES]	0.00	0.00	0.00
5MA-[ESP-SHA1]-[ESP-3DES]	0.00	0.00	0.00
6MA-[AH-MD5]-[ESP-3DES]	1.51	2.21	0.80
7MA-[AH-SHA1]-[ESP-3DES]	4.72	1.61	0.73
Average	3.11	1.91	0.77

Appendix O - Hardware and Software Information

Computers	Processor	Memory
East	Intel Celeron 566 MHz	128 MB
West	Pentium Pro 200	32 MB
Dusk	Pentium III 1 GHz	512 MB

Software	Version
Linux Red Hat	7.0
Linux kernel	2.2.16-22
Pcmcia package	3.1.25
Apache server	1.3.12-25
Freeswan	1.7
Sendmail	8.11
Netscape Communicator	4.75
Ethereal (on Windows NT)	0.8.13

Special Settings Used

Netscape Communicator on all clients	Go to Edit, Preferences, Advanced, Cache Cache set to "zero"
Apache server on EAST Every request to the server is to be set up uniquely. There is significant overhead in that process (allocating handles, authorizing, etc.).	In httpd.conf **KeepAlive =Off**

Extra Information

To disable the ident protocol	In sendmail.cf set **Timeout.ident= 0 s**
Recommended settings for good performance [20]	**net/ipv4/tcp_sack = 1** **net/ipv4/tcp_window_scaling = 1** **net/ipv4/tcp_timestamps = 1**
To set the Send Window	**echo xx > /proc/sys/net/core/wmem_default** **echo xx > /proc/sys/net/core/wmem_max**
To set the Receive Window	**echo xx > /proc/sys/net/core/rmem_default** **echo xx > /proc/sys/net/core/rmem_max**
To change the MTU size	Ifconfig eth0 mtu xxx Ifconfig ipsec0 mtu xxx
To change the Buffer size in Sendmail	Set **O DaemonPortOptions= SndBufSize=xx** **O DaemonPortOptions= RcvBufSize=xx**

Wireless card and Access Point

The pcmcia wireless card was installed into West using an ISA pcmcia card adapter [21]. The hardware information for the access point are shown below:

Model Number	Raytheon 24200 Raylink Access Point
Hardware Revision	1.03A4
Boot Software Version	1.00
System Software Version	1.06
Hopping Sequence	15
Geographic Region	North America
Encapsulation Mode is	Disabled
Protocol Filter Mode is	Disabled

Wireless card configuration

CONFIG.OPTS

```
# /etc/pcmcia/Config.opts
#
# Local PCMCIA Configuration File
#
#-------------------------------------------------------------
------------
#source./ray_cs.opts
# System resources available for PCMCIA devices

include port 0x100-0x4ff, port 0x800-0x8ff, port 0xc00-
0xcff
include memory 0xc0000-0xfffff
include memory 0xa0000000-0xa0ffffff, memory 0x60000000-
0x60ffffff

# Extra port range for IBM Token Ring
include port 0xa00-0xaff

# Resources we should not use, even if they appear to be
available
# First built-in serial port
exclude irq 4
# Second built-in serial port
exclude irq 3
# First built-in parallel port
exclude irq 7
```

```
# PS/2 Mouse controller port, comment this out if you don't
have a PS/2
# based mouse
exclude irq 12

#-------------------------------------------------------
------------
# options for loadable modules
# Options for Raylink/WebGear driver: uncomment only one
line...
# Generic ad-hoc network
#module "ray_cs" opts "essid=ADHOC_ESSID hop_dwell=128
#beacon_period=256 translate=0"

# Infrastructure network for older cards
module "ray_cs" opts "net_type=1 essid=ESSID091599 translate=1"
#Ad-hoc did not work in Linux
# Infrastructure network for WebGear
#module "ray_cs" opts "net_type=1 essid=ESSID1 translate=1
hop_dwell=128 beacon_period=256"
```

NETWORK.OPTS

```
#/etc/pcmcia/network.opts
# Network adapter configuration
#
# The address format is "scheme,socket,instance,hwaddr".
#
# Note: the "network address" here is NOT the same as the
IP address.
# See the Networking HOWTO.  In short, the network address
is the IP
# address masked by the netmask.
#
case "$ADDRESS" in
*,*,*,*)
    INFO="Sample private network setup"
    # Transceiver selection, for some cards -- see 'man
ifport'
    IF_PORT=""
    # Use BOOTP (via /sbin/bootpc, or /sbin/pump)? [y/n]
    BOOTP="n"
    # Use DHCP (via /sbin/dhcpcd, /sbin/dhclient, or
/sbin/pump)? [y/n]
    DHCP="n"
    # If you need to explicitly specify a hostname for DHCP
requests
    DHCP_HOSTNAME=""
```

```
    # Host's IP address, netmask, network address,
broadcast address
    IPADDR="10.0.4.1"
    NETMASK="255.255.255.0"
    NETWORK="10.0.4.0"
    BROADCAST="10.0.4.255"
    # Gateway address for static routing
    GATEWAY="10.0.4.1"
    # Things to add to /etc/resolv.conf for this interface
    DOMAIN=""
    SEARCH=""
    DNS_1=""
    DNS_2=""
    DNS_3=""
    # NFS mounts, should be listed in /etc/fstab
    MOUNTS=""
    # If you need to override the interface's MTU...
    MTU=""
    # For IPX interfaces, the frame type and network number
    IPX_FRAME=""
    IPX_NETNUM=""
    # Extra stuff to do after setting up the interface
    start_fn () { return; }
    # Extra stuff to do before shutting down the interface
    stop_fn () { return; }
    # Card eject policy options
    NO_CHECK=n
    NO_FUSER=n
    ;;
esac

# This is used to hook into Red Hat's network configuration
tools.
# You can delete it if that isn't desired.  We look for
network
# options in /etc/sysconfig/network-scripts if it appears
that the
# interface can't be set up using settings given higher up
in this
# file.

is_true $PUMP || is_true $BOOTP || is_true $DHCP || \
if [ ! "$IPADDR" -a -f /etc/sysconfig/network-
scripts/ifcfg-$2 ] ; then
    INFO="Red Hat netconf setup"
    start_fn () {
     . /etc/sysconfig/network-scripts/ifcfg-$1
```

```
     if [ "$ONBOOT" = "yes" ] ; then log /sbin/ifup $1 ; fi
    }
    stop_fn () {
     log /sbin/ifdown $1
    }
fi
```

Appendix P - IPSEC.CONF

Sample file :

```
# /etc/ipsec.conf - FreeS/WAN IPSEC configuration file
# basic configuration
config setup
     # THIS SETTING MUST BE CORRECT or almost nothing will
work;
     # %defaultroute is okay for most simple cases.
     interfaces="ipsec0=eth0"
     #manualstart="east-west"
     # Debug-logging controls:  "none" for (almost) none,
     "all" for #lots.
     klipsdebug=none
     plutodebug=none
          # Use auto= parameters in conn descriptions to
     control #startup actions.
     plutoload=%search
     plutostart=%search

# connection to secure all traffic between East and West
# This current configuration runs ESP with 3DES and MD5
conn eastGW-westGW
     #auth=ah
     keyingtries=0
     # Left security gateway, subnet behind it, next hop
toward right.
     left=10.0.1.2
     leftsubnet=10.0.3.0/24
     leftnexthop=10.0.1.1
     # Right security gateway, subnet behind it, next hop
toward left.
     right=10.0.1.1
     rightsubnet=10.0.2.0/24
     rightnexthop=10.0.1.2
     spi=0x200
     #Using ESP-3DES with SHA1
     #esp=3des-sha1-96
     #Using ESP -3DES with MD5
     esp=3des-md5-96
     #Using AH with MD5 authentication
     #ah=hmac-md5-96
     #Using AH with SHA1 authentication
     #ah=hmac-sha1-96
     #Using ESP-3DES
     #esp=3des
```

```
     #The authentication key for MD5-128 bits for AH
     #ahkey=0x12345678_9abcdef0_2468ace0_13579bdf
     #The authentication key for MD5-128 bits for ESP
     espauthkey=0x12345678_9abcdef0_2468ace0_13579bdf
     #The authentication key for SHA1-160 bits for AH
     #ahkey=0x12345678_9abcdef0_2468ace0_13579bdf_12345678
     #The authentication key for SHA1-160 bits for ESP
     #espauthkey=0x12345678_9abcdef0_2468ace0_13579bdf_1234
5678
      #The encryption key for 3DES--192 bits
     espenckey=0x01234567_89abcdef_02468ace_13579bdf_123456
78_9abcdef0
```

Appendix Q – FreeS/WAN Bugs

Even though, versions 1.5 and 1.4 had less bugs reported (see below), they both caused an error when recompiling the kernel. Only version 1.7, the latest version at that time went through the whole installation without errors. Version 1.8 came out just after version1.7 was installed and it was the alternative in case version 1.7 failed.

	FREESWAN BUGS Obtained from BUGS files in Freeswan-1.x files	**Versions**			
		1.4	**1.5**	**1.7**	**1.8**
1	The number of IPSec interfaces is hardcoded at 4 rather than being configurable	X	X	X	X
2	KLIPS cannot cope with IP packets employing IP options.	X	X	X	X
3	There are some ill-defined problems with sending large packets through Transport-mode connections, especially in 2.2.xx kernels.	X	X	X	X
4	There appears to be a kernel memory leak if rekeying occurs while a Connection is carrying traffic. The effect is small unless rekeying is used very frequently.	X	X	X	X
5	There are too many ways for packets to get around the security of a system. In particular, suppose you have the following, with security gateways X and Y serving subnets S and T: S======X.....Y======T A packet which shows up at Y, in clear text, claiming to be from S, with a destination in T, will be forwarded... even if there is an IPSec tunnel between X and Y which ought to be encrypting all such packets. The damage such packets could do is limited, but denial-of-service attacks are an obvious possibility. This problem deals with the center of the IP processing machinery in the Linux 2.0.xx kernels which is very complicated. However, KLIPS2 is expected to fix this problem.	X	X	X	X
6	Another "packet leak" arises because at startup, shutdown, or restart, there is a brief period when the network is up but IPSec is not. This exposure can be reduced (not eliminated) using the somewhat ill-documented forwardcontrol parameter.	X	X	X	X
7	A similar leak occurs because there is no simple way to *replace* a route using the Linux 2.2.xx route(8) command. It has to be done with a delete/add sequence, which leaves a timing window in which there is no route for the destination. (The 2.2.xx re-engineering should remove this problem)	X	X	X	X
8	Minor difficulties can arise if more than one subnet is behind a single security gateway, e.g.: S======X.....Y======T \\ ======U If U wants to talk to S encrypted, but T wants to talk to S in clear (no IPSec), it actually is possible but it has to be done with manual "keying", which is a little messy if the U-S connection is automatically keyed, because the two connections share a route which Pluto is not aware of.	X	X	X	X
9	Pluto assumes that it knows what KLIPS is capable of doing, and “chaos” will ensue if it is wrong – in particular, if it is asked to negotiate a compressed connection but the kernel doesn't support IPComp.			X	X
10	If there are multiple connections specified between the same two security gateways, either all or none must specify compression. Otherwise the result is unpredictable.			X	X
11	Installing a new FreeS/WAN on top of an old one doesn't update kernel configuration options, so if new options are added, a virgin kernel is needed instead.			X	X
12	Manual keying is somewhat broken, and won't work very well without "echo 0 >/proc/sys/net/ipsec/inbound_policy_check" on both ends.			X	
13	Neither ping nor tcpdump can consistently see incoming packets emerging from a compressed connection.			X	
	REVISION DATE:	01/24/00	06/26/00	10/30/00	11/29/00

Vita

George Hadjichristofi was born in Nicosia, Cyprus on November 14, 1974. He earned a Fulbright scholarship in 1995 which allowed him to study in the U.S.A. He began his undergraduate studies at Virginia Tech in August 1995. He earned his Bachelors and Masters degree in Computer Engineering at Virginia Polytechnic Institute and State University. He will continue his education at Virginia Tech by joining the PhD Computer Engineering program. His area of concentration is Network Security.

Education

M.S. Computer Engineering, Dec 2001
Virginia Polytechnic Institute & State University, Blacksburg, VA
B.S. Computer Engineering, May 1999
Virginia Polytechnic Institute & State University, Blacksburg, VA

Experience

Graduate Research, VPI & SU, Dept. of Computer Engineering (Fall 2000 - Fall 2001)
Worked on the NAVCIITI (Navy Collaborative Integrated Information Technology Initiative) project sponsored by the ONR (Office of Naval Research). The project investigated network infrastructure for the VON (Virtual Operations Network), which is a rapidly-deployable internetwork of naval vessels at sea. His work concentrated on the security aspects for establishing a VON.

Graduate Teaching Assistant, VPI & SU, Dept. of Computer Science (Fall 1999 - Spring 2000)
Assisted in teaching, and grading for the course: Computer Organization and Architecture.