ST. XAVIER’S COLLEGE

**(Affiliated to Tribhuvan University)**

Maitighar, Kathmandu



**END SEMESTER MINOR PROJECT CHAPTER 2**

**ON**

**“सुरक्षित कार्यालय”-** **A Network Security Design Proposal for Small Organizations (CSC-404)**

For the partial fulfillment of the requirement for the degree of Bachelor of Science

in Computer Science and Information Technology awarded by Tribhuvan University

**Under the supervision of**

**Er.Rajan Karmacharya**

**Supervisor/Lecturer**

**Submitted by**

**Suyoj Man Tamrakar (TU Roll No. – 4778/071)**

**Submitted to**

ST. XAVIER’S COLLEGE

**Department of Computer Science**

**Maitighar, Kathmandu, Nepal**

**6th May, 2018**

**CHAPTER 2: LITERATURE REVIEW**

**2.1 Background and Research**

Information and communication are two of the most important strategic issues for the success of every enterprise. While today nearly every organization uses a substantial number of computers and communication tools (telephones, fax, and personal handheld devices), they are often still isolated. While managers today are able to use the newest applications, many departments still do not communicate and much needed information cannot be readily accessed [1].

Computer networks allow the user to access remote programs and remote databases either of the same organization or from other enterprises or public sources. Computer networks provide communication possibilities faster than other facilities. Because of these optimal information and communication possibilities, computer networks may increase the organizational learning rate, which many authors declare as the only fundamental advantage in competition [2].

The requirement for communications has evolved as networks have evolved. There is a need to exchange information. For most of mankind’s history the speed at which information could be shared over a long distance depended on how fast a messenger could run or ride a horse [3]. It was not until the mid-nineteenth century, with the widespread use of the telegraph and later the telephone and radio communications, that it became possible to communicate information between different parts of the world in real time. It was some years after the development of the computer that the need to provide remote access to information arose. Initially, teletypewriter terminals were used to access mainframe computers to carry out remote job entry by inputting from paper tape readers and outputting to the teletype printer [4].

Security on the Internet and on Local Area Networks is now at the forefront of computer network related issues. 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 [5]. 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 [6].

Network attacks have been discovered to be as varied as the system that they attempt to penetrate. Attacks are known to either be intentional or unintentional and technically competent intruders have been interested in targeting the protocols used for secure communication between networking devices [7].This review addresses how highly sophisticated intruders are penetrating internet networks despite high levels of security. But as the intruders increase, the network experts are deriving many techniques in preventing attackers from accessing company networks.

**2.2 The Origin and Development of Network Security**

The first computer networks consisted of the military ARPANET and university computers connected to each other through it. Over time, this framework would evolve into the Internet and open a vast range of opportunities for individuals and institutions to interact online. The development of these early networks saw the emergence of threats to them and the need to protect valuable data [8].

During the 1980's and 90's, hackers began to emerge as a serious threat to network security. Computer attacks aimed at government, military, and commercial networks became more serious. The increased danger prompted The Computer Fraud and Abuse Act of 1986 and the first Computer Emergency Response Team (CERT) to address the issue and educate computer users about security issues [9].

With the 1990's came the Internet explosion and a whole new level of threats to networks and your own personal information. In response to the risks, network security experts developed better encryption methods, Internet protocols, and secure socket layer technologies to protect against malware, hacking and identity theft [10].

**2.3 VLAN and its Importance in Network Security**

A VLAN allows several networks to work virtually as one LAN. One of the most beneficial elements of a VLAN is that it removes latency in the network, which saves network resources and increases network efficiency. In addition, VLANs are created to provide segmentation and assist in issues like security, network management and scalability. Traffic patterns can also easily be controlled by using VLANs [11].

The key benefits of implementing VLANs include:

1. Allowing network administrators to apply additional security to network communication.
2. Making expansion and relocation of a network or a network device easier
3. Providing flexibility because administrators are able to configure in a centralized environment while the devices might be located in different geographical locations.
4. Decreasing the latency and traffic load on the network and the network devices, offering increased performance [12].

**2.3.1 Techniques to Configure VLAN**

#### 2.3.1.1 Port Based VLAN

In this case, the VLAN has a set of physical ports with one or more routers. Each router may have a VLAN, but a VLAN usually has several switches. Some port-based VLAN cannot include a physical segment. The port based VLAN is illustrated in the Figure. In that Figure two VLAN are implemented: red and yellow. Both networks have stations in different locations [13].

#### MAC Based VLAN

This kind of VLAN eliminates the Port based VLAN, because the end stations are grouped by Media Access Control (MAC) address. The location of the VLAN stations can vary, because the MAC addresses are in the Network Interface Card (NIC). In other words, the VLAN is user oriented. There is a very important disadvantage in MAC address based VLAN, all the workstations should be initialized; after that they can be relocated [14].

#### Layer-3 Based VLAN

In this variation, the VLAN uses the protocol in order to distinguish the workstations that it has. It is very important to emphasize that layer-3 based VLAN can use the switches to connect the users. Other feature is the compatibility with TCP/IP, instead of IPX, DECnet or AppleTalk, because these do not imply initial configuration [15].

#### Policy Based VLAN

The Policy based VLAN is the most powerful, dynamic and flexible; because it can be reorganized in order to satisfy the needs of personnel or departments. The changes are based in a set of rules, the main parameters that these rules involve are the resources optimization and security [16].

## Virtualization and its Importance in Enterprise Networks

Virtualization has changed the world of datacenter infrastructure in enterprises. It has helped enterprises to reduce the footprint in their datacenters with converged infrastructure and automate the provisioning of the compute nodes. With virtualization, the compute nodes can now be provisioned in a matter of seconds. But compute nodes are not the only component in a datacenter infrastructure. There is network that connects these devices and there is storage that stores all the data [17].

Enterprise network infrastructure has profoundly impacted information systems business world. As small, mid-size businesses, various devices and data move beyond the traditional security of the corporate landscape, cyber-attacks will continue to grow at an exponential proportion [18].

Virtualized infrastructure provides a layer of abstraction between computing storage, networking hardware, and the applications running on it. Their study further explained that the deployment of virtual infrastructure is non-disruptive to the system, because the user experiences are typically un-noticed or unchanged. The authors conclude by emphasizing that virtual infrastructure provide enterprise system management, the opportunity to manage pooled resources across the enterprise, thereby, allowing Information Technology (IT) managers to be more responsive to dynamic system needs to better leverage infrastructure investments [19].

Virtualization does two things tremendously well:

* + 1. It allows an enterprise system to run multiple workloads on a single machine with great isolation between those workloads. By providing this hardware-level abstraction and strong isolation between multiple host operating systems, if one workload crashes, the other can continue to run unobstructed.
    2. It’s also great at suspending, resuming and migrating images around an IT environment, in run-time. Without even shutting down an image, jobs can be moved to new machines without any sort of disruption in performance [20].

Live VM migration is being widely utilized in virtualized data centers and clouds due to its capability of maintaining high system performance under dynamic workloads. However, VM migration requires considerable network bandwidth and other resources, which may in consequence lead to performance degradations of the migrating VM during the period of migration. While that resource demand and VM performance drop are usually affordable for a single VM migration due to the short period of that process, it is challenging to manage multiple concurrent migrations because the system may not have enough resources immediately to meet the dramatic resource demands from many VMs. As a result, it will take much longer time for multiple migrations to complete, which leads to long performance degradations for those VMs [21, 22].

While convenient, the use of VMs gives rise to further challenges such as the intelligent allocation of physical resources for managing competing resource demands of the users. In addition, enterprise service consumers with global operations require faster response time, and thus save time by distributing workload requests to multiple clouds in various locations at the same time [23]. This creates the need for establishing a computing atmosphere for dynamically interconnecting and provisioning clouds from multiple domains within and across enterprises. There are many challenges involved in creating such clouds and cloud interconnections [24].

**2.5 Firewall and its Importance in Network Security**

A firewall is a type of software or hardware device that helps protect your computer from being attacked over the Internet. It monitors inbound and outbound activity coming from your network for suspicious activity, blocking items that are considered dangerous based on a set of security rules [25].

A firewall also establishes the first line of defense against attacks, viruses, and malware.

The important functions of Firewall are as follows:

1. Protects your computer from unauthorized access.
2. Blocks unwanted content.
3. Prevents ransomware from gaining traction.
4. Creates a secure network for multi-person interaction, such as online video games.
5. Helps keep your private information such as online banking credentials or social security number safe [26].

#### Types of Firewalls

1. **Client-Based Firewalls**

* **Proxy firewall**: Also known as a gateway firewall, a proxy firewall is a network security system that protects network resources by filtering messages at the application layer [27].
* **Unified Threat Management firewall**: A Unified Threat Management (UTM) firewall is often used alongside antivirus software. It is focused on being simple and easy to use [28].

1. **Hardware Firewalls**

* **Traditional firewall**: Also referred to as a Stateful Inspection Firewall, allows or denies certain traffic activity based on a specific protocol. It monitors activity from beginning to close of a connection [29].
* **Network Address Translation firewall**: Considered as one of the most secure firewall methods, a Network Address Translation (NAT) firewall hides a network of computers under a single IP address. A specific computer's IP address is only visible to other computers in the network [30].
  1. **Solutions for Network Security in Enterprise Network**
     1. **Cisco Solutions**

Enterprise services from Cisco are advertised as being world-class, premier consulting and being on a technical support ecosystem. According to the IHS Infonetics Router and Switch Vendor Leadership: Global Service Provider Survey (June 2015), Cisco was named the top manufacturer of edge and core routers and carrier Ethernet switches [31]. Cisco is the leader in that market share.

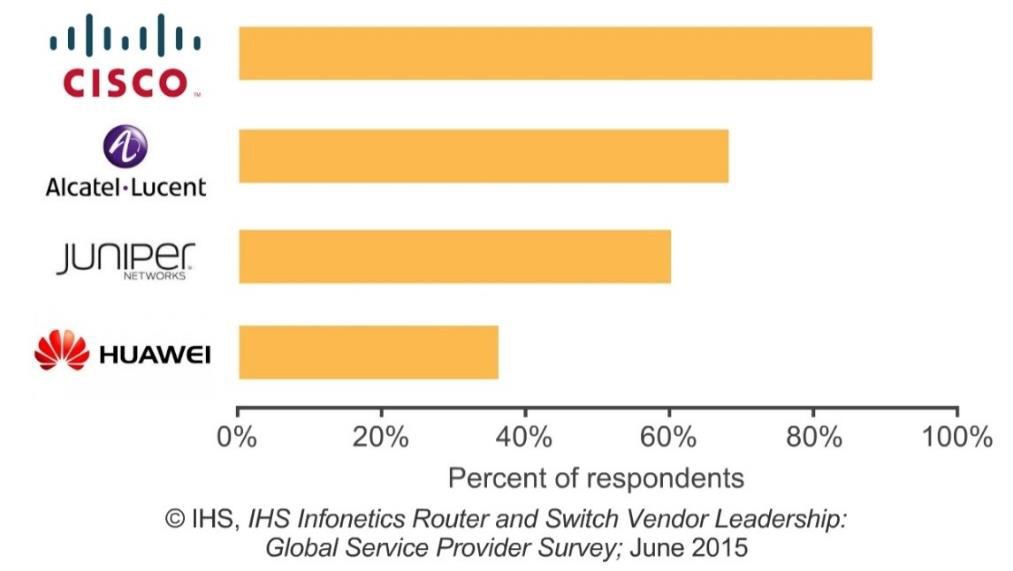


Figure 1: Top manufacturers of edge, core routers and carrier Ethernet switches [31].

A cisco enterprise service combines forward-looking vision with tactical expertise to deliver solutions that are transformational in nature, accelerating business results and time to value. Cisco is firmly grounded in reality, aligning business imperatives with technical architecture to deliver practical, measurable IT initiatives that fuel business growth while optimizing cost allocation. Cisco seamlessly aligns business and technical architectures with their growing suite of products, systems, and solutions to provide true value throughout businesses. Their network planning and preparation phase makes it easier for enterprises to evaluate business goals and state of infrastructure [32].

* + 1. **Juniper Solutions**

Juniper is seen as a head to head competitor of Cisco in terms of participation in the network edge architectures and data centers. Juniper primarily focuses on business services by providing solutions to enterprise, data centers and cloud. Juniper specializes on their equipment, for the purposes of hyper fast and dedicated heavy weight transmissions per day [33].

Juniper Networks transforms the business of networking by delivering solutions to service providers and enterprises that support today's applications with high performance. Juniper Networks' focus on technology, leadership and technical excellence has produced an award-winning portfolio of secure and dependable platforms. Juniper offers a premier line of diverse networking and security products. These network routing and security solutions are sized for the small office on up to the largest IP backbone sites in the world [34].

In Juniper's comprehensive networking portfolio are a wide variety of high- performance, reliable network routing, Ethernet switching platforms and optimized application delivery. Included are data center acceleration, WAN acceleration, J-Series & M-Series routing and EX-Series Ethernet Switching platforms. Based on a common product architecture featuring the proven JUNOS modular operating system, these platforms ensure an efficient and predictable IP infrastructure and enable secure, dependable user experiences at scale [35].

* + 1. **Akamai Solutions**

Success in today’s hyper-connected world is based largely on an organization’s ability to deliver engaging online experiences – despite the performance and security weaknesses presented by the public Internet [36]. Akamai addresses this challenge head on, enabling customers to:

* Optimize for multi-device delivery
* Scale to deliver quality video over IP
* Accelerate enterprise and branch office connections
* Secure cloud-based data, applications and websites

Akamai has deployed the most pervasive, highly distributed cloud optimization platform, delivering over 2 trillion Internet interactions daily and creating a powerful layer of defense to withstand today’s attacks while anticipating and mitigating future threats [37]. As networks and applications continue to grow in complexity and the world becomes even more reliant on the Internet, Akamai’s CDN, cloud, mobile and security services deliver a secure, high-quality experience on any device. By enabling businesses to reach broadcast scale audiences, process secure transactions and make enterprise business applications available to a mobile global workforce, Akamai removes the complexities of technology and helps companies accelerate innovation [38].

Cisco and Akamai customers increasingly use the Internet to run business-critical applications. In addition, the dramatic increase in business-critical HTTP traffic on networks is forcing customers to make difficult decisions between their WAN budgets and application priorities. Akamai and Cisco share many of the same customers and can address the traffic increase together to enable new applications without increasing the WAN budget. The companies intend to integrate leading routing, WAN optimization, and Akamai caching and acceleration into the leading application delivery platform, the Cisco Integrated Services Routers (ISR) with Cisco Application Experience (AX), referred to as the Cisco ISR-AX platform. Both companies see the potential performance and cost benefits of an optimized hybrid WAN for enterprises and their branch offices [39].

* + 1. **VMware Solutions**

Enterprise IT customers are approaching a crossroads where on-premises capacity is becoming limited. In addition, the speed of the business is in many cases outpacing the speed at which IT can deliver the necessary infrastructure. Previously, IT teams have been required to design, procure, install, configure and manage an increasing number of discrete infrastructures to satisfy the business’s needs. This process takes time to complete and can slow down the progress of business itself. Even the seemingly simple task of adding capacity to existing VMware vSphere infrastructure often must go through a long internal vetting and approval process [40].

VMware Infrastructure is the most widely deployed software for optimizing and managing IT environments through virtualization – from the desktop to the data center. VMware first introduced virtualization technology to the x86 computing platform in 1999, and since then has saved its 100,000 customers billions of dollars in capital and operating costs [41]. VMware Infrastructure abstracts the operating system from the hardware it’s running on, providing standardized virtual hardware for operating systems and their applications that enables the virtual machines to run simultaneously and independently on one or more shared processors. With virtualization, customers can easily consolidate many disparate server workloads onto more reliable and higher performance hardware [42].

VMware Infrastructure transforms a mix of industry standard x86 servers and their existing processors, memory, disk and networking into a pool of logical computing resources. Operating systems and their applications are isolated into secure and portable virtual machines. System resources are then dynamically allocated to each virtual machine based on need and prioritization, providing mainframe-class capacity utilization and control of server resources. Virtual machines can run on any physical server in a resource pool and be shifted between those servers seamlessly with zero downtime [43]. As a result, virtual machines can be dynamically and automatically allocated to the most appropriate host in the resource pool to guarantee service levels to software applications. By aggregating hardware resources into resource pools, IT environments can be optimized to dynamically support changing business needs while ensuring flexibility and efficient utilization of hardware resources [44].

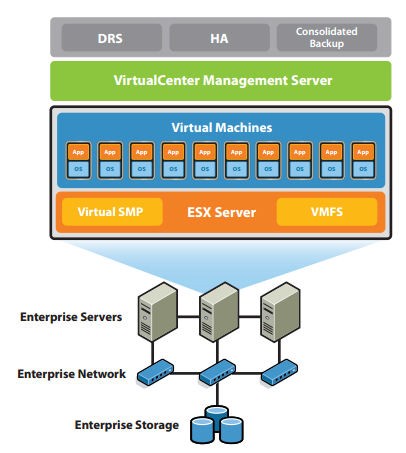


Figure 2: VMware: infrastructure for enterprise networks [42].

vCloud Air provides IT organizations with quick and easy access to compute, memory and storage resources by adding capacity derived from VMware vCloud Suite to their on-premises data center. By having infrastructure as a service (IaaS) based on VMware technology readily available, IT organizations can quickly deploy new workloads and migrate existing ones to vCloud Air without having to modify components at the application layer [43]. However, to make a functional outsourced data center and hybrid cloud, the following key considerations must be addressed before this process of deployment and migration of new and existing workloads begins:

* Establishing and configuring cloud networks
* Connecting on-premises vSphere to vCloud Air
* Deploying supporting infrastructure
* Migrating templates and media

After these four basic issues have been properly addressed, users can view their outsourced data center as ready to accept workloads. This document aims to improve users’ understanding of these considerations so they are fully prepared to embrace the cloud at their own pace in this new era of IT as a service [40] [44].

The main purpose of an enterprise network is to reduce isolated users and workgroups. All systems should be capable of communicate and provide and desired information. Additionally, physical systems and devices should be able to maintain and provide satisfactory performance, reliability and security. Enterprise computing models are developed for this purpose, facilitating the exploration and improvement of established enterprise communication protocols and strategies. In scope, an enterprise network may include local and wide area networks (LAN/WAN), depending on operational and departmental requirements [45].Recent empirical studies reveal that the size of some enterprise networks and the complexity of their routing designs rival or even surpass those of carrier networks. Far more enterprise networks than carrier networks are in operation today, and their designs are highly customized to the needs of individual companies, universities, government agencies, or other types of organizations. However, despite their complexity, prevalence, and diversity, enterprise networks have received little attention from the research community [46].

These networks are a key component in the success of a modern enterprise as it connects users to business applications and services. A fast and reliable enterprise network service that connects all of an organization’s offices is no longer a luxury, it is crucial to business success [47]. The productivity of a workforce can be attributed to and enhanced by the quality of the enterprise network. As the enterprise network has grown and become more important, the operational and financial challenges of operating the network have become more of a burden to organizations. The challenges of operating the network need to be addressed in a way that enhances not only performance and reliability, but also security, privacy, and compliance. Complete enterprise network architecture can effectively address this growing challenge [48].

Today, an enterprise network functionally extends well outside its conventional and controllable borders. This new generation network is borderless, dynamic, and organic with a high level of virtualization. It expands and contracts its reach and services with the movement of users, rise of new technologies, inclusion of new partners and supply chains, advent of new attacks, and enhanced use of resources [44].Enterprise networking is transitioning from network-centric solutions to transformational architectures, services, and comprehensive solutions. Emerging Internet technologies and new security threats are challenging all known paradigms of networking, and require a fresh architectural and design review of many existing enterprise networks [49].

Conventional networking was mainly concerned with routing and switching. The network, end devices, and users were not aware of each other [50]. The new generation of enterprise networking offers a variety of technologies to associate the end devices, applications, and services into one ecosystem. It allows for traffic recognition, application recognition, quality-of-service (QoS) techniques, dynamic and network- based traffic management, media aware routing, and acceleration of traffic-based on priority, context, and classes of service. Video-enabled devices are becoming media and status capable, reporting quality parameters to the network. Device, application, service, and location awareness and traffic acceleration are becoming core properties of extended enterprise networks [51].

In the current scenario, enterprises are rooted into network based functions. But while designing and implementing the enterprise network in most cases, enterprises are unaware of technical facts and also fail to put forward the requirement. Thus, most of the enterprise is founded in simplified flat designs, where there are multiple layer 2 devices with single broadcast domains; an edge router and switches being other components of the network. Some of the enterprises are concerned with security feature and implement firewalls. Only protecting the private network doesn’t fulfill network requirements of the enterprise. They should have redundancies, 24/7 power supply, high availability, agility and quality of service [52, 53].

A successful enterprise network requires dedicated job roles that handle daily tasks necessary to help the enterprise thrive. Unfortunately, many enterprises pass small chunks off to business unit and never make it a formal part of someone's job description. One benefit of an enterprise network is that we can monitor and analyze. As team members discuss ways to make the office more efficient, someone needs to be responsible for effectively monitoring the information that flows within the enterprise network and then delivering the feedback to someone who can take action [54, 55].

**REFRENCES**

[1] Ictglobal.com. (2018). The Importance of Computer Networks. [online] Available at: http://www.ictglobal.com/imp\_networks.html [Accessed 15 Apr. 2018].

[2] Teraits.com. (2018). [online] Available at: http://www.teraits.com/pitagoras/marcio/gpi/b\_POppenheimer\_TopDownNetworkDesign\_3rd\_ed.pdf [Accessed 15 Apr. 2018].

[3] London.ac.uk. (2018). [online] Available at: https://london.ac.uk/sites/default/files/study-guides/data-communications-and-enterprise-networking-2.pdf [Accessed 15 Apr. 2018].

[4] Anon, (2018). [online] Available at: http://www.koslowandhuntmd.com/forms-of-enterprise-in-20th-century-italy-boundaries-structures-and.pdf [Accessed 16 April 2018].

[5] Pdfs.semanticscholar.org. (2018). [online] Available at: https://pdfs.semanticscholar.org/a4a5/ef4f2e937dc407a4089019316b054e8e3043.pdf [Accessed 17 April 2018].

[6] Theseus.fi. (2018). [online] Available at: https://www.theseus.fi/bitstream/handle/10024/47351/Sulaimon\_Adeniji.pdf?sequence=1 [Accessed 18 April 2018].

[7] Theseus.fi. (2018). [online] Available at: https://www.theseus.fi/bitstream/handle/10024/47351/Sulaimon\_Adeniji.pdf?sequence=1 [Accessed 19 April 2018].

[8] Ecpi.edu. (2018). The Evolution of Network Security | ECPI University. [online] Available at: https://www.ecpi.edu/blog/evolution-network-security [Accessed 20 April 2018].

[9] Ecpi.edu. (2018). The Evolution of Network Security | ECPI University. [online] Available at: https://www.ecpi.edu/blog/evolution-network-security [Accessed 20 April 2018].

[10] Tripwire, I. (2018). Understanding the Evolution of Network Security. [online] The State of Security. Available at: https://www.tripwire.com/state-of-security/security-data-protection/understanding-evolution-network-security/ [Accessed 21 April 2018].

[11]

[12] Techopedia.com. (2018). What is a Virtual Local Area Network (VLAN)? - Definition from Techopedia. [online] Available at: https://www.techopedia.com/definition/4804/virtual-local-area-network-vlan [Accessed 22 April 2018].

[13]

[25] V-Soft Consulting Group, I. (2018). The Importance of Using a Firewall. [online] Blog.vsoftconsulting.com. Available at: https://blog.vsoftconsulting.com/blog/importance-of-using-a-firewall [Accessed 28 April 2018].