Jemal Mohammed Tahir

Testing Virtual Private Network (VPN) Interoperability

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Thesis

05 May 2015

Author(s) Title Number of Pages Date	Jemal Mohammed Tahir Testing Virtual Private Network (VPN) Interoperability 58 pages + 3 appendices 05 May 2015
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Computer Networks and Security
Instructor(s)	Erik Pätynen, Senior Lecturer

While corporations are growing their businesses, they may demand additional remote branch offices in a disparate location. These remote offices need to have a connection to their central corporate network so as to get access to resources and services securely over the public network. To achieve this demand, deploying Virtual Private Networks (VPNs) is an alternate technology.

The primary objective of this final year project was to test secure VPN interoperability between two different vendors' gateways that are connected using a site-to-site VPN network, so that the data can be transported back and forth securely over a non-secure network infrastructure that is the Internet.

Practically, this final year project was carried out in a laboratory environment deploying two different vendor gateway devices to simulate a company's sites which are in different geolocations. The network devices were configured to use an IPsec site-to-site VPN and the VPN tunnel formed was tested.

Moreover, this project verified the interoperability between dissimilar vendors via a secure VPN which is an IPsec site-to-site VPN. It can be concluded that interoperability was achieved and the data transported through the public network was tested and it was confirmed that the data was secure and encrypted.

As a corporate branch office grows in size, VPN authentication using Preshared Key (PSK) is not scalable and therefore it is a good choice to consider having a central certificate authority (CA) to authenticate VPN peers.

Keywords	VPN, IPsec VPN, site-to-site VPN, IPsec interoperability

Contents

Appendices

Abbreviations

3DES	Triple Digital Encryption Standard
AES	Advanced Encryption Standard
API	Application Programming Interface
ARP	Address Resolution Protocol
ASICs	Application Specific Integrated Circuits
ATM	Asynchronous Transfer Mode
CAM	Content Addressable Memory
CPU	Central Processing Unit
DES	Digital Encryption Standard
DH	Diffie-Hellman
FDDI	Fibre Distributed Data Interface
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HMAC	Hashed Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDEA	International Data Encryption Algorithm
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IKEv1	Internet Key Exchange version 1
IKEv2	Internet Key Exchange version 2
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Organization for Standardization ‘
ISP	Internet service provider
LAN	Local Area Network
LLC	Logical Link Control
MAC	Media Access Control
MD5	Message Digest 5
MPLS	Multiprotocol Label Switching
NAT	Network Address Translation
OSI	Open Systems Interconnection

OTP	One-time pad
PAT	Port Address Translation
PDU	Protocol Data Unit
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RC	Rivest Cipher
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman
SHA-1	Secure Hash Algorithm 1
SHA-2	Secure Hash Algorithm 2
TCP	Transmission Control Protocol Internet Protocol)
TCP	Transmission Control Protocol
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network

1 Introduction

In the past, business corporations would implement leased or dedicated lines to connect to their branch office or telecommuters so as to ensure secure data transfer. However, for corporations using dedicated leased line is not practical in terms of cost, space coverage and time needed for installation. In recent years, with the rapid development of network technology, the direction of the technology has changed dramatically and the Internet has become abundant, almost everywhere. However, the Internet is exposed to attackers sniffing sensitive information. Virtual Private Networks (VPNs) have become an alternative solution to security breaches which result in the use of public networks, which is unsecure, for private communications.

As security is the top priority, an established VPN allows packets to tunnel via the public network by providing a secure connection as if they were on private networks. A VPN tunnel implements cryptographic techniques to protect on intercepting VPN packet by attackers when it traverses through the public carrier network. The main VPN technologies that provide secure communication are IPsec VPN and SSL VPN.

IPsec is a protocol of suite that is geared around security of data communication. IPsec consists of pieces for authentication, data integrity, confidentiality, and anti-reply attack prevention. IPsec VPN secures the tunnel that is established over a non-secure network.

The goal of this final year project is to test secure VPN interoperability between two different vendors' gateways, Cisco ASA 5505 and Juniper SRX240 that are connected using an IPsec site-to-site VPN network, so that the data can be transported back and forth securely over a non-secure public network infrastructure that is the Internet. The project is directed for students who have a basic knowledge of networking. The structure of this thesis is divided into 8 chapters. Chapter 2 will discuss Internetworking, LAN, WAN and firewalls of a computer networking. Chapter 3 will explain the VPN devices, remote-access VPN, and site-to-site VPN. Chapter 4 will describe the benefits of VPN and chapter 5 the IPsec security protocol. Chapter 6 will explain VPN gateway products and chapter 7 the research and project implementation. Chapter 8 will include discussion and conclusion of the project.

2 Computer Networking

2.1 Internetworking

Recently the Internet has changed the world in the sector of communication channels, where intercommunication has become vital in our daily lives. The computer revolution is a key factor for the dramatic change in the information sector. The Internet encompasses thousands of computer networks that interconnect a bulk of computing devices around the globe. [1]

The demand of networks and networking shown an exponential increase in the past two decades. To point out some of the benefits for the telecommuters, headquarters, branch offices, or home offices are to offer connection whether they are located in the same place or a different geolocation and share different services and resources. For example they can share data, printers, video conferences and VoIP services. [5]

An internetwork is a combination of multiple local area networks connected through gateway devices that contribute and forward routing information of packets among the networks. The gateways can be routers, firewall appliances, or layer 3 switches that have configured their interfaces using the IPv4 or IPv6 addressing scheme. Figure 1 below illustrates those different internetworking technologies that are interconnected via routers, bridges and switches. The internetworking technology mentioned in figure 1 will be illustrated in section 2.3 and 2.4 in detail. For example LAN (Local Area Networks) and WAN (Wide Area Networks) and. FDDI and Token Ring are legacy technology which has been replaced with a new technology that are economical and scalable. [2]

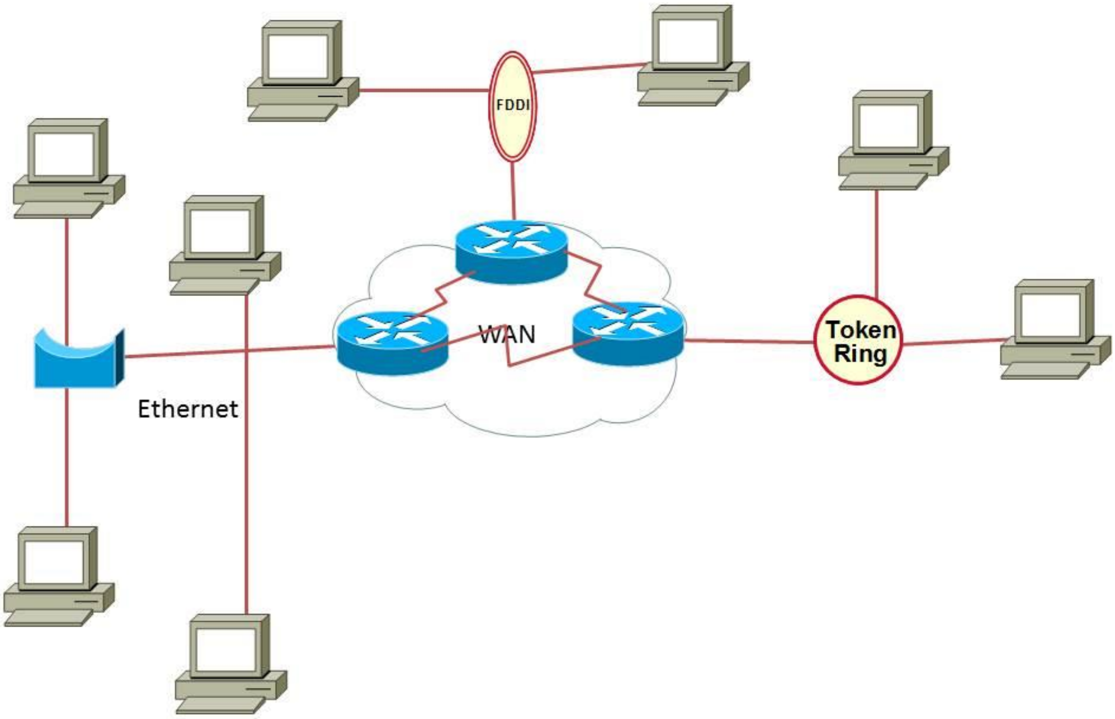


Figure 1. An Internetwork Formed from Different Network Segments.

Establishing a working and efficient internetworking is not an easy task. There are certain areas needed to be addressed to maintain smooth working conditions. Some of the internetworking challenges are listed below:

- Connectivity issue: The issue when connecting different multiple networks is to get successful connectivity to the other end device. For example the end device is implementing a different networking technology and different kinds of media running at various bandwidth levels. [2]
- Reliability: Expecting network connectivity of the company to work and services are reachable all the time. [2]
- Centralized network management: Additionally, it is good to secure the network from inside and outside users. Most of the security attacks come from users in the internal network. Implementing network management that gives trouble-shooting and managing of security issues, configuration and performance in the network. [2]

- Adaptation to change: Internetworks must be flexible to change to this dynamic world, since technology is changing all the time. [2]

It is time now to introduce some of the commonly used internetworking devices and their functions in the communication system.

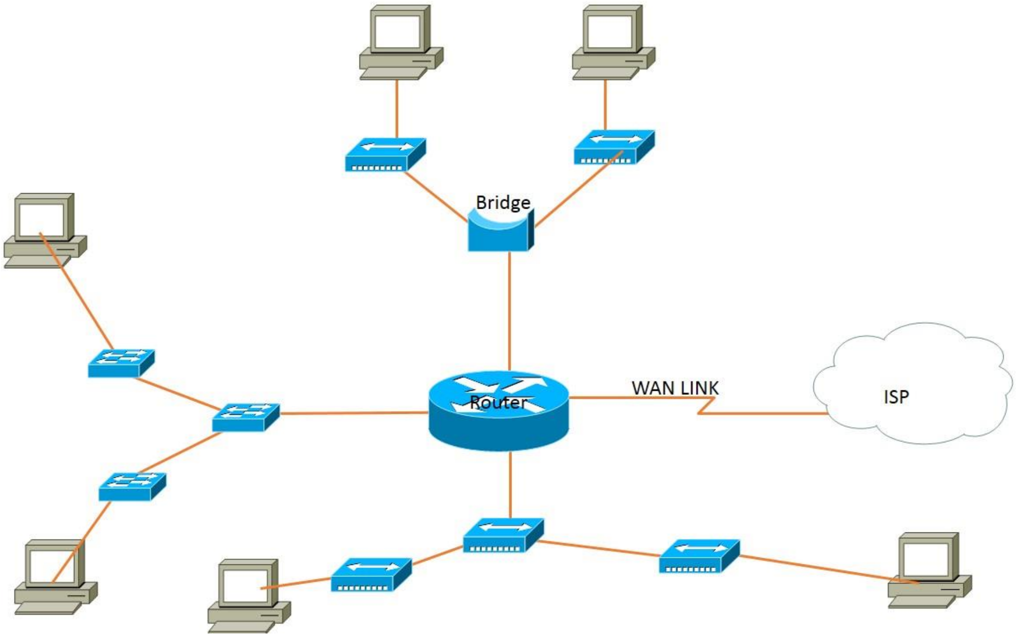


Figure 2. Internetworking Devices

Figure 2 illustrates some of the internetworking devices such as Router, Bridge, Switches and Hubs. Each of the above internetworking devices are discussed below:

- An Ethernet Hub, which is a multiport repeater, is a device connecting many Ethernet devices into a single logical topology network that can send data across the connected perimeter network. An Ethernet hub is primarily kind of a repeater. When a hub transmits data, it will repeat the signal to all ports and this will create a problem when another port sends traffic at the same time. This broadcast message will be send to all interfaces results as a collision effect. A hub is one collision domain. A collision domain as the name indicates it is a collision of signals in a network segment. [6]

- A switch is a layer 2 device which uses Application Specific Integrated Circuits (ASICs) to form and update Media Access Control (MAC) table. Switches and bridges, which are layer 2 devices, are fast compared to routers, because they do not spend time looking at the IP layer header information. Rather they look at the frame header to forward, flood or drop the frame. When a data frame is sent to the interface, the switch will track the connected devices' MAC address and saves the MAC addresses to its Content Addressable Memory (CAM) table. Switches filter data frames based on layer 2 information which is MAC address. [6]
- A router is an internetworking device which connects multiple logical networks. Router interfaces are separate broadcast domains and collision domains. They do not forward broadcast traffic to the other network segment and they forward IP packets based on the destination IP address, provided that some of routers' functions in an internetwork are packet selection, packet switching, connecting internetworks and choosing best path for the routing. [6]

Discussion about layers and function of different protocols of the OSI (Open Systems Interconnection) model will be discussed latter in this chapter. Internetworking has many advantages in a communication networks. Some of the benefits the benefits of the OSI layers are described as follows:

- Minimizing traffic congestion: Implementing internetworking decreases broadcast or multicast domain, that is most of the traffic destined to LAN will be forwarded in the LAN area and those who are destined across the WAN area will cross the internetworking. [5]
- Disparate geolocation: Connecting different sites with WAN links.

Let us look at an example that shows how an internetwork communication is carried out. For this lab setup, the devices implemented are two routers, two switches and two computers. The idea of this example is to show that how broadcast services work in an internetwork in a simple example. Furthermore, WireShark is implemented on the links to track how the packets or frames travel in the network.

Table 1. Device IP Addressing Interface Summary

Device	Interface	IP Address	Subnet Mask	Default Gateway	Switch Port
R1	fa0/0	10.0.0.1	255.255.255.0	N/A	N/A
	e3/0	192.168.1.1	255.255.255.0	N/A	SW1 fa0/1
R2	fa0/0	10.0.0.2	255.255.255.0	N/A	N/A
	e3/0	192.168.2.1	255.255.255.0	N/A	SW2 fa0/1
SW1	N/A	N/A	N/A	N/A	N/A
SW2	N/A	N/A	N/A	N/A	N/A
PC1	e0	192.168.1.10	255.255.255.0	192.168.1.1	SW1 fa0/2
PC2	e0	192.168.2.20	255.255.255.0	192.168.2.1	SW2 fa0/2

Table 1 illustrates the IP addressing scheme for the network topology shown in figure 3 below. After providing the necessary network information topology and implementing a basic configuration setup, such as IP addressing and routing information of the network devices, moreover a static default route is configured between R1 and R2 to advertise their local subnets to each other. The computers that are shown in figure 3 below are configured their IP address and the default gateways according to the table 1 shown above. Switches in this topology are just for extending the connection to the local area networks. There is no need to configure the switches in this scheme. The topology for the scheme looks like the screen shot below in figure 3.

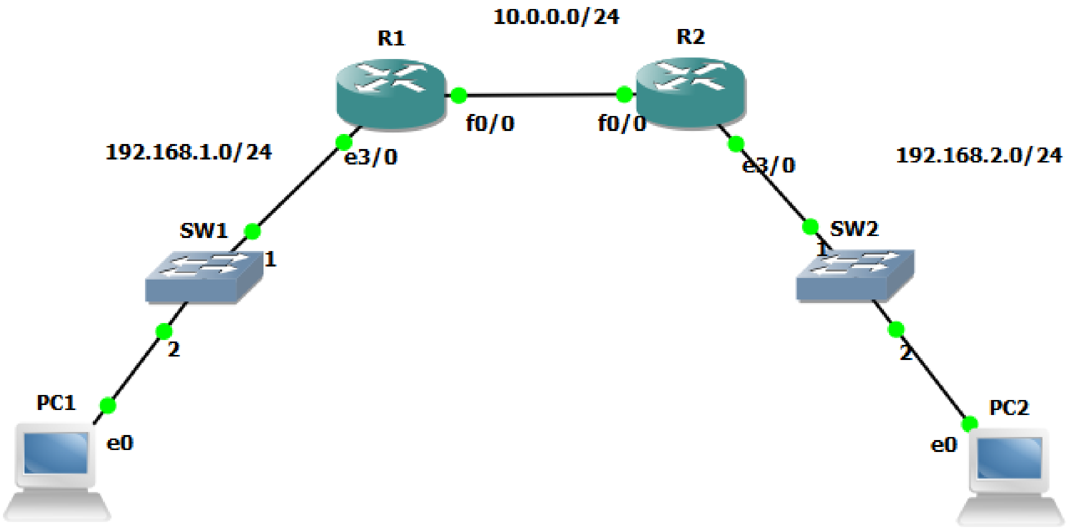


Figure 3. Network Topology for Broadcast Device Discovery.

Figure 3 illustrates the network topology of the routers, switches and computers to their respective interfaces. In the topology the network addresses are show with a 24-bit mask which is 255.255.255.0.

The running configuration can be shown with a command `show run` in the privileged exec mode shown in listing 1 and 2 below. In the `show run` command output of the running configurations lists configured parts are shown below.

```
R1# show run
!
interface FastEthernet0/0
 ip address 10.0.0.1 255.255.255.0
no shutdown
 duplex full
!
interface Ethernet3/0
 ip address 192.168.1.1 255.255.255.0
no shutdown
 duplex full
!
ip route 0.0.0.0 0.0.0.0 10.0.0.2
!
ip route 192.168.1.0 255.255.255.0 10.0.0.2
```

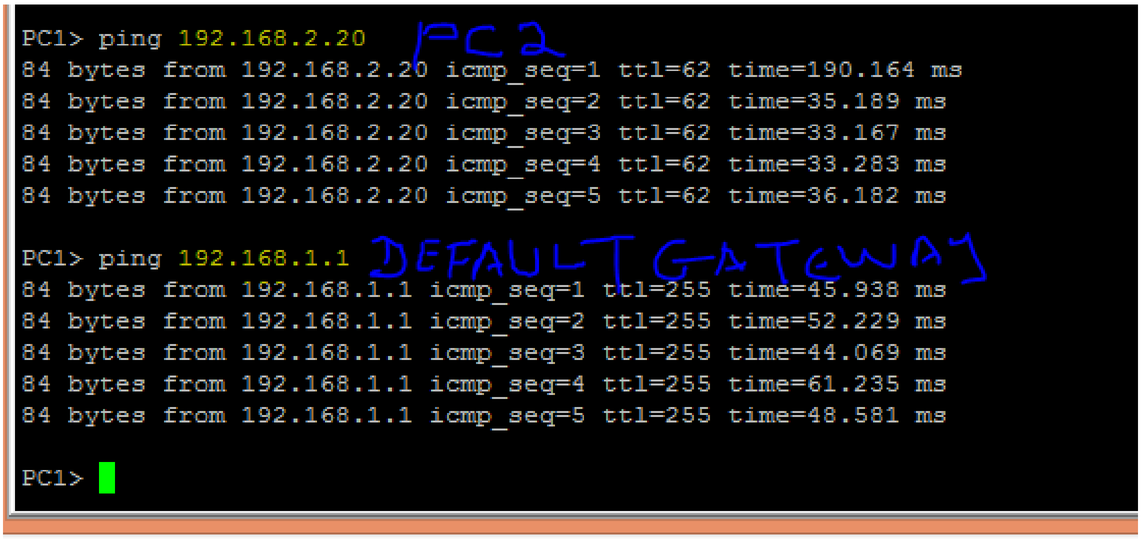
Listing 1. Router (R1) Configuration

Listing 1 illustrates the running configuration of router R1.

```
R2# show run
!
interface FastEthernet0/0
 ip address 10.0.0.2 255.255.255.0
no shutdown
 duplex full
!
interface Ethernet3/0
 ip address 192.168.2.1 255.255.255.0
no shutdown
 duplex full
!
ip route 0.0.0.0 0.0.0.0 10.0.0.1
ip route 192.168.2.0 255.255.255.0 10.0.0.1
!
```

Listing 2. Router (R2) Configuration

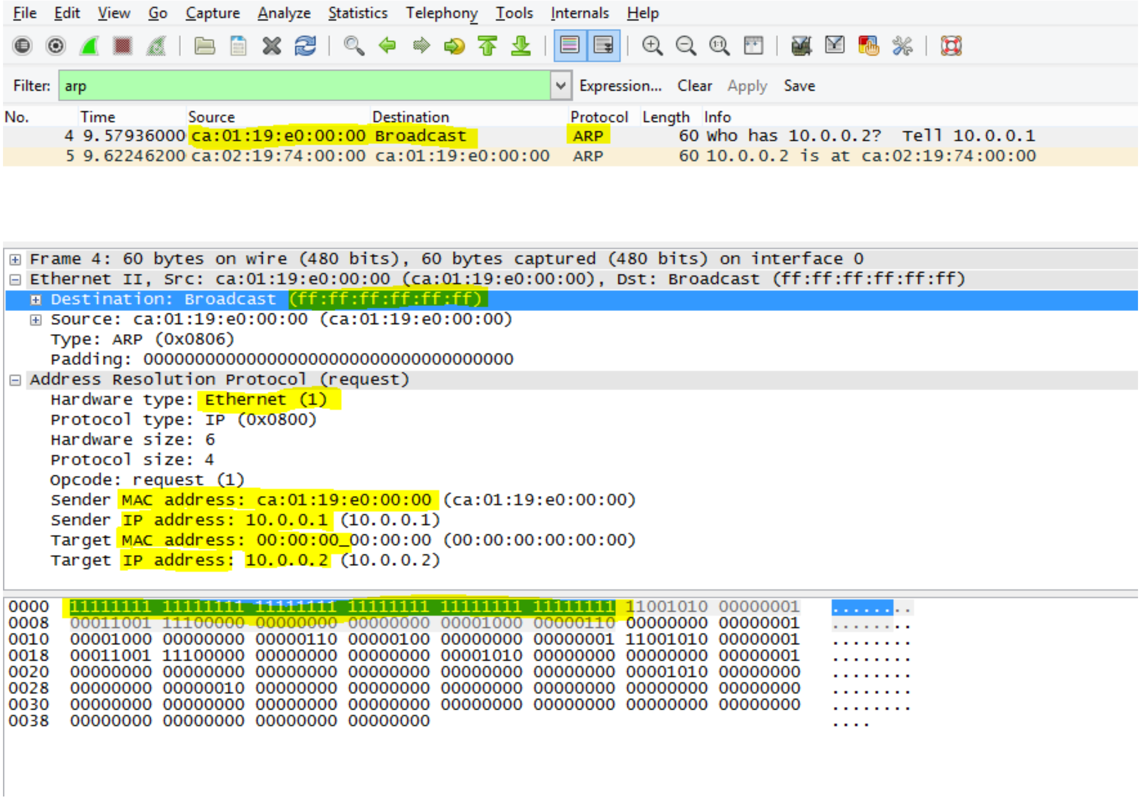
Listing 2 illustrates the running configuration of router R2.



```
PC1> ping 192.168.2.20
84 bytes from 192.168.2.20 icmp_seq=1 ttl=62 time=190.164 ms
84 bytes from 192.168.2.20 icmp_seq=2 ttl=62 time=35.189 ms
84 bytes from 192.168.2.20 icmp_seq=3 ttl=62 time=33.167 ms
84 bytes from 192.168.2.20 icmp_seq=4 ttl=62 time=33.283 ms
84 bytes from 192.168.2.20 icmp_seq=5 ttl=62 time=36.182 ms

PC1> ping 192.168.1.1
84 bytes from 192.168.1.1 icmp_seq=1 ttl=255 time=45.938 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=255 time=52.229 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=255 time=44.069 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=255 time=61.235 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=255 time=48.581 ms

PC1>
```

Figure 4. Ping Result from PC1 to PC2 and Default Gateway.

Figure 4 shows a successful ping from PC1 to the default gateway, which basically means that the PC1 knows how to get out to another network. A default gateway is a node or a router which connects to another network in an internetworking environment. In addition to that, PC1 pings successfully to another computer PC2 in a remote network which shows that there is end-to-end connectivity.



Filter: arp

```
No.    Time         Source              Destination         Protocol  Length  Info
     4 9.57936000   ca:01:19:e0:00:00   Broadcast           ARP           60  Who has 10.0.0.2?  Tell 10.0.0.1
     5 9.62246200   ca:02:19:74:00:00   ca:01:19:e0:00:00   ARP           60  10.0.0.2 is at ca:02:19:74:00:00
```

```
⊞ Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊟ Ethernet II, Src: ca:01:19:e0:00:00 (ca:01:19:e0:00:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Source: ca:01:19:e0:00:00 (ca:01:19:e0:00:00)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: ca:01:19:e0:00:00 (ca:01:19:e0:00:00)
    Sender IP address: 10.0.0.1 (10.0.0.1)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 10.0.0.2 (10.0.0.2)
```

```
0000  11111111 11111111 11111111 11111111 11111111 11111111 11001010 00000001   ........
0008  00011001 11100000 00000000 00000000 00001000 00000110 00000000 00000001   ........
0010  00001000 00000000 00000110 00000100 00000000 00000001 11001010 00000001   ........
0018  00011001 11100000 00000000 00000000 00001010 00000000 00000000 00000001   ........
0020  00000000 00000000 00000000 00000000 00000000 00000000 00001010 00000000   ........
0028  00000000 00000010 00000000 00000000 00000000 00000000 00000000 00000000   ........
0030  00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000   ........
0038  00000000 00000000 00000000 00000000                                       ....
```

Figure 5. Packet Analysis between R1 and R2 Using WireShark.

Figure 5 illustrates the inspection of the packet traffic in the cable between R1 and R2 using WireShark. WireShark is an open-source packet filtering tool which is a great tool for packet filtering. An Internet Control Message Protocol (ICMP) is initiated from R1 to R2 and at the same time the WireShark is configured to capture traffic on the link that connects R1 to R2. From the WireShark analysis only the Address Resolution Protocol (ARP) message has been filter among the list of the WireShark captured, so that to identify how the ARP message is sent from R1 to R2. From the WireShark captured result, the first ARP request is send as a broadcast destination which is ffff.ffff.ffff in the hexadecimal format.

Internetworking Models

At the beginning of internetworking, computer communication was restricted in a way that they communicated with computers of similar vendors. For instance, some companies used DEC net products, IBM products but not both because those products had different standards and were not compatible. To define a common framework for internetworking communication, the International Organization for Standardization (ISO) developed a model called Open Systems Interconnection (OSI) reference model and the Defence Advanced Research Projects Agency (DARPA) designed TCP/IP (Transmission Control Protocol/Internet Protocol) model. [5]

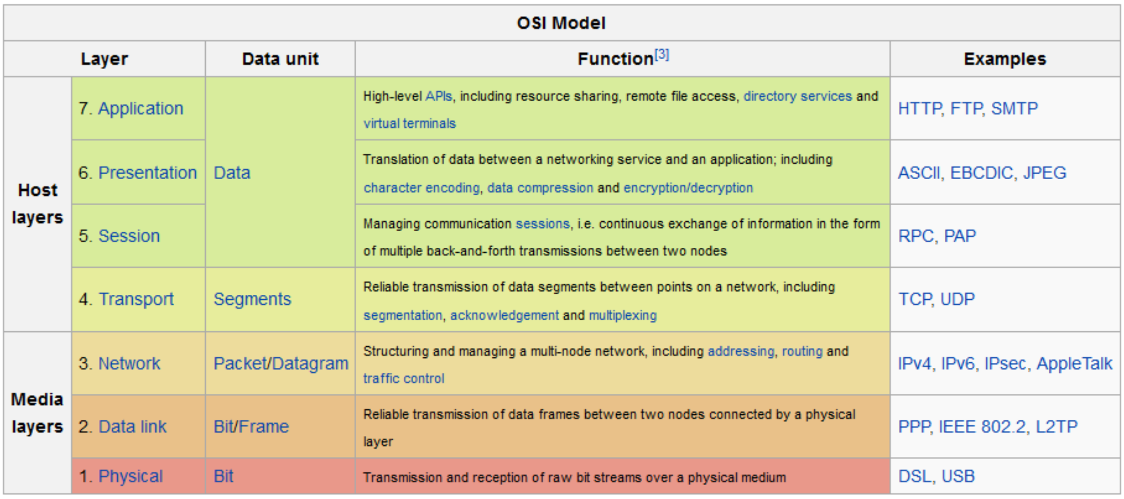
OSI Reference Model

The OSI reference model is a standardized architecture defining network communications. It allows cross-platform communication for different vendors like Apple, Dell, or IBM to communicate with each other. The OSI model is a logical or conceptual model that breaks down a communication system into seven abstraction layers. [5]

Basically, an OSI reference model is a hierarchical model that comprises seven abstraction layers. Its specific protocols from top to bottom layers are application, presentation, session, transport, network, data-link, and physical layers respectively as shown in figure 6 below. Each layer has its own unique functions and protocols. [5]

There are many benefits of OSI model architecture. To mention some of the advantages of the OSI reference models are described below: [5]

- It breaks down network communication into smaller chunks that accelerate designing, developing and troubleshooting components.
- It cooperates inter-vendor development by implementing the common standardized component architecture.
- It ensures interoperable technology for different vendors.
- It reduces complications.



OSI Model

Layer		Data unit	Function[3]	Examples
Host layers	7. Application	Data	High-level APIs, including resource sharing, remote file access, directory services and virtual terminals	HTTP, FTP, SMTP
	6. Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption	ASCII, EBCDIC, JPEG
	5. Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes	RPC, PAP
	4. Transport	Segments	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing	TCP, UDP
Media layers	3. Network	Packet/Datagram	Structuring and managing a multi-node network, including addressing, routing and traffic control	IPv4, IPv6, IPsec, AppleTalk
	2. Data link	Bit/Frame	Reliable transmission of data frames between two nodes connected by a physical layer	PPP, IEEE 802.2, L2TP
	1. Physical	Bit	Transmission and reception of raw bit streams over a physical medium	DSL, USB

Figure 6. OSI Layers. Reprinted from OSI Model (2014) [7].

Figure 6 shows a list of OSI model layers, data unit, functions of the layers and some of the corresponding protocols. For example, in layer 7 which is the application layer the unit in this layer is data unit. The functions are high level Application Programming Interfaces (APIs) and protocols such as Hypertext Transfer Protocol (HTTP), Hypertext Transfer Protocol Secure (HTTPS) and File Transfer Protocol (FTP). Let us discuss each layers of the OSI model:

1. Application Layer: This layer is the layer 7 of the OSI reference model and also it is the nearest layer to the user sitting on the computer host that is trying to browse or use some resources over the network like the servers, email, videos, or voice. This means that users can make communication directly to the OSI application layer through an API. When validating the communication node or host, the application layer identifies and determine whether the intended peer communication partner is available or not prior to data transfer. Some of the examples this layer is using includes Telnet, File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP). [2]
2. Presentation Layer: The presentation layer engages in translation and formatting services. This layer helps communication which is sent from one application layer and can be understood on other end application layer. Some of the functionalities of this layer are data compression, decompression, and encryption and decryption services.[2]

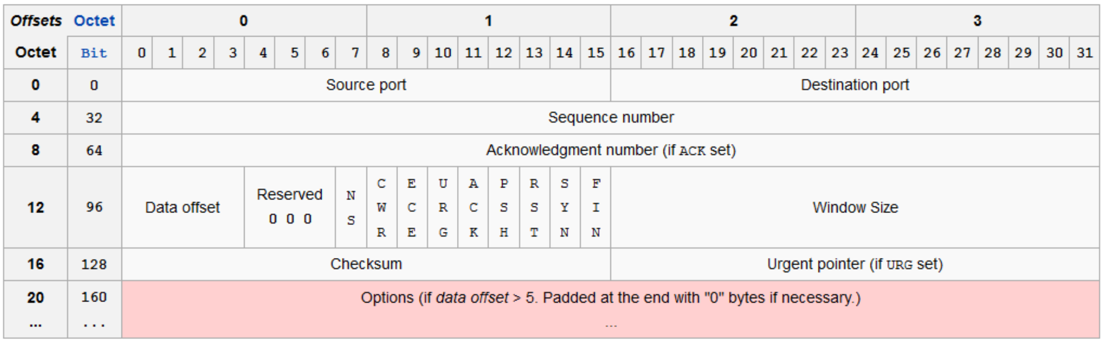
3. Session Layer: This layer provides session management. It sets up and tear down connections to other users.
4. Transport Layer: This layer gives service to host-to-host communication by assuring the communication channel to be either reliable or unreliable communication. The two main protocols used in this layer are TCP (for reliable communication) and UDP (for unreliable communication).It also implements flow control and multiplexing data control mechanisms.[5]
5. Network Layer: This layer is layer 3 of the protocol stack of the OSI model and is serving as device addressing. IP is the protocol used for device addressing. This layer is used to connect different networks in an internetwork by implementing a router device for routing and updating purposes. [5]
6. Data Link Layer: This layer engages in physical data transmission and some of this layer's services are flow control, error alerting, and topology scheme.[5]
7. Physical Layer: This layer is the first layer of the OSI model and is located at the bottom layer of the stack list and its function is to send bits and receiving bits. [6]

Transmission Control Protocol (TCP) / Internet Protocol (IP) Model

TCP/IP model is a condensed model of the OSI reference model. TCP/IP model shrinks the application, session, and presentation layer into the process layer. TCP/IP layer has four layers: [5]

- Application
- Transport
- Internet
- Network Access

Transmission Control Protocol (TCP), which is a reliable data communication, receives a chunk of data information from an application layer of the OSI reference model and divides that into smaller chunks of data segments. It adds a sequence number to each data segment so that the destination TCP peer application can build up the data segments back to the original full data. After the data segments are sent from the sender host, the TCP expects an acknowledgment from the recipient peer host, and retransmits the data in case if any data segment is missing or not acknowledged. First the TCP stack forms a connection which is called virtual circuit. During the initial TCP 3-way handshake, the two TCP peer stack layers must agree on the size of the data information that they are going to exchange before the recipient sends an acknowledgement back. The User Datagram Protocol (UDP) is preferred for unreliable data communication such as real-time video and VoIP. [3]



<table>
<tr><th><em>Offsets</em></th><th>Octet</th><th colspan="8">0</th><th colspan="8">1</th><th colspan="8">2</th><th colspan="8">3</th></tr>
<tr><th>Octet</th><th>Bit</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><th>0</th><td>0</td><td colspan="16">Source port</td><td colspan="16">Destination port</td></tr>
<tr><th>4</th><td>32</td><td colspan="32">Sequence number</td></tr>
<tr><th>8</th><td>64</td><td colspan="32">Acknowledgment number (if ACK set)</td></tr>
<tr><th>12</th><td>96</td><td colspan="4">Data offset</td><td colspan="3">Reserved
0 0 0</td><td>N
S</td><td>C
W
R</td><td>E
C
E</td><td>U
R
G</td><td>A
C
K</td><td>P
S
H</td><td>R
S
T</td><td>S
Y
N</td><td>F
I
N</td><td colspan="16">Window Size</td></tr>
<tr><th>16</th><td>128</td><td colspan="16">Checksum</td><td colspan="16">Urgent pointer (if URG set)</td></tr>
<tr><th>20
...</th><td>160
...</td><td colspan="32">Options (if <em>data offset</em> > 5. Padded at the end with "0" bytes if necessary.)
...</td></tr>
</table>

Figure 7. Transmission Control Protocol Header. Reprinted from Transmission Control Protocol (2014) [21].

Figure 7 illustrates the TCP header elements such as segment header, data, source port, destination port, sequence number, acknowledgment, flags, and data offset.

2.2 Internetwork Addressing

Internetwork addressing is the addressing of network devices individually or as a group. The network device addressing scheme varies with the layers they reside as well as the protocols they use. There are three categories of addressing network devices: network layer address, mac address and data link layer address. [2]

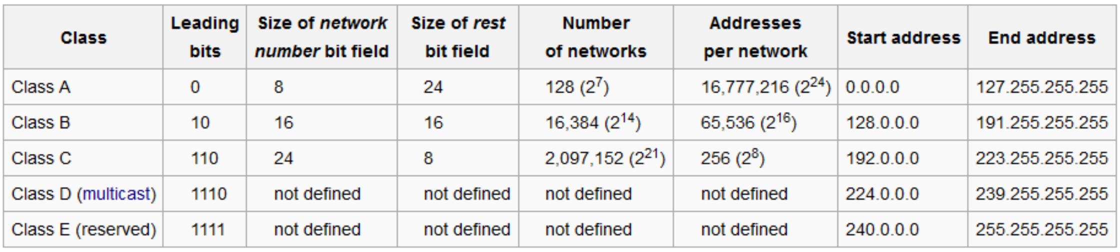
Data Link Layer Addresses

A data link layer addresses is layer 2 in the OSI reference model. It can uniquely identify the physical network connection in an internetwork devices. This address is assigned to the devices by the manufacturer to the specific devices. [2]

The data link layer has two sublayers, the MAC address sub layer and Logical Link Layer (LLC). The MAC address are assigned by the vendor and they are 48 bits long. [2]

Network Layer Addresses

The network addresses located at the layer 3 of the OSI model and the relationship to the devices is virtual or logical addresses unlike MAC addresses which are fixed to the devices. In network layers addressing the most common protocols are IPv4 and IPv6 protocols. An IP address is a software address that is designed to identify numerical addresses assigned to each device in an IP network. It allows different devices on an internetwork to communicate regardless of the LANs the nodes reside in. [2]



Class	Leading bits	Size of *network number* bit field	Size of *rest* bit field	Number of networks	Addresses per network	Start address	End address
Class A	0	8	24	128 (2^{7})	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^{8})	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

Figure 8. Classes of Network Address. Reprinted from Classful Network (2014) [22].

Figure 8 illustrates that classes of network addressing used to address hosts.

The IP address expression 10.0.0.0/24 is used in this project for describing the IP address ranges. It actually means that the IP address starts with 10.0.0.0 and the rightmost 8 bits will vary. The 8 is calculated by using 32 bit. So 10.0.0.0/24 means it covers the address range from 10.0.0.0 to 10.0.0.255. The Request for Comments (RFC) 1918 of private IP network addresses are implemented for the internal networks. Those IP address are not routed over the Internet but they reside in the local network. The private network rages are: [24]

- 10.0.0.0-10.255.255.255 (or 10.0.0.0/8)
- 172.16.0.0-172.31.255.255 (or 172.16.0.0/12)
- 192.168.0.0-192.168.255.255 (or 192.168.0.0/16)

2.3 Local Area Network (LAN)

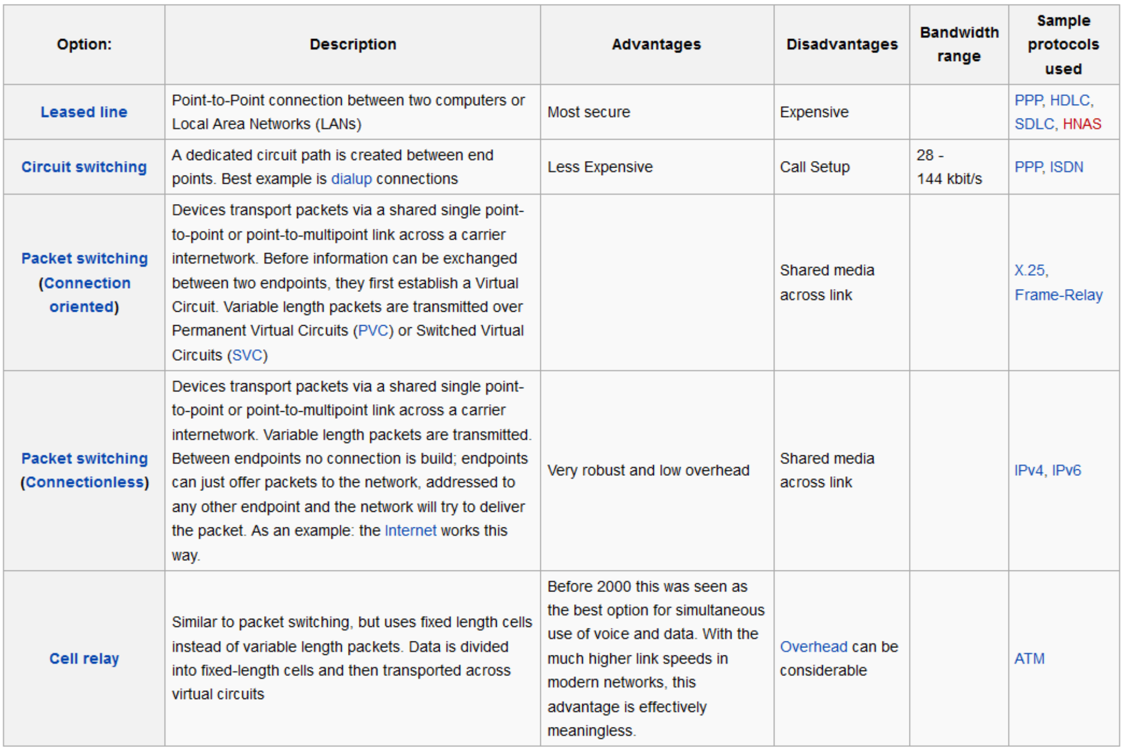
A LAN is a group of computer networks confined to a limited geographic area such as home, school building, office building or organizations. It typically connects devices like personal computers, shared printers, and servers. It can be connected to a locally cabled or wireless connection. A LAN is usually a high-speed data communication network. The LAN protocols resides at the data link layer and physical layers of the OSI model. A data link layer formats the Protocol Data Unit (PDU) message into a frame, and adds headers and trailers into the frame. A physical layer sends and receives bits. [6]

Basically, for a communication in a LAN there is a standard protocol called the Institute of Electrical and Electronics Engineers (IEEE) 802 family standard. For example, 802.3 is Ethernet, 802.2 Logical Link Control (LLC) or 802.11 wireless LAN or WI-FI. The IEEE 802 standard has two sublayers, LLC and MAC. The MAC is a physical hardware addressing. The Logical Link Control (LLC) is used for identifying network layer protocols and for encapsulation. [5]

The LAN data transmission mechanism has three categories: unicast, broadcast, and multicast. When a single packet is transferred from a source to a single destination device it is a unicast transmission, one packet to one. Multicast transmission is sending information to a group of destination nodes, one packet to groups. Broadcast transmission is sending information to all destination nodes, one packet to all. [2]

2.4 Wide Area Network (WAN)

A WAN is a network that encompasses a large geographical area and is used to connect multiple networks or LANs for communication. A WAN link defines a new type of the bottom three layers of the OSI model connectivity: the physical layer, the data link layer, and the network layer. It allows links to the internet or other offices. Figure 9 simplifies some WAN connectivity technology such as leased lines, circuit switching, packet switching and cell relay. [5]



Option:	Description	Advantages	Disadvantages	Bandwidth range	Sample protocols used
Leased line	Point-to-Point connection between two computers or Local Area Networks (LANs)	Most secure	Expensive		PPP, HDLC, SDLC, HNAS
Circuit switching	A dedicated circuit path is created between end points. Best example is dialup connections	Less Expensive	Call Setup	28 - 144 kbit/s	PPP, ISDN
Packet switching (Connection oriented)	Devices transport packets via a shared single point-to-point or point-to-multipoint link across a carrier internetwork. Before information can be exchanged between two endpoints, they first establish a Virtual Circuit. Variable length packets are transmitted over Permanent Virtual Circuits (PVC) or Switched Virtual Circuits (SVC)		Shared media across link		X.25, Frame-Relay
Packet switching (Connectionless)	Devices transport packets via a shared single point-to-point or point-to-multipoint link across a carrier internetwork. Variable length packets are transmitted. Between endpoints no connection is build; endpoints can just offer packets to the network, addressed to any other endpoint and the network will try to deliver the packet. As an example: the Internet works this way.	Very robust and low overhead	Shared media across link		IPv4, IPv6
Cell relay	Similar to packet switching, but uses fixed length cells instead of variable length packets. Data is divided into fixed-length cells and then transported across virtual circuits	Before 2000 this was seen as the best option for simultaneous use of voice and data. With the much higher link speeds in modern networks, this advantage is effectively meaningless.	Overhead can be considerable		ATM

Figure 9. WAN Technology Connectivity Options. Reprinted from Wide Area Network (2007) [10].

Figure 9 illustrates different WAN options and protocols used in WAN technology.

A Virtual Private Network (VPN) which is a major topic of this thesis is a type of WAN technology. It connects different company or sites which are located at different geo-location and makes it like, the connected company or sites, as if they are connected locally.

2.5 Firewalls

A firewall is a device, hardware or software or both, that is designed to prevent an unauthorized outside user from accessing a network or host. It is a network security that prevents inside users from sending sensitive information or accessing an unsecured network. It protects hosts by implementing boundaries or restricting IP network connectivity. [4]

A firewall needs a proper set of rules or proper security policy to prevent inside host or subnet vulnerability. To connect to the unsecure network a firewall implements a set of security policy and use proxy address. Firewalls can implement Network Address Translation (NAT), Port Address (PAT) or Virtual Private Network (VPN).

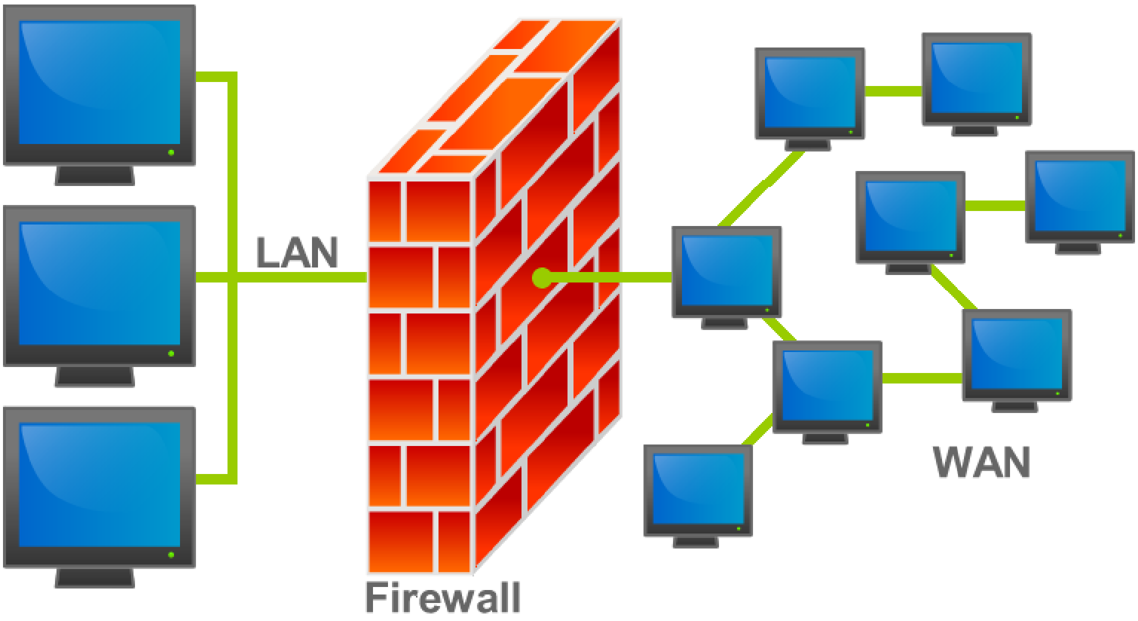


Figure 10. Firewall Location in the Network. Reprinted from Firewall (2007) [11]

Figure 10 illustrates the position of a common firewall in an internetwork.

This project uses firewall or gateway appliances from two different vendors. Those are Cisco ASA 5505 and Juniper SRX240, they are connected and implemented using a VPN scenario to securely communicate over the public network.

3 Virtual Private Networks (VPNs)

3.1 Overview of VPNs

Virtual Private Network (VPN) is a generic term that is used to establish secure communication channel over public network infrastructure that is Internet or service provider network. The Internet domain network is sometimes known as the VPN backbone. It is important for transferring multiple data traffic over the public network for VPNs oriented communication or for non-VPN oriented communication. [13]

VPN could refer to the network connectivity between two remote sites. If the VPN acronym is break down into its' individual letters, the letter V in a VPN stands for virtual and it refers to a logical connection between the two network devices. The letter P stands for private and it refer that the logical network that is created between two devices is private. The letter N is for network, of course a VPN is a WAN link network. For example, one user may be connected to the public network in corporate site 1 and another user may be connected to the public network in corporate site 2, a logical network or virtual network could be built between the two sites using the Internet as a transport medium. The word private refers to the communication between the two sites which is private. [13]

However, if we had a VPN established between remote sites over the public network that is the Internet, what would prevent the data from an eavesdropper who is sniffing on the communication wire? To protect the data from malicious manipulation the VPN ingredients of confidentiality, authentication, data integrity and anti-replay comes to play. The eavesdropper cannot exploit the data since it is encrypted and he/she does not have the right key to exploit the data content. [13]

3.2 VPN Devices and Technologies

VPN Devices

In a corporate network or organization infrastructure a VPN terminator device erects in different area of the infrastructure network. The VPN devices that are erected in the customer and service provider can be clarified as follows. [8]

- Customer (C) devices: Those devices belong to the customer network and they are not connected to the service provider infrastructure. Some of the C devices are routers and switches that reside within the customer network. The customer devices do not have any clue about the VPN network.

- Customer Edge (CE) devices: The CE devices are connected through the service provider network and they are located, as the name indicates, within the customer edge network. In a CE- based network the devices know about the VPN network, but in the Provider Edge (PE)-based network they do not know whether there is a VPN at all. Some examples of the CE devices that reside in this network are Customer Edge routers and Customer Edge switches.
- Service Provider (P) devices: The P devices are not connected directly to customer networks. The P devices do not know whether there is a VPN at all. Some examples of the P devices are routers and switches with in the perimeter of the provider network.
- Service Provider Edge (PE) devices: The PE devices are directly connected to the customer C network through the customer CE devices. Additionally, in the PE-based network VPNs the PE devices know about the VPN network. But in the CE-based VPNs the PE devices are not aware if there is a VPN network at all. Some examples of the devices are Provider Edge router, Provider Edge switch, and Provider Edge devices that have ability to route and switch.
- Network Access Servers (NAS) devices: NAS devices are points of access for components between modem devices network such as Public Switched Telephone Network (PSTN) and a packet switched network. A NAS device can act as a tunnel end in a remote access VPN.
- VPN gateways: A VPN concentrator is used as a VPN tunnel end in CE- based site-to-site VPN.

There are many different kinds of commercially implemented VPNs. A VPN can be categorized into two primary broad categories: site-to-site and remote-access VPNs.

VPN Technologies

The VPN technologies implemented for connecting two peers over an unsecure network form a logical network connection. These logical network connections could be established at layer 2 or layer 3 of the OSI reference model. The VPN technologies formed could differ from layer to layer. For the layer 2 of the OSI model layer 2 VPNs are formed and for the layer 3 of the OSI model layer 3 VPNs are formed. A VPN connection made between sites using either Layer 2 VPNs or Layer 3 VPNs ideally they are similar. The idea includes adding a header information to the front of the data segment content. [20]

Layer 2 VPNs

Layer 2 VPNs as the name indicates work at the layer 2 of the OSI reference model. They are point-to-point WAN links and perform connectivity between sites over a logical connection called a virtual circuit. A virtual circuit is a logical connection between two points in an internetwork from end to end, and can cover a large area of elements and multiple physical segments of a network. The two most common Layer 2 VPN technologies are Asynchronous Transfer Mode (ATM) and Frame Relay. ATM and Frame Relay network connection providers can give best site-to-site connectivity to a company by configuring a permanent virtual circuit (PVC) across a shared network infrastructure. They also offer great Quality of Service (QoS) characteristics, especially for delay-sensitive services such as voice. [20]

Layer 3 VPNs

Communication between two peers is said to be Layer 3 VPN if the header information is for the layer 3 of the OSI reference model. Layer 3 VPNs could be either a point-to-point WAN link connection to connect two sites such as GRE and IPsec, or could perform connection any-to-any connectivity to multiple sites such as MPLS VPNs. [20]

IPsec VPNs is a major concern that should be dealt with if the VPN technology is implemented to throughput a secure data communication between VPN peers. In this project IPsec VPN of the Layer 3 VPNs technology is implemented to connect two disparate sites and communicate securely over the public Internet. [20]

3.3 Remote-access VPN

A remote-access VPN provides access, resources or services, to a telecommuter or a remote user who is securely connected to the remote site or corporate network. They provide that functionality by running client software on the users or telecommuters to create secure communication to the corporate VPN concentrator. Users or telecommuters access the services or resources as if they were in the LAN of the corporate network. [9]

In the early days, company users that need to have remote connectivity to access the company service were implementing dial-in networks and ISDN or Public Switched Telephone Network (PSTN) which is expensive. But by implementing a Virtual Private Network to dial-up to ISP is cost-effective. [9]

Remote-access VPNs can be either IPsec VPNs or SSL VPNs. A remote-access VPN provides transparent functionality to the end-user or telecommuter who is remotely accessing the corporate services or resources. A remote-access VPN could be a clientless VPN or client-based VPN. A Clientless VPN uses a web browsers based VPN to securely create a remote-access tunnel. The client-based VPN implements client software which needs to be installed in the host Operating System (OS) to create a remote-access tunnel. [9]

Large business organizations with multiple IT departments may setup and deploy their own remote-access VPN to give service to their resources. The remote-access VPNs are beneficial for the telecommuters. But for organization with thousands of employees and with many branch offices, implementing a remote-access VPN is not a wise decision. However, in such organizations' situation site-to-site VPNs are effective alternative solution.

3.4 Site-to-site VPN

A site-to-site VPN is a VPN implementation where companies may have two or more sites that need to securely connect and communicate with each other. Site-to-site VPNs are primarily deployed to secure data between two remote sites in a corporate organization, or between a corporate organization and an individual user who is a telecommuter. Site-to-site VPNs are more common practice on the WAN connection over the public network infrastructure that is the Internet than over the private LANs networks. However, nowadays many corporate organizations are hiding data information between multiple sites of the private LAN networks to protect data communication. A LAN to LAN VPNs also provide a cheaper connectivity cost and high availability over the dedicated leased private links. They can provide network redundancy, if there is a failure in private networks. [9]

4 Benefits of VPN Security

4.1 Overview of Cryptography

Cryptography is a study and process of message secrecy, so that only an intended peer can decipher the ciphered text. In the field of information technology cryptography provides access control and information confidentiality. In this project the basic components of cryptography, such as hashing algorithms, encryption, and management of keys which are used by VPN are discussed. [13]

Ciphers

A cipher is an algorithm with a set of predefined rules to perform an encryption algorithm or a decryption algorithm. Basically there are many methods of encryption algorithms available. [13]

1. Substitution: This method of cipher is used by substituting one character for another. To make it hard to guess the ciphered text, it is possible to shift the text by more than one letter of the character. In the VPN concentrator, if substitution mechanism were implemented, both remote peers must share the key so that they can understand and encrypt as well as decrypt the shared data.
2. Polyalphabetic: This cipher mechanism is using multiple characters to switch between them implementing a trigger character in the ciphered data unlike to substitution using a single character.
3. Transposition: This cipher method implements rearrangement of characters held in the position of plaintext to form cipher text.

Keys

A key is an instruction that directs how to build a crypto device to cipher text in a special way. For example, using a one-time pad (OTP) which is used only once, to cipher text a

32-bit data 32 bit key is needed. Each bit is calculated mathematically with its reciprocate bit from the data to result in encrypted data. [13]

Block and Stream Ciphers

A cipher algorithm can encrypt a message in bits and bytes or on a block of messages at a time, based on the cipher methods. [13]

Block Ciphers

A block cipher algorithm is a symmetric algorithm key, in which the same secret key is used to cipher and decipher the data which operates in a block of bits. It takes a 64-bit block of plain text and produces a 64-bit of cipher text. Some of the examples of symmetrical block ciphers are discussed as follows: [13]

- Blow fish
- Digital Encryption Standard (DES)
- International Data Encryption Algorithm (IDEA)
- Advanced Encryption Standard (AES)
- Triple Digital Encryption Standard (3DES)

A block cipher is easy in software implementation. A block cipher algorithm is strong and a single error damages the whole block of data. [13]

Stream Ciphers

A stream cipher algorithm is a symmetric algorithm key, in which the same secret key is used to cipher and decipher the data. It operates using one bit at a time against the bits of the key stream to encrypt the data. This cipher method is less overhead than the block cipher because of the cipher stream does not need to the same to the block size. Stream ciphers are easier in mathematical analysis. Stream ciphers are not applicable for software implementation and a single error damages only a single bit of data not the whole block of cipher data. [12]

Symmetric and Asymmetric Encryption

An encryption algorithm or a cipher is a mathematical function that is engaged in the encryption and decryption data process. Generally, in the encryption algorithm there are two mathematical functions, one to encrypt data and one to decrypt the data. [13]

Symmetric Encryption Algorithm

Symmetric encryption algorithms are a class of algorithms, in which they perform encryption and decryption process with the same shared secret key. When two network devices are connected through a VPN, both network peers need the same secret key to be shared to successfully communicate using a symmetric key algorithm. Therefore, the sender and receiver should have the exact same shared secrete to establish a communication. It is a traditional way of making cryptography. The average key length of the symmetric encryption algorithm is between 40 to 256 bits. The more the key length is the tougher the algorithm will be. [13]

Nowadays, VPNs use a symmetric encryption algorithm to protect the data. The reason to implement a symmetric algorithm to protect network traffic is because it is faster to implement and less CPU overhead than with the asymmetric encryption algorithm. [12]

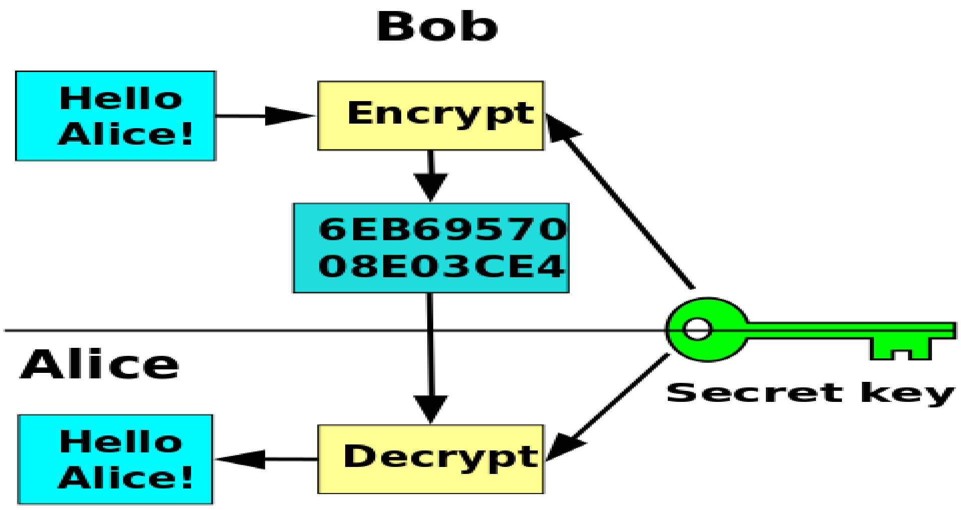


Figure 11. Symmetric-key cryptography scheme. Reprinted from Symmetric Key Encryption (2014) [17].

Figure 11 illustrates a simple example of how the symmetric encryption algorithm takes place. Alice and Bob share the same secret key so that Alice can decrypt Bob's encrypted message. Common examples of the symmetric encryption algorithms are described as follows: [13]

- DES
- 3DES
- AES
- IDEA
- Blowfish
- The RC series

Asymmetric Encryption Algorithm

Asymmetric encryption algorithms or public-key algorithms are a class of algorithms that involves two different key which function as mathematically together as a key pair: one is secret (or private) and one is public. Asymmetric algorithms are used sparingly because they consume high a CPU over head when implementing key pairs to encrypt and decrypt huge data. [13]

In a VPN termination asymmetric encryption algorithms are implemented to authenticate a VPN partner or generate a keying material that could be used by the symmetric encryption algorithm.

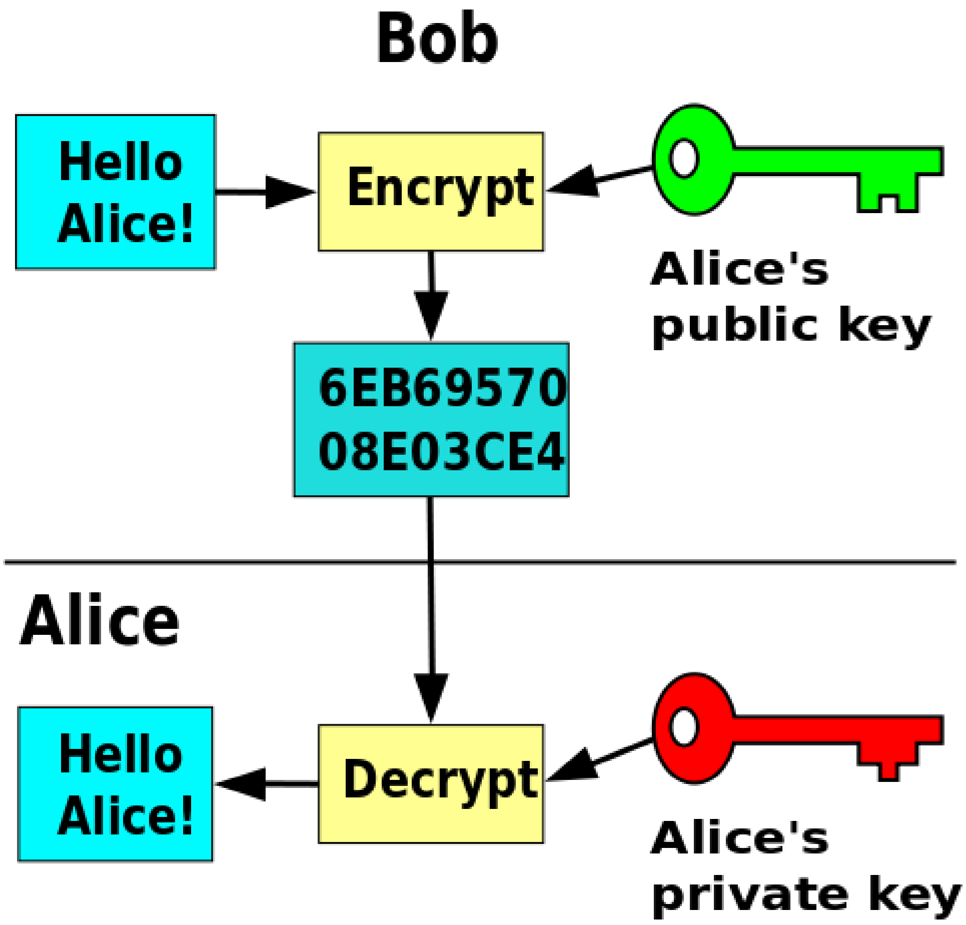


Figure 12. Asymmetric key encryption scheme. Reprinted from Public Key Encryption (2006) [18]

Figure 12 shows that an asymmetric key encryption algorithm implements key pairs, one private key and one public key. The public key is available to anyone who wants to use it publicly but the private key is only stored in the device that have private-public key. Some of the examples of asymmetric algorithms are described as follows: [12]

- Rivest-Shamir-Adleman (RSA)
- Diffie-Hellman
- Digital Signature Algorithm
- ElGamal
- XTR

Diffie-Hellman (DH)

The main aim of the DH , which is a key management algorithm, is making sure that each pair produces the same secret number after the exchange of some value in clear text format. The produced secret key number could then be used as the symmetric key algorithm.

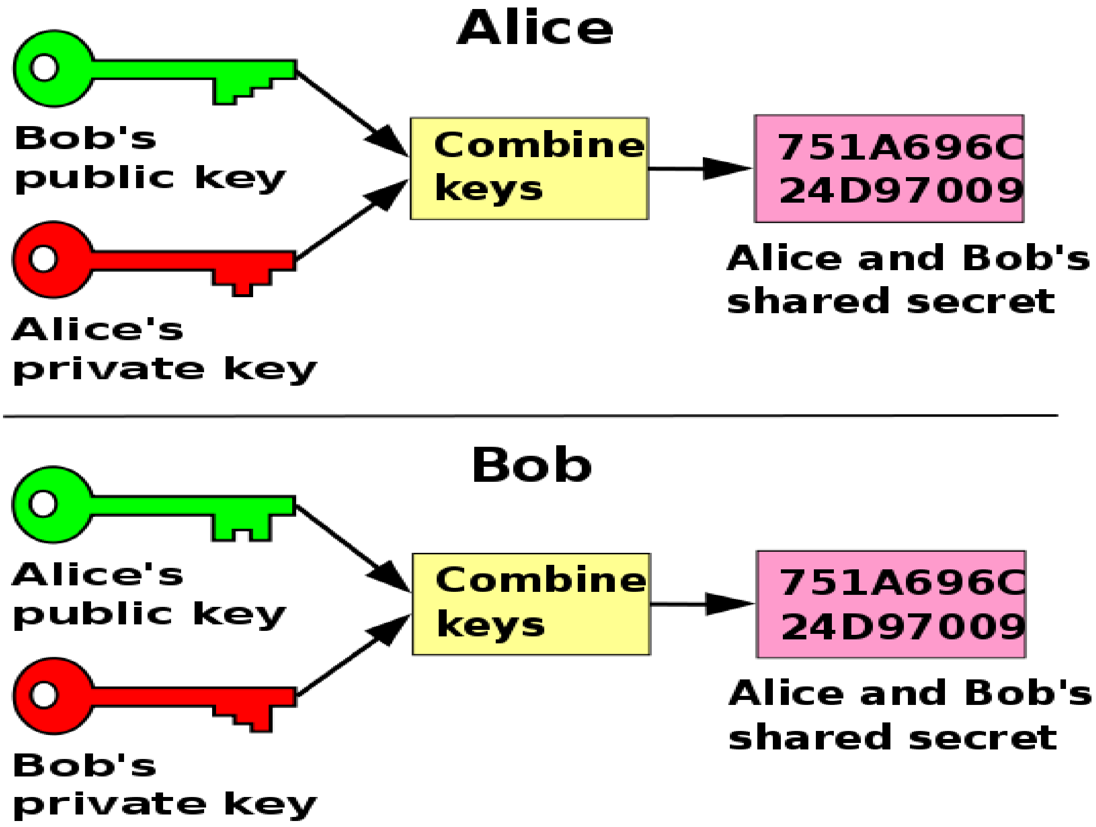


Figure 13. Diffie–Hellman Key Exchange Scheme. Reprinted from Diffie–Hellman (2006) [19]

Figure 13 shows the DH exchange keys in which each peer generates a public-private key and shipped the public key publicly. After receiving an authenticated message of each peer to their public keys, both Alice and Bob can start to compute mathematically the shared secrete key. This shared secrete key can be implanted in a symmetric encryption algorithm.

In VPN concentrators the DH algorithms are frequently used to automate key exchange used in symmetric key algorithm. For example, the Internet Key Exchange (IKE) protocol in the IPsec VPN uses the DH algorithm method to perform a secure and reliable environment for key exchange over unsecure network communication. [13]

Hashes

Hashes are used for making verification of data integrity, which means making sure that the data has not been tapered. The hashing function is a mathematical process that takes a chunk of data and creates a small-size hash value. This method is a one way function, which means that if two computing devices that are capable of running a hashed algorithm take the same data and run the same hash function, the result of the hashed value is the same. If the result is different it means that the data has been modified or misused. Some of the most popular hashing algorithms are described as follows: [13]

- Message Digest 5 (MD5)
- Secure Hash Algorithm 1 (SHA-1)
- Secure Hash Algorithm 2 (SHA-2)

Hashed Message Authentication Code (HMAC)

Hashed Message Authentication Code (HMAC) is similar to hashes but it adds some features which makes it better than a hashing algorithm. HMAC implements the method of hashing and includes in the mathematical formula calculation some additional secrete keys so that only the other peer who knows the secrete key is able to calculate and verify the hashed message.

4.2 Confidentiality

Confidentiality is the protection of information exchange between two peers. It means that only authorized peers or system can access sensitive or classified information. Any message sent over the Internet the actual message packet can be seen by anyone who is eavesdropping the communication but not the content of the packet which is cipher text. It is meaning less to the eavesdropper unless it is decrypted which is impossible if the secret key is known. [12]

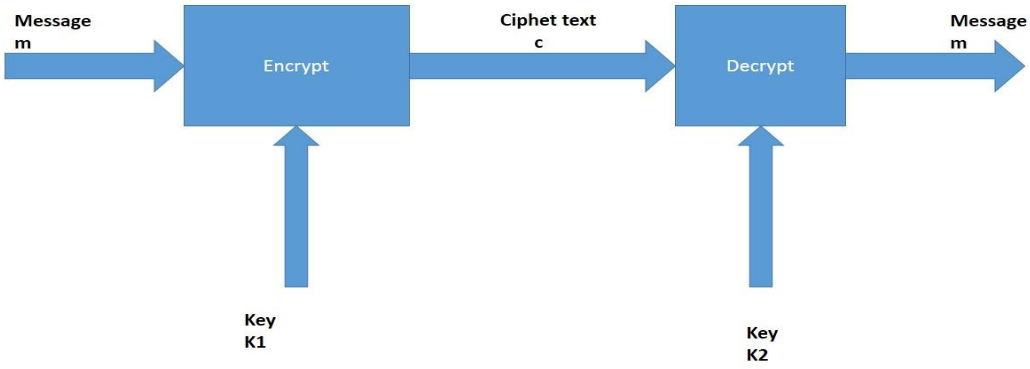


Figure 14. Confidentiality Encryption Process

As figure 14 illustrates, a message m is sent to the encryption box to be encrypted with some key K1 to give the result of encryption to cipher text c. The cipher text is sent to the other peer so that the peer can put it into the decryption box with his own key K2 to get the result message m which is the original message. The eavesdropper could easily get the cipher text but it is impossible to decrypt it unless the eaves have the secret key K1.If K1 is equivalent to K2, then the algorithm is a symmetric encryption algorithm which is a shared secret key. If K1 is not equal to K2, the encryption algorithm is an asymmetric algorithm.

4.3 Data Integrity

A VPN data transmission goes through the public network and anyone eavesdropping the communication can intercept and modify the data. To mitigate this problem, it is important to consider the data integrity algorithm. This encryption algorithm adds a hash to the payload so that to verify the integrity of the original payload. If the transmitted hash matches the received hash, then the data is safe and has not been intercepted. But, if there is no match, then it has been intercepted and modified. Data integrity is verifying the content of the message whether it is misused or tampered during the communication between two peers. Data integrity is making sure that the communication is accurate between both ends. [12]

Let us see an example of how to verify data integrity when one downloads a file from a website or server and saves it on his/her computer. For example, an error can happen while downloading a file or there could be some part of the file lost. To check the integrity of the downloaded file from the server or a website, one can crosscheck the message digest algorithm 5 (MD5) value from the server against the generated value on the local computer. For instance if one run the download file on his/her own Operating System (OS) and the value generated should be the same with the value on the server. This proves that the file is not misused or lost up on the download journey. [12]

The most common data integrity hashing algorithms are described as follows.

- HMAC
- MD-5

4.4 Authentication

Authentication proves that the communication is set up with the correct VPN peer. Some of the authentication types are: [13]

- Username and password
- One-time password
- Biometric
- Preshared keys (PSK)
- Digital certificates

4.5 Anti-reply Protection

Anti-reply protection checks that each packet is unique and is not replayed. A reply attack is a form of network attack in which a valid VPN traffic is maliciously repeated or delayed. For example, an unwanted user might capture a VPN traffic with the intent to maliciously reply the packet and fake one of the VPN peers that he/she is a legitimate peer. To mitigate such problems, VPNs implement anti-rely protection mechanism. [12]

5 Internet Protocol Security (IPsec)

5.1 IP Security Overview

Ensuring that a communication is secure and destined safe and sound when it crosses the public network, which is unsecure, is corporations' and users' aim. These types of features can be made by implementing IPsec VPN technologies. When implementing an IPsec VPN between corporate networks or users to a corporate network, the data transferred over the network is secure in a way that no-one has seen it and no-one altered its content.

IP security is a protocol of suite that is geared around security of data communication. IPsec consists of pieces for authentication, data integrity, confidentiality, and anti-reply attack prevention. IPsec implements data integrity checking to prove that the data was not misused. It also implements an encryption mechanism in such a way that to prove no-one has eavesdropped at the data. When two sites use a VPN connection, IPsec VPN, each site is authenticated to determine whether each side fulfils the security parameters. [25]

5.2 IPsec Framework

IPsec is an Internet Engineering Task Force (IETF) standard that works at layer 3 of the OSI reference model, protecting and authenticating IP packets between VPN peers. It is defined in RFCs 2401 to 2412. IPsec framework is an open standard protocol suit which allows to be defined as the technology advances to newer and better algorithms without reinforcing the existing IPsec standard. IPsec provides data confidentiality, data integrity, data authentication, and anti-replay protection between participating VPN peers at the IP layer. IPsec secures a path between a pair of firewall gateways or between a firewall gateway and a node. The main purpose to implement IPsec in VPN communication peers is to get confidentiality to the transmission. Confidentiality is achieved by encrypting the sensitive payload. [25]

The goal of the IPsec is to provide the following services:

- Confidentiality

- Integrity
- Authentication of the VPN peers
- Anti-replay protection

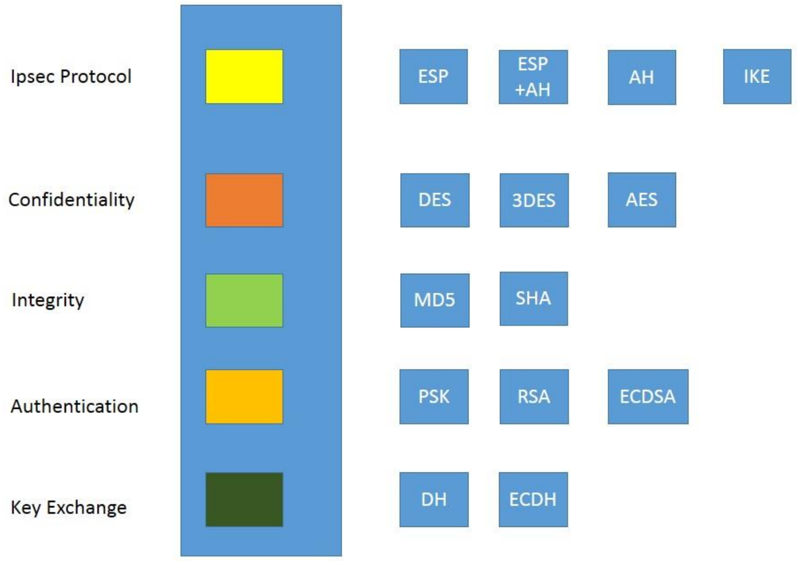


Figure 15. IPsec Framework Components

Figure 15 illustrates the IPsec framework components. When implementing IPsec VPN to firewalls to give security services, the IPsec framework components will be a guideline for selecting components that suite the scenario. The IPsec protocol selection could be Authentication Header (AH), Encapsulating Security Payload (ESP), ESP plus AH, or AH. The encryption algorithm choice could also be DES, 3DES, or AES.
The authentication algorithm to provide data integrity could be MD5 or SHA. [25]

5.3 IPsec Protocol

IPsec is a collection of protocols that provide encryption, authentication and key management system for ensuring the VPN peers privacy, authenticity and integrity of data as the information crosses the unsecure network. IKE and IPsec are the two building blocks for the formation of the IPsec tunnel. IKE is responsible for determining identities and secrets. The IPsec tunnel is used to transport data securely via a tunnel. As shown in figure 15 above, there are two IPsec framework protocols AH and ESP. [12]

Authentication Header (AH)

AH, which is IP protocol 51, is defined in rfc4302. It is implemented in VPN communication, when confidentiality is not a major concern. In VPN communication peers AH provides the IP packets with data integrity and authentication services. It is a mechanism of verifying whether the data in transit is misused or not. It does not offer an encryption mechanism, but all the packets are transported in clear text which is not secure. AH provides the following services: [26]

- Authentication
- Data origin integrity
- Anti-reply protection

Encapsulating Security Payload (ESP)

ESP, which is protocol 50, is defined in rfc4303. It is implemented in a VPN communication, when confidentiality is a major concern. In VPN communication peers AH provides the IP packets with data integrity, confidentiality and authentication services. It offers encryption service by performing encrypting on the IP payload. Encrypting the IP packet using ESP, hides the data content, source and destination IP addresses. It performs authentication for both ESP header and inner IP packet. ESP provides the following services: [27]

- Encryption
- Authentication
- Data origin integrity
- Anti-reply protection

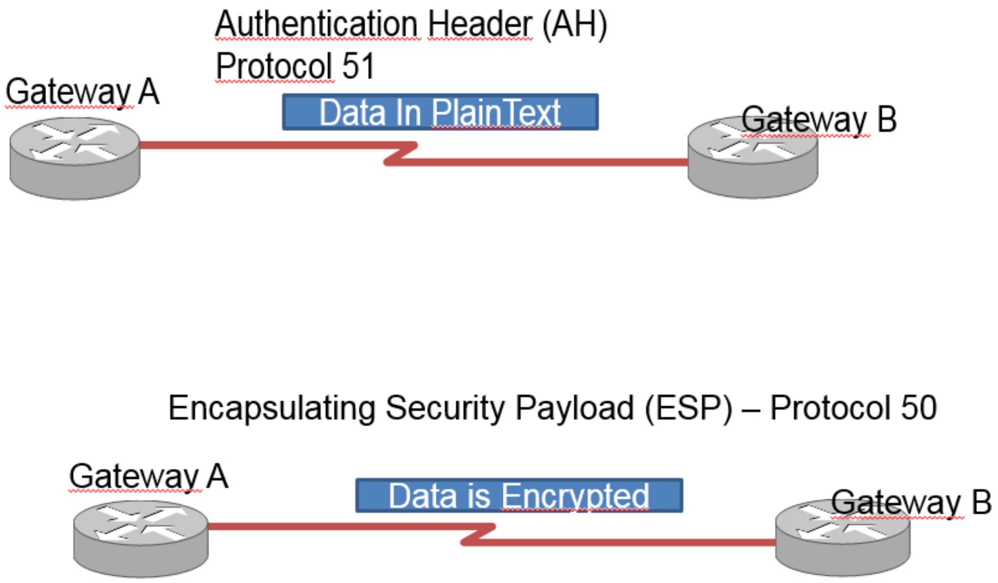


Figure 16. IPsec Security Protocols.

Figure 16 illustrates the IPsec security protocols AH and ESP in a VPN gateway peers. In AH the data is sent in clear text format which is unsecure and in the case of the ESP the data is sent encrypted which is secure communication.

IPsec Modes of Operation

IPsec security protocols, AH and ESP, can be carried out in two different modes of operation. [12]

- Transport mode
- Tunnel mode

In this project the ESP protocol with the tunnel mode is implemented, since the goal of this project is to perform an encryption to the data and transport it through the tunnel to a remote authenticated peer.

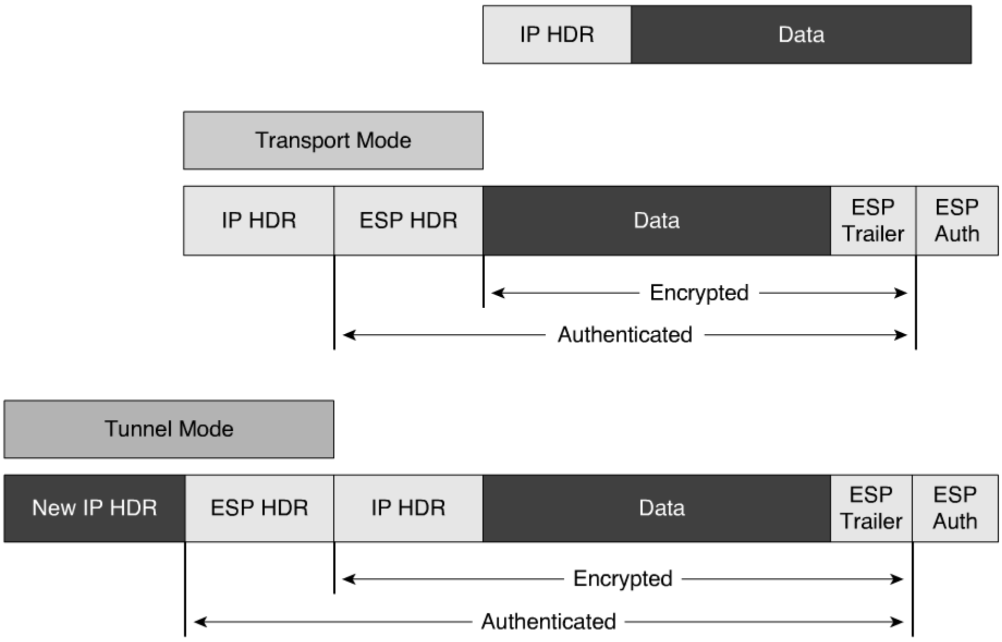


Figure 17. ESP with Tunnel Mode and Transport Mode.

Figure 17 shows the IPsec security protocol, ESP in tunnel and transport mode.

Transport Mode

The transport mode gives protection in the OSI layer stack from the transport layer and above. It performs protection to the data payload but it does not protect the original IP address. The original IP is used to transport the data through the Internet. The ESP transport mode is not with the Network Address Translation (NAT), since communication is end-to-end or between hosts. [13]

Tunnel Mode

The tunnel mode gives protection to data and the source IP packet. This original IP packet is encrypted and it is also encapsulated with a new IP packet. In this project the ESP tunnel mode is implemented between ASA 5505 and SRX240 firewalls.

5.4 Internet Key Exchange (IKE) Protocol

IPsec implements confidentiality in a VPN communication that performs frequent generation of new encryption keys. The IKE protocol is used in VPN solution to authenticate a remote peer and to generate keys. IKE negotiate a security association (SA), which is a rule of engagement between two VPN peers in an IPsec communication and holds all the needed fields to perform successful communication. IPsec listens to IKE request on the UDP port 500. IKE protocol provides the following functions: [28]

- Negotiation of SA parameters
- Key generation
- Key refresh
- Manageable manual configuration

There are two versions of IKE protocol, IKEv1 and IKEv2. This project implements IKEv1.

IKEv1 Modes

The IKE protocol implements three modes of operation to perform secure communication between a VPN peers. The IKE modes of operations are described as follows. [28]

- Main mode
- Aggressive mode
- Quick mode

IKEv1 phases

IKE protocol executes two phases to establish a VPN peers. [12]

1. IKE phase 1: In this phase the two VPN peers execute the initial negotiation of SAs. The SA formed is bidirectional which means that the same encryption key is used to send and receive data. Some of the cryptographic parameters negotiated in this phase are hashing mechanism, transform set, DH, authentication method, and lifetime.
2. IKE phase 2: This is the actual tunnel used to protect user data. This phase is unidirectional which means that a separate key is needed to send and receive data. This phase establishes the IPsec SAs.

IPsec Site-to-site VPN

IPsec VPN site-to-site implements five important steps to establish negotiation. [13]

1. An IPsec tunnel is formed when an interesting traffic from the local host is sent to the remote VPN local host. An interesting traffic travels between IPsec peers that match the crypto ACL.
2. IKE phase 1
3. IKE phase 2
4. IPsec tunnel formation
5. IPsec tunnel teardown

6 VPN Gateway Products

6.1 Cisco Adaptive Security Appliance (ASA) Firewall

The Cisco Adaptive Security Appliance (ASA) series are in different shapes and sizes. However they give the same functionality as a firewall gateway. The ASA is an advanced gateway security device that provides a stateful packet filtering service, VPN cluster capability in one device, and for other models Intrusion Prevention System (IPS) functionalities. The ASA provides many advanced capabilities, such as virtualized firewalls, clustering, a data-link layer firewall, network layer firewall, IPsec VPN, Secure Sockets Layer (SSL) VPN, and clientless Secure Sockets Layer (SSL) VPN support. Basically, larger model numbers have larger capacity for throughput. Some of the various ASA models are ASA 5505, 5510, 5520, 5540, and 5550. [12]

Cisco ASA 5505 provides a variety of security technologies and can be effectively used as a firewall using different deployment mechanisms. In this project an ASA 5505 is implemented to create a gateway or a firewall and prevent internal networks from external attacks. At the same time internal users are allowed to access the public internet. The Cisco ASA security appliance is feature rich set of hardware and software applications, which help to upgrade its functionality beside the stateful packet filtering functionality and packet control mechanisms. [12]

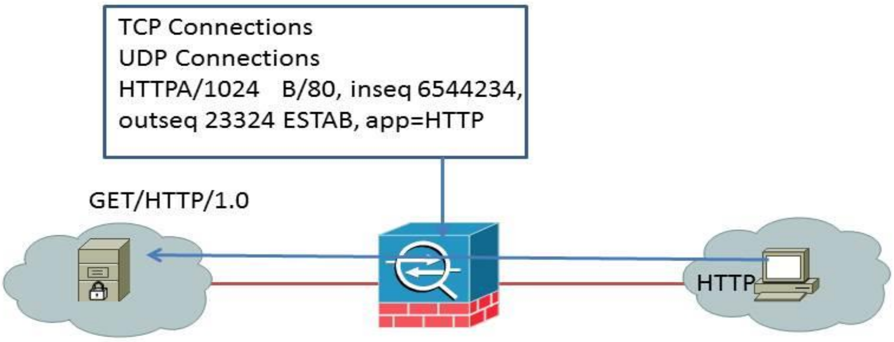


Figure 18. State Table Created for All Inspected Traffic

Figure 18 simplifies that the ASA keep information in a state table. The stateful packet filtering algorithm produces randomly TCP sequence numbers, port numbers, and TCP flags. It controls return packets to verify that they are valid and listed in the statefu session table.

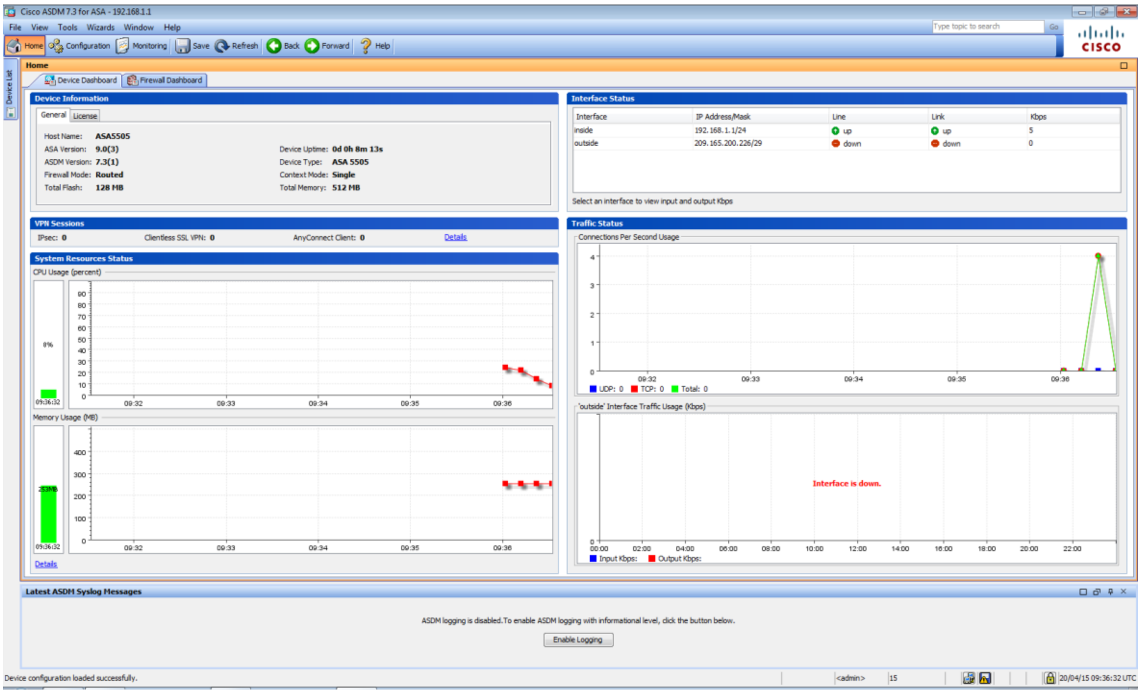
ASA 5500 series provide network services. Some of the services offered are described as follows: [12]

- NAT services
- DHCP services
- IP routing services
- VPN services

In this project the Cisco ASA 5505 is implemented. The Cisco ASA 5505 can be used for small offices, home offices, and enterprise teleworkers. It has an 8 port built-in layer

2 switch and can be configured to Virtual LAN (VLAN). The VLAN interface are needed for layer 3 connectivity.

Cisco ASA 5505 console management can be done either by Command Line Interface (CLI) or Graphical User Interface (GUI). The Cisco Adaptive Security Device Manager (ASDM) is the GUI management for Cisco ASA. ASDM is a web browser that runs Hyper Text Transfer Protocol (HTTP) or HTTP over SSL (HTTPS).



Host Name: **ASA5505**
ASA Version: **9.0(3)**
ASDM Version: **7.3(1)**
Firewall Mode: **Routed**
Total Flash: **128 MB**
Device Uptime: **0d 0h 8m 13s**
Device Type: **ASA 5505**
Context Mode: **Single**
Total Memory: **512 MB**

Interface	IP Address/Mask	Line	Link	Kbps
inside	192.168.1.1/24	● up	● up	5
outside	209.165.200.226/29	● down	● down	0

Select an interface to view input and output Kbps

IPsec: **0** Clientless SSL VPN: **0** AnyConnect Client: **0**

🟦 UDP: 0 🟥 TCP: 0 🟩 Total: 0

Interface is down.

🟦 Input Kbps: 🟥 Output Kbps:

ASDM logging is disabled.To enable ASDM logging with informational level, click the button below.

Device configuration loaded successfully. <admin> 15 20/04/15 09:36:32 UTC

Figure 19. The ASA 5505 GUI Application

Figure 19 shows the GUI ASA 5505. The GUI is a management tool that is used to setup, configure, monitor, and troubleshoot the Cisco ASA. This project is using CLI mode to manage the Cisco ASA family.

6.2 Juniper SRX Firewall

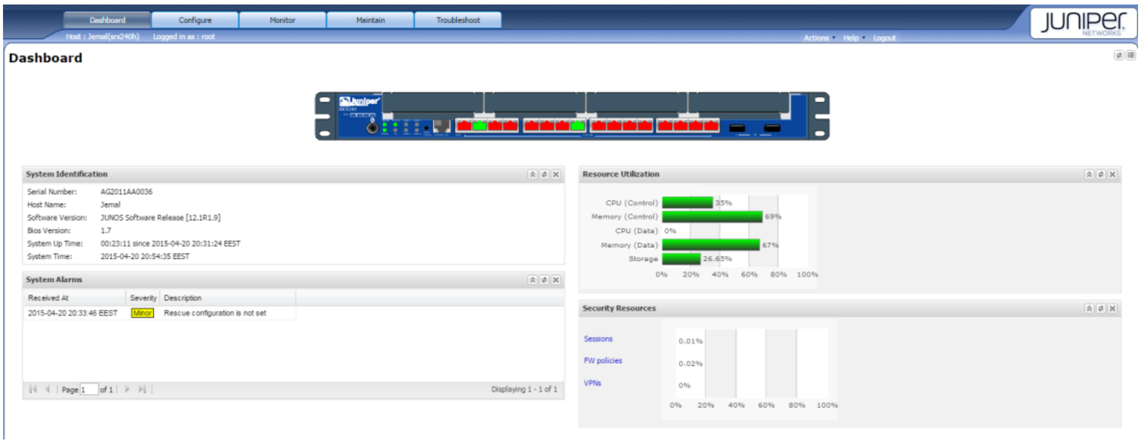
The Juniper SRX series service gateway offers many services like the Cisco ASA 5500 series does. Some of the services are described as follows: [16]

- Routing
- Switching

- Security
- VPN service

This project is implementing the SRX240 service gateway. The SRX240 has 16 Gigabit Ethernet ports and also ports can be offer layer 2 switching capability.

Juniper SRX240 console management can be done either by Command Line Interface (CLI) or Graphical User Interface (GUI). The J-Web is the GUI management for Cisco ASA. J-Web is a web browser that runs Hyper Text Transfer Protocol (HTTP) or HTTP over SSL (HTTPS).



Host : Jemal(srx240h) Logged in as : root

Dashboard

System Identification

Serial Number:	AG2011AA0036
Host Name:	Jemal
Software Version:	JUNOS Software Release [12.1R1.9]
Bios Version:	1.7
System Up Time:	00:23:11 since 2015-04-20 20:31:24 EEST
System Time:	2015-04-20 20:54:35 EEST

System Alarms

Received At	Severity	Description
2015-04-20 20:33:46 EEST	Minor	Rescue configuration is not set

Page 1 of 1 Displaying 1 - 1 of 1

Figure 20. The SRX240 GUI Application

Figure 20 shows the GUI SRX240. The GUI is a management tool that is used to setup, configure, monitor, and troubleshoot the Juniper SRX series. This project is using CLI mode to manage the SRX240.

7 Research Project and Project Implementation

7.1 Requirements

Corporations in the business world may demand continuous expansion on their business activity as the company keeps growing by adding more offices. These offices could be remote offices which are in disparate locations. The remote offices need to connect to their central corporate network so that to have network connectivity for data transfer and access services or resources. Network administrators need to connect all remote offices to the central corporate offices providing a secure communication channel by implementing different security policies.

This thesis project describes the necessary steps to configure a site-to-site VPN between Cisco ASA 5505 and Juniper SRX240 firewalls.

The project requires the following resources:

- 4 switches
- 3PCs
- 1 ASA 5505 (OS version 9.0(3) and Base license)
- 1 SRX240 (JUNOS Software Release [12.1R1.9])
- WireShark sniffing tool (Version 1.12.4)
- Ethernet cable
- Console cable for managing network devices

7.2 Network Topology Design and Implementation

The network topology design used for this thesis project looks like one in figure 21 below.

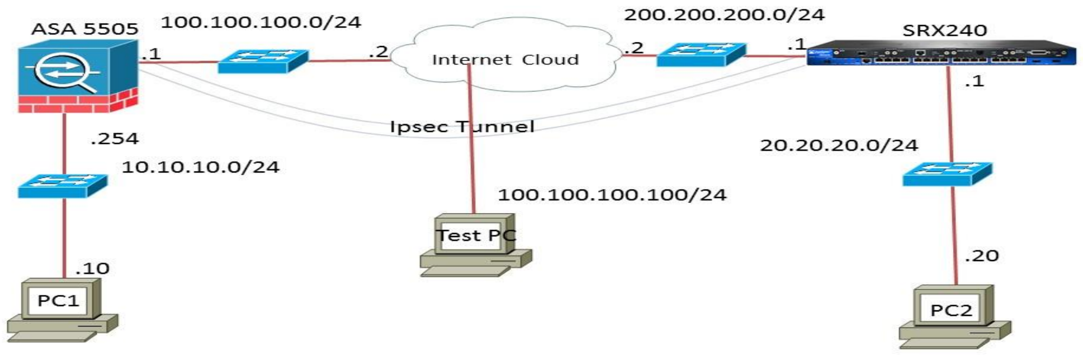


Figure 21. Topology Diagram

Figure 21 illustrates the simulation lab used for this project. There are three computers, one ASA 5505, and one SRX240. The switches in the topology diagram are not configured but they are used for connecting and extension purposes.

Two remote sites are connected via IPsec VPN. One site is implementing a Cisco ASA 5505 IP address of 100.100.100.1 facing the Internet, and a private subnet of 10.10.10.0/24 is connected behind the firewall. The second site is implementing Juniper SRX240 with an IP address of 200.200.200.1 facing the Internet and the private subnet of 20.20.20.0/24 is connected behind the firewall.

The ASA 5505 and the SRX 240 are the firewall gateways and they are connected using a site-to-site IPsec VPN through the unsecure network to provide secure tunnel connectivity to their LANs. Site-to-site or LAN-to-LAN IPsec VPN connects two disparate LAN locations over the Internet. The LANs of each side are using private IP addressing scheme as shown in the topology above figure 21. This project is implementing an IPsec VPN tunnel between the ASA 5505 and SRX240, to establish secure tunnel and forward the private LANs, which are behind the firewalls, inside this tunnel.

7.3 IP Addressing Scheme

The IP addressing format used in this project is IPv4. An IPv4 is a network address and it is a unique 32-bit number used to identify network devices in an internetwork. IPv4 has two parts, one is the host part and the second is the network part. The host part is used to identify specific devices in an internetwork and the network part is used to identify the networks or subnets the devices reside.

Table 2. IP Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
ASA 5505	VLAN 1 (E0/1)	10.10.10.254	255.255.255.0	N/A
ASA 5505	VLAN 2 (E0/0)	100.100.100.1	255.255.255.0	N/A
SRX240	INSIDE (G0/0/1)	20.20.20.0	255.255.255.0	N/A
SRX240	OUTSIDE (G0/0/2)	200.200.200.1	255.255.255.0	N/A
PC1	NIC	10.10.10.10	255.255.255.0	10.10.10.254
PC2	NIC	20.20.20.20	255.255.255.0	20.20.20.1
Test PC	NIC	100.100.100.100	255.255.255.0	100.100.100.2

Table 2 shows the IP addressing interface summary of each device in the topology.

Configuring a basic device setting for each device such as host name and interface IP addresses as shown in the topology above. The configuration for ASA 5505 and SRX 240 is given blow:

```
hostname ASA-5505
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 10.10.10.254 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 100.100.100.1 255.255.255.0
!
```

Listing 3. Basic ASA 5505 configuration

Listing 3 illustrates that the IP address 10.10.10.254/24 is assigned to VLAN 1 in the inside network with high a security level and VLAN2 with the IP address of 100.100.100.1/24 on the outside network facing the Internet with a low security level.

```
system {
    host-name SRX240;
}

interfaces {
    ge-0/0/1 {
        unit 0 {
            family inet {
                address 20.20.20.1/24;
            }
        }
    }
    ge-0/0/2 {
        unit 0 {
            family inet {
                address 200.200.200.1/24;
            }
        }
    }
    st0 {
        unit 0 {
            family inet;
        }
    }
}
```

Listing 4. Basic SRX240 Configuration

As listing 4 illustrates, the IP address 20.20.20.1/24 is configured to the inside network and the IP address 200.200.200.1/24, which is facing the Internet, is configured to the outside network.

7.4 IPsec Site-to-site VPN Configurations

7.4.1 ASA 5505 IPsec VPN Configuration

This project is implementing the IKEv1 site-to-site IPsec VPN. In order to configure IPsec VPN site-to-site there are five sequence steps to be accomplished.

Step 1: Configuring Interesting Traffic

An interesting traffic is the traffic that is going to use the IPsec tunnel or the traffic that is going to be encrypted or protected. In ASA 5505 encrypting interesting traffic is accomplished using the access list or Crypto ACL. Traffic from the private network of the ASA 5505 which is 10.10.10.0/24 is needed to be encrypted. The ACL has been configured as follows:

```
access-list LOCAL-TO-REMOTE extended permit ip 10.10.10.0 255.255.255.0
20.20.20.0 255.255.255.0
```

According to the above configuration, the Crypto ACL needs to identify only the outbound traffic. The permit statement stands for the specific traffic which must be encrypted.

Network Address Translation (NAT) Configuration

It is important to notice when configuring NAT on the firewall for normal Internet access to exclude the traffic that need to be encrypted from NAT. This is because IPsec does not work with NAT. First network object should be created to configure NAT as shown below:

```
object network srx240host
 subnet 20.20.20.0 255.255.255.0
object network asainsidenetwork
 subnet 10.10.10.0 255.255.255.0

nat (outside,inside) source static srx240host srx240host destination static
asainsidenetwork asainsidenetwork
nat (inside,outside) source static asainsidenetwork asainsidenetwork destination
static srx240host srx240host
nat (inside,outside) dynamic interface
```

Listing 5. Configuring NAT

As listing 5 shows, a network object **asainsidenetwork** is used to translate network behind ASA 5505 10.10.10.0/24 to the global address of the outside ASA 5505 interface.

Step 2: Configuring IKEv1 Phase 1

IKEv1 phase 1 of the IPsec VPN configuration is used to establish a secure communication channel for both VPN peers and data transmission. In phase 1 process, they negotiate the cryptography parameters such as encryption algorithm and shared secret key for authentication of the remote VPN partner. In this phase the configured parameters are as follows:

- Hashing: SHA
- Authentication: Pre-shared Key (PSK)
- DH group: 5
- Lifetime: 86400 seconds
- Encryption: AES

The IKEv1 phase1 has been configured as follows:

```
crypto ikev1 policy 100
 authentication pre-share
 encryption aes
 hash sha
 group 5
 lifetime 86400
```

The next configuration is about the pre-shared key and type of the VPN. These are configured as follows:

```
tunnel-group 200.200.200.1 type ipsec-l2l
tunnel-group 200.200.200.1 ipsec-attributes
 ikev1 pre-shared-key anytextstrongkey
```

Step 3: Configuring IKEv1 Phase2 (IPsec)

In IKEv1 phase 1 a secure channel has been established and the next step is to set up the VPN to negotiate the IPsec security parameters which is the rule of engagement for the peers to set the VPN. It will be used to secure data and messages inside the tunnel. Important tasks that are performed in phase 2 are:

- Negotiate IPsec security parameters and IPsec transform sets
- Forming of IPsec Security Associations(SAs)
- Periodic check-up of the IPsec SAs if the connection is up and secure

The next configuration is about IKEv1 phase 2 or IPsec configuration on the ASA 5505 as follows:

```
crypto ipsec ikev1 transform-set CISCO esp-aes esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map outside_map 100 match address LOCAL-TO-REMOTE
crypto map outside_map 100 set peer 200.200.200.1
crypto map outside_map 100 set ikev1 transform-set CISCO
crypto map outside_map 100 set security-association lifetime seconds 2
crypto map outside_map interface outside
```

Step 4: Verification for Encryption Payload

The above three steps concluded the configuration for ASA 5505 configuration part in a site-to-site IPsec VPN. Now let us verify that every communication is secure and the data transfer is working as it should be and the firewall is working according to the configuration. The commands `show crypto isakmp sa` and `show crypto ipsec sa` shows that the tunnel is up, established and the communication is encrypted as well as bidirectional. The outputs of the two commands are shown in listing 6:

```
ASA-5505# show crypto isakmp sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 200.200.200.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE
```

Listing 6. Output of Tunnel Formation

As listing 6 shows, the SA is established and the tunnel is up and running. In the output listing the **`State    : MM_ACTIVE`** means that the tunnel is formed and it is fine.

```
ASA-5505# show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 100, local addr: 100.100.100.1
```

```
      access-list LOCAL-TO-REMOTE extended permit ip 10.10.10.0 255.255.255.0
20.20.20.0 255.255.255.0
      local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
      remote ident (addr/mask/prot/port): (20.20.20.0/255.255.255.0/0/0)
      current_peer: 200.200.200.1

      #pkts encaps: 19, #pkts encrypt: 19, #pkts digest: 19
      #pkts decaps: 19, #pkts decrypt: 19, #pkts verify: 19
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 19, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
      #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
      #TFC rcvd: 0, #TFC sent: 0
      #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 100.100.100.1/0, remote crypto endpt.:
200.200.200.1/0
```

Listing 7. Data Bi-directional Encryption

As listing 7 shows, the data is sent securely and is encrypted and decrypted by the ASA 5505 firewall successfully. The output listing of **`#pkts encrypt: 19`** and **`#pkts decrypt: 19`** shows that data encryption mechanism was bidirectional.

7.4.2 SRX240 IPsec VPN

The IPsec VPN configuration allows users on the local subnet of the SRX240 to communicate securely with users on the remote local subnet of the ASA 5505 and vice versa.

Table 3. The SRX240 Interfaces, Static Routes, and Security Zone Parameters

Feature	**Name**	**Configuration Elements**
Interfaces	ge-0/0/2	200.200.200.1/24
	ge-0/0/1	20.20.20.1/24
	st0.0(tunnel)	
Static routes	0.0.0.0/0	The next-hop is 200.200.200.2
	10.10.10.0/24	The next-hop is st0.0
Security zones	trust	all system-services allowed
		Interface ge-0/0/1.0 resides to this zone
	untrust	ping and ike is allowed services
		Interface ge-0/0/2.0 is found in this zone
	vpn	Tunnel Interface(st0.0) is bound to this zone

Table 3 shows the srx240 configuration parameters such as the configured interfaces, static routes, and the security zones.

Step 1: IKEv1 Phase 1 Configuration

The SRX240 IKEv1 phase 1 configuration parameters have three features such as proposal, policy, and gateway.

The command line configuration of these three parameters on the SRX240 is as follows:

```
  proposal IKE_proposal_1 {
    authentication-method pre-shared-keys;
    dh-group group5;
    authentication-algorithm sha1;
    encryption-algorithm aes-128-cbc;
}
policy ike-policy-1 {
    mode main;
    proposals IKE_proposal_1;
    pre-shared-key ascii-text "$9$jBkmT69pRhrz3hrev7Nik."; ## SECRET-DATA
}
gateway ASA {
    ike-policy ike-policy-1;
    address 100.100.100.1;
    dead-peer-detection {
        always-send;
        interval 60;
        threshold 5;
    }
    local-identity inet 200.200.200.1;
    external-interface ge-0/0/2.0;
    general-ikeid;
}
```

Listing 8. Policy, Proposal, and Gateway configuration.

Listing 8 shows the policy, proposal, and gateway configuration of the SRX240 firewall.

Step 2: IKEv1 Phase 2

The IKEv1 phase 2 is also called the IPsec phase and it has three features such as policy, proposal, and VPN. The command line configuration of these three parameters on the SRX240 is as follows:

```
proposal ipsec_proposal_1 {
    protocol esp;
    authentication-algorithm hmac-sha1-96;
    encryption-algorithm aes-128-cbc;
    lifetime-seconds 3600;
}
policy ipsec_policy_1 {
    proposals ipsec_proposal_1;
}
vpn ASA {
    bind-interface st0.0;
    ike {
        gateway ASA;
        proxy-identity {
            local 20.20.20.0/24;
            remote 10.10.10.0/24;
            service any;
        }
        ipsec-policy ipsec_policy_1;
    }
}
```

Listing 9. Policy, Proposal, and VPN

Listing 9 shows the policy, proposal, and VPN configuration of the SRX240 firewall.

Step 3: Configuring Policy Configuration

The SRx240 security zone policy configuration.

```
 from-zone trust to-zone vpn {
    policy trust_to_vpn_policy {
        match {
            source-address INSIDE;
            destination-address ASA;
            application any;
        }
        then {
            permit;
        }
    }
}
from-zone vpn to-zone trust {
    policy vpn_to_trust_policy {
        match {
            source-address ASA;
            destination-address INSIDE;
            application any;
        }
        then {
            permit;

        }
    }
}
```

Listing 10. Security Zone Policy Configuration

Listing 10 shows the security zone policy configuration of the SRX240 firewall.

Step 4: Verification for Encrypted Payload

The commands `show security ike sa` and `show security ipsec sa` shows that the tunnel is up, established and the communication is encrypted as well as bidirectional. The output of the two commands are shown as the following listings:

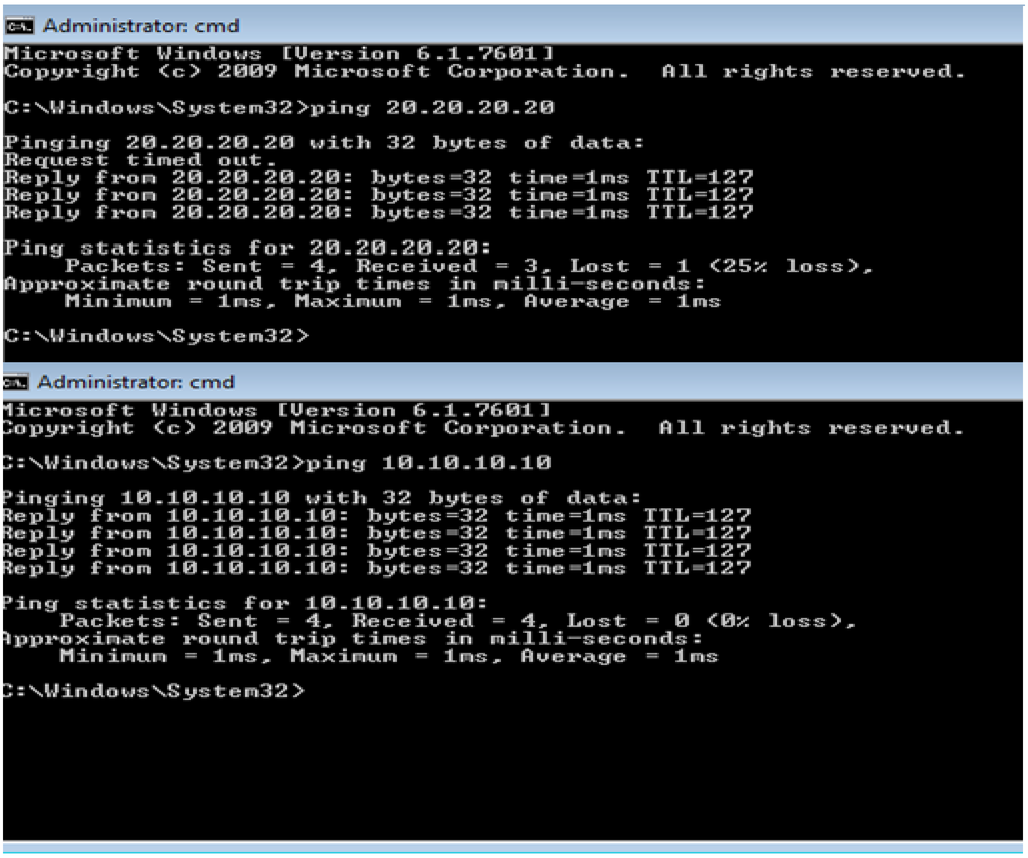
```
admin@SRX240> show security ike sa
Index   State  Initiator cookie  Responder cookie  Mode          Remote Address
8128168 UP     f91baf5e85661b52  82d0470ec4411777  Main           100.100.100.1

admin@SRX240> show security ipsec sa
  Total active tunnels: 1
  ID    Algorithm       SPI      Life:sec/kb  Mon vsys Port  Gateway
  <131073 ESP:aes-128/sha1 69b7a61 3439/  4608000 - root 500  100.100.100.1
  >131073 ESP:aes-128/sha1 86668602 3439/  4608000 - root 500 100.100.100.1
```

As shown in the above output command, we can see that there is one IPsec SA pair and port 500 is used, which means that re is no NAT traversal implemented. Also, we can see the security parameter indexes (SPIs) used for both directions, as well as the lifetime and data usage.

7.5 Analysis

As shown in the figure 21 above for site-to-site VPN, each VPN gateways are securing users on the 10.10.10.0/24 and 20.20.20.0/24 networks which are behind the firewalls. The two gateways become IPsec VPN peers form an IPsec tunnel to each other over the public network infrastructure that is the Internet.

After connecting and configuring network devices, to check the end to end connectivity between the LANs of the gateways, I used “ping” to verify network reachability between hosts behind the firewall.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\System32>ping 20.20.20.20

Pinging 20.20.20.20 with 32 bytes of data:
Request timed out.
Reply from 20.20.20.20: bytes=32 time=1ms TTL=127
Reply from 20.20.20.20: bytes=32 time=1ms TTL=127
Reply from 20.20.20.20: bytes=32 time=1ms TTL=127

Ping statistics for 20.20.20.20:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Windows\System32>
```

```
licrosoft Windows [Version 6.1.7601]
opyright (c) 2009 Microsoft Corporation.  All rights reserved.

:\Windows\System32>ping 10.10.10.10

inging 10.10.10.10 with 32 bytes of data:
eply from 10.10.10.10: bytes=32 time=1ms TTL=127
eply from 10.10.10.10: bytes=32 time=1ms TTL=127
eply from 10.10.10.10: bytes=32 time=1ms TTL=127
eply from 10.10.10.10: bytes=32 time=1ms TTL=127

ing statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
pproximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

:\Windows\System32>
```

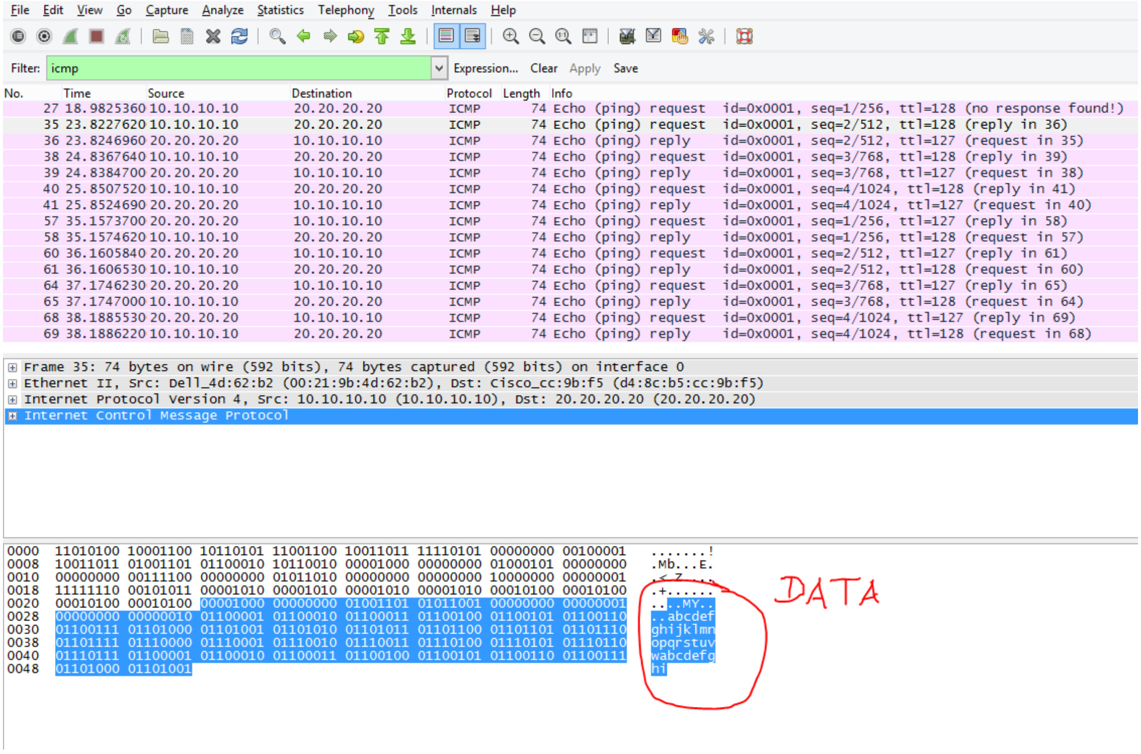
Figure 22. End-to-end Connectivity

Figure 22 shows successful end to end connectivity from both firewall end hosts.

To check if the interesting traffic, which is data send from local host to the remote host, is using the tunnel for communication.

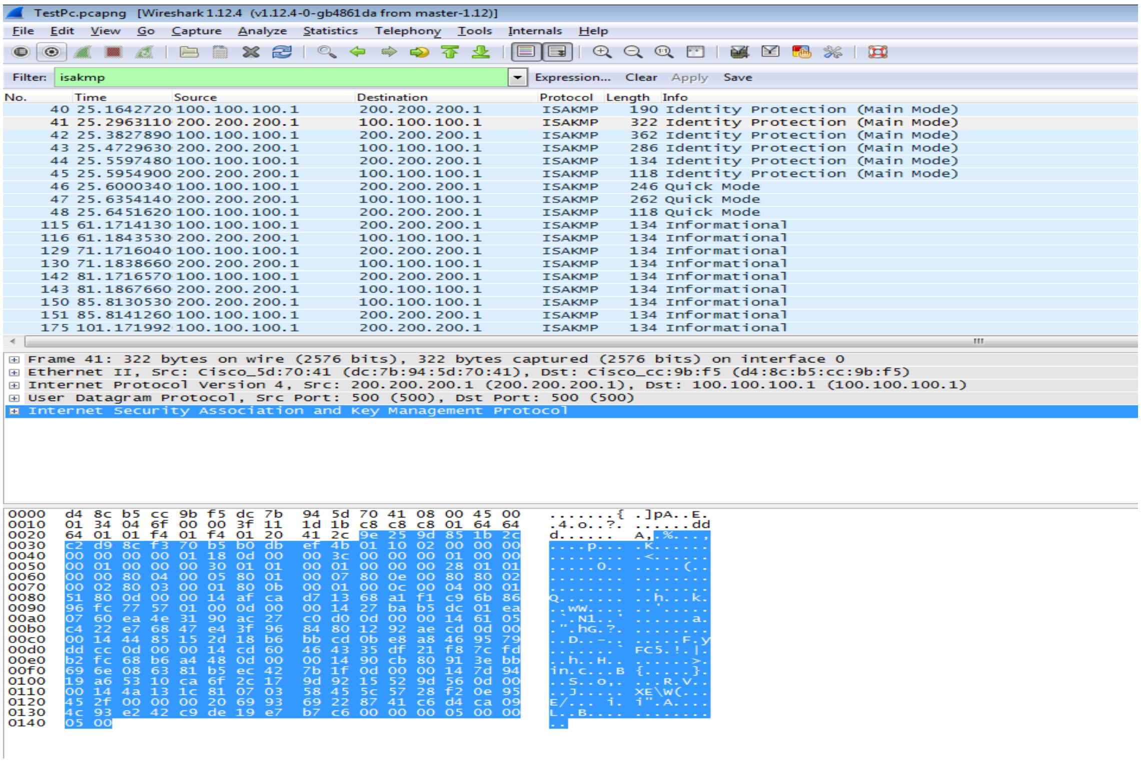
I use WireShark to investigate the communication between the hosts behind the gateways. As the “ping” message sent from hosts as shown the in figure 20 above, the “Test PC “ in the network topology show in fig 19 above is running WireShark to capture the communication.

Figure 23 illustrates that the captured data sent from ASA 5505 host to SRX240 host. As the data send from the host behind ASA 5505, it will pass through the gateway and triggered the security association with the SRX240 VPN peer. IKE phase 1 is initiated and negotiate DH to run and they authenticate each other as shown in figure 23 below.


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save
DATA

```
Filter: icmp

No.  Time        Source       Destination  Protocol Length Info
  27 18.9825360 10.10.10.10   20.20.20.20  ICMP     74 Echo (ping) request  id=0x0001, seq=1/256, ttl=128 (no response found!)
  35 23.8227620 10.10.10.10   20.20.20.20  ICMP     74 Echo (ping) request  id=0x0001, seq=2/512, ttl=128 (reply in 36)
  36 23.8246960 20.20.20.20   10.10.10.10  ICMP     74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=127 (request in 35)
  38 24.8367640 10.10.10.10   20.20.20.20  ICMP     74 Echo (ping) request  id=0x0001, seq=3/768, ttl=128 (reply in 39)
  39 24.8384700 20.20.20.20   10.10.10.10  ICMP     74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=127 (request in 38)
  40 25.8507520 10.10.10.10   20.20.20.20  ICMP     74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=128 (reply in 41)
  41 25.8524690 20.20.20.20   10.10.10.10  ICMP     74 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=127 (request in 40)
  57 35.1573700 20.20.20.20   10.10.10.10  ICMP     74 Echo (ping) request  id=0x0001, seq=1/256, ttl=127 (reply in 58)
  58 35.1574620 10.10.10.10   20.20.20.20  ICMP     74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=128 (request in 57)
  60 36.1605840 20.20.20.20   10.10.10.10  ICMP     74 Echo (ping) request  id=0x0001, seq=2/512, ttl=127 (reply in 61)
  61 36.1606530 10.10.10.10   20.20.20.20  ICMP     74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=128 (request in 60)
  64 37.1746230 20.20.20.20   10.10.10.10  ICMP     74 Echo (ping) request  id=0x0001, seq=3/768, ttl=127 (reply in 65)
  65 37.1747000 10.10.10.10   20.20.20.20  ICMP     74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=128 (request in 64)
  68 38.1885530 20.20.20.20   10.10.10.10  ICMP     74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=127 (reply in 69)
  69 38.1886220 10.10.10.10   20.20.20.20  ICMP     74 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=128 (request in 68)

⊞ Frame 35: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
⊞ Ethernet II, Src: Dell_4d:62:b2 (00:21:9b:4d:62:b2), Dst: Cisco_cc:9b:f5 (d4:8c:b5:cc:9b:f5)
⊞ Internet Protocol Version 4, Src: 10.10.10.10 (10.10.10.10), Dst: 20.20.20.20 (20.20.20.20)
⊞ Internet Control Message Protocol

0000  11010100 10001100 10110101 11001100 10011011 11110101 00000000 00100001   .......!
0008  10011011 01001101 01100010 10110010 00001000 00000000 01000101 00000000   .Mb...E.
0010  00000000 00111100 00000000 01011010 00000000 00000000 10000000 00000001   .<.Z....
0018  11111110 00101011 00001010 00001010 00001010 00001010 00010100 00010100   .+......
0020  00010100 00010100 00001000 00000000 01001101 01011001 00000000 00000001   ....MY..
0028  00000000 00000010 01100001 01100010 01100011 01100100 01100101 01100110   ..abcdef
0030  01100111 01101000 01101001 01101010 01101011 01101100 01101101 01101110   ghijklmn
0038  01101111 01110000 01110001 01110010 01110011 01110100 01110101 01110110   opqrstuv
0040  01110111 01100001 01100010 01100011 01100100 01100101 01100110 01100111   wabcdefg
0048  01101000 01101001                                                         hi
```

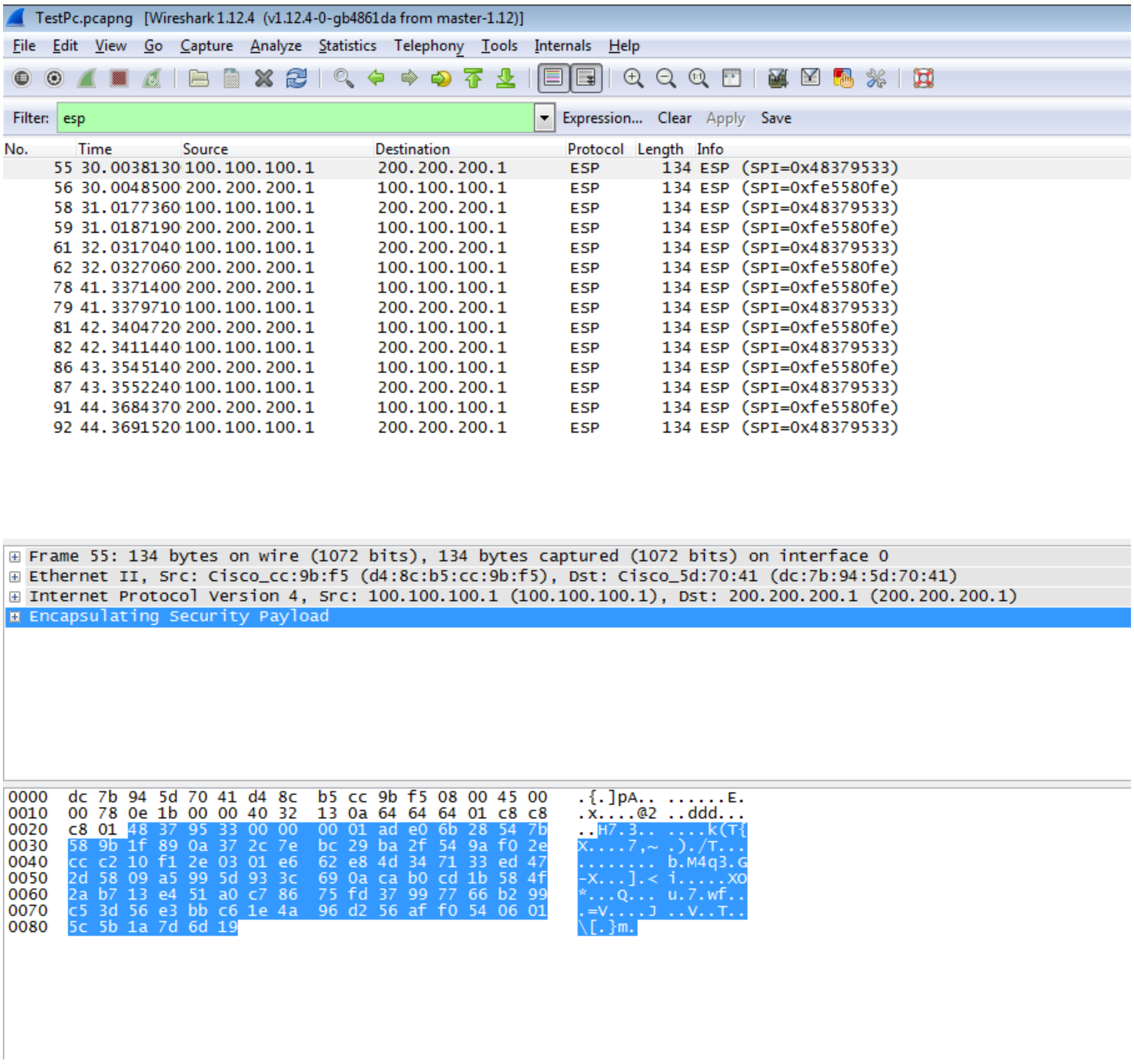
Figure 23. WireShark Screenshot for Host behind ASA 5505


TestPc.pcapng [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

```
Filter: isakmp

No.  Time        Source          Destination     Protocol Length Info
  40 25.1642720 100.100.100.1   200.200.200.1   ISAKMP   190 Identity Protection (Main Mode)
  41 25.2963110 200.200.200.1   100.100.100.1   ISAKMP   322 Identity Protection (Main Mode)
  42 25.3827890 100.100.100.1   200.200.200.1   ISAKMP   362 Identity Protection (Main Mode)
  43 25.4729630 200.200.200.1   100.100.100.1   ISAKMP   286 Identity Protection (Main Mode)
  44 25.5597480 100.100.100.1   200.200.200.1   ISAKMP   134 Identity Protection (Main Mode)
  45 25.5954900 200.200.200.1   100.100.100.1   ISAKMP   118 Identity Protection (Main Mode)
  46 25.6000340 100.100.100.1   200.200.200.1   ISAKMP   246 Quick Mode
  47 25.6354140 200.200.200.1   100.100.100.1   ISAKMP   262 Quick Mode
  48 25.6451620 100.100.100.1   200.200.200.1   ISAKMP   118 Quick Mode
 115 61.1714130 100.100.100.1   200.200.200.1   ISAKMP   134 Informational
 116 61.1843530 200.200.200.1   100.100.100.1   ISAKMP   134 Informational
 129 71.1716040 100.100.100.1   200.200.200.1   ISAKMP   134 Informational
 130 71.1838660 200.200.200.1   100.100.100.1   ISAKMP   134 Informational
 142 81.1716570 100.100.100.1   200.200.200.1   ISAKMP   134 Informational
 143 81.1867660 200.200.200.1   100.100.100.1   ISAKMP   134 Informational
 150 85.8130530 200.200.200.1   100.100.100.1   ISAKMP   134 Informational
 151 85.8141260 100.100.100.1   200.200.200.1   ISAKMP   134 Informational
 175 101.171992 100.100.100.1   200.200.200.1   ISAKMP   134 Informational

⊞ Frame 41: 322 bytes on wire (2576 bits), 322 bytes captured (2576 bits) on interface 0
⊞ Ethernet II, Src: Cisco_5d:70:41 (dc:7b:94:5d:70:41), Dst: Cisco_cc:9b:f5 (d4:8c:b5:cc:9b:f5)
⊞ Internet Protocol Version 4, Src: 200.200.200.1 (200.200.200.1), Dst: 100.100.100.1 (100.100.100.1)
⊞ User Datagram Protocol, Src Port: 500 (500), Dst Port: 500 (500)
⊞ Internet Security Association and Key Management Protocol

0000  d4 8c b5 cc 9b f5 dc 7b  94 5d 70 41 08 00 45 00   .......{ .]pA..E.
0010  01 34 04 6f 00 00 3f 11  1d 1b c8 c8 c8 01 64 64   .4.o..?. ......dd
0020  64 01 01 f4 01 f4 01 20  41 2c 9e 25 9d 85 1b 2c   d......  A,.%...,
0030  c2 d9 8c f3 70 b5 b0 db  ef 4b 01 10 02 00 00 00   ....p... .K......
0040  00 00 00 00 01 18 0d 00  00 3c 00 00 00 01 00 00   ........ .<......
0050  00 01 00 00 00 30 01 01  00 01 00 00 00 28 01 01   .....0.. .....(..
0060  00 00 80 04 00 05 80 01  00 07 80 0e 00 80 80 02   ........ ........
0070  00 02 80 03 00 01 80 0b  00 01 00 0c 00 04 00 01   ........ ........
0080  51 80 0d 00 00 14 af ca  d7 13 68 a1 f1 c9 6b 86   Q....... ..h...k.
0090  96 fc 77 57 01 00 0d 00  00 14 27 ba b5 dc 01 ea   ..wW.... ..'.....
00a0  07 60 ea 4e 31 90 ac 27  c0 d0 0d 00 00 14 61 05   .`.N1..' ......a.
00b0  c4 22 e7 68 47 e4 3f 96  84 80 12 92 ae cd 0d 00   .".hG.?. ........
00c0  00 14 44 85 15 2d 18 b6  bb cd 0b e8 a8 46 95 79   ..D..-.. .....F.y
00d0  dd cc 0d 00 00 14 cd 60  46 43 35 df 21 f8 7c fd   .......` FC5.!.|.
00e0  b2 fc 68 b6 a4 48 0d 00  00 14 90 cb 80 91 3e bb   ..h..H.. ......>.
00f0  69 6e 08 63 81 b5 ec 42  7b 1f 0d 00 00 14 7d 94   in.c...B {.....}.
0100  19 a6 53 10 ca 6f 2c 17  9d 92 15 52 9d 56 0d 00   ..S..o,. ...R.V..
0110  00 14 4a 13 1c 81 07 03  58 45 5c 57 28 f2 0e 95   ..J..... XE\W(...
0120  45 2f 00 00 00 20 69 93  69 22 87 41 c6 d4 ca 09   E/... i. i".A....
0130  4c 93 e2 42 c9 de 19 e7  b7 c6 00 00 00 05 00 00   L..B.... ........
0140  05 00                                              ..
```

Figure 24. WireShark Screenshot for IKE Phase 1

Before IPsec is set up all the original IP, TCP and application header information and payload are I plain text, anyone who is sniffing the communication could easily manipulate the data. After IPsec is created, all the communication are using the protected tunnel and the payload is cipher text.


TestPc.pcapng [Wireshark 1.12.4 (v1.12.4-0-gb4861da from master-1.12)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: esp
Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
55	30.0038130	100.100.100.1	200.200.200.1	ESP	134	ESP (SPI=0x48379533)
56	30.0048500	200.200.200.1	100.100.100.1	ESP	134	ESP (SPI=0xfe5580fe)
58	31.0177360	100.100.100.1	200.200.200.1	ESP	134	ESP (SPI=0x48379533)
59	31.0187190	200.200.200.1	100.100.100.1	ESP	134	ESP (SPI=0xfe5580fe)
61	32.0317040	100.100.100.1	200.200.200.1	ESP	134	ESP (SPI=0x48379533)
62	32.0327060	200.200.200.1	100.100.100.1	ESP	134	ESP (SPI=0xfe5580fe)
78	41.3371400	200.200.200.1	100.100.100.1	ESP	134	ESP (SPI=0xfe5580fe)
79	41.3379710	100.100.100.1	200.200.200.1	ESP	134	ESP (SPI=0x48379533)
81	42.3404720	200.200.200.1	100.100.100.1	ESP	134	ESP (SPI=0xfe5580fe)
82	42.3411440	100.100.100.1	200.200.200.1	ESP	134	ESP (SPI=0x48379533)
86	43.3545140	200.200.200.1	100.100.100.1	ESP	134	ESP (SPI=0xfe5580fe)
87	43.3552240	100.100.100.1	200.200.200.1	ESP	134	ESP (SPI=0x48379533)
91	44.3684370	200.200.200.1	100.100.100.1	ESP	134	ESP (SPI=0xfe5580fe)
92	44.3691520	100.100.100.1	200.200.200.1	ESP	134	ESP (SPI=0x48379533)

```
⊞ Frame 55: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface 0
⊞ Ethernet II, Src: Cisco_cc:9b:f5 (d4:8c:b5:cc:9b:f5), Dst: Cisco_5d:70:41 (dc:7b:94:5d:70:41)
⊞ Internet Protocol Version 4, Src: 100.100.100.1 (100.100.100.1), Dst: 200.200.200.1 (200.200.200.1)
⊞ Encapsulating Security Payload
```

```
0000  dc 7b 94 5d 70 41 d4 8c  b5 cc 9b f5 08 00 45 00   .{.]pA.. ......E.
0010  00 78 0e 1b 00 00 40 32  13 0a 64 64 64 01 c8 c8   .x....@2 ..ddd...
0020  c8 01 48 37 95 33 00 00  00 01 ad e0 6b 28 54 7b   ..H7.3.. ....k(T{
0030  58 9b 1f 89 0a 37 2c 7e  bc 29 ba 2f 54 9a f0 2e   X....7,~ .)./T...
0040  cc c2 10 f1 2e 03 01 e6  62 e8 4d 34 71 33 ed 47   ........ b.M4q3.G
0050  2d 58 09 a5 99 5d 93 3c  69 0a ca b0 cd 1b 58 4f   -X...].< i.....XO
0060  2a b7 13 e4 51 a0 c7 86  75 fd 37 99 77 66 b2 99   *...Q... u.7.wf..
0070  c5 3d 56 e3 bb c6 1e 4a  96 d2 56 af f0 54 06 01   .=V....J ..V..T..
0080  5c 5b 1a 7d 6d 19                                  \[.}m.
```

Figure 25. WireShark Screenshot for IKE phase 2

Figure 25 illustrates the IKE phase 2 which is the actual IPsec tunnel is formed and the payload is encrypted. IPsec Protocol ESP is used to encrypt the payload.

8 Discussion and Conclusion

The main goal of this final year project was to test secure VPN interoperability between two different vendors' gateways, Cisco ASA 5505 and Juniper SRX240 that are connected using an IPsec site-to-site VPN network, so that the data can be transported back and forth securely over a non-secure public network infrastructure that is the Internet. As a result, the simulated lab network of the designed project implementation was successful. I achieved the main objectives of the project.

While I was doing this final year thesis, I gained knowledge on the Cisco and Juniper firewall configurations and deploying IPsec site-to-site VPNs. It was also good opportunity to expose myself to the CLI and GUI management of both vendors. Form the technology point of view, I have learned about VPN technologies, Security mainly on encryption algorithms and IPsec to secure the VPN network.

As the branch sites grows in size, a VPN authentication using Preshared Key (PSK) is not scalable and therefore it is a good choice to consider having a central certificate authority (CA) to authenticate VPN peers.

References

1 James F.Kurose, Keith W.Ross. Computer Networking: A Top-Down Approach. 6th ed. Massachusetts, USA. Pearson Education Limited; 2013.

2 Cisco. Internetworking Technologies Handbook. 4th ed. Indianapolis, USA. Cisco Systems, Inc.; 2004.

3 Joseph Steinberg, Timothy Speed. SSL VPN: Understanding, evaluating, and planning secure, web-based remote access. New York, USA. Packt Publishing Ltd; 2005.

4 Mark Lucas, Abhishek Singh, Chris Cantrell. Fire Wall Policies and VPN Configurations. Canada. Syngress Publishing, Inc.; 2006.

5 Todd Lammle. CCNA Routing and Switching Study Guide. Indianapolis, USA. John Wiley & Sons, Inc. 2013.

6 Wendell Odom. Cisco CCENT/CCNA ICND1 100-101: Official Cert Guide. Indianapolis, USA. Pearson Education, Inc.; 2013.

7 OSI Model

URL: http://en.wikipedia.org/wiki/OSI_model.

Accessed 23 March 2015.

8 Vijay Bollapragada, Mohamed Khalid, Scott Wainner. IPsec VPN Design. Indianapolis, IN 46240 USA. Cisco Systems, Inc.; 2005.

9 Naganand Doraswamy, Dan Harkins. IPsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks. 2nd ed. NJ 07458, USA. Prentice-Hall, Inc.; 2003.

10 Wide Area Network.

URL: http://en.wikipedia.org/wiki/Wide_area_network

Accessed 29 March 2015.

11 Firewall

URL: http://en.wikipedia.org/wiki/File:Firewall.png

Accessed 2 April 2015.

12 Catherine Paquet. Implementing Cisco IOS Network Security (IINS 640-554) Foundation Learning Guide.2nd ed.Indianapolis, USA. Cisco Press; 2013.

13 Keith Barker, Scott Morris. CCNA Security 640-554 Official Cert Guide. Indianapolis, USA.Cisco Press; 2013.

14 Mark Lewis. Comparing, Designing, and Deploying VPNs. Indianapolis, USA. Cisco Systems, Inc.; 2013.

15 Jazib Frahim, Omar Santos, Andrew Ossipov. Cisco ASA: All-in-one Next-Generation Firewall, IPS, and VPN Services. 3rd ed. Indianapolis, USA.Cisco Press; 2014.

16 Brad Woodberg and Rob Cameron. Juniper SRX Series. USA. O’Reilly Media, Inc.; 2013.

17 Symmetric Key Encryption

URL: http://commons.wikimedia.org/wiki/File:Symmetric_key_encryption.svg

Accessed 6 April 2015.

18 Public Key Encryption

URL: http://commons.wikimedia.org/wiki/File:Public_key_encryption.svg

Accessed 6 April 2015.

19 Diffie-Hellman

URL: http://commons.wikimedia.org/wiki/File:Public_key_shared_secret.svg

Accessed 6 April 2015.

20 Vijay Bollapragada, Mohamed Khalid, Scott Wainner. IPsec VPN Design. Indianapolis, IN 46240 USA. Cisco Systems, Inc.; 2005.

21 Transmission Control Protocol

URL: http://en.wikipedia.org/wiki/Transmission_Control_Protocol

Accessed 9 April 2015.

22 Classful Network

URL: http://en.wikipedia.org/wiki/Classful_network

Accessed 10 April 2015.

23 Charlie Scott, Paul Wolfe, Mike Erwin. Virtual Private Network. . 2nd ed. USA. O'Reilly; 1999.

24 Private Networks

URL: https://tools.ietf.org/html/rfc1918

Accessed 10 April 2015.

25 IPsec Protocol

URL: https://www.ietf.org/rfc/rfc2401.txt

Accessed 10 April 2015.

26 Authentication Header

URL: https://tools.ietf.org/html/rfc4302

Accessed 10 April 2015.

27 Encapsulating Security Payload

URL: https://www.ietf.org/rfc/rfc4303.txt

Accessed 10 April 2015.

28 The Internet Key Exchange (IKE)

URL: https://www.ietf.org/rfc/rfc2409.txt

Accessed 10 April 2015.

NOTE: The URLs Cited in this list were functional in May 2015.

ASA 5505 Firewall Configuration

```
ASA-5505# show running-config
: Saved
:
ASA Version 9.0(3)
!
hostname ASA-5505
domain-name asasrx.com
enable password 9D8jmmmgkfNZLETh encrypted
xlate per-session deny tcp any4 any4
xlate per-session deny tcp any4 any6
xlate per-session deny tcp any6 any4
xlate per-session deny tcp any6 any6
xlate per-session deny udp any4 any4 eq domain
xlate per-session deny udp any4 any6 eq domain
xlate per-session deny udp any6 any4 eq domain
xlate per-session deny udp any6 any6 eq domain
names
!
interface Ethernet0/0
 switchport access vlan 2
!
interface Ethernet0/1
!
interface Ethernet0/2
 shutdown
!
interface Ethernet0/3
 shutdown
!
interface Ethernet0/4
 shutdown
!
interface Ethernet0/5
 shutdown
!
interface Ethernet0/6
 shutdown
!
interface Ethernet0/7
 shutdown
!
```

```
interface Vlan1
 nameif inside
 security-level 100
 ip address 10.10.10.254 255.255.255.0
!
interface Vlan2
 nameif outside
 security-level 0
 ip address 100.100.100.1 255.255.255.0
!
ftp mode passive
dns server-group DefaultDNS
 domain-name asasrx.com
object network srx240host
 subnet 20.20.20.0 255.255.255.0
object network asainsidenetwork
 subnet 10.10.10.0 255.255.255.0
access-list LOCAL-TO-REMOTE extended permit ip 10.10.10.0 255.255.255.0 20.20.20.0 255.255.255.0
pager lines 24
logging console debugging
mtu inside 1500
mtu outside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
no arp permit-nonconnected
nat (outside,inside) source static srx240host srx240host destination static asainsidenetwork asainsidenetwork
nat (inside,outside) source static asainsidenetwork asainsidenetwork destination static srx240host srx240host
!
object network asainsidenetwork
 nat (inside,outside) dynamic interface
route outside 0.0.0.0 0.0.0.0 100.100.100.2 1
timeout xlate 3:00:00
timeout pat-xlate 0:00:30
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout floating-conn 0:00:00
dynamic-access-policy-record DfltAccessPolicy
```

```
user-identity default-domain LOCAL
http server enable
http 10.10.10.0 255.255.255.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
crypto ipsec ikev1 transform-set CISCO esp-aes esp-sha-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map outside_map 100 match address LOCAL-TO-REMOTE
crypto map outside_map 100 set peer 200.200.200.1
crypto map outside_map 100 set ikev1 transform-set CISCO
crypto map outside_map 100 set security-association lifetime seconds 28800
crypto map outside_map interface outside
crypto ca trustpool policy
crypto isakmp identity address
no crypto isakmp nat-traversal
crypto ikev1 enable outside
crypto ikev1 policy 100
 authentication pre-share
 encryption aes
 hash sha
 group 5
 lifetime 86400
crypto ikev1 policy 65535
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
telnet 10.10.10.0 255.255.255.0 inside
telnet timeout 10
ssh timeout 5
console timeout 0

threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
tunnel-group 200.200.200.1 type ipsec-l2l
tunnel-group 200.200.200.1 ipsec-attributes
 ikev1 pre-shared-key *****
!
class-map inspection_default
 match default-inspection-traffic
!
```

```
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect ip-options
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
  inspect icmp
!
service-policy global_policy global
prompt hostname context
no call-home reporting anonymous
call-home
 profile CiscoTAC-1
  no active
  destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService
  destination address email callhome@cisco.com
  destination transport-method http
  subscribe-to-alert-group diagnostic
  subscribe-to-alert-group environment
  subscribe-to-alert-group inventory periodic monthly
  subscribe-to-alert-group configuration periodic monthly
  subscribe-to-alert-group telemetry periodic daily
Cryptochecksum:599f26f2fac7d40f564989c1876f2ad3
: end
```

SRX 240 Firewall Configuration

```
admin@SRX240# show | no-more
## Last changed: 2015-04-01 00:04:55 EEST
version 12.1R1.9;
system {
    host-name SRX240;
    time-zone Europe/Helsinki;
    root-authentication {
        encrypted-password "$1$0.lzEXJk$eg9bk8L3uQt9QNpgXpL7A0"; ## SECRET-DATA
    }
    login {
        user admin {
            uid 2002;
            class super-user;
            authentication {
                encrypted-password "$1$bBP9prRu$dIYIepmdT0hjzh4M6Cc6i/"; ## SECRET-DATA
            }
        }
    }
    services {
        ssh {
            protocol-version v2;
            connection-limit 3;
        }
    }
    syslog {
        user * {
            any emergency;
        }
        file messages {
            any notice;
            authorization info;
        }
        file interactive-commands {
            interactive-commands any;
        }
    }
}
interfaces {
    ge-0/0/1 {
        unit 0 {
            family inet {
                address 20.20.20.1/24;
            }
        }
    }
    ge-0/0/2 {
        unit 0 {
            family inet {
                address 200.200.200.1/24;
            }
        }
    }
    st0 {
        unit 0 {
            family inet;
        }
    }
}
routing-options {
    static {
        route 0.0.0.0/0 next-hop 200.200.200.2;
        route 10.10.10.0/24 next-hop st0.0;
    }
}
security {
    ike {
        traceoptions {
            file ike.log size 5000000;
            flag all;
        }
        proposal IKE_proposal_1 {
            authentication-method pre-shared-keys;
            dh-group group5;
            authentication-algorithm sha1;
            encryption-algorithm aes-128-cbc;
        }
        policy ike-policy-1 {
            mode main;
            proposals IKE_proposal_1;
            pre-shared-key ascii-text "$9$jBkmT69pRhrz3hrev7Nik."; ## SECRET-DATA
        }
        gateway ASA {
            ike-policy ike-policy-1;
            address 100.100.100.1;
            dead-peer-detection {
                always-send;
                interval 60;
                threshold 5;
            }
            local-identity inet 200.200.200.1;
            external-interface ge-0/0/2.0;
            general-ikeid;
        }
    }
    ipsec {
        proposal ipsec_proposal_1 {
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm aes-128-cbc;
            lifetime-seconds 3600;
        }
        policy ipsec_policy_1 {
            proposals ipsec_proposal_1;
        }
        vpn ASA {
            bind-interface st0.0;
            ike {
                gateway ASA;
                proxy-identity {
                    local 20.20.20.0/24;
                    remote 10.10.10.0/24;
                    service any;
                }
                ipsec-policy ipsec_policy_1;
            }
        }
    }
    policies {
        from-zone trust to-zone vpn {
            policy trust_to_vpn_policy {
                match {
                    source-address INSIDE;
                    destination-address ASA;
                    application any;
                }
                then {
                    permit;
                    log {
                        session-init;
                        session-close;
                    }
                }
            }
        }
        from-zone vpn to-zone trust {
            policy vpn_to_trust_policy {
                match {
                    source-address ASA;
                    destination-address INSIDE;
                    application any;
                }
                then {
                    permit;
                    log {
                        session-init;
                        session-close;
                    }
                }
            }
        }
    }
    zones {
        security-zone trust {
            address-book {
                address INSIDE 20.20.20.0/24;
            }
            host-inbound-traffic {
                system-services {
                    all;
                }
            }
            interfaces {
                ge-0/0/1.0;
            }
        }
        security-zone vpn {
            address-book {
                address ASA 10.10.10.0/24;
            }
            interfaces {
                st0.0;
            }
        }
        security-zone untrust {
            address-book {
                address OUTSIDE 200.200.200.0/24;
            }
            host-inbound-traffic {
                system-services {
                    ping;
                    ike;
                }
            }
            interfaces {
                ge-0/0/2.0;
            }
        }
    }
}
```

Testing Listing

ASA 5505 testing

```
ASA-5505# show route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 100.100.100.2 to network 0.0.0.0

C    100.100.100.0 255.255.255.0 is directly connected, outside
C    10.10.10.0 255.255.255.0 is directly connected, inside
S*   0.0.0.0 0.0.0.0 [1/0] via 100.100.100.2, outside



ASA-5505# show running-config object
object network srx240host
 subnet 20.20.20.0 255.255.255.0
object network asainsidenetwork
 subnet 10.10.10.0 255.255.255.0

ASA-5505# show running-config nat
nat (outside,inside) source static srx240host srx240host destination static
asainsidenetwork asainsidenetwork
nat (inside,outside) source static asainsidenetwork asainsidenetwork destination
static srx240host srx240host
!
object network asainsidenetwork
 nat (inside,outside) dynamic interface

ASA-5505# show nat
Manual NAT Policies (Section 1)
1 (outside) to (inside) source static srx240host srx240host   destination static
asainsidenetwork asainsidenetwork
    translate_hits = 8, untranslate_hits = 8
2 (inside) to (outside) source static asainsidenetwork asainsidenetwork   des-
tination static srx240host srx240host
    translate_hits = 0, untranslate_hits = 0
```

```
Auto NAT Policies (Section 2)
1 (inside) to (outside) source dynamic asainsidenetwork interface
    translate_hits = 103, untranslate_hits = 319

ASA-5505# show xlate
9 in use, 12 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
       s - static, T - twice, N - net-to-net
NAT from outside:20.20.20.0/24 to inside:20.20.20.0/24
    flags sIT idle 0:15:36 timeout 0:00:00
NAT from inside:10.10.10.0/24 to outside:10.10.10.0/24
    flags sIT idle 0:15:36 timeout 0:00:00
NAT from inside:10.10.10.0/24 to outside:10.10.10.0/24
    flags sIT idle 0:19:13 timeout 0:00:00
NAT from outside:20.20.20.0/24 to inside:20.20.20.0/24
    flags sIT idle 0:19:13 timeout 0:00:00
TCP PAT from inside:10.10.10.10/1117 to outside:100.100.100.1/1117 flags ri idle
0:00:09 timeout 0:00:30
TCP PAT from inside:10.10.10.10/1116 to outside:100.100.100.1/1116 flags ri idle
0:00:22 timeout 0:00:30
TCP PAT from inside:10.10.10.10/1115 to outside:100.100.100.1/1115 flags ri idle
0:00:13 timeout 0:00:30
TCP PAT from inside:10.10.10.10/1114 to outside:100.100.100.1/1114 flags ri idle
0:00:21 timeout 0:00:30
UDP PAT from inside:10.10.10.10/57934 to outside:100.100.100.1/57934 flags ri
idle 0:18:02 timeout 0:00:30

ASA-5505# show crypto isakmp sa

IKEv1 SAs:

   Active SA: 1
    Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1   IKE Peer: 200.200.200.1
    Type    : L2L             Role    : initiator
    Rekey   : no              State   : MM_ACTIVE

ASA-5505# show crypto ipsec sa
interface: outside
    Crypto map tag: outside_map, seq num: 100, local addr: 100.100.100.1
    access-list LOCAL-TO-REMOTE extended permit ip 10.10.10.0 255.255.255.0 20.20.20.0 255.255.255.0
    local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
    remote ident (addr/mask/prot/port): (20.20.20.0/255.255.255.0/0/0)
    current_peer: 200.200.200.1

    #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 7
    #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 7
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 7, #pkts comp failed: 0, #pkts decomp failed: 0
    #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
    #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
    #TFC rcvd: 0, #TFC sent: 0
    #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
    #send errors: 0, #recv errors: 0

    local crypto endpt.: 100.100.100.1/0, remote crypto endpt.: 200.200.200.1/0
    path mtu 1500, ipsec overhead 74(44), media mtu 1500
    PMTU time remaining (sec): 0, DF policy: copy-df
    ICMP error validation: disabled, TFC packets: disabled
    current outbound spi: 48379533
    current inbound spi : FE5580FE

  inbound esp sas:
    spi: 0xFE5580FE (4267016446)
       transform: esp-aes esp-sha-hmac no compression
       in use settings ={L2L, Tunnel, IKEv1, }
       slot: 0, conn_id: 4096, crypto-map: outside_map
       sa timing: remaining key lifetime (kB/sec): (3914999/1918)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x000000FF
  outbound esp sas:
    spi: 0x48379533 (1211602227)
       transform: esp-aes esp-sha-hmac no compression
       in use settings ={L2L, Tunnel, IKEv1, }
       slot: 0, conn_id: 4096, crypto-map: outside_map
       sa timing: remaining key lifetime (kB/sec): (3914999/1918)
       IV size: 16 bytes
       replay detection support: Y
       Anti replay bitmap:
        0x00000000 0x00000001
```

SRX240 testing

```
admin@SRX240> show security ike security-associations
Index   State  Initiator cookie  Responder cookie  Mode           Remote Address
2788778 UP     e1e1150cabfaa57a  30a46706d347998c  Main            100.100.100.1

admin@SRX240> show security ike security-associations detail
IKE peer 100.100.100.1, Index 2788778,
  Role: Initiator, State: UP
  Initiator cookie: e1e1150cabfaa57a, Responder cookie: 30a46706d347998c
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 200.200.200.1:500, Remote: 100.100.100.1:500
  Lifetime: Expires in 28697 seconds
  Peer ike-id: 100.100.100.1
  Xauth assigned IP: 0.0.0.0
  Algorithms:
   Authentication        : hmac-sha1-96
   Encryption            : aes128-cbc
   Pseudo random function: hmac-sha1
  Traffic statistics:
   Input  bytes  :                 1244
   Output bytes  :                 1408
   Input  packets:                   10
   Output packets:                   11
  Flags: IKE SA is created
  IPSec security associations: 1 created, 0 deleted
  Phase 2 negotiations in progress: 0

    Negotiation type: Quick mode, Role: Initiator, Message ID: 0
    Local: 200.200.200.1:500, Remote: 100.100.100.1:500
    Local identity: 200.200.200.1
    Remote identity: 100.100.100.1
    Flags: IKE SA is created

admin@SRX240> show security ipsec security-associations
  Total active tunnels: 1
  ID    Algorithm       SPI      Life:sec/kb  Mon vsys Port  Gateway
  <131073 ESP:aes-128/sha1 23ec768c 3525/ unlim -  root 500   100.100.100.1
  >131073 ESP:aes-128/sha1 467537c 3525/ unlim -   root 500   100.100.100.1

admin@SRX240> show security ipsec security-associations detail
  Virtual-system: root
  Local Gateway: 200.200.200.1, Remote Gateway: 100.100.100.1
  Local Identity: ipv4_subnet(any:0,[0..7]=20.20.20.0/24)
  Remote Identity: ipv4_subnet(any:0,[0..7]=10.10.10.0/24)
  Version: IKEv1
    DF-bit: clear
    Direction: inbound, SPI: 23ec768c, AUX-SPI: 0
                              , VPN Monitoring: -
    Hard lifetime: Expires in 3470 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 2836 seconds
    Mode: Tunnel, Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (128 bits)
    Anti-replay service: counter-based enabled, Replay window size: 64

    Direction: outbound, SPI: 467537c, AUX-SPI: 0
                              , VPN Monitoring: -
    Hard lifetime: Expires in 3470 seconds
    Lifesize Remaining:  Unlimited
    Soft lifetime: Expires in 2836 seconds
    Mode: Tunnel, Type: dynamic, State: installed
    Protocol: ESP, Authentication: hmac-sha1-96, Encryption: aes-cbc (128 bits)
    Anti-replay service: counter-based enabled, Replay window size: 64

admin@SRX240> show security ipsec statistics | no-more
ESP Statistics:
  Encrypted bytes:             3120
  Decrypted bytes:             1560
  Encrypted packets:             26
  Decrypted packets:             26
AH Statistics:
  Input bytes:                    0
  Output bytes:                   0
  Input packets:                  0
  Output packets:                 0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
```