SECURING COMMUNICATIONS BETWEEN DUAL MULTI-CAMPUS CORE

Minor Project Synopsis

Submitted To:-
Prof. Mohanjit Kaur
Submitted By:-
Komaldeep Singh Mangat (1921161/2005011)
Muanpreet Kaur (1921062/1905361)
Banipreet Singh (1921058/1905356)

Department of Information Technology
Guru Nanak Dev Engineering College, Ludhiana

Content

Introduction

We made this project on college campus in which we have shown two different campuses. These campuses are in WAN network. One campus is located in Ludhiana and another one is in Chandigarh. Both are connected with Internet Service Provider (ISP), by which our domains are not secured. It means those domains which are connected with ISP are not secured. In this project we have configured network security which secures our end to end network. The data which is to be transferred in end to end network will be the secured data and it is not read by the center domain. In this we can send our data in encrypted form. To make the data encrypted, we used VPN-GRE (IPSEC) and security algorithm like HMAC(MD5),SHA,3DES.

IMPORTANCE OF PROJECT: Wide Area Networks are spread over a (very) wide area so that companies and institutes that are located far from each other are directly connected via the network. Wide Area Networks have – mostly on more than one location – external connections with other big networks. Internet Service Providers (ISPs) and multinationals with many offices frequently own a WAN themselves. Regional education networks and company networks between several establishments are also examples of Wide Area Networks. Two great advantages of WAN are allowing secure and fast data transmission between the different nodes in the network. Many WANs also implement sophisticated monitoring procedures to account for which users consume the network resources. This is, in some cases, used to generate billing information to charge individual user

SYSTEM ANALYSIS

The existing network consists of hubs and there are dial up connections in between various offices of the College campus because of which both LAN and WAN links are very slow and users regularly face problem in transmitting their data over the links. Most of the time there is network congestion in the network because of which the work is suffering and users are not able to perform up expectation.

In the proposed design, hubs will be replaced with switches so as to improve the LAN connectivity. Switches would be operating at 100 Mbps as compared to hubs which operate at 10 Mbps. Moreover switches are manageable so VLANS can be created on them so as to decrease broadcast traffic and to enhance security as well. As far as WAN is concerned all the dial up links would be replaced with ISDN, Frame-Relay and Leased Line connection so as to

Objectives

1. Objective of the project is to connect various campus of the college by using LAN and WAN technologies.
2. The project aims to assess the security issues related to access control configuration on a Cisco router on the network and to design an upgraded secure configuration using multiple access control techniques.
3. Currently it is observed that the access to the router is exploited using stolen passwords by users on the network.
4. The identified threat has to be mitigated using appropriate feature and technology available on the router and explanation on how it would achieve the requirement such that only the administrator of the network has access to the router.

FEASIBILITY STUDY

1 Economic Feasibility

Economic analysis is the most frequently used method for evaluating the effectiveness of a new system. More commonly known as cost/benefit analysis, the procedure is to determine the benefits and savings that are expected from a candidate system and compare them with costs. If benefits outweigh costs, then the decision is made to design and implement the system.

2 Legal Feasibility

Determines whether the proposed system conflicts with legal requirements, e.g. a Data Processing system must comply with the local Data Protection Acts.

3 Operational Feasibility

Is a measure of how well a proposed system solves the problems, and takes advantages of the opportunities identified during scope definition and how it satisfies the requirements identified in the requirements analysis phase of system development.

METHODOLOGY

- For safe and secure communication between two buildings, suppose MBA Block and Admin Office. Start by establishing a LAN (Local Area Network) in each building and then connect the two buildings by using WAN (Wide Area Network).
- Connect the WAN of both the buildings through routers by applying following protocols such as, EBGP (External Border Gateway Protocol), OSPF (Open Shortest Path First), ISP (Internet Service Provider) etc.
- After the connection is established, the messages which are to be sent are encrypted thoroughly, using some algorithms such as HMAC (Hash- Based Message authentication Code), 3DES (Data Encryption Standard).
- By symmetric Encryption, the data is encrypted and is sent to VPN-GRE tunnel. When message is received, it is decrypted by using the same key.
- Hence our message is reached successfully. For every message which is to be sent is sent by using the same protocols as mentioned above.
- The biggest benefit of using this is that it is feasible and can be managed easily and provide more security than the existing system.
- As we use tunnel like technique which is G.R.E (Generic Routing Encapsulation).In this the data is encapsulated and is sent through more secure path. Which is hidden from the intruders hence providing less chances of data leakage.

REQUIREMENTS OF THE SYSTEM

Hardware :

- Processor: Intel core i3 or above
- Processor Speed: 2.40 GHz CPU
- RAM: 4 GB or above

Network Requirement :

- Network Topology diagram.
- Identify the hardware required like routers, switches, access points (Cisco)
- The network has to be segregated into guest and staff
- The guest network should not have access to the staff network.
- TCP/IP Network design and IP address table.
- Configurations and features which are required to be configured on the devices.

The project aims to assess the security issues related to access control configuration on a Cisco router on the network and to design an upgraded secure configuration using multiple access control techniques. Currently it is observed that the access to the router is exploited using stolen passwords by users on the network. The identified threat has to be mitigated using appropriate feature and technology available on the router and explanation on how it would achieve the requirement such that only the administrator of the network has access to the router

Network and Security requirement:

- Only the administrator should have access to the route.
- The access control should have multiple level of security.
- Users on the network should be unable to access the router.
- Unique passwords should be used wherever appropriate.

REFERENCES

[1]Science Direct “Cryptography Techniques” [Online] Available:
https://www.sciencedirect.com/topics/computer-science/cryptographictechnique [Accessed on: March 15, 2022]

[2] Tutorial Points “Data Encryption Standard” [Online] Available:https://www.tutorialspoint.com/cryptography/
data_encryption$_{s}tandard.htm[Acessedon : March22, 2022]$

[3]Hash-based message authentication codes (HMAC) [Online] Available:
https://cryptography.io/en/latest/hazmat/primitives/mac/hmac/ [Accessed on: April 2, 2022]