Design and Implementation of ISAKMP Cryptographic Technique on an Educational Institution

Tasniya Ahmed[1], Israt Jahan[2] and Liton Jude Rozario[3]
[1]Department of Computer Science & Engineering, Jahangirnagar University, Savar, Dhaka,Bangladesh
[2]Department of Computer Science & Engineering, Jahangirnagar University, Savar, Dhaka,Bangladesh
[3]Department of Computer Science & Engineering, Jahangirnagar University, Savar, Dhaka,Bangladesh
tasniyaahmed0011@gmail.com, isratju1@yahoo.com, litonjrozario@yahoo.com

Abstract-The purpose of this paper is to describe how to design a network for an educational institution where cryptographic ISAKMP policy is applied for ensuring the security of the network. Confidential papers like question papers are sometimes sent from one department to other. If the necessary security is not involved there, third party will steal the papers which can cause a disaster in the education system. This paper discusses the ISAKMP cryptographic policy and provides step by step instructions to avoid third party's interruption in the educational institution.

Keyword-Access Control List (ACL),Internet Security Association and Key Management Protocol (ISAKMP), Internet key Exchange (IKE),Internet Protocol Security (IPsec),Security Associations (SAs).

1. INTRODUCTION

This project is designed for secure computer network connection. It is a network application and used for a specific organization having a computerized network system. The system has been proposed to improve the efficiency of security of any educational institution as well as it is for business organization. It will eliminate the need for a lot of paper work and will help in secure communication. The network administrator will monitor the process of transferring data segments in the system to avoid collision and broadcast. This report is descriptive type of research on Network System design and configuration for secure efficient communication management of educational institution. Our work simplifies network design and saving bandwidth and control congestion. This design will helpful us to be familiar with time effectively.

After gathering theoretical and practical knowledge about configuration and management of professional network this project work has been printed out that it makes a revolutionary change in the field of network management.

IPsec is not a single protocol, but rather a set of services and protocols that provide a complete Protection. Since IPsec works at the IP layer, it can provide these protections for any higher-layer TCP/IP application or protocol without the need for additional security methods, which is a major strength [1].

IPsec provides the ability to encrypt any higher level messaging. IPsec includes two protocols, AH

To understand the current research being done, one must understand its background and must have knowledge of the working of the internet, its vulnerabilities and the methods which can be used to secure the system. Internet has become more and more widespread. In today's world internet is available everywhere in our house, in our work place, mobiles, cars everything is connected to the internet and if an unauthorized person is able to get access to this network he can not only spy on us but he can easily mess up our lives. And it is more important for an educational institution. The main purpose of this project work is the elimination of the drawbacks traditional system which includes less secure since anybody can see the sent messages, time consuming and less efficient, possible problems in interoperability, external network can access the system networks etc.

2. IP SECURITY PROTOCOLS(IPsec)

security solution for an IP network. These services and protocols combine to provide various types of and ESP, which provide security for IP packets. The AH provides authentication, integrity and replay protection. The ESP provides authentication, integrity, replay protection and confidentiality. Authentication and integrity can be used with or without confidentiality and vice-versa. These protocols need certain parameters in order to establish each connection. The parameters are collected in an entity called security association or SA. When two nodes have established matching SAs, sent and received packets can take advantage of the security services [2].

IKE is a key management protocol standard that is used in conjunction with the IPsec standard. IPsec can be configured without IKE, but IKE enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard[3].

2.1 Internet Key Exchange (IKE) protocol

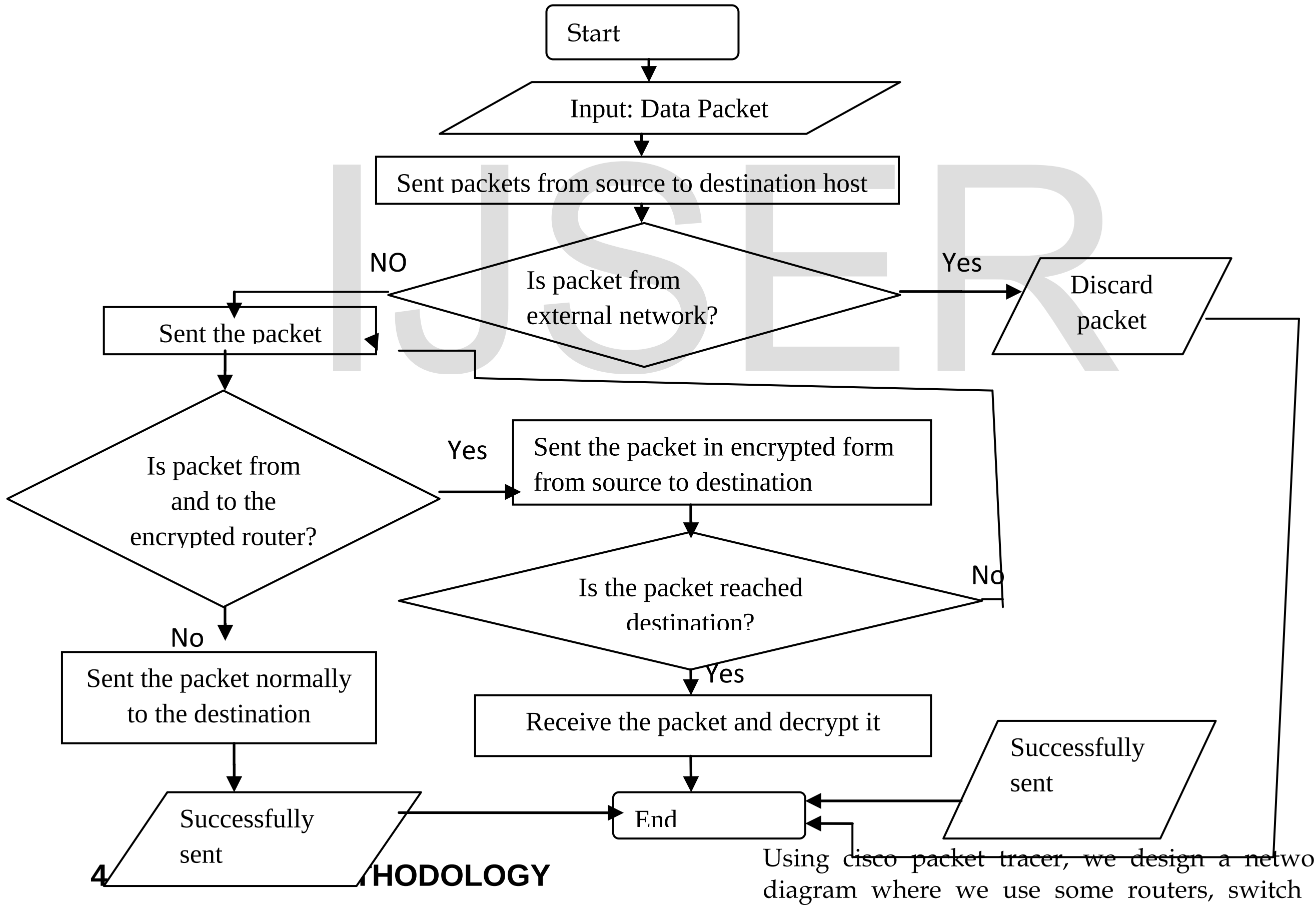
The Internet Key Exchange (IKE) protocol is the main part of the IPsec implementation, and is used to negotiate between two parties to share secret key by creating a SA.During the negotiation, the IPsec protocols are agreed upon, the hash function, authentication key, encryption algorithm, and encryption key data are exchanged, and the duration of security association is set[2].It builds upon the ISAKMP .

2.2 ISAKMP protocol

ISAKMP is an acronym for Internet Security Association and Key Management Protocol. ISAKMP utilize security concepts necessary for establishing Security Associations and cryptographic keys in Internet environment by negotiating, establishing, modifying and deleting Security Associations and their attributes. ISAKMP can be implemented over IP or any other transport protocol [4].

ISAKMP combine the security concepts of key management, authentication, and security associations to establish the required security for private communications on the Internet.

3. PROPOSED FLOWCHART


Start
Input: Data Packet
Sent packets from source to destination host
Is packet from external network?
NO
Yes
Discard packet
Sent the packet
Is packet from and to the encrypted router?
Yes
Sent the packet in encrypted form from source to destination
Is the packet reached destination?
No
Yes
No
Sent the packet normally to the destination
Receive the packet and decrypt it
Successfully sent
End
Successfully sent

4 HODOLOGY

The proposed methodology is described in six steps as follows:

4.1Firstly, Design the Network diagram

Using cisco packet tracer, we design a network diagram where we use some routers, switch as departments, PCs as hosts. There is a external network which is connected to the system but the network cannot access to the system.

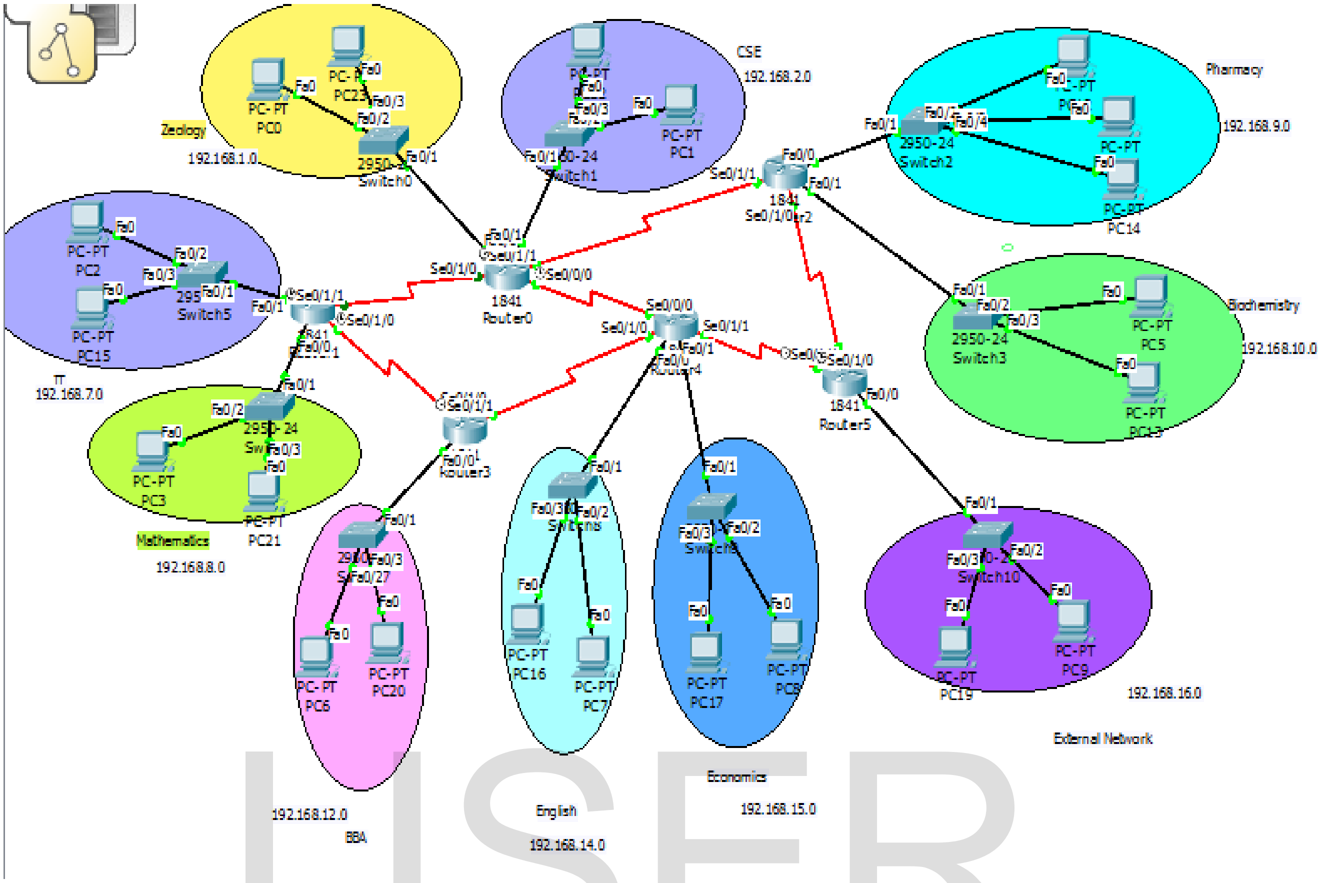


Figure 1: Design of the network system using packet tracer.

4.2 Configure the PCs

We configure the entire host according to the configuring methods in packet tracer.

4.3 Configure the routers

a. Router is a special type of computer which connects and allows communication between two networks. Routers are used to direct packets to its destination. Routers examine a packets destination IP address and determine the best path by using a routing table [5]. We configure all the routers according to routing tables.

b. To route, routers build Routing Tables that contains: The destination network and subnet mask, the “next hop” router to get to the destination network, Routing metrics and Administrative Distance [6].

4.4 Applying OSPF

Open Shortest Path First (OSPF) is a common TCP/IP gateway protocol used to distribute routing information within a single Autonomous System (AS). OSPF can operate within a hierarchy. The largest entity within the hierarchy is the autonomous system (AS), which is a collection of networks under a common administration that share a common routing strategy. An AS can be divided into a number of areas, which are groups of contiguous networks and attached hosts. Routers with multiple interfaces can participate in multiple areas [7].

OSPF uses a link state routing algorithm which is also known as Shortest Path first protocol (SPF).Link is an interface of a router. Link state is the status between routers, also a router interface and its relationship to its neighboring routers. SPF algorithm accumulates costs along each path from source to destination. Each router determines its own cost to each destination at minimum cost [8].

4.5 Apply the ACL to prevent the access of external networks

Access control lists (ACLs) perform packet filtering to control the movement of packets through a network. Packet filtering provides security by limiting the access of traffic into a network, restricting user and device accessto a network, and preventing traffic from leaving a network. IPaccess listsreduce the chance ofspoofing and denial-of-service attacks, and allow dynamic, temporary user-access through a firewall [9].

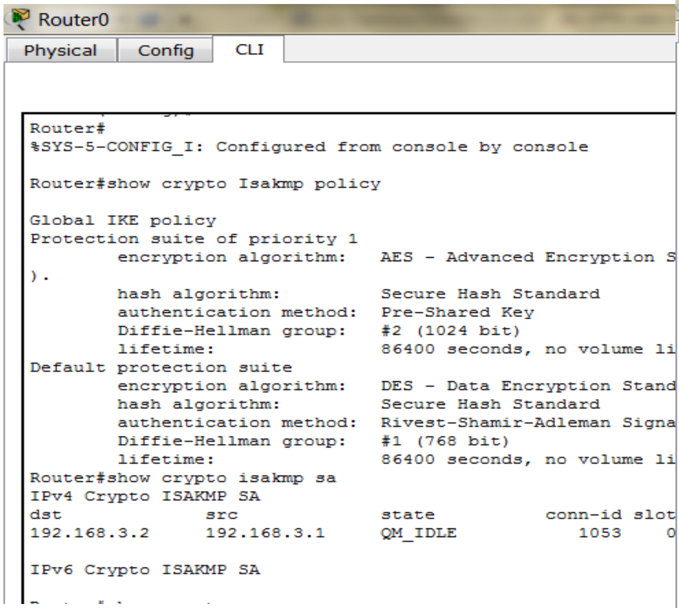
So, ACL is a router configuration script thatcontrolswhether a router permits or denies packets to passbased on criteriafound in the packet header.

Two types:

1. Standard ACL(1-99)
   a. Deny source IP address.
   b. Applied closest to the destination.
2. Extended ACL(100-199)
   a. Deny/permit source & destination IP address.
   b. Applied closest to the source.

5. RESULTS AND DISCUSSION

5.1ISAKMP cryptographic technique between CSE and IT department



```
Router#
%SYS-5-CONFIG_I: Configured from console by console

Router#show crypto Isakmp policy

Global IKE policy
Protection suite of priority 1
        encryption algorithm:   AES - Advanced Encryption S
).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume li
Default protection suite
        encryption algorithm:   DES - Data Encryption Stand
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signa
        Diffie-Hellman group:   #1 (768 bit)
        lifetime:               86400 seconds, no volume li
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot
192.168.3.2     192.168.3.1     QM_IDLE           1053    0

IPv6 Crypto ISAKMP SA
```

4.6 Finally, apply the ISAKMP cryptographic technique on the networks

ISAKMP is the negotiation protocol that lets two hosts agree on how to build an IPsec security association. There are five policy parameters in ISAKMP:

a. IKE policy encryption with AES or DES, to protect the data and ensure privacy.

b. IKE policy hash with Secure Hash algorithm or MD-5, to ensure the identity of the sender, and to ensure that the message has not been modified in transit.

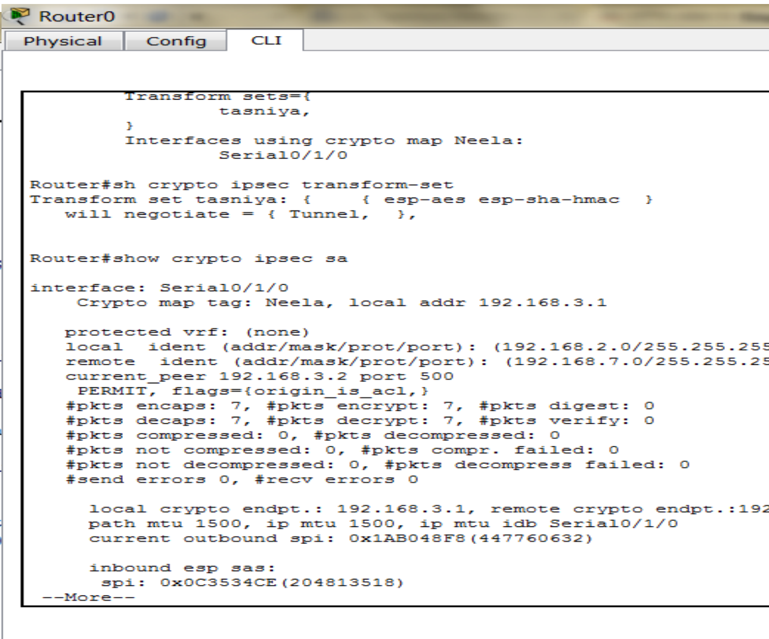
c. IKE key exchange with Diffie- Hellman: Group 1 (768-Bit) or group 2(1024-bits, to determine the strength of the encryption-key-determination algorithm. The security appliance uses this algorithm to derive the encryption and hash keys.

d. IKE lifetime, a limit to the time the security appliance uses an encryption key before replacing it.

e. IKE authentication with RSA public key or pre-share, to ensure the identity of the peers [10].

Figure 2: ISAKMP policy

Figure 2 shows the five policy parameters of ISAKMP which we used to protect our network.



```
        Transform sets={
                tasniya,
        }
        Interfaces using crypto map Neela:
                Serial0/1/0

Router#sh crypto ipsec transform-set
Transform set tasniya: {    { esp-aes esp-sha-hmac  }
   will negotiate = { Tunnel,  },


Router#show crypto ipsec sa

interface: Serial0/1/0
    Crypto map tag: Neela, local addr 192.168.3.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.2.0/255.255.255
   remote  ident (addr/mask/prot/port): (192.168.7.0/255.255.25
   current_peer 192.168.3.2 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 7, #pkts encrypt: 7, #pkts digest: 0
   #pkts decaps: 7, #pkts decrypt: 7, #pkts verify: 0
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 0, #recv errors 0

     local crypto endpt.: 192.168.3.1, remote crypto endpt.:192
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/1/0
     current outbound spi: 0x1AB048F8(447760632)

     inbound esp sas:
      spi: 0x0C3534CE(204813518)
 --More--
```

Figure 3: Crypto IPsec Security Associations

From figure 3 we can observe that 7 encrypted packets are received by the receiver that is decrypted.

5.2 Discussion:

Visually our contribution is not so big on this project. As we didn't get resources for real life implementation, we tried to show our studies and talent through simulator. But we brought a real life implementation procedure in a frame.

6. CONCLUSION

This paper is a type of research on Network System design and configuration for secure and efficient communication management of educational institution. Our work simplifies network design, save bandwidth and control congestion. Security is the main key term to protect confidential data of each and every machine. The main goal of this is research is to design a secured network system for an educational institution. We have described the fundamentals ideas about secured network system, the uses and benefits of implementing ISAKMP policy and ACL and finally the objectives of this project. We also provide step by step instructions to avoid third party's interruption in the educational institution. To implement this project we use CISCO PACKET TRACER to simulate the network. This is an open source academic network simulator. It works similar with the real time network setup and operations.

7. FUTURE WORK

Through our whole working, we utilized our network concept briefly using CISCO SIMULATOR. All the network design and simulation are done considering real networking.
We believe that with sufficient equipment we can implement our simulated work. We can bring the whole educational institution like a University within a secured network system in cost effective and efficient way ensuring the security issues.

REFERENCES

[1] Charles M Kozierok, *The TCP/IP guide: a comprehensive, illustrated internet protocols reference (*No Starch Press, Inc. 38 Ringold Street, San Francisco ,William Pollock, 2005*).*

[2] Hani Alshamrani , Internet Protocol Security (IPSec) Mechanisms,*International Journal of Scientific & Engineering Research, Volume 5, 2014, ISSN 2229-5518 .*

[3] *Internet Key Exchange Protocol,* (*Cisco systems Inc ,2001*)

[4] Prof. Dr. P. Trommler, *FWPF Internet Security*(*GSO FH Nurnberg, Fachrichtung Informatik,2004*).

[5] MalinBornhager *,Router and Routing Basics*(Svenska-CNAP Halmstad University, © 2002)

[6] Aaron Balchunas, *Cisco CCNA Study Guide* (v2.44 © 2014){book}

[7] Merilee Ford, H. Kim Lew, Steve Spanier, and Tim Stevenson,*Internetworking Technology Overview* (New Riders Pub ,1997).

[8] MalinBornhager *,Link-State Routing Protocols*(Version 2002-1, © 2002, Svenska-CNAP Halmstad University).

[9] *Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S*(Americas Headquarters Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706).

[10] *Cisco Security Appliance Command Line Configuration Guide*(Americas Headquarters Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA).