“Cloud Systems – Using SDN (and NFV) to support firewall capabilities for a small business”

Name
Paul Doherty

Student ID
19214574

Email
paul.doherty23@mail.dcu.ie

Program
2019/2020 MCM1 M.Sc. in Computing
-
Module
CA687 Cloud Systems

Submission Date
20/04/2020

Word Count
743

An assignment submitted to Dublin City University, School of Computing for module CA687 Cloud Systems.

I understand that the University regards breaches of academic integrity and plagiarism as grave and serious. I have read and understood the DCU Academic Integrity and Plagiarism Policy. I accept the penalties that may be imposed should I engage in practice or practices that breach this policy.

I have identified and included the source of all facts, ideas, opinions, viewpoints of others in the assignment references. Direct quotations, paraphrasing, discussion of ideas from books, journal articles, internet sources, module text, or any other source whatsoever are acknowledged and the sources cited are identified in the assignment references.

I declare that this material, which I now submit for assessment, is entirely my own work and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work. By signing this form or by submitting this material online I confirm that this assignment, or any part of it, has not been previously submitted by me or any other person for assessment on this or any other course of study. By signing this form or by submitting material for assessment online I confirm that I have read and understood DCU Academic Integrity and Plagiarism Policy available (http://www.dcu.ie/registry/examinations/index.shtml)

Name: Paul Doherty

Date: 20/04/2020

Introduction

This solution demonstrates a typical telecommunications network for a small business with suitable dynamic access controls in place to control access to different services. It uses SDN (Software Defined Networking) and Network Function Virtualization (NFV) to enable a virtual firewall that can be configured with rules to allow traffic between different nodes in the network. These rules can be updated through a single “controller” using a REST-based interface to centrally administer the flow of traffic in the network.

Motivation for Application

The motivation behind choosing this solution was primarily to demonstrate the capabilities of SDN. The network communications infrastructure for a small business feels like a nice fit for this. By using NFV, the amount of physical equipment required can be reduced and security can be centrally administered in a simple manner. The inspiration was derived from one of the “Applications of SDN” from the course notes, namely “Security Services”.

Network Topology and Core Functions

The network diagram in the appendix displays the traffic flows within the business. The servers support the traditional business services which are offered by a small business, e.g. payroll, website, etc. The users of these services include both internal (marketing, finance departments) and members of public. Internal users have more access rights than members of the public. Indeed depending on the role of the internal user they may have superior access rights than other users, e.g. Finance users.

The topology is a custom tree topology with 2 outer perimeter switches / routers controlling traffic flow from users to the inner core switches. The topology is modelled using Mininet and created

using a custom Python script. The MiniEdit tool was also considered in creating the topology but the script allowed more appropriate naming of variables, mac addresses, etc. The controller leverages the standard REST firewall from the RYU SDN framework.

Administration of access rights are configured in the central controller, as seen in the MiniNET diagram. This controller is the core of the SDN and it improves network management and streamlines the technical operations of the business.

The initial state of the network is to deny traffic flow between all nodes on the network. The controller is then updated with the appropriate rules to support traffic flow between individual nodes (specific IP addresses) or groups of nodes (IP subnet ranges). The controller communicates with each of the switches in the network (via southbound interface) and configures them with the appropriate network configuration.

The administrator of the network uses REST based interfaces to interact with the Ryu controller and to to add / remove access control rules. These interfaces are based on the Ryu Web Server functionality.

Evaluation Design and Test Results

After the network is initially created and the controller is enabled, all traffic flow between nodes on the network is completed disabled. At this point, it is not possible for any 2 nodes on the network to communicate with each other. This was verified using the Mininet command ‘pingall’.

The firewall rules were subsequently updated and again ‘pingall’ was attempted to assess which nodes were able to ‘ping’ one another. The results were as expected. Only those nodes that were allowed to ‘ping’ one another could.

The final test was to validate that the users were able to SSH onto the boxes which it was intended for them to access. A subset of users and servers were used to validate this. For all of these tests, “Blocked Packets” are visible in the console and using Wireshark. The actual flow tables on the switch were viewed using “dpctl dump-flows” command.

Challenges & Lessons Learned

Mininet is a very useful tool for creating a wide variety of virtual networks representing real networks. It is very flexible and is a tool that I will use again for conducting such experiments. I presented a simple enough tree topology network here but one could imagine using the tool to model much more complex networks.

Initial attempts to engage and use the Ryu controller were challenging due to dependencies, configuration, etc. However once it was operational it proved very useful for supporting the firewall based SDN. The rules were easily administered centrally and propagated by the controller to the switches.

The biggest challenge was trying to find a good use case that could build upon the knowledge gained on the course in the areas of SDN and VNF. However in conclusion I feel that the firewall based security system is a very good application of these technologies.

Appendix

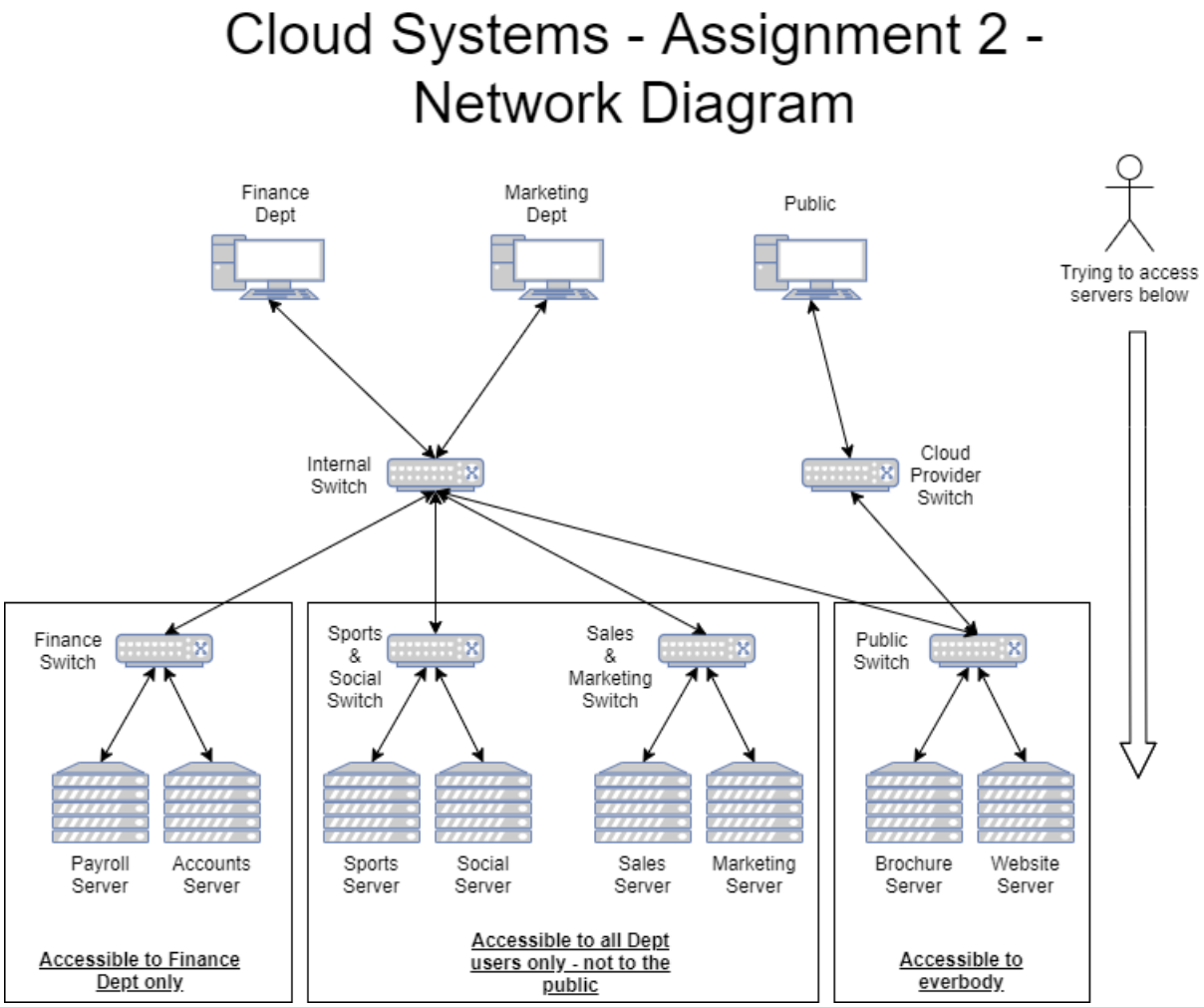
Source Code

https://github.com/paul-19214574/cloud-systems-assignment2

Screencast

https://www.youtube.com/watch?v=Stz_FGBxtgo

Network Diagram



MiniNAM Diagram