

INTERNATIONAL SCHOOL OF MANAGEMENT & TECHNOLOGY

ASSIGNMENT COVER SHEET

|  |  |  |  |
| --- | --- | --- | --- |
| STUDENT DETAILS | | | |
|  | | | |
| Student ID |  | Reg No. |  |
| Family Name | Shrestha | Given Name | Bisesh |
| Enrolment Year | 2019 | Section | N4 |
| Semester | 3rd semester | Email | bisesh@ismt.edu.np |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| UNIT DETAILS | | | | |
| Unit Title | Network Security | Unit Code | L/615/1646 | |
| Assessor Name | Suman Koirala | Issued Date | 20 April 2021 | |
| Assignment Title | NIC Asia Bank Network System | | | |
| Assignment No | 01 | Submission Date | | 10 June 2021 |
| Qualification | BTEC HND in Computing | Campus | | ISMT |





**STUDENT ASSESSMENT SUBMISSION AND DECLARATION**

When submitting evidence for assessment, each student must sign a declaration confirming that the work is their own.

|  |  |  |  |
| --- | --- | --- | --- |
| Student Name | Bisesh Shrestha | Assessor Name | Suman Koirala |
| Issue Date | 12 March 2020 | Submission Date | 12 May 2020 |
| Programme | Networking | | |
| Unit Name | Network Security | | |
| Assignment Title | NIC Asia Bank Network System | | |

**Plagiarism**

Plagiarism is a particular form of cheating. Plagiarism must be avoided at all costs and students who break the rules, however innocently, may be penalized. It is your responsibility to ensure that you understand correct referencing practices. As a university level student, you are expected to use appropriate references throughout and keep carefully detailed notes of all your sources of materials for material you have used in your work, including any material downloaded from the Internet. Please consult the relevant unit lecturer or your course tutor if you need any further advice.

**Student Declaration**

I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.

Pearson Education 2018  
Higher Education Qualifications



Contents

[Part 1 5](#_Toc94705881)

[Introduction 7](#_Toc94705882)

[Network Security Devices 7](#_Toc94705883)

[Firewall: 7](#_Toc94705884)

[IPS 9](#_Toc94705885)

[Enterprise Routers: 10](#_Toc94705886)

[Content Filtering Devices 11](#_Toc94705887)

[Network Security Protocols 11](#_Toc94705888)

[ VPN: 11](#_Toc94705889)

[ AES: 12](#_Toc94705890)

[ HyperText Transport Protocol Secure 13](#_Toc94705891)

[ SSL 13](#_Toc94705892)

[ IPSec 14](#_Toc94705893)

[Purpose and Requirements of a Secure Network: 14](#_Toc94705894)

[Purpose: 15](#_Toc94705895)

[ To deliver client services in a secure manner: 15](#_Toc94705896)

[ To maintain a higher level of security on the network: 15](#_Toc94705897)

[ Protect the network from a different type of attack: 15](#_Toc94705898)

[ To protect the assets of the organization: 16](#_Toc94705899)

[ To prepare from uncertain disaster: 16](#_Toc94705900)

[Requirements: 16](#_Toc94705901)

[ Proper planning requirement: 17](#_Toc94705902)

[ Awareness training for all the issues regarding cyber-attacks: 17](#_Toc94705903)

[ Highly qualified IT professionals for the design: 17](#_Toc94705904)

[ Implementation of network security (Physical and Virtual Security 17](#_Toc94705905)

[Selecting Network Hardware and Software for the Network: 17](#_Toc94705906)

[1. Router 17](#_Toc94705907)

[2. Switch 18](#_Toc94705908)

[3. Firewall (Cisco ASA 5506-X with FirePOWER Services) 18](#_Toc94705909)

[Conclusion 20](#_Toc94705910)

[Part 2 21](#_Toc94705911)

[Introduction 22](#_Toc94705912)

[Configuring network security on the network: 22](#_Toc94705913)

[Different Cryptographic types of Network Security: 24](#_Toc94705914)

[a) Symmetric Key: 25](#_Toc94705915)

[b) Asymmetric Key: 25](#_Toc94705916)

[c) Hash Function: 26](#_Toc94705917)

[Test Plan for the Network: 27](#_Toc94705918)

[Comprehensive Network Test using the Test Plan: 28](#_Toc94705919)

[Conclusion 31](#_Toc94705920)

[Bibliography 33](#_Toc94705921)

# Part 1

Prepare a report covering the following topics:

1. Conduct a detailed analysis of Network Security principles and aspects covering devices needed to implement a secured network.
2. Discussions of possible Network Security protocols and associated technologies that will enable a secure network for the regional to headquarter of State 5.

**Report on:**

**Network security principles and protocols**

**Prepared by: Bisesh Shrestha**

# Introduction

This part covers relevant information that are focused on the topic of Network Security Devices and Protocols, where numerous equipment such as Firewalls, VPN Concentrators, and other related devices, as well as protocols like as SSL, IPsec, and DNSSEC, must be described. And, in accordance with the scenario, a study into the sole purpose and requirements of a secure network, as well as the hardware and software to be utilized in the network.

# Network Security Devices

Security is more vital in a network than networking equipment like routers, switches, repeaters, and servers for data flow, and we need extra components like Network Security Devices for the network's optimal security to assure limited access to critical information. Safeguards against unauthorized access, risks, and security threats are also incorporated. Network security devices include firewalls, VPN concentrators, and other network security devices, as well as networking hardware such as routers and switches. A network device can support a wide range of security implementations and provide dozens of security services, but in this part, we'll only look at a few:

## Firewall:

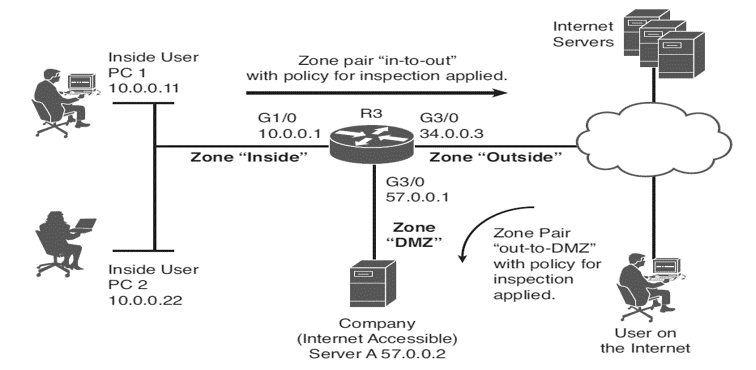
Firewalls are network security devices that monitor and 'curate' network traffic according to a set of pre-determined rules. A firewall creates a barrier between your internal private network and the rest of the internet.

Firewalls can be both software applications and hardware devices, as we'll see shortly. Along with network protection, hardware firewalls can perform other tasks, such as dynamically assigning identifying IP addresses to networked devices. (LOGIX, n.d.)

There are four types of firewalls: packet-filtering firewalls, Stateful packet-filtering firewalls, proxy firewalls and web application firewalls.

A firewall's main components are packet filtering, application gateways, and logging and detection of suspicious activities. Operators are warned via email or pagers when a large number of login attempts are discovered, for example, and intrusion/detection systems make changes if the limitations are exceeded. The firewall will perform brilliantly if the above-mentioned components are appropriately deployed.

A zone-based firewall, for example, is a type of firewall that filters packets and URLs without requiring an Access Control List (ACL). It works by creating a zone in the user interface that acts as a logical area for devices with similar levels of trust. The admin creates the zone, which is specified by specific names, and then the policies are implemented. What transmit (user) traffic is allowed to be initiated is specified in the policies.



**Fig: Working of Zone-Based Firewall**

The zone-based firewall is illustrated in the above-clipped diagram, which has three zones: inside, out, and DMZ, with the inner and outside zones having a pair of "in-to-out" with inspection rules applied. In addition, in the DMZ, the "out-to-DMZ" inspection policy was introduced. When traffic is inspected on the corporate server, it is allowed between the zones, and session information is saved in the zone-based firewall's stateful database. Return traffic can now be allowed even if there is no zone pair or policy in the direction of the return traffic.

## IPS

An intrusion prevention system (IPS) is a network security technology that can not only identify but also block intruders from launching any known attack. Firewalls and intrusion detection systems are combined in intrusion prevention systems. However, adopting an IPS on a large scale can be expensive, therefore companies should carefully consider their IT risks before investing. Furthermore, some intrusion prevention systems are not as quick or as reliable as firewalls and intrusion detection systems, thus an IPS may not be the best option when speed is critical. (netwrix blog, n.d.)

There are a variety of intrusion prevention technologies available, including:

* System memory and process protection

This type of intrusion prevention strategy resides at the system level. Memory protection is a method that prevents one process from corrupting the memory of another on the same computer. Process protection is made up of a technique for monitoring process execution as well as the ability to stop processes that are suspected of being malicious.

* Inline network devices

This form of intrusion prevention approach puts a network device right in the middle of network traffic, allowing it to modify and stop attack packets as they pass through the device's interfaces. It functions similarly to a router or firewall with IDS signature-matching capabilities. Before the packet is sent to the destination network, it is detected and responded to in real time.

* Session sniping

By delivering a TCP RST message to both ends of the connection, this form of intrusion prevention approach terminates a TCP session. The TCP RST is sent when an attempted attack is detected, and the attempted exploit is flushed from the buffers, preventing the attack. To be functional, TCP RST packets must have the proper sequence and acknowledgement numbers.

* Gateway interaction devices

This type of intrusion prevention method allows a detection device to communicate with network gateway devices like routers and firewalls in a dynamic way. When an attack is discovered, the detection device can tell the router or firewall to stop it.

## Enterprise Routers:

A router's principal function is to transfer packets from one broadcast domain to another. However, product providers such as Cisco give many more functions in addition to the primary idea of serving as a device or platform from which to provide numerous network services. Nowadays, "integrated service routers," which emphasize the products' versatile character, are more common. This provides the router with the extra benefit of increasing network security. A router is required for WAN/LAN connectivity, and a LAN switch is required to provide a high-performance local network as well as connectivity to the router and WAN. VOIP services, VPN, and a variety of security services were required by several branches. . Here is the diagram which illustrates the security services provided by a Cisco router:

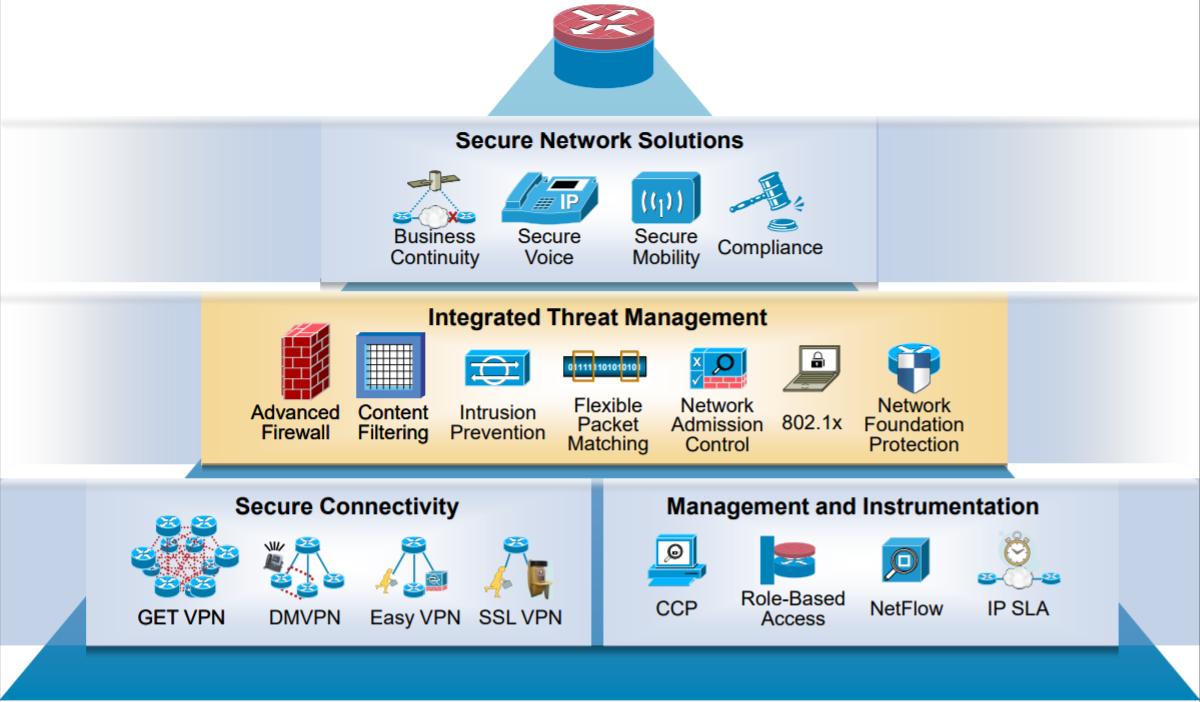


Fig: Cisco Router Security Services

Cisco Integrated Services Router Security Innovations are numerous, and some of them include enterprise-level VPN, routing, and Quality of Service integration (DMVPN, GET VPN, SSL VPN, and Easy VPN). Application firewall, intrusion prevention system, and URL filtering are just a few of the security services available. There are also a number of integrations, including voice, wireless, switching, and enhanced security. Additionally, a secure WAN backup is available by DSL, cable, 3G, or satellite.

## Content Filtering Devices

Online content that is possibly harmful or objectionable is filtered out using content filtering devices. Incoming emails, frequent spam, and even webpages are all examples of this. As the name implies, these gadgets scan web information and verify its safety by running it through their own blacklist of phrases. Some CFDs can also save and warn you about well-known spam sites and email addresses before you interact with them.

When someone tries to view unverified, potentially harmful content on these devices, they get a "Access Denied" error.

This network security device's default setting filters pornographic or hostile content. Aside from that, your company can ban product-selling spam and unsolicited newsletters.

# Network Security Protocols

A network protocol is a set of rules that govern how data is exchanged between devices connected to the same network. In essence, it enables connected devices to interact with one another despite variations in internal operations, structure, or design. Network protocols are responsible for allowing you to interact with individuals all over the world, and they play an important part in modern digital communications.

Because of established rules integrated into devices' software and hardware, network protocols enable devices to engage with each other in the same way that speaking the same language facilitates communication between two humans. Neither local area networks (LAN) nor wide area networks (WAN) could function the way they do today without the use of network protocols. (comptia, n.d.)

Now, the details explanation of various network security protocols are given below:

### VPN:

A virtual private network (VPN) establishes a secure tunnel over a public network, allowing for connections between client and firewall, router and router, and firewall and firewall. It connects to a secure private network using the internet as the public backbone, allowing remote employees to connect to their office network.

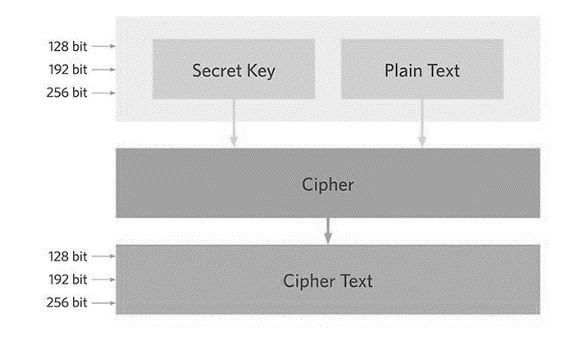
Remote access VPN and site-to-site VPN are the two forms of VPN. We needed a VPN type router with the fastest network speed, as well as software in both end-points in different organizations, to create a VPN. There are several different types of VPN protocols, including:

1. PPTP (Point-to-Point Protocol): This protocol is developed by Microsoft to secure a dial-up connection which mainly operates in the Data-Link Layer of OSI Reference Model.
2. L2F (Layer 2 Forwarding Protocol): This protocol is developed by Cisco which is similarly works in Data Link Layer as PPTP.
3. L2TP (Layer 2 Tunneling Protocol): This protocol is developed by IETF and it is a mixture of PPTP and L2F.
4. IPSec (Internet Protocol Security): IPsec is an open standard for VPN implementation and operates on the network layer.

### AES:

The Advanced Encryption Standard (AES) is a network security standard that the US government employs to encrypt sensitive data and protect classified information. It's a symmetric block cipher that was created in the late 1990s for usage in hardware and software in a limited environment. It provides security by resisting attack when compared to other ciphers, is cost-effective, and gives an algorithm's versatility through straightforward implementation. When properly implemented, it is secure since the AES encrypted keys must be protected. AES maintains network security by the use of trong passwords, password managers, multifactor authentication, firewall, and antivirus software.

Because AES symmetric ciphers (security-key) use the same key for encryption and decryption, both the sender and the receiver required the same symmetric ciphers. There are three kinds of block ciphers: AES-128, AES-192, and AES-256 which has an only difference in the size as AES-128 uses a 128-bit length key as a symmetric cipher.



**Fig: AES Design**

AES Encryption is based on an algorithm that specifies a set of changes to be applied to data stored in an array. The data is initially stored in an array, and then it is encrypted repeatedly when it is modified by ciphers. The rounds are then decided by the length of the key, with 10 rounds for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Each cycle includes different transformations, such as the substitution of data using a substitution table, the shifting of data rows, and so on. Longer keys necessitated additional rounds in order to finish the encryption.

### HyperText Transport Protocol Secure

HTTPS (HyperText Transport Protocol Secure) is a secure data transfer protocol for two or more systems. To construct an encrypted link, it used Secure Socket Layer (SSL), currently known as Transport Layer Security (TLS). Because data sent through HTTPS is encrypted, thieves are unable to decipher and change it as it travels from the browser to the website. Thieves will be unable to decipher the data packets even if they seize them due to the tight encryption associated with them. (w3school, n.d.)

### SSL

SSL encrypts the segments of network connections above the Transport Layer. There are various versions of SSL which consist of SSLv1, SSLv2, SSLv3, and TLS where TLS is the IETF standard that succeeded SSL.

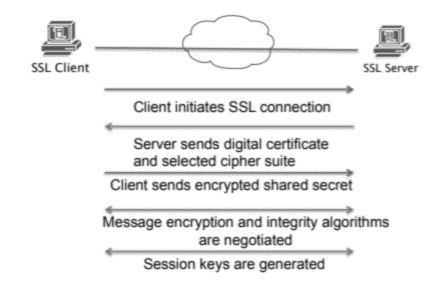


Fig: SSL Handshake (Das, 2020)

The SSL handshake establishes a session between the SSL client and the SSL server, ensuring a secure connection. After the initial handshake, encryption is employed to define a secret key, which employs symmetric cryptography. It also employs asymmetric cryptography for peer identification (RSA or DSS). Because the message transit includes message integrity verification using a keyed MAC, the connection is secure and dependable.

### IPSec

The Internet Protocol Security (IPSec) standard is an IETF standard that enables encrypted peer-to-peer communication by utilizing network layer encryption to ensure data confidentiality, integrity, and authentication. It ensures data secrecy and integrity by computing the checksum or hash value of data at either end of the tunnel. Signatures and certificates are also used for authentication. Data integrity and source authentication, as well as anti-replay protection, are some of the advantages that aid in the detection of data alteration that signatures "verification" can detect.

IPsec and SSL are the encryption methods used in a VPN concentrator when accessing files, with IPsec requiring a complicated configuration and client software to obtain access to the private network. Because of the way it's set up, it's only available in select areas. For example, if IPsec is only setup in a cafeteria, we can only access a specific domain from the cafeteria, which is reliable for some organizations but not for others.

Secure Socket Layer (SSL) is an expanded version of IPsec that requires no additional configuration and may be accessed from any place. Depending on the needs of the company, one of two VPN concentrators might be chosen.

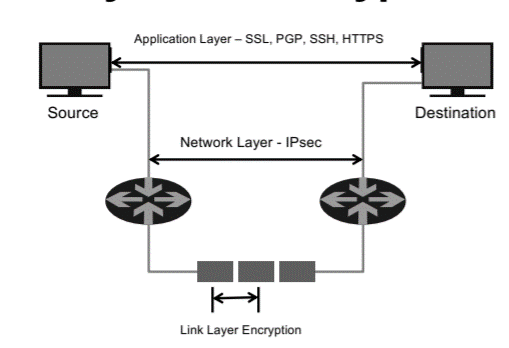


Fig: different layer of Encryption (APAN, n.d.)

# Purpose and Requirements of a Secure Network:

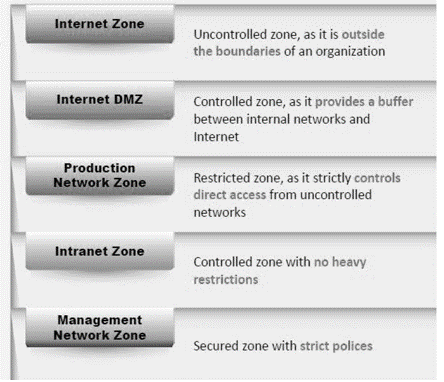
As stated in the scenario, NIC Asia Bank is a large commercial bank that serves all of Nepal's financial centers. The bank needs to plan a fully operating and secure network in the Karnali Province, hence the following are the goals and requirements for network planning:

## Purpose:

* To deliver client services in a secure manner: The main goal is to give the client with all financial services, such as ATM service, mobile banking, and other services that are essential to serve the client safely. All authentication procedures should be simple and secure at the same time in order to get the most out of all of the client's offerings. Biometrics and automated log out on the client end can provide some authentication protection, but this complicates matters for hackers because it limits the user's access for a specific amount of time.

For maximum security, multi-factor authentication (MFA) is also a critical component on the client end, and it must be implemented in the bank mobile app. Many people do not change their passwords, and using MFA prevents attackers from gaining a access to the network by requiring additional information.

* To maintain a higher level of security on the network: Although we previously discussed client-side security, overall network security is equally critical for a secure bank network. To provide a higher level of security on the bank's network, security devices such as firewalls, VPN concentrators, switches, and routers, as well as various protocols such as IPsec, SSL, AES, and others, must be deployed, both in terms of software and hardware.
* Protect the network from a different type of attack:The bank also seeks to strengthen its preventive and mitigation methods in order to protect the network from various attacks. Attacks include spear phishing and ransomware, mobile malware, insider threats, Cyberware, retailer data breaches, and big data for fraud detection. Attacks are on the rise and will continue to do so in the coming years. As a result, banks should position themselves as a defense against critical dangers such as cloud computing risks, advanced persistent threats, viruses and worms, botnets, and other hazards.

To protect the network from an attack, we must set up network security zoning according to the criteria. The network security zoning method enables banks to maintain a secure network environment by determining the appropriate security levels for distinct internet and intranet zones. It aids in the efficient monitoring and management of inbound and outgoing traffic.

***Fig: Example of the network security zone.***

* To protect the assets of the organization:The bank's most significant asset is the system that allows it to provide services to customers. Because the services required the most care, the company's core network has become a highly valued asset. Due to the high level of competition in today's banking business, banks must provide services on a constant ba sis.

As a result, various backup plans and scalable solutions must be established in order to protect those priceless assets. The most important requirement is to build with more modern and powerful equipment, with security and service accessibility as top priorities. Furthermore, better planning and implementation methodologies were necessary for network implementation.

* To prepare from uncertain disaster: The bank's services are more likely to be continuous, and the bank will incur losses if they are unavailable for even a minute. When it comes to abandoning the service, clients have a variety of options to choose from. A backup strategy should be in place for a network that serves as the core and stores apps and other data. This necessitates careful risk management strategy.

## Requirements:

From the above-discussed purpose for a secure network of NIC Asia Bank, here the basics requirements are going to be discussed as:

* Proper planning requirement:Based on previous network design and all the previous threats regarding network we need to gather all the information. The information is based on the network in the past with its usability, security, and resilience. And, based on those data, we need to gather all the planning and requirements to design the network securely.
* Awareness training for all the issues regarding cyber-attacks: If there are any attacks in the past in the case of NIC Asia, the bank was hacked previously a few years ago. And, by acknowledging those issue the system should be planned to mitigate those kind of issues is needed and training based on those attacks should be provided to mitigate from those issues.
* Highly qualified IT professionals for the design: With Network Security Analyst and many highly skilled IT professionals are required to design reliable networks with certain security regulations. They indeed have a lot of experience with previous design and based on that experience IT professionals design the network.
* Implementation of network security (Physical and Virtual Security**):** In the network, network security must be implemented both physically and virtually. As per the requirement, when physically designing the network, security devices such as firewalls, VPN concentrators, and others should be included to make the network safer.
* Furthermore, virtual security implementations such as firewall policy, firewall group policy, biometrics, system auditing, and monitoring, as well as analyzing monitoring results. With all main policy implementation and security audits performed on a regular basis over a period of time. This is something that can have a big influence with penetration testing to test network security, and it will help to update the network over time as needed.

# Selecting Network Hardware and Software for the Network:

When it comes to constructing a secure network, a range of hardware and software is used, some for a single task and others for many processes. So, in order to provide optimum security to a bank, routers, switches, VPN concentrators, and biometrics are the most commonly used hardware, all of which have security factors, while software such as system monitoring tools and security programs play a significant role in keeping the bank secure.

The following is a list of hardware that is required for security:

## Router

A router is a hardware device that connects many channels for different networks via each network's network interface. The router, which serves as a processing unit for data packets, is usually found among the network layers that determine the data transit channel. The router duplicates information packets for use during transmission from one network to another. The router uses a protocol or set of rules to determine which information packets should be forwarded to which network interfaces. Different types of routers perform different functions depending on the needs of the network system.

 *Fig: Router (Cisco 4461) (Cisco1, 2019)*

## Switch

The network switch's security section is considerably superior than switching packets to receive and forward data to the destination since it strengthens it in multiple ways. The network is redundant and secure as a result of the switch's STP and VLAN features. STP helps to avoid loops in redundant trunk links, whereas VLAN helps to divide a network into separate virtual LANs. Switch spoofing and double-tagging attacks are two instances of risks that can be reduced by implementing VLAN hopping protection in the switch. Furthermore, the switch is a network device that can provide security as well as packet switching in a network.



*Fig: Cisco Catalyst Switch 2960-24TT (Anon., 2019)*

## Firewall (Cisco ASA 5506-X with FirePOWER Services)



*Fig: Cisco ASA 5506-X with FirePOWER Services (Cisco2, 2019)*

The Cisco firewall devices model Cisco ASA 5506-X with FirePOWER Services was chosen after a thorough examination of all of its features and qualities, as well as its cost-effectiveness for the project, based on the following criteria:

The following are some of the advantages of the Cisco ASA 5506-X with FirePOWER:

1. Outstanding multilayer protection: The multilayered protection helps to deliver superior security, earning the maximum security for both NGIPS and AMP, blocking 99.4% and 99.2% of threats, respectively.
2. Superior multilayer protection: The multilayered protection helps to provide superior security which also has earned the highest security for both NGIPS and AMP as it blocks 99.4% and 99.2% of threats respectively.
3. Simplified management and lower costs: The more simple management of the firewall gives visibility and also control over activity across the network. The insights gained into users, apps, devices, threats, files, and vulnerabilities, the extended protection from the data center to mobile devices. The firepower management center gives the possibility to all the extended protection.
4. Unified security services and tack automation: The integrated approach to threat defense reduces capital and operating costs as well as administrative complexity by consolidating multiple security services in a single platform. It automates security tasks to increase agility and speed remediation.

The characteristics of the Cisco ASA 5506-X with FirePOWER are as follows:

|  |  |  |
| --- | --- | --- |
| S.N | Specifications | Capacity |
|  | Solid-state drive | 50 GB mSata6 |
|  | Relative humidity | 90 percent non-condensing |
|  | Dimensions (H \* W \* D) | 1.72 x 7.871 x 9.23 in.  (4.369 x 19.992 x 23.444 cm) |
|  | Temperature | 32 to 104ºF (0 to 40ºC) |
|  | Serial console port - RJ45 (up to 115.2 kbps) | 1 |
|  | Dedicated management port | Yes (Shared) |
|  | AC range line voltage | External, 90 to 240 volts alternating current (VAC) |

*Table: Specification of Cisco ASA - 5506*

**With hardware devices, we need also some specific security software in the network which are:**

As the system uses numerous servers, routers, switches, and other components to construct a secure network, the software employed in this hardware is the most crucial component of them all. The server, for example, runs Windows Server 2012 r2, Cisco IOS, Windows 10, and other operating systems, all of which offer a diverse set of features and software depending on the hardware. All operating systems include licensed software from the default vendor, ensuring the security of the software. These operating systems may also help you construct a secure network because they include a lot of software, such as an in-built firewall, intrusion detection system, user and group management software, various server programs, and a variety of other applications. . For example, in Windows Server 2012 r2, there are pre-configured servers as well as multiple server options in the OS that allow you to manually design a server while considering various security policies. Similarly, with other operating systems, there are a variety of options.

# Conclusion

Finally, the assignment focuses on the documentation of numerous Network Security entities, including the devices in the network that contribute to security, as well as several network principles. With that in mind, the different types of VPNs are defined, as well as their key differences. Along with VPN, additional network security protocols such as HTTPs, SSL, and others are explored. Following the debate, the major purpose and requirements of a secure network are highlighted, including a list of numerous requirements such as appropriate planning, network security implementation, and highly qualified IT personnel. Finally, the various hardware and software requirements for constructing a secure network are outlined.

# Part 2

Design and implement a network prototype using a network simulator (or lab devices), which incorporates high levels of Network Security. You also need to provide the following written material as a formal report:

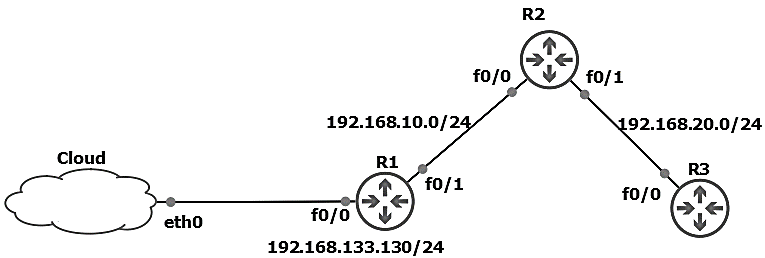
* 1. A rationale for the selection of the networking devices for the prototype.
  2. A detailed explanation of how the security protocols will work with IPv4 and IPv6.

# Introduction

A number of deployment and testing stages are required for this task. This initiates the network design phase, which is followed by the verification and deployment of network security, which is subsequently tested. There must also be a description of various cryptographic types of network security, such as symmetric, asymmetric, and hash functions. Following that, a test of network security using tools like ping and tracert is required.

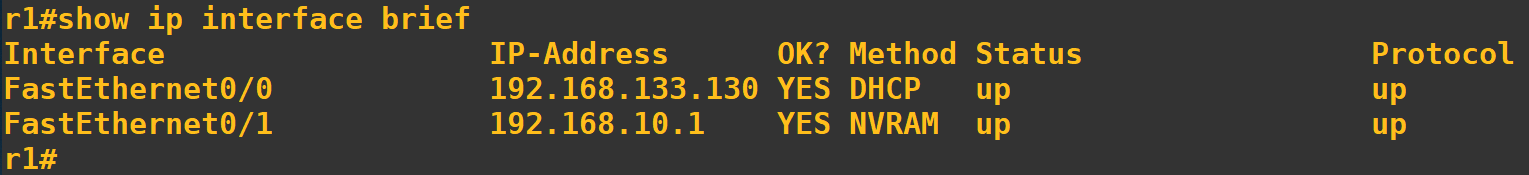
# Configuring network security on the network:

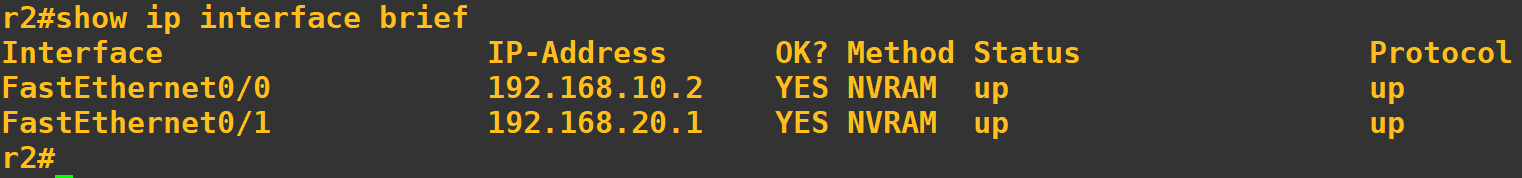
Concerning the previous part, the purpose and requirements of a secure network. The configuration which needs to be done in the network to make it secure is discussed here.



**Fig: Simple Network Diagram to test Network Security**

Each Network Management Server is deployed in its own VM, and all Cisco device images (Cisco IOS C3725 Image) are put in the GNS3 VM. Furthermore, the routers are linked to the network administration tools and network security via Host-only adapters and static routes. In routers with a static IP address and area 0, the OSPF Routing Protocol is enabled. The IP setup of routers is shown here, as well as other basic configuration such as changing the hostname; OSPF routing is not described because it is the most basic configuration.





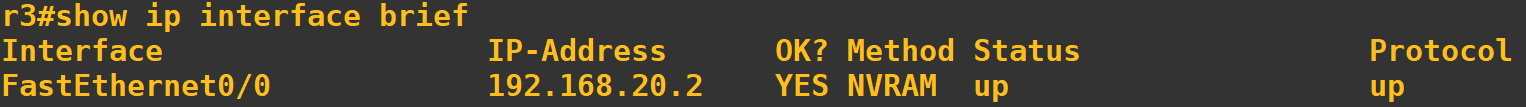
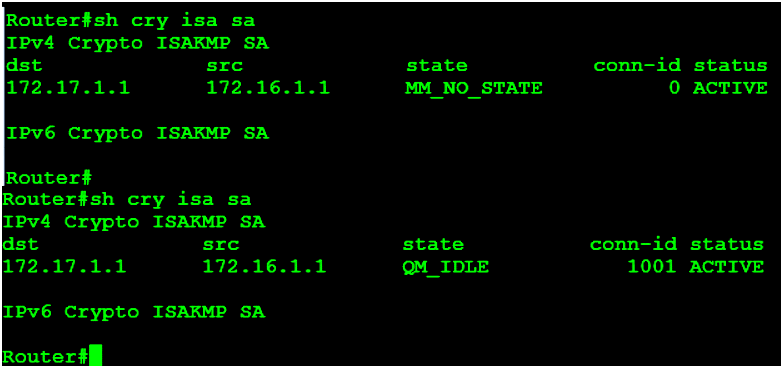


Fig: “show ip interface brief” in r1, r2, and r3

The scenario involves the NIC Bank, which has several branches as well as the headquarters, and the security of the headquarters must be rigid and secure in order to provide a smooth workflow in the bank. And, in order to do so, the bank must configure the security policy in a variety of network devices, including servers, routers, firewalls, switches, and many others. To accomplish this, the following configuration is required:

1. When the backbone router communicates with the router of another branch using the internet, the level of trust between the networks connected by a backbone router becomes very low as it is used to forward all the traffic between the branches. For that, the goal to adapt security in these kinds of the router, the responsibility to manage and operate the router should only be provided to authorize a party which also secure the routing information.
2. The most important factor in securing these devices is to turn off the services that are not in use, as general security practices for routers and firewalls are to support traffic and protocols a network service, and the services that need to be turned off while not in use are CDP (Cisco Discovery Protocol), TCP and UDP Small Servers, Finger Server, HTTP Server, Bootp Server, Configuration Auto-Loading, Proxy ARP, IP Source routing, SNMP Services, IP When only the services that are required are running, the chances of the network being exploited are reduced, which increases network security.
3. A firewall can protect a network from external attacks by examining all packets of a message attempting to pass through the network and rejecting the packets that do not meet the security restrictions. However, it does not protect the data as it is transmitted from one network to another. Data transmitted from one network to another via the Internet is susceptible to access at many points between the source and destination. The secure socket layer (SSL) and IPSec is one means of providing secure communications between points connected via the Internet. And, here is the example of the implemented IPsec configuration which shows the crypto session from the destination to its source where the state transition from not having connection to get connected and authenticated and in the idle condition.



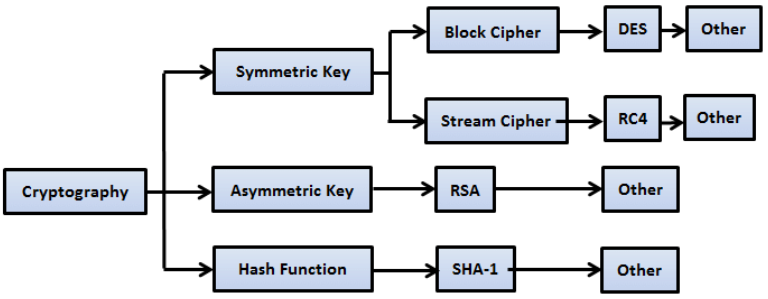
**Fig: IPSec configuration – “sh crypto isa sa” command**

1. All administrators' usernames and passwords should be well managed using a centralized solution or by using AAA user access control, which provides authentication, authorization, and accounting to the connection. TACACS+ protocol is useful for this because it manages all access control. Along with the control in the access, the access controls lists must be implemented in order to filter malicious traffic packets and to implement rate limiting. This is advantageous because external traffic that does not need to access the internal network can be blocked by blocking the source IP address that does not belong to the internal network.
2. A poor router filtering configuration can reduce the overall security of an network, expose internal network components to scans and attacks, and make it easier for attackers to avoid detection. Careful router configuration can help prevent a (compromised) site from being used as part of a distributed denial of service (DDoS) attack, by blocking spoofed source addresses. DDoS attacks use several compromised sites to flood a target site with sufficient traffic or service requests to render it useless to legitimate users.
3. Using Cisco IOS firewall Intrusion Detection System (IDS) is a real-time IDS designed to enhance border router security by detecting, reporting, and terminating unauthorized activity. A unique benefit of implementing an IDS on a router, especially a border router, is that all network traffic flows through it and may be examined.

# Different Cryptographic types of Network Security:

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix graphy means “writing”. (Anon., 2020)

Cryptography techniques are derived from mathematical concepts and a set of rule-based calculations known as algorithms to convert messages in ways that make them difficult to decode. These algorithms are used for cryptographic key generation, digital signing, and verification in order to protect data privacy, internet browsing, and confidential transactions such as credit card and debit card transactions.



### Symmetric Key:

The Secret Key Cryptography (SKC) algorithm, which is primarily used for secrecy and confidentiality and employs a single key for both encryption and decryption, is employed by Symmetric Keys. In general, an encryption system in which the sender and receiver of a message encrypt and decode messages using a single common key. Self-synchronizing stream ciphers or synchronous stream ciphers are used in this type of encryption. The stream ciphers operate on a single bit at a time and use a feedback mechanism to change the key on a regular basis. In self-synchronizing stream ciphers, the decryption process is kept in sync with the encryption process, and each bit in the keystream is calculated as a function of the preceding n bits. Block cipher encrypts one fixed-size block of data at a time. In a block cipher, a given plaintext block always encrypts to the same cipher text when using the same key whereas the same plaintext will encrypt to the different cipher text in a stream cipher.

### Asymmetric Key:

Asymmetric cryptography, also known as Public-key cryptography, refers to a cryptographic algorithm which requires two separate keys, one of which is private and one of which is public. The public key is used to encrypt the message and the private one is used to decrypt the message. The primary benefit of public-key cryptography is that it allows people who have no preexisting security arrangements to exchange messages securely. The need for sender and receiver to share secret keys via some secure channel is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared. Some examples of public-key cryptosystems are Elgamal, RSA, Diffie-Hellman, and DSA, the Digital Signature Algorithm. Because conventional cryptography was once the only available means for relaying secret information in the network, the expense of secure channels and key distribution relegated its use only to those who could afford it, such as governments and large banks (or small children with secret decoder rings). ]

RSA is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public-key cryptography. RSA is widely used in electronic commerce protocols and is believed to be secure given sufficiently long keys and the use of up-to-date implementations. RSA uses a variable size encryption block and a variable size key. The key-pair is derived from a very large number, n, that is the product of two prime numbers chosen according to special rules; these primes maybe 100 or more digits in length each, yielding an n with roughly twice as many digits as the prime factors. The public key information includes n and a derivative of one of the factors of n; an attacker cannot determine the prime factors of n (and, therefore, the private key) from this information alone and that is what makes the RSA algorithm so secure.

### Hash Function:

A cryptographic hash function is an algorithm that takes an arbitrary amount of data input—a credential—and generates a fixed-size output of encrypted text known as a hash value, or simply "hash." That enciphered text can then be saved instead of the password and used to verify the user later. (Anon., 2015)

Certain properties of cryptographic hash functions impact the security of password storage.

* Non-reversibility, or one-way function. A good hash should make it very hard to reconstruct the original password from the output or hash.
* Diffusion, or avalanche effect. A change in just one bit of the original password should result in change to half the bits of its hash. In other words, when a password is changed slightly, the output of enciphered text should change significantly and unpredictably.
* Determinism. A given password must always generate the same hash value or enciphered text.
* Collision resistance. It should be hard to find two different passwords that hash to the same enciphered text.
* Non-predictable. The hash value should not be predictable from the password.

# 

# Test Plan for the Network:

A test plan is established for this section of the component to evaluate all of the network's setup and to see if the deployed network security design's functionality is as intended. The test plan is established, as indicated in the table below, which includes S.No, Date, Test Device, and What to be tested? That is, it goes like this:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| S.N | Date | Test Device | What to be tested? | How to be tested? |
|  | 02 Sept, 2020 | AD Server | User & Group Management  User Rights  And, other configuration test. | For AAA, AD Server is needed and as deployed several Users and group are created which are tested by accessing the router using credentials that are allowed to User which limits some to read only and some to read and write. |
|  | 10 Sept, 2020 | Routers | Password Configuration | With AD server, the routers are configured along with centralized management TACGUI and check AAA for routers by using remote login and try accessing from non-authorize and authorize user. |
|  | Checking Configuration of Access Control List and Verifying It With NAT Verification | By pinging from client end device to the address configured in ACL. |
|  | Routing Protocol Configuration Test Firewall Configuration Test | The protocols like EIGRP, OSPF needs to be tested if they are working properly using tools like tracert. |

**Table: Test Plan for the network**

## 

# Comprehensive Network Test using the Test Plan:

As per the test plan stated above, here are some test in the network which is done to verify the security and the configuration in the network:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Test Step** | | **Tools Used** | | **Expected Output** | | **Actual Output** | **Remarks** |
| 1. **What was tested: ADDS Server Usability** | | | | | | | |
| The ADDS Config page is verify to add user. | | Windows Server 2012 R2 | | The user should be added to the group without any error. | | The user were easily added to the group without any error. | After configuration, it was easy to use the ADDS Server. |
| **Fig: ADDS Server Test** | | | | | | | |
| 1. **What was tested: TACGUI Server (AAA)** | | | | | | | |
| From the same domain, r1 request to login to the r2 using TACACUS+ and TACGUI. | | GNS3 (A network topology) | | The user should login to the router r2 using given credentials. | | The expected output is achieved. | TACGUI is ready for the work as only authenticated user are allowed to access the network. |
| The log in TACACS+: | | | | | | | |
| 1. **What was tested: ACL in r2** | | | | | | | |
| The ACL is configured in r2 and tested through Laptop 2 | | GNS3 (a network topology) | | The laptop should be allowed to access the network as per the list. | | The ACL is failed to configured as expected. |  |
| Configuring in r2:    A user in the network:    **Fig: ACL in r2 test** | | | | | | | |
| 1. **What was tested: Graylog (Routers Centralized Log Management)** | | | | | | | |
| The R1 try to create test log to check VM configuration. | Graylog VM | | The log created by r1 should be registered in Graylog. | | After sending test log, Graylog successfully traced the log. | | The centralize Syslog helps to detect unauthorized logs. |
| **Fig: Syslog Server Test** | | | | | | | |
| 1. **What was tested: VLAN configuration in r1** | | | | | | | |
| A PC connected to r1 is allowed to VLAN 10 only which is of 10.0.0.0 network. | GNS3 | | The PC much get connected with VLAN 10 network and don’t get access to VLAN 20 network which is of 20.0.0.0 | | As expected, the PC worked fine. | | All the VLAN configuration are fine. |
| **Fig: VLAN Configuration Test** | | | | | | | |

**Table: Network Test using Test Plan**

# Conclusion

Finally, this task necessitates network design, which is then secured. The design of the network is provided first, followed by a discussion of how it is configured. The configuration approach is detailed in further detail, including how and why the setting is necessary. Following that, the various cryptographic types are explored, including Hash Function, Asymmetric, and Symmetric key. With all of this documentation, the network is tested using a well-structured test strategy.

# Bibliography

(n.d.). Retrieved from LOGIX: https://blog.logix.in/network-security-devices/

(n.d.). Retrieved from netwrix blog: https://blog.netwrix.com/2019/01/22/network-security-devices-you-need-to-know-about/

(n.d.). Retrieved from comptia: https://www.comptia.org/content/guides/what-is-a-network-protocol#:~:text=A%20network%20protocol%20is%20an,internal%20processes%2C%20structure%20or%20design.

(n.d.). Retrieved from w3school: https://www.w3schools.in/cyber-security/network-protocols-and-its-security/

Adomey, M. K. (n.d.). *itu.int*. Retrieved March 16, 2020, from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/01-Introduction%20to%20Cryptography.pdf

APAN. (n.d.). *APAN.* Retrieved March 12, 2020, from https://apan.net/meetings/apan47/files/36/36-01-01-01.pdf

ARRINGTON, J. (2017). *BestIPHider*. Retrieved March 11, 2020, from https://bestiphider.com/vpn-concentrator/

*cisco.com*. (2019). Retrieved March 02, 2019, from https://www.cisco.com/c/en/us/support/switches/catalyst-2960-24tt-l-switch/model.html

Cisco1. (2019). *Cisco*. Retrieved March 15, 2020, from https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/data\_sheet-c78-732542.html#ProductSpecifications

Cisco2. (2019). *Cisco*. Retrieved September 12, 2019, from https://www.cisco.com/c/en/us/products/collateral/security/asa-firepower-services/datasheet-c78-742475.html

Das, R. (2020). *INFOSEC*. Retrieved March 11, 2020, from https://resources.infosecinstitute.com/category/certifications-training/securityplus/sec-domains/technologies-and-tools-in-security/installing-and-configuring-network-components-to-support-organizational-security/technologies-and-tools-vpn-concentrators/#

*geeksforgeeks*. (2020). Retrieved from https://www.geeksforgeeks.org/cryptography-and-its-types/

*synopsys*. (2015). Retrieved from https://www.synopsys.com/blogs/software-security/cryptographic-hash-functions/