Configuration Manual

MSc Research Project
MSc Cybersecurity (MSCCYB1)

Yash Saraswat
Student ID: X20184867

School of Computing
National College of Ireland

Supervisor: Prof. (Dr) Rohit Verma

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Yash Saraswat		
Student ID:	X20184867		
Programme:	MSc Cybersecurity (MSCCYB1)	**Year:**	2022
Module:	Research Project		
Lecturer:	Prof. (Dr) Rohit Verma		
Submission Due Date:	19-September-2022		
Project Title:	Enhancing the security of a network fabric using firewalls and load balancer		
Word Count:	960	**Page Count:**	5

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Yash

Date: 19-September-2022

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Yash Saraswat
Student ID: X20184867

1 Overview

Security, integrity, and availability of the network infrastructure is extremely important in order to ensure the smooth continuity of organisations and businesses. In this research report, we have proposed the usage of next-generation firewall cluster possessing strict security policies along with load balancer possessing strict redundancy policies for providing a defence mechanism to the network fabric against a wide range of latest attack vectors.

The functionality and effectiveness of the proposed network fabric was evaluated using well-known attack vectors, such as malicious packets flooding, SQL injections, phishing attempts, and malicious payloads. Successful detection and blockage of all threat vectors took place after few failed experiments. The steps which were used to deploy the proposed network fabric are illustrated in the following sections.

2 Tools used

The following tools were used to practically implement the research project:

(1) VMware Workstation Pro 16.2.4:

Download and install VMware Workstation Pro from its official website[1]. VMware Workstation was used to deploy Emulated Virtual Environment – Next Generation (EVE-NG) VM which was further used to locally host the proposed network fabric.

(2) EVE-NG OVF version 5.0.1-13:

Download EVE-NG OVF file from its official website[2]. OVF file was deployed on VMware Workstation in order to locally host the network fabric on Windows 11 base-machine.

(3) WinSCP 5.21.2:

Download and install WinSCP from its official website[3]. WinSCP was used to transfer EVE-NG 'qcow2' images of networking devices from base-machine to local EVE-NG server.

(4) Anaconda 2022.05:

Download and install Anaconda from its official website[4]. 'EnsureSecurityRule.py' file was compiled on the first Palo Alto NGFW using Anaconda’s Spyder in order to ensure the commitment and deployment of security rules and configurations.

[1] https://www.vmware.com/latam/products/workstation-pro/workstation-pro-evaluation.html
[2] https://www.eve-ng.net/index.php/download/#DL-COMM
[3] https://winscp.net/eng/download.php
[4] https://www.anaconda.com/products/distribution

(5) PuTTY 0.77:

Download and install PuTTY from its official website[5]. PuTTY was used run Linux commands to facilitate the preparation of 'qcow2' images for EVE-NG server.

(6) pan-python:

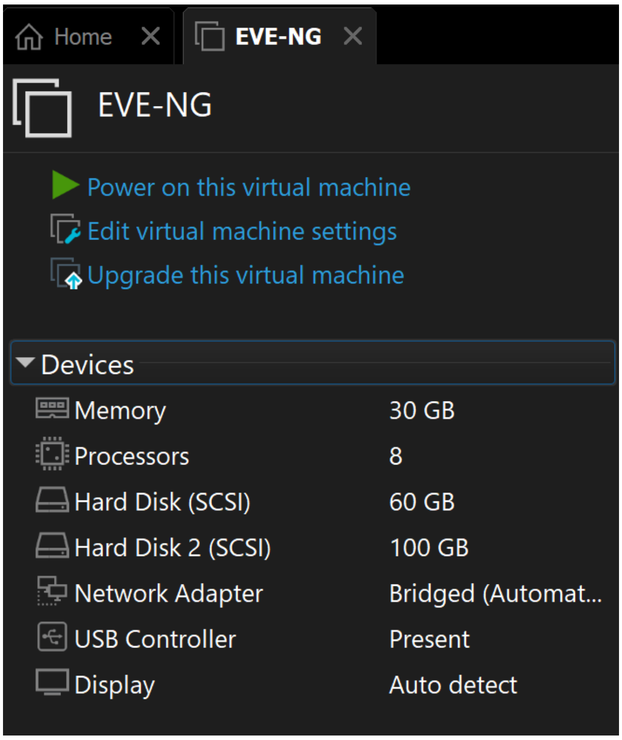
Download pan-python repository from GitHub[6]. This repository was used to generate API key in order to setup the connection and communication link of base-machine with both Palo Alto NGFW APIs.

3 EVE-NG lab setup

The hardware specifications of Windows 11 base-machine are as follows: 32.0 GB RAM, 1 TB SSD, Intel Core i7 10th Gen processor.

We have used VMware Workstation to import and install EVE-NG OVF file and allotted 30.0 GB RAM, 160 GB Hard Disk (SCSI) and Bridged (Automatic) Network Adapter to ensure the deployment of EVE-NG VM properly. The documentation of EVE-NG server installation on VMware Workstation can be found on the original website of EVE-NG[7]. The configurations of EVE-NG VM can be referred from the Figure (Figure 1).

Vojnak *et al*. (Vojnak *et al*., 2019), and Li (Li, 2021) recommended the deployment of heavy networking images using VMware Workstation due to its better compatibility with Windows environment in comparison with VirtualBox.


Home
EVE-NG
EVE-NG
Power on this virtual machine
Edit virtual machine settings
Upgrade this virtual machine
Devices

Memory	30 GB
Processors	8
Hard Disk (SCSI)	60 GB
Hard Disk 2 (SCSI)	100 GB
Network Adapter	Bridged (Automat...
USB Controller	Present
Display	Auto detect

Figure 1: EVE-NG VM configurations

[5] https://www.putty.org/

[6] https://github.com/kevinsteves/pan-python/releases

[7] https://www.eve-ng.net/index.php/documentation/installation/virtual-machine-install/

4 Preparation of images

(1) Cisco Router:

Download 'vios-15' image of Cisco router from its original website. The steps to convert router image into 'qcow2' image can be found on the original website of EVE-NG[8].

(2) Cisco Switch:

Download 'viosl2-15.5' image of Cisco switch from its original website. The steps to convert switch image into 'qcow2' image can be found on the original website of EVE-NG[9].

(3) Palo Alto Networks Next-Generation Firewall

Download 'paloalto-9.0.4' image of Palo Alto firewall from its original website. The steps to convert Palo Alto image into 'qcow2' image can be found on the original website of EVE-NG[10].

(4) Kali Linux

Download 'linux-kali-large-2019.3' image of Kali Linux from its original website. The steps to convert Kali Linux image into 'qcow2' image can be found on the original website of EVE-NG[11].

(5) F5 Load balancer

Download 'bigip-14.1.1-0.0' image of F5 Load Balancer from its original website. The steps to convert load balancer image into 'qcow2' image can be found on the original website of EVE-NG[12].

(6) Windows 10

Download 'win-10ENT' image of Windows 10 Enterprise from its original website. The steps to convert Windows 10 image into 'qcow2' image can be found on the original website of EVE-NG[13].

5 Load images on EVE-NG environment

Transfer all the folders from Windows 11 base-machine to EVE-NG server through WinSCP as represented in the Figure (Figure 2). The folders should be loaded at the following directory of EVE-NG server: '/opt/unetlab/addons/qemu'.

[8] https://www.eve-ng.net/index.php/documentation/howtos/howto-add-cisco-dynamips-images-cisco-ios/

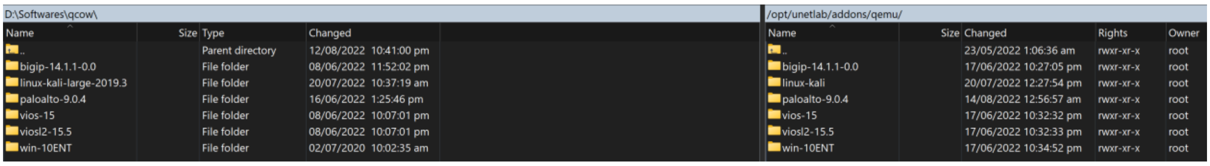
[9] https://www.eve-ng.net/index.php/documentation/howtos/howto-add-cisco-iol-ios-on-linux/

[10] https://www.eve-ng.net/index.php/documentation/howtos/howto-add-palo-alto/

[11] https://www.eve-ng.net/index.php/documentation/howtos/howto-create-own-linux-host-image/

[12] https://www.eve-ng.net/index.php/documentation/howtos/howto-add-f5-bigip/

[13] https://www.eve-ng.net/index.php/documentation/howtos/howto-create-own-windows-host-on-the-eve/



D:\Softwares\qcow\

Name	Size	Type	Changed
..		Parent directory	12/08/2022 10:41:00 pm
bigip-14.1.1-0.0		File folder	08/06/2022 11:52:02 pm
linux-kali-large-2019.3		File folder	20/07/2022 10:37:19 am
paloalto-9.0.4		File folder	16/06/2022 1:25:46 pm
vios-15		File folder	08/06/2022 10:07:01 pm
viosl2-15.5		File folder	08/06/2022 10:07:01 pm
win-10ENT		File folder	02/07/2020 10:02:35 am

/opt/unetlab/addons/qemu/

Name	Size	Changed	Rights	Owner
..		23/05/2022 1:06:36 am	rwxr-xr-x	root
bigip-14.1.1-0.0		17/06/2022 10:27:05 pm	rwxr-xr-x	root
linux-kali		20/07/2022 12:27:54 pm	rwxr-xr-x	root
paloalto-9.0.4		14/08/2022 12:56:57 am	rwxr-xr-x	root
vios-15		17/06/2022 10:32:32 pm	rwxr-xr-x	root
viosl2-15.5		17/06/2022 10:32:33 pm	rwxr-xr-x	root
win-10ENT		17/06/2022 10:34:52 pm	rwxr-xr-x	root

Figure 2: Transfer of folders from base-machine to EVE-NG server

6 LAB setup

Login to EVE-NG homepage from the browser using 'admin' credentials and import 'EVE-NG.zip' which is inside 'x20184867_ICTSolution.zip' folder. The 'x20184867.unl' file has been loaded on EVE-NG server as illustrated in the Figure (Figure 3). Click on the UNL file and open the lab in order to view the proposed network fabric.

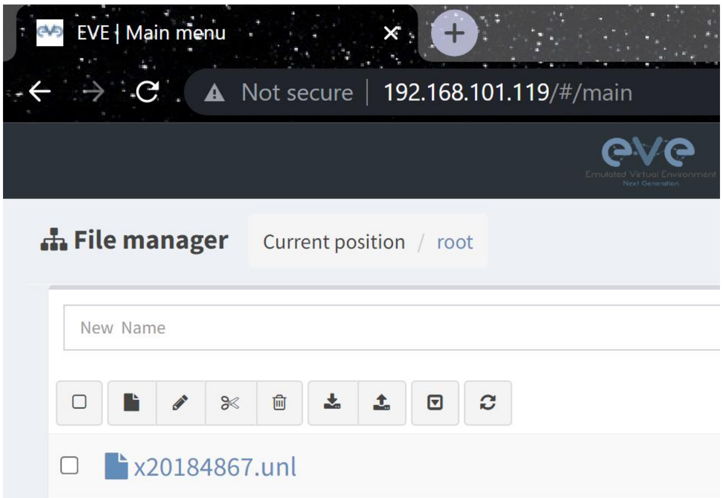


Figure 3: Import UNL file

7 Bootup all nodes

Start each networking node inside the lab after a gap of few minutes in order to reduce the chances of immediate RAM utilisation and unusual CPU usage spikes. The password for both NGFWs and load balancer is set to 'King@12345'.

8 Web application

Download and install XAMPP on both Windows 10 nodes[14]. Copy 'kite' folder from 'x20184867_ICTSolution.zip' folder and paste it inside the 'htdocs' folder of XAMPP in order to locally host the web application at port number 80.

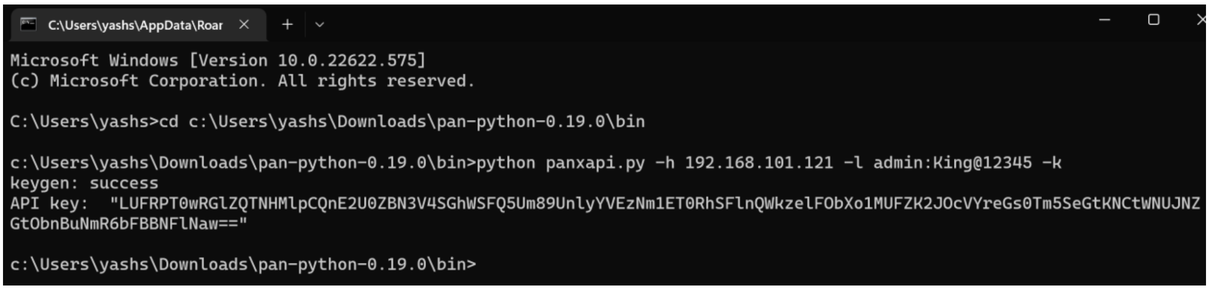
9 Palo Alto Python API

Navigate to 'pan-python' bin folder and use the following command in order to generate the API key as illustrated in the Figure (Figure 4):

[14] https://www.apachefriends.org/

'python panxapi.py -h 192.168.101.121 -l admin:King@12345 -k'.

Use command 'pip install pan-os-python' in Spyder for installing all PAN-OS SDK packages. Go to 'NGFW' folder in 'x20184867_ICTSolution.zip' and open 'EnsureSecurityRule.py' file from Spyder. Compile the file for ensuring the deployment of security rules and configurations on NGFW cluster.



```
Microsoft Windows [Version 10.0.22622.575]
(c) Microsoft Corporation. All rights reserved.

C:\Users\yashs>cd c:\Users\yashs\Downloads\pan-python-0.19.0\bin

c:\Users\yashs\Downloads\pan-python-0.19.0\bin>python panxapi.py -h 192.168.101.121 -l admin:King@12345 -k
keygen: success
API key:  "LUFRPT0wRGlZQTNHMlpCQnE2U0ZBN3V4SGhWSFQ5Um89UnlyYVEzNm1ET0RhSFlnQWkzelFObXo1MUFZK2JOcVYreGs0Tm5SeGtKNCtWNUJNZ
GtObnBuNmR6bFBBNFlNaw=="

c:\Users\yashs\Downloads\pan-python-0.19.0\bin>
```

Figure 4: Palo Alto NGFW API key generation

References

Li, Z. (2021) ‘Comparison between common virtualization solutions: VMware Workstation, Hyper-V and Docker’, in *2021 IEEE 3rd International Conference on Frontiers Technology of Information and Computer (ICFTIC).* Greenville, SC, USA, 12-14 November 2021, pp. 701–707, IEEE Xplore. doi: 10.1109/ICFTIC54370.2021.9647226.

Vojnak, D. T. *et al.* (2019) ‘Performance Comparison of the type-2 hypervisor VirtualBox and VMWare Workstation’, in *2019 27th Telecommunications Forum (TELFOR).* Belgrade, Serbia, 26-27 November 2019, pp. 1–4, IEEE Xplore. doi: 10.1109/TELFOR48224.2019.8971213.