Network Model Architecture

Rafat Khandaker

ECPI University

Technical Proposal

**Executive Summary**

As a cyber network security administrator, I have specialized in understanding the importance of valuable assets in an organization and defend it against cyber-attacks. With the increase attempts to breach network security, new companies must follow a standardized compliance to protect itself against cyber threats. These defense tactics will include: defending attacks against cloud services; Ability for a company to recover from cloud breach disasters; Risks associated with offshore hiring; Ability for a company to audit access to cloud services; Ability for a company to monitor growing assets, alongside security; Providing quality of service to our customers. Working alongside our team of 10 Network administration, 20 developers & external HR department, we will be able to scale the needs of this business while ensuring security to its assets.

**Addressing Security Concerns**

Our current company architecture involves providing programmers and consultants access to our infrastructure, cloud services through a DSL (Direct Service Line). This will ensure that our that our programmers maintain maximum up-time and connection to our infrastructure to push updates to projects. In order to stabilize this workflow, providing maximum up time connection to employees, while maintaining a good security architecture. Let us analyze security concerns with offshore employment connecting into cloud services. In an article written in CSO from IDG blogs, Dean Davison addresses the “Top 10 risks of offshore outsourcing.” He explains that companies move into offshore hiring, over exceed their expectation for savings **(Davison, 2004)**. There are many risks associated with Offshore expansion, including Data security protection where we cannot expect IT organizations, offshore, to follow the same standards and robust security practices that are followed internally. Capability Maturity Model, explains a company's readiness to adopt an offshore model **(Davison, 2004)**. This model describes a repeatable model that can track internal process. Loss of business knowledge is a concern for offshore modeling, when employees are hired and dismiss their position. A company should have a secure way of handing information over and restricting access to it the same way, a process known as “Knowledge Transfer” **(Davison, 2004)**. Underestimating how failure to deliver can impact company assets.

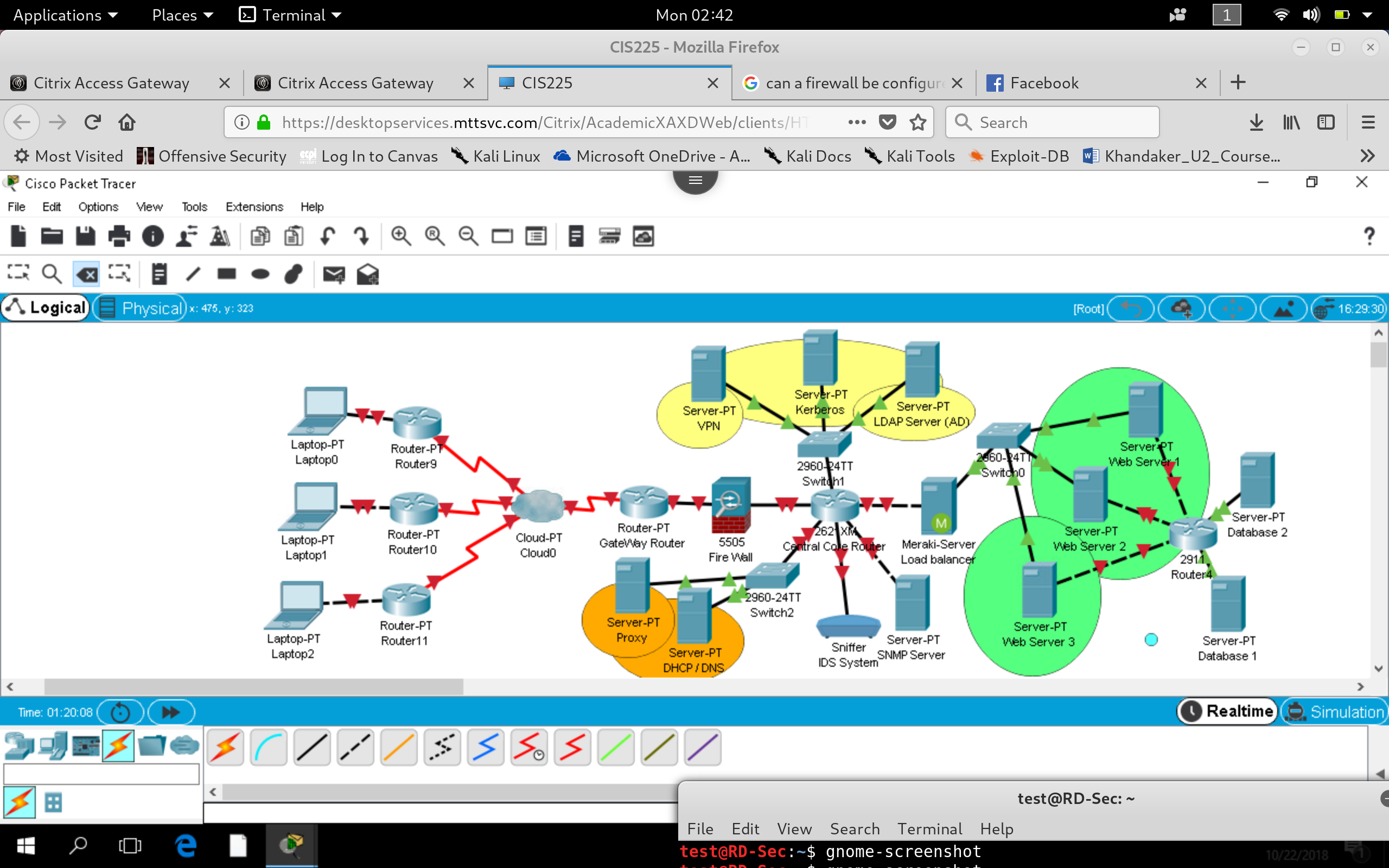
Security in our company design should also include the technology used in place. Let us assess all the concerns of hosting a cloud model & network related security. According to "Cloud Computing Fundamentals”, delivered by Kris, Jamsa, are some concerns a company should address when migrating to cloud services. In the text: Cloud hosted environments are limited by the vendor. There are a wide variety of Cloud Services and each vendor has their own compliance structure. Cloud environments give control of our company’s data and internal operations to 3rd party vendors **(Jamsa, 2013)**. Alongside our cloud infrastructure, network security is needed to prevent any potential external attacks between user nodes and the cloud service. According to InfoSec Institute, common Cloud computing attacks through network include: Denial of Service, Malware Injection Attack, Side Channel Attack, Brute forcing, Authentication and MiTM attacks **(InfoSec, 2018)**.

**Providing Security Suggestions**

From my analysis of this company’s business architecture, I suggest we take steps to document the company’s assets, key important information, size of the digitized information, security role groups of individuals and engineer the “principle of least privilege,” approach to distributing business permissions. Let us establish a baseline for our technological security, document what is required from securing minimum assets & what is required from securing high risk assets. Let us a build an infrastructure addressing and take measures for testing our cloud hosted infrastructure, in development and deployment of its services. Let us create comprehensive auditing systems that will keep active logs from users accessing our services. Let us distribute appropriate permissions between project managers and programmers to maintain the flow of workload. Let us make sure that knowledge transfer will not be a problem between offshore employee hires, giving responsibility to senior management to retain and build on transferring knowledge. Let us create documentation, back out procedures and create a home base infrastructure to host our service incase our cloud provider fail to deliver the needs of our business. Let us keep an active back up our own services & provide internal servers to back up data from the cloud deployment. Let us create thorough disaster recovery procedures, from loss of employees, loss of data, loss of provider. Let us generate good reports from weekly/ monthly to yearly progression of our business. Let us provide active feedback surveys from our customers to find suggestions to grow business on a stable security platform.

In conclusion, security compliance in a company will require professionals to think outside the box. Today, cyber-attacks may come in many forms. Attackers today, are willing to work between the lines to penetrate security through physical, psychological and technological attacks. In order for us to combat these attacks, we have to understand the needs of our business, It's important assets and weaknesses in our business protocol. In this particular case study, we have a growing business, that Is operating in an offshore environment where employees will work remotely, accessing a 3rd party cloud environment. The cloud environment will host our company’s assets. So, to tie the knot, the goal of our security analysis is to address the potential risks and provide a stable business solution to ensure the smooth transition between this working architecture.

**NETWORK DIAGRAM:**



**Network Availability**

Weight distributed bandwidth between Router to Router configuration, Access resources through switch via VLAN configuration. Improving network bandwidth and implementing "principle of least

privilege" philosophy of design

Auditing and authentication via user active directory accounts, allowing users within network to retain identity and only users with identity can access services.

Management of authenticated sessions via Kerberos, IP address scaling VIA DHCP configuration & Secure access into resources via VPN. Limiting access into unnecessary traffic via Firewalls and Proxy.

Improved performance through load balancing

Use of Virtualization on each server to scale the service resource by running multiple instances of each service

**Technical Specifications**

**1) Gateway Router:** is connected to a serial link to the Internet to intercept Incoming traffic into intranet work, will contain highest bandwidth rating to allow maximum optimization of network utilization. Without a ACL list, reducing processing on this router to only handle initial traffic routing.

**2)** **Fire Wall:** Intercepts the Gateway connection and limits traffic based on port incoming and outgoing traffic requirements

**3) Core Router:** Distributes Network traffic into different Server farms for different tasks. Configured with ACL and communication restrictions. Also Configured with SNMP port & Port mirroring to allow traffic to be processed by IDS System.

**1) Gateway Router:** is connected to a serial link to the Internet to intercept Incoming traffic into intranet work, will contain highest bandwidth rating to allow maximum optimization of network utilization. Without a ACL list, reducing processing on this router to only handle initial traffic routing.

**2)** **Fire Wall:** Intercepts the Gateway connection and limits traffic based on port incoming and outgoing traffic requirements

**3) Core Router:** Distributes Network traffic into different Server farms for different tasks. Configured with ACL and communication restrictions. Also Configured with SNMP port & Port mirroring to allow traffic to be processed by IDS System.

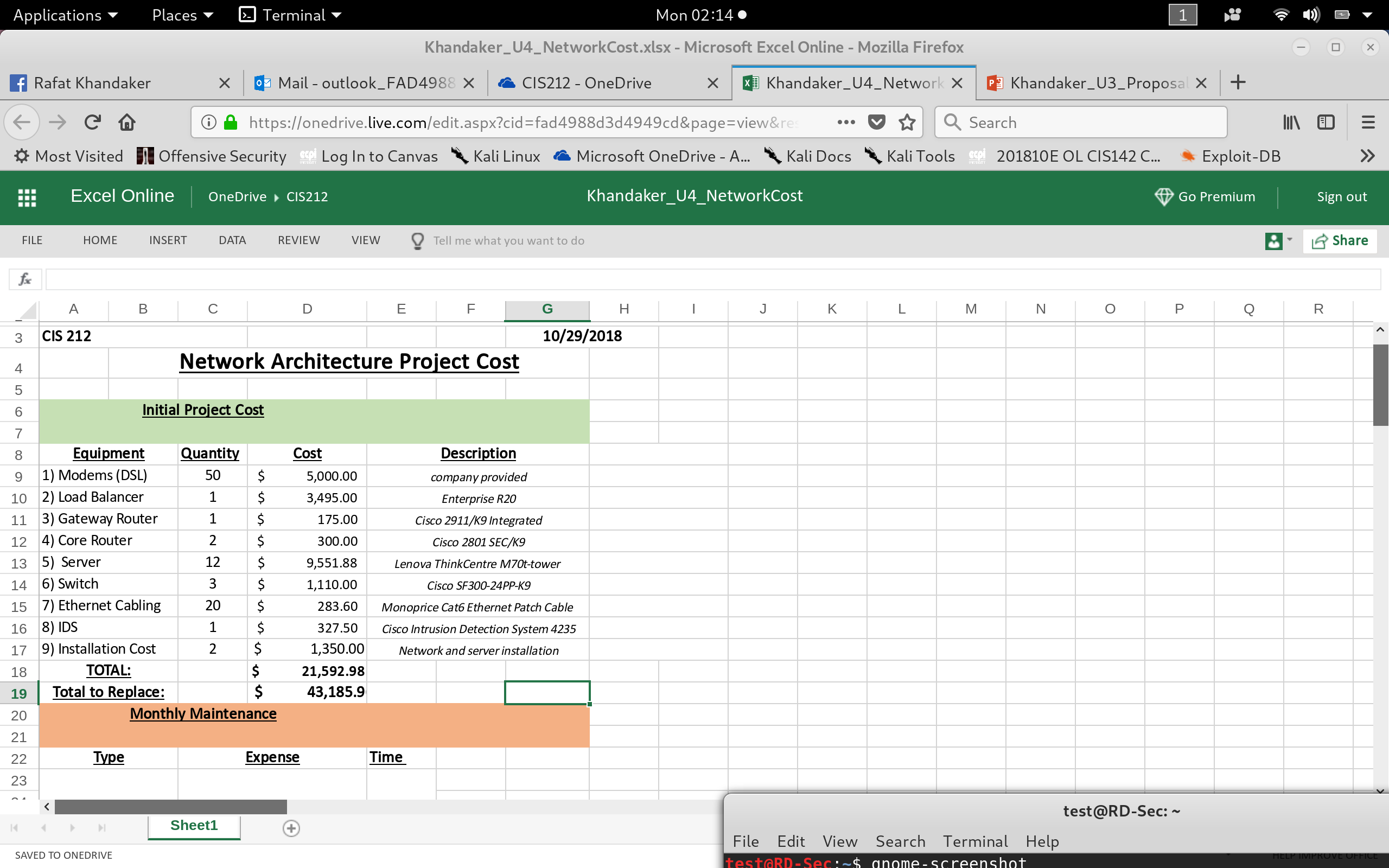
**6) Orange Server Farm:** Includes proxy and DHCP service to new devices through VPN and internal static servers with leased IP address. Separated DHCP assignment into separate broadcast domain usually because BootP protocol will request new lease time for new authenticated devices through VPN, traffic can be segmented and monitored separately for new devices this way. Proxy is used to cache default web pages and prevent users from accessing unauthorized sites from internal network, improving network bandwidth utilization and security.

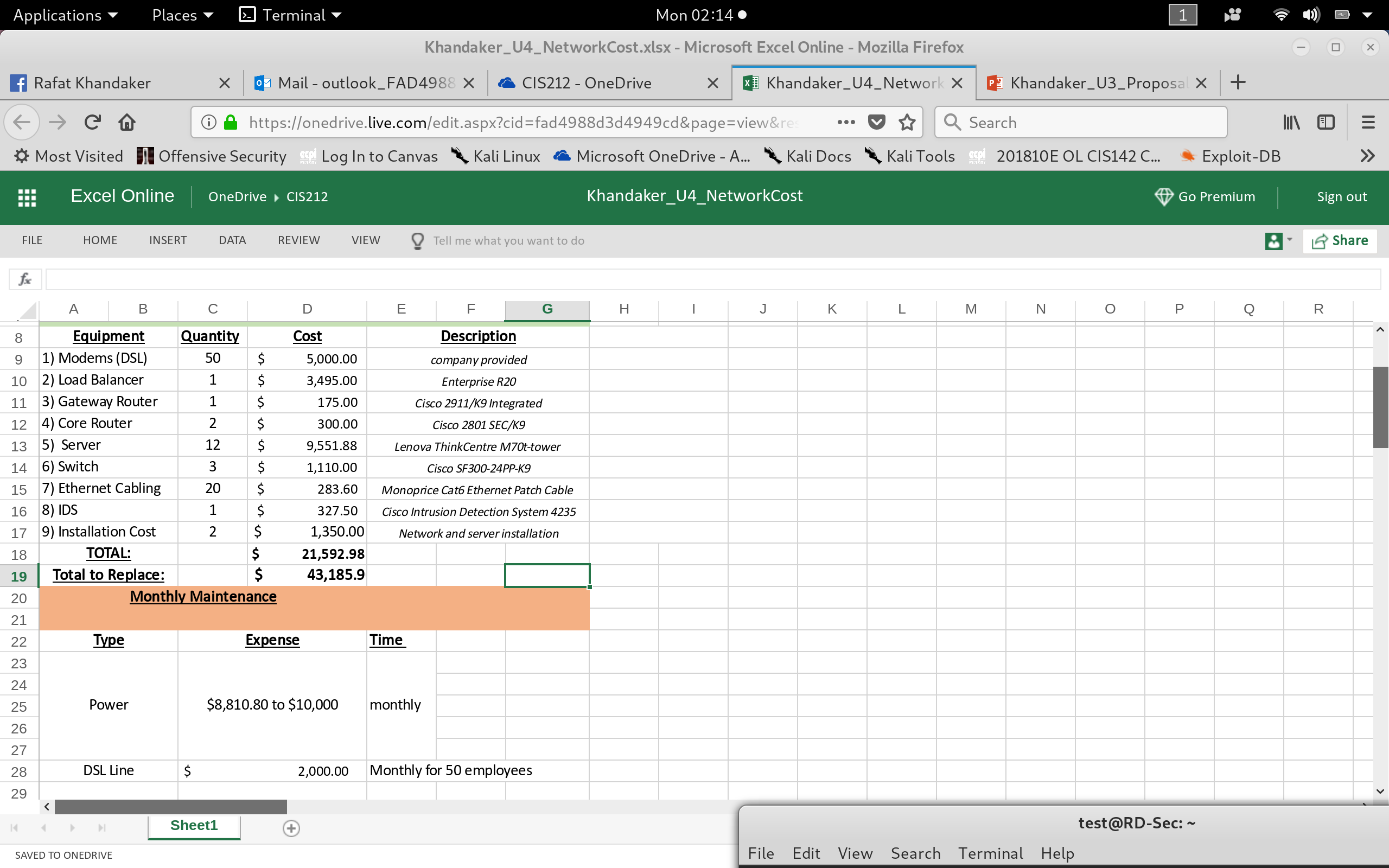
**7) Load Balancer:** traffic requesting access to web resources will be directed through load balancer to improve performance of web service utilization. This segments HTTP request traffic into this node and ACL of core router can be configured with appropriate security through this node.

**8) Green Server Farm:** Included within the same collision domain for faster packet switching capabilities through load balanced HTTP requests into web services.

**9)** **Terminating Database Router:** Router segmenting Database servers to separate broadcasting into unnecessary request to database server, router can be configured with ACL to restrict unnecessary port-based access into links. Also, segmenting links so only web services can communicate with Database servers, not intended for direct access, unless by administrator. System can be accessed in a different way for production environment.

**Budgeting and Scalability**





Total System cost is **$20,000.** Recommendation to create failsafe environment and double the number of devices in expenditure.

Total System x2 will be **$40,000.**

Installation cost brings price to: **$43,185**

Double the system requirement will ensure fail-safe solution that can migrate service in case of failure and adopt for scalability. Cost savings include the ability to be robust and minimize damage to business operations. Current model cannot recover from disaster failure. The amount of damage to business will equate to the loss of money due to business operations plus replacement damages to recover operations. This may require a new robust system anyway. Potential loss from current model can be expected to be **3 times** the investment to migrate to a robust and fail-safe system. Savings include **%70** **loss** of business operations due to failure.

Potential for cloud migration:

**Cloud Bursting** option to accommodate for potential growth of the company. Scaling Microsoft services with Azure in the Infrastructure layer. Offers scalability for reduced cost of implementing infrastructure solution.

**References**

**(1)** Kris, Jamsa. (2013). *Cloud Computing.* Cengage

**(2)** Ciampa**,** M.(2016). *CompTIA Security+ Guide to Network Security Fundamentals.* Cengage

**(3)** Davison, Dean.(2004). *Top 10 Risks of Offshore Outsourcing*. Retrieved From: <https://www.csoonline.com/article/2117420/data-protection/top-10-risks-of-offshore-outsourcing.html>

**(4)**  Cloud Computing: Attack Vectors and Counter Measures. (2018)**.** Retrieved from: <https://resources.infosecinstitute.com/cloud-computing-attacks-vectors-and-counter-measures/#gref>