E-Learning Network System Design and Analysis

[1]Zaid Hashim Jaber, [2]Hayder Ayad Dawood, [3]Mamoun Jassim Mohammed

[1] Department of Computer Science, College of Science, Baghdad University, Iraq
[2] College of Business Administration , Albayan University, Iraq
[3] Department of Computer Engineering , College of Engineering Al-Iraqia University, Iraq
[1]zaidhashim@gmail.com, [2]hayder.alsultany@gmail.com, [3]Mamoun_87@yahoo.com

Abstract

E-learning system implies skill and knowledge transference in a computerized and networking-based way. Technologies have started to create a difference in education. Accordingly, many universities have adopted learning management system (LMS) to enhance both teaching and learning processes. Mostly, LMS is used in student registration, the delivery and tracking of e-learning courses and content, and in testing as well. However, building such a learning system might lead to encounter certain issues related to scalability, management, and security. The proposed network design has been set to solve such problems. Basically, to manage the accounts' accessibility and privileges, the domain controller server has been used. Network segmentation is proposed to separate the network into multiple broadcast domains to avoid problems related to broadcast like that of a broadcast storm. Lastly, to achieve the scalability, VPN secured tunnels are used to connect several far distance sites through the Internet.

Keywords: E-Learning Network, LMS.

1. Introduction

E-learning is both leads to changing and causes changes in education. It helps understand the way education should be organized and managed. It encourages the educational institutions managers to deal with different activities that require adopting new procedures and finding alternative ways to address emerging challenges that go beyond educational issues [1].
E-learning is a planned teaching process that can occur in different places other than a regular school. For such a system to be invested in distance learning, teaching, communication, creation and management, it requires having certain components and processes. . It further requires special techniques like that course design, particular forms of instructions, special methods of communication through electronic and other technologies, like essential organizational and administrative arrangements [2,11].
Security on the Internet and on Local Area Networks is now at the forefront of computer network related issues [1]. The evolution of networking and the Internet, the threats to information and networks have risen dramatically. Many of these threats have become cleverly exercised attacks causing damage or committing theft. The Internet continues to grow exponentially. As personal, government and business-critical applications become more prevalent on the Internet, there are many immediate benefits. However, these network-based applications and services can pose security risks to individuals as well as to the information resources of companies and government. In many cases, the rush to get connected comes at the expense of adequate network security. Information is an asset that must be protected [2].

- **Issues Related to E-learning System Network Design**

During the last two decades, security issues were given the priority by the computer network researchers when using Internet and Local Area Networks (LAN) in application designs [1].

Apparently, the evolution of the Internet and networking has directed the attention to threats targeting the information and networks in a dramatically way. Many of these risks were cleverly exercised to cause damage or commit theft. That is to say, though the use of internet has entered into personal, government and business-critical applications, causing as a result many immediate benefits, yet it is not void of any disadvantages. That is; such network-based applications and services have led to many security risks to individuals as well as to the information resources of companies and government. A case in point is when one rushes to get connected without checking whether the network security being connected to is protected, safe or adequate. [2]

The issue of security has grown more and more with the development of personal computers, LANs, and the wide-open world of the Internet; this is because the networks of today has become more open. As e-business and Internet applications continue to grow, finding the balance between being isolated and being open considered as a critical task.

Firewall devices are software or hardware that enforce an access control policy between two or more networks. Such technology were introduced in businesses to create a kind of balance between security and simple outbound access to the Internet, as the ones used for e-mail and Web surfing services. Network security is the most vital component in information security. This is because it helps secure all information passed through networked computers [3, 4].

As the computers and networked systems increased in their popularity, the need for having reliable computers and network security has become increasingly necessary and essential. This is because such an increase opposes an increase in the number of various kinds of internet threats. Speaking of the campus network, it is critical and plays an important role in any organization. Accordingly, network architecture and security has become as important as air, water, food, and shelter. Computer network security threat and architecture are highly critical issues. Apparently, the security may include identification, authentication and authorization, and surveillance camera to protect integrity, availability, accountability, and authenticity of computer hardware or network equipment. There is no ready-made procedure to be followed when designing a secure network. Generally any design should take into account the needs of an organization [5,6].

Recently, the infrastructure of the designed network has become a critical part of some IT organizations. It is urgently needed to support future expansion in a reliable, scalable and secure manner. These considerations in designing a network require from the designer to define the client's unique situation, i.e., the current technology, application, and data architecture. To make an e-learning system for universities, a physical network infrastructure is required for a contemporary university network. University Management and IT manager can identify the kind of network they want to set up, the upcoming plans, and its expected growths. Contingencies for the future area, power, and another resource must be part of the physical layout of a university. Building a contemporary university network atmosphere also demands functional as well as safety elements that go beyond IT department’s obligations and skills[7].

However, there are some other issues that might be encountered when designing a network. These include the following: management, scalability, availability, and integrity. The present research is concerned with proposing a network design to improve the network performance of the e-learning system. Accordingly,

the rest of the sections of the paper will be dedicated to conduct a survey for the available literature review. Then, it will be followed a section on the initial network design and the proposed enhanced network design. Later, the main steps of the network configuration and the results will be examined and discussed. After that the conclusion will be summarized and finally suggestions for future works will be highlighted [8].

2. Literature Review

Lalita Kumari et al., introduced various problems that were related to current network information security together with their solutions. They represented the current security status of the campus network, analyzed security threats to the campus network and finally described the strategies that help maintain such security [3].

Ramaswamy described and analyzed three generations of network segmentation techniques – Virtual Switches and Physical NIC-based, VLAN-based and Overlay-based, as well as the overlay-based virtual network segmentation and its characteristics, such as scalability and ease of configuration. Cloud Data centers are generally made up of Virtualized hosts. Network Segmentation (Isolation), Traffic flow control using firewalls and IDS/IPS are basic components that are needed to form the primary network-based security techniques where the first one represents the foundation to the other two [7].

Neal Wagner, et al., examined an alternative method for evaluating the segmentation of architectures . This objective was met by using a continuous-time Markov chain that helps model the changes in the network state based on relevant network parameters, like that of vulnerability arrival rate, patch rate, etc. The model was realized by an event-based network simulation and demonstrated via a case study to evaluate a range of candidate architectures [8].

Jiejun, et. al., c a multi-layer alternative and compared the latter to a link layer approach. Results have shown that the multi-layer architecture provides better services. That is; an efficient cross-domain mobility and an effective security protection was provided to wireless communications across heterogeneously managed network domains. The researchers further implemented a point-to-point layer-independent security model and a differentiated policy management model to realize the multi-layer architecture. The implementation and experiments confirmed once more the efficiency and effectiveness of the suggested design [9].

Umesh discussed the tools and solutions available for network management. He further discussed the challenges involved in implementing such network management solutions and proposed a simple solution for a pro-active network management solution. This solution was tested by implementing the previously proposed solution in a large enterprise. The implementation made the stakeholders able to achieve higher efficiency and do proactive network management [10].

3. Proposed enhanced System design

The proposed system is mainly a modified campus network through which the higher authority can directly contact any employee/staff/department. This system helps recall the individual e-mailing system. Such e-mails can be done through different communicating network tools; however, the suggested system is fully maintained by the university authority itself. This feature by itself helps the university authority ensure security without relying on those communicating networking tools; this is because the system is secured by itself, and so different network threats will be prevented by themselves. Such a feature increases the capability of the university authority as well as maintains their privacy.

However, this section illustrates two types of schematic diagrams that revolve around the E-learning network design. The former demonstrates the traditional (simple) schematic diagram of e-learning network whereas the latter illustrates the suggested enhanced e-learning network design. The following figure illustrates the initial schematic diagram of the e-learning network.

As it is seen, the schematic diagram contains a data center which consists of a database and a web application server as the main servers. This data center is connected to the inside hosts of other departments through a switched network. The diagram further includes a figure that in return contains wireless users connected to the datacenter using point to point WLAN (2.4 GHz or 5 GHz).

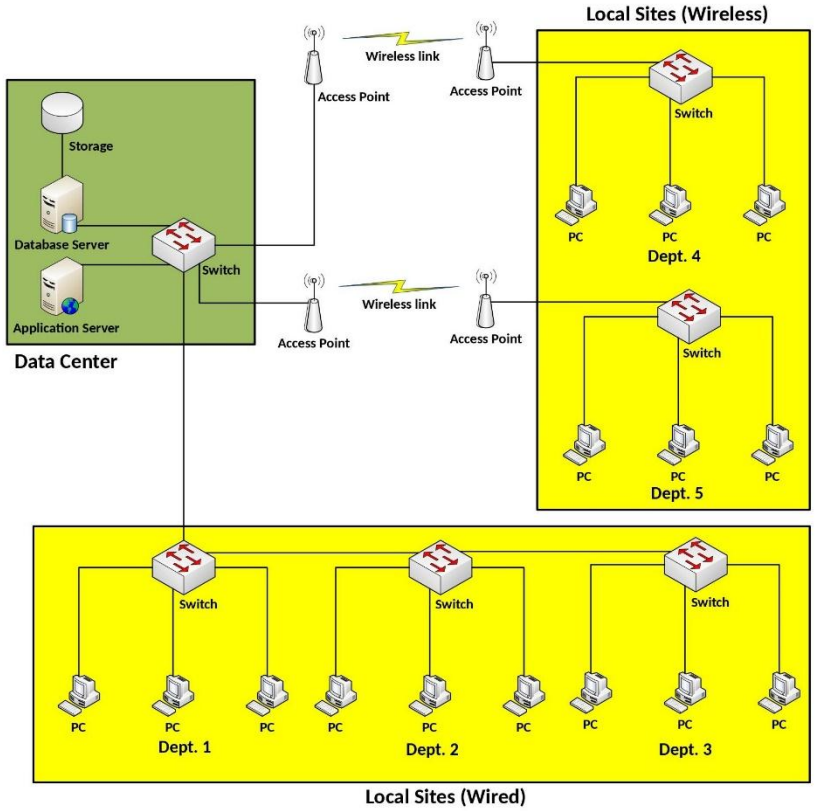

Figure 2. Schematic Diagram of the Designed E-learning Network

The main advantage of using wireless connection is to allow the departments which are in different buildings to be connected to the main network. The model of all switches that is used in Figure 1 is Cisco Catalyst 2960.

However, there were some other encountered in this suggested network, like that of Network segmentation, Multi-layer security, Management issue and Scalability issue. Speaking of network segmentation, it consists of two main issues: broadcast domain and broadcast storm.

A. Network segmentation: - all hosts including the wireless hosts are connected to the same broadcast domain; a matter which causes high traffic issue. For example, when any host sending a broadcast, the latter will reach all hosts connected to this network, including the servers in the datacenter.

However, in some cases, the broadcast may cause broadcast storm when STP (Spanning Tree Protocol) is not enabled in the switches.

B. The Multi-layer security issue contains the following issues:-

- Application layer issue: - The terms non-central authentication and privilege mean that non-legit station can access the system.
- Link layer issue includes the following: -
- Broadcast domain issue as it is illustrated in Network segmentation issue; and
- Wireless security and disturbances because the frequency bands (2.4 GHz and 5 GHz) are un-license bands and available to public.

C. Management issue:-

This network does not contain specific station or server for managing purposes or any other devices. Besides, there is no log and auditing system to monitor the activities of the devices and users in the network.

D. Scalability issues:-

As it shown in Figure 1, the network is suitable for connecting hosts within short distance in wired stations using a wire network. the distance was approximately from 100 to 150 meters whereas for wireless users using WLAN, it was 1 to 2 KM depending on the signal strength, the surrounding interference and on obstacles.

In this section, the enhance network design has been proposed to overcome the above mentioned issues through:-

After illustrating the simply designed network for e-learning system and for facing potential issues, the researchers will demonstrate the way the proposed network design is enhanced to overcome the above mentioned problems through several solutions as shown in Figure two.

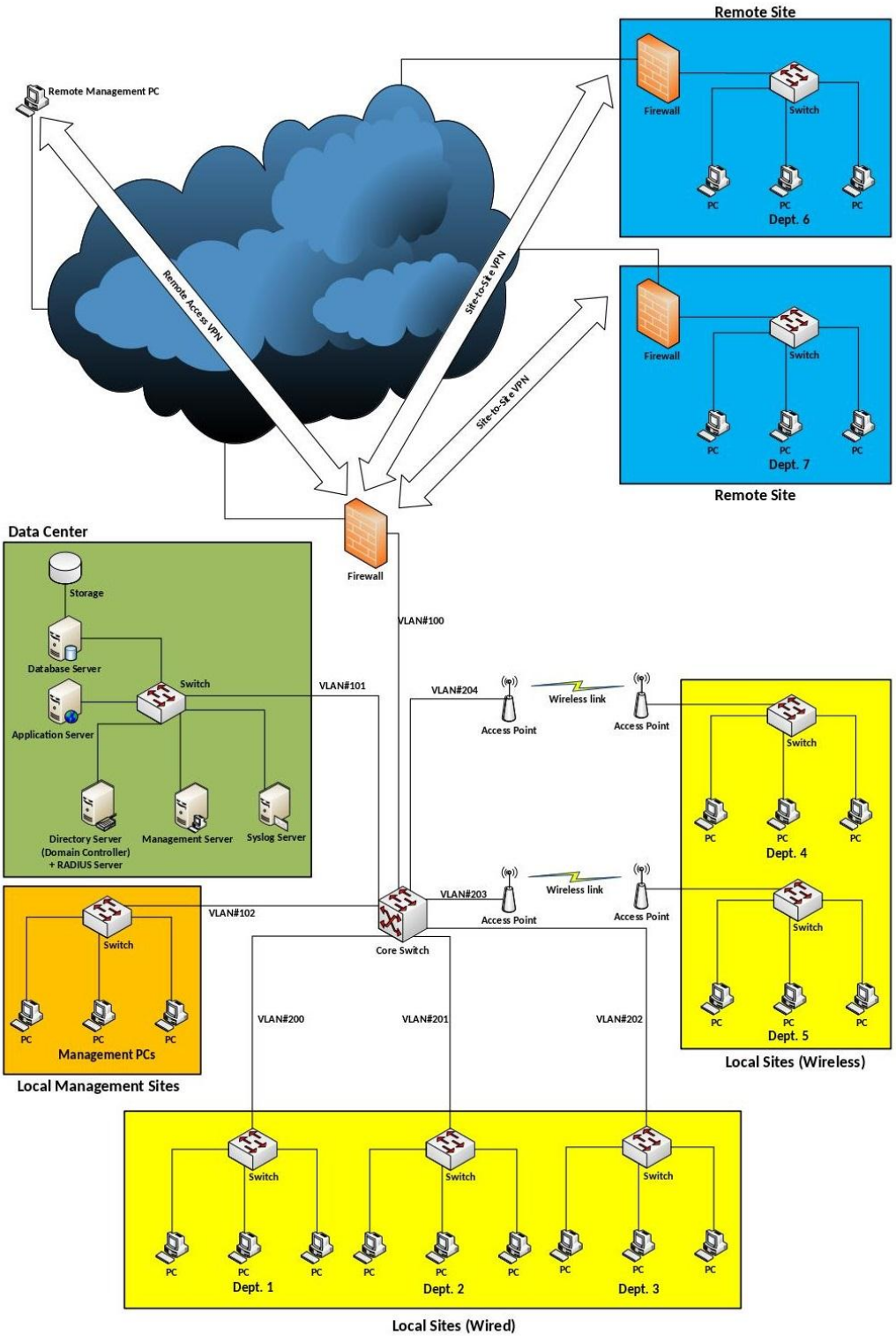

Figure 2 an enhanced network design

To overcome the single broadcast domain issue, a core switch, Cisco Catalyst Multilayer switch, was proposed to isolate the broadcast domain of datacenter; ie., each of the wired and remote departments. Such a step was accomplished by assigning a unique VLAN ID for datacenter and for the other wired and wireless departments. The core switch was also used to route the traffic from the datacenter to other departments and vise-versa. As for DHCP server for all VLANs, it was used to avoid the manual IP address configuration for hosts.

In addition to the primary servers (database and application server) in the data center, there were also two additional physical servers. The first server consisted of the domain controller and RADIUS server. The domain controller was used to make users' profile with a permission and privilege to the system. The RADIUS server, on the other hand, was used for obtaining the central credentials (username and password) of other network devices. Consequently, the authentication to the stations and network devices was central rather than local. The second server was the Syslog and NTP server; the Syslog server was used to record the different network activities whereas the NTP server was used to synchronize the clock of all other terminals in the system and was needed for the log time in the Syslog server.

WiFi Access II (WPA2) can be used to solve the wireless security through encrypting the wireless point to point's connections and making the difference between the two channels equal to40 GHz. Such a step helps avoid the interference with another possible wireless security of hidden SSID and MAC filtering.

The management issue was the main problem in each data center; it helps prevent the random access and control non-legit met connection. The domain controller server is proposed to solve this problem by controlling each of the stations connected to the system and by ensuring the availability of a secured connection and controlled privilege for each user using dedicated VLAN. For managing the Network operation center (NOC) purposes, the administrator needs to configure all the setup by accessing the management server first via RDP. Basically, this server contains all the required management tools like putty for SSH connection and RDP for remote desktop connection. Further, the management server can be used as SNMP server for critical states of the system.

Connecting far-distance sites in other cities can increase scalability. This action can be done by creating a site to site a secured VPN tunnel between the central site and the remote sites through using an unsecured public internet connection. Each site needs one public IP address and a firewall which is Cisco ASA for establishing site to site VPN connection. Internet can be used for management and emergencies purposes to configure the devices and server from the outside. This is done by establishing a Remote Access VPN connection between the PC management and the local site which contains the data center through the internet.

4. Configuration and discussion
   This section shows the main configuration of the network devices in the data center and the remote branches based on the information shown in Table 1.

Table 1 IP address Info

No.	Server name	Description	IP address
Data Center Network Devices			
1	Data Center Core Switch	VLAN 100 (Core switch to ASA)	192.168.100.1
		VLAN 101 (Data Center)	192.168.101.1
		VLAN 102(MGMT)	192.168.102.1
		VLAN 200(Dept.1)	192.168.200.1

		VLAN 201(Dept.2)	192.168.201.1
		VLAN 202(Dept.3)	192.168.202.1
		VLAN 203(Dept.4)	192.168.203.1
		VLAN 204(Dept.5)	192.168.204.1
2	Data Center Firewall	Private (VLAN 100)	192.168.100.2
		Public	Assigned by ISP
Servers			
1	Database	VLAN 101	192.168.101.2
2	Application	VLAN 101	192.168.101.3
3	Domain Controller + RADIUS	VLAN 101	192.168.101.4
4	Syslog + NTP	VLAN 101	192.168.101.5
Local Sites			
1	MGMT stations	VLAN 102	192.168.102.0/24
2	Dep.1 Stations	VLAN 200	192.168.200.0/24
3	Dep.2 Stations	VLAN 201	192.168.201.0/24
4	Dep.3 Stations	VLAN 202	192.168.202.0/24
5	Dep.4 Stations	VLAN 203	192.168.203.0/24
6	Dep.5 Stations	VLAN 204	192.168.204.0/24
Remote Sites			
1	Remote Branch1 Firewall	Public	Assigned by ISP
		Private	172.31.1.1
2	Remote Branch2 Firewall	Public	Assigned by ISP
		Private	172.31.2.1
3	Remote Branch1 Stations		172.31.1.0/24
4	Remote Branch2 Stations		172.31.2.0/24

First to configure the steps below are needed to configure core switch (Catalyst Cisco Multilayer Switch 3750) in the data center

1- Assign the ports to specific VLANs

```
!interface connected to Cisco ASA 5510
interface FastEthernet0/1
      switchport access vlan 100
      switchport mode access
!
!interface connected to Data Center
interface FastEthernet0/2
      switchport access vlan 101
      switchport mode access
!
!interface connected to MGMT
interface FastEthernet0/3
      switchport access vlan 102
      switchport mode access
!
!interface connected to Dept.1
interface FastEthernet0/3
      switchport access vlan 200
      switchport mode access
!
!interface connected to Dept.2
interface FastEthernet0/3
      switchport access vlan 201
      switchport mode access
!
!interface connected to Dept.3
interface FastEthernet0/3
      switchport access vlan 202
      switchport mode access
!
!interface connected to Dept.4
interface FastEthernet0/3
      switchport access vlan 203
      switchport mode access
!
!interface connected to Dept.5
interface FastEthernet0/3
      switchport access vlan 204
      switchport mode access
```

2- Assign IP addresses to each VLAN

```
!IP address of Core Switch-to-ASA VLAN
interface Vlan100
      ip address 192.168.100.1 255.255.255.0
!
!IP address of Data Center VLAN
interface Vlan101
      ip address 192.168.101.1 255.255.255.0
!
!IP address of MGMT VLAN
interface Vlan102
      ip address 192.168.102.1 255.255.255.0
!
!IP address of Dept.1 VLAN
interface Vlan200
      ip address 192.168.200.1 255.255.255.0
!
!IP address of Dept.2 VLAN
interface Vlan201
      ip address 192.168.201.1 255.255.255.0
!
!IP address of Dept.3 VLAN
interface Vlan202
      ip address 192.168.202.1 255.255.255.0
!
!IP address of Dept.4
interface Vlan203
      ip address 192.168.203.1 255.255.255.0
!
!IP address of Dept.5 VLAN
interface Vlan204
      ip address 192.168.204.1 255.255.255.0
```

3- Configure DHCP Server for all VLANs except Data Center VLAN (Note that the DHCP Pool for all VLANs is from Host ID= 50 to Host ID= 100 and the DNS for all VLANs is the IP address of Domain Controller which is 192.168.101.4)

```
!Exclude all the IP address from DHCP Pools
ip dhcp excluded-address 192.168.102.1 192.168.102.49
ip dhcp excluded-address 192.168.102.101 192.168.102.254
ip dhcp excluded-address 192.168.200.1 192.168.200.49
ip dhcp excluded-address 192.168.200.101 192.168.200.254
ip dhcp excluded-address 192.168.201.1 192.168.201.49
ip dhcp excluded-address 192.168.201.101 192.168.201.254
ip dhcp excluded-address 192.168.202.1 192.168.202.49
ip dhcp excluded-address 192.168.202.101 192.168.202.254
ip dhcp excluded-address 192.168.203.1 192.168.203.49
ip dhcp excluded-address 192.168.203.101 192.168.203.254
ip dhcp excluded-address 192.168.204.1 192.168.204.49
ip dhcp excluded-address 192.168.204.101 192.168.204.254
!
!DHCP pool for MGMT VLAN
ip dhcp pool MGMT VLAN
      network 192.168.102.0 255.255.255.0
      default-router 192.168.102.1
      dns-server 192.168.101.4
!
!DHCP pool for Dept.1 VLAN
ip dhcp pool Dept.1 VLAN
      network 192.168.200.0 255.255.255.0
      default-router 192.168.200.1
      dns-server 192.168.101.4
!
!DHCP pool for Dept.2 VLAN
ip dhcp pool Dept.2 VLAN
      network 192.168.201.0 255.255.255.0
      default-router 192.168.201.1
      dns-server 192.168.101.4
!
!DHCP pool for Dept.3 VLAN
ip dhcp pool Dept.3 VLAN
      network 192.168.202.0 255.255.255.0
      default-router 192.168.202.1
      dns-server 192.168.101.4
!
!DHCP pool for Dept.4 VLAN
ip dhcp pool Dept.4 VLAN
      network 192.168.203.0 255.255.255.0
      default-router 192.168.203.1
      dns-server 192.168.101.4
!
!DHCP pool for Dept.5 VLAN
ip dhcp pool Dept.5 VLAN
      network 192.168.204.0 255.255.255.0
      default-router 192.168.204.1
      dns-server 192.168.101.4
```

4- Enable IP routing and configure the required routes

```
!Enable IP routing
ip routing
!
!Default route to Cisco ASA 5510
ip route 0.0.0.0 0.0.0.0 192.168.100.2
```

5- Configure the core switch as RADIUS client and connect it to the RADIUS server (IP address of the RADIUS server is 192.168.101.4)

```
!Enable authentication and authorization through RADIUS Server
aaa new-model
aaa authentication login default group radius local
aaa authorization exec default group radius group radius local
!
!Define RADIUS Server and its secret key
radius-server host 192.168.101.4 auth-port 1645 key SECRET1
!
!Enable SSH authentication through RADIUS server
line vty 0 4
      login authentication default
      transport input ssh
line vty 5 15
      login authentication default
      transport input ssh
```

6- Configure the core switch as Syslog and NTP client and connect it to the Syslog and NTP server (IP address of the Syslog server is 192.168.101.5)

```
!Connect to Syslog server
logging trap debugging
logging 192.168.101.5
!
!Connect to NTP server
ntp server 192.168.101.5 key 0
```

7- Configure the necessary access control list to prevent all VLANs (except MGMT VLAN) and the remote branches to access the Data Center VLAN using RDP and SSH.

```
!Access list that deny remote sites from accessing Data Center using
RDP or SSH
access-list 101 deny tcp 172.31.0.0 0.0.255.255 192.168.101.0
0.0.0.255 eq 3389
access-list 101 deny udp 172.31.0.0 0.0.255.255 192.168.101.0
0.0.0.255 eq 3389
access-list 101 deny tcp 172.31.0.0 0.0.255.255 192.168.101.0
0.0.0.255 eq 22
access-list 101 permit ip 172.31.0.0 0.0.255.255 192.168.101.0
0.0.0.255
!
!Access list that deny local sites (except MGMT VLAN) from accessing
Data Center using RDP or SSH
access-list 102 permit tcp 192.168.102.0 0.255.255.255 192.168.101.0
0.0.0.255 eq 3389
access-list 102 permit udp 192.168.102.0 0.255.255.255 192.168.101.0
0.0.0.255 eq 3389
access-list 102 permit tcp 192.168.102.0 0.255.255.255 192.168.101.0
0.0.0.255 eq 22
access-list 102 deny tcp 192.168.0.0 0.0.255.255 192.168.101.0
0.0.0.255 eq 3389
access-list 102 deny udp 192.168.0.0 0.0.255.255 192.168.101.0
0.0.0.255 eq 3389
access-list 102 deny tcp 192.168.0.0 0.0.255.255 192.168.101.0
0.0.0.255 eq 22
access-list 102 permit ip 192.168.0.0 0.0.255.255 192.168.101.0
0.0.0.255
!
!Access list that deny remote sites from accessing Data Center using
RDP or SSH
interface Vlan100
      ip access-group 102 in
interface Vlan101
      ip access-group 101 out
```

Then configure the local firewall ASA (Cisco ASA 5510) to provide site-site VPN connection to remote branches (the public IP address is required for the outside interface and assigned by ISP).

1- Configure the interfaces (IP address, name and security level)

```
!Outside interface connected to Internet (Public IP address is
assigned by ISP)
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address DataCenterPublicIPAdd DataCenterPublicSubMask
!
!Inside interface connected to Core Switch
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 192.168.100.2 255.255.255.0
```

2- Configure necessary routes

```
!Outside route connected to Internet (Assigned by ISP)
route outside 0.0.0.0 0.0.0.0 DataCenterDefGat
!
!Inside route connected to internal network via Core Switch
route inside 192.168.0.0 255.255.0.0 192.168.100.1
```

3- Configure the Internet Security Association and Key Management Protocol (ISAKMP) policies for IKEv1 (authentication, encryption, hash, Diffie-Hellman and lifetime) and enable IKEv1 on the outside interface that terminates the VPN tunnel

```
!ISAKMP Policies for IKEv1
crypto ikev1 policy 10
       authentication pre-share
       encryption aes-256
       hash sha
       group 5
       lifetime 86400
!
!Enable IKEv1 on the outside interface
crypto ikev1 enable outside
```

4- Configure IKEv1 transform set to protect data transferred and IPSec SA lifetime

```
!IKEv1 transform-set
crypto ipsec ikev1 transform-set TS esp-aes-256 esp-sha-hmac
!
!IPSec SA lifetime
crypto ipsec security-association lifetime seconds 86400
```

5- Configure ACLs (Access Control List) for interesting traffic, one for each remote site

```
!ACL for interesting traffic to Remote Site 1
access-list RS1 extended permit ip 192.168.1.0 255.255.255.0
172.31.1.0 255.255.255.0
access-list RS1 extended permit ip 192.168.101.0 255.255.255.0
172.31.1.0 255.255.255.0
!
!ACL for interesting traffic to Remote Site 2
access-list RS1 extended permit ip 192.168.1.0 255.255.255.0
172.31.2.0 255.255.255.0
access-list RS1 extended permit ip 192.168.101.0 255.255.255.0
172.31.2.0 255.255.255.0
```

6- Configure LAN-to-LAN tunnels, one for each Remote Site

```
!Substitute the tunnel-group name with the public IP addresses of
the remote firewall
!Tunnel group for Remote Site 1
tunnel-group Branch1IPAdd type ipsec-l2l
tunnel-group Branch1IPAdd ipsec-attributes
      ikev1 pre-shared-key SiteSecret1
!
!Tunnel group for Remote Site 2
tunnel-group Branch2IPAdd type ipsec-l2l
tunnel-group Branch2IPAdd ipsec-attributes
      ikev1 pre-shared-key SiteSecret2
```

7- Configure the crypto maps (one for each Remote Site) then apply them to the outside interface

```
!Crypto map for Remote Site 1 (peer IP address is assigned by peer ISP)
crypto map Outside_Map 10 match address RS1
crypto map Outside_Map 10 set peer Branch1PublicIPAdd
crypto map Outside_Map 10 set security-association lifetime seconds
86400
!
!Crypto map for Remote Site 2 (peer IP address is assigned by peer ISP)
crypto map Outside_Map 11 match address RS2
crypto map Outside_Map 11 set peer Branch2PublicIPAdd
crypto map Outside_Map 11 set security-association lifetime seconds
86400
!
!Apply crypto map to outside interface
crypto map Outside Map interface outside
```

8- Configure the local firewall as Syslog and NTP client

```
!Connect to Syslog server
logging enable
logging trap debugging
logging host inside 192.168.101.5
!
!Connect to NTP server
ntp server 192.168.101.5
```

9- Configure the local firewall as RADIUS client

```
!Connect to RADIUS server
aaa-server AuthOutbound (inside) host 192.168.101.4
      key SECRET2
```

For remote firewalls (Cisco ASA 5505) in branch1 and branch2 the following steps are applied to establish the connection between them and the local firewall (Cisco ASA 5510) in the datacenter (these steps are used in the firewall in branch1 and can be applied to firewall in branch2 with few changes in parameters like the IP addresses and access control list).

1- Configure the remote firewall interfaces (IP address, name and security level)

```
!Outside interface connected to Internet (Public IP address is
assigned by ISP)
interface Vlan2
 nameif outside
 security-level 0
 ip address Branch1IPAdd Branch1SubMask
!
!Inside interface connected to internal network
interface Vlan1
 nameif inside
 security-level 100
 ip address 172.31.1.1 255.255.255.0
```

2- Configure the default routes

```
!Outside route connected to Internet
route outside 0.0.0.0 0.0.0.0 Branch1DefGat
```

3- Configure it as DHCP server

```
!DHCP server configuration
dhcpd address 172.31.1.10-172.31.1.30 inside
dhcpd dns 192.168.101.4
```

4- Configure the Internet Security Association (SA) and the Key Management Protocol (ISAKMP) policies for IKEv1 (authentication, encryption, hash, Diffie-Hellman and lifetime) and enable IKEv1 on the outside interface that terminates the VPN tunnel

```
!ISAKMP Policies for IKEv1
crypto ikev1 policy 10
       authentication pre-share
       encryption aes-256
       hash sha
       group 5
       lifetime 86400
!
!Enable IKEv1 on the outside interface
crypto ikev1 enable outside
```

5- Configure IKEv1 transform set to protect the data transferrd and IPSec SA lifetime

```
!IKEv1 transform-set
crypto ipsec ikev1 transform-set TS esp-aes-256 esp-sha-hmac
!
!IPSec SA lifetime
crypto ipsec security-association lifetime seconds 86400
```

6- Configure the ACL (Access Control List) for the interesting traffic to the Data Center

```
!ACL for interesting traffic to Remote Site 1
access-list LS extended permit ip 172.31.1.0 255.255.255.0
192.168.1.0 255.255.255.0
access-list LS extended permit ip 172.31.1.0 255.255.255.0
192.168.101.0 255.255.255.0
```

7- Configure LAN-to-LAN tunnel to the Data Center

```
!Substitute the tunnel-group name with the public IP addresses of
the local firewall
!Tunnel group to the Data Center
tunnel-group DataCenterPublicIPAdd type ipsec-l2l
tunnel-group DataCenterPublicIPAdd ipsec-attributes
      ikev1 pre-shared-key SiteSecret1
```

8- Configure the crypto map then apply them to the outside interface

```
!Crypto map configuration
crypto map Outside_Map 10 match address LS
crypto map Outside_Map 10 set peer DataCenterPublicIPAdd
crypto map Outside_Map 10 set security-association lifetime seconds
86400
!
!Apply crypto map to outside interface
crypto map Outside_Map interface outside
```

9- Configure the remote firewall as Syslog and NTP client

```
!Connect to Syslog server
logging enable
logging trap debugging
logging host inside 192.168.101.5
!
!Connect to NTP server
ntp server 192.168.101.5
```

10- Configure the remote firewall as RADIUS client

```
!Connect to RADIUS server
aaa-server AuthOutbound (inside) host 192.168.101.4
      key SECRET2
```

```
!Outside interface connected to Internet
interface Vlan1
 nameif outside
 security-level 0
 ip address Branch2IPAdd Branch2SubMask
!
!Inside interface connected to internal network
interface Vlan2
 nameif inside
 security-level 100
 ip address 172.31.2.1 255.255.255.0
```

Conclusion

In this work, an enhanced E-learning system has been proposed. For managing the accounts' accessibility and privileges, a domain controller server has been introduced, and a network segmentation was intended to separate the network into multiple broadcast domains to avoid broadcast problems, like that of a broadcast storm. Besides, to achieve the scalability, VPN secured tunnels have been used to connect several far distance sites through the Internet. To conclude, by applying the proposed approaches in securing and managing the network parts, the e-learning system has been given a high level of stable performance in the aspect of stability, integrity, confidently on both the network and application layer.

Future Work

- High availability – Redundancy

Peer-to-peer storage aims to build large-scale, reliable and available storage from many small-scale unreliable, low-availability distributed hosts. Data redundancy is the key to any data guarantees. However, preserving redundancy in the face of highly dynamic membership is costly. Consequently, the researchers used a simple resource usage model to measure the behavior from the Gnutella file-sharing network. This usage helps to argue that the large-scale cooperative storage is limited by likely dynamics and cross-system bandwidth - not by local disk space. The researchers further examined some bandwidth optimization strategies, like the delayed response to failures, admission control, and the load-shifting. They found that such strategies do not alter the underlying problem. Accordingly, they concluded that when redundancy, data scale, and dynamics are all high, the needed cross-system bandwidth is unreasonable.

- Encryption (network level) for intranet users
  With the improvement of information level, more and more enterprises are conscious of the importance of the intranet security. Usually, a variety of means, such as IDS, IPS, firewalls, and VPN are utilized to ensure that the intranet can work correctly. However, they only defend attacks from an external network; this is because all these measures are based on the assumption that the internal network is reliable. However, the reality is often not like this. According to the survey of FBI/CSI, more than 80% attacks come from internal staffs. They may bring viruses into intranet with the mobile disk, and take sensitive information away from the intranet. If no useful measure is devised to manage the whole internal network, the internet is then considered unreliable and uncontrollable.
- SAN for data storage
  With the increasing requirement for large storage repositories, network storage has become essential for massive data storage. Vast amounts of new data are generated by humans every year. Humans and applications use data in various formats, including texts, video, audio, and images. It is very much vital for the network storage system to have a high capacity, high availability and scalable. With the help of SAN and NAS, storage can be efficiently utilized. Both technologies alleviate the need to eliminate direct-attached storage to aid more flexible storage access. SAN and NAS use open industry-standard network protocols to provide storage facility. NAS uses NFS and CIFS protocol, and SAN uses the iSCSI, FCP and FCoE protocols to ensure the facility of the storage.

REFERENCES

[1] Akin T.," Hardening Cisco Routers," O'Reilly & Associates, 2002.
[2] Kim J., Lee K., Lee C.," Design and Implementation of Integrated Security Engine for Secure Networking," In Proceedings International Conference on Advanced Communication Technology, 2004.
[3] Chen S., Iyer R., and Whisnant K., "Evaluating the Security Threat of Firewall Data Corruption Caused by Instruction Transient Errors," *In Proceedings of the 2002 International Conference on Dependable Systems & Network, Washington, D.C., 2002.*
[4] Kim H., "Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, FEBRUARY 2004.
[5] Security Problems in Campus Network and Its Solutions, 1Lalita Kumari, 2Swapan Debbarma, 3Radhey Shyam, Department of Computer Science1-2, NIT Agartala, India, National Informatics Centre, India.
[6] Network Security: History, Importance, and Future "University of Florida Department of Electrical and Computer Engineering Bhavya Daya ".
[7] Ramaswamy Chandramouli, "Analysis of Network Segmentation Techniques in Cloud Data Centers", National Institute of Standards & Technology 100 Bureau Drive, Gaithersburg, MD, USA.
[8] Wagner, Neal & Sahin, Cem Safak & Pena, Jaime & Riordan, James & Neumayer, Sebastian. (2017). Capturing the Security Effects of Network Segmentation via a Continuous-Time Markov Chain Model. 17. 10.22360/springsim.2017.anss.032.

[9] Kong, Jiejun & Gerla, Mario & S Prabhu, B & Gadh, Rajit. (2018). Providing multi-layer security support for wireless communications across multiple trusted domains.
[10] Hodeghatta Rao, Umesh. (2011). Challenges of Implementing Network Management Solution. International Journal of Distributed and Parallel systems. 2. 10.5121/ijdps.2011.2506.
[11] P. Oliveira, C. Cunha and M. Nakayama, "Learning Management Systems (LMS) and e-learning management: an integrative review and research agenda", JISTEM, vol.13 no.2, Aug. 2016.