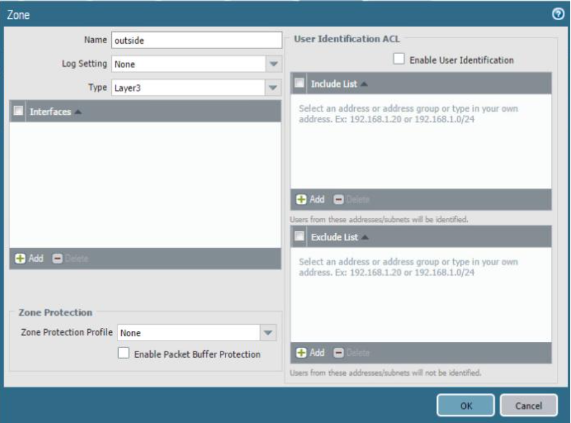
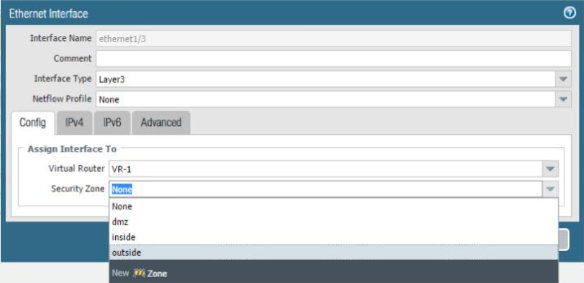
**Siddhant Kumar**

**Essentials Project 1**

**Module 1A (LAB 1): Creating a Zero Trust Environment:**

In this first module, I created a zero-day trust environment by creating zones, applying security policies and testing it. A total of three zones were created inside, outside and in the DMZ for different purposes. We also created NAT Policies for packets. After committing all the changes, I tested it by visiting a webpage and all the traffic is visible in the firewall logs.



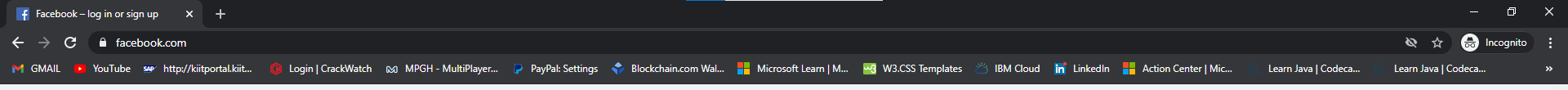
* Creating Zones:
* Configuring Ethernet Interfaces:

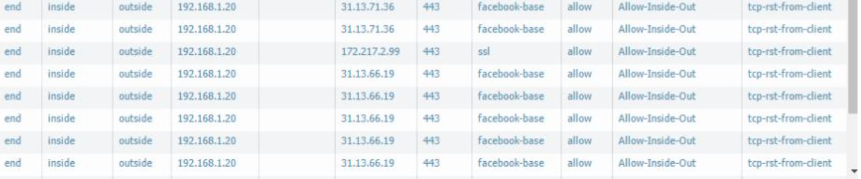


* Creating Rules:



* NAT Configuration

Using Facebook.com for the same

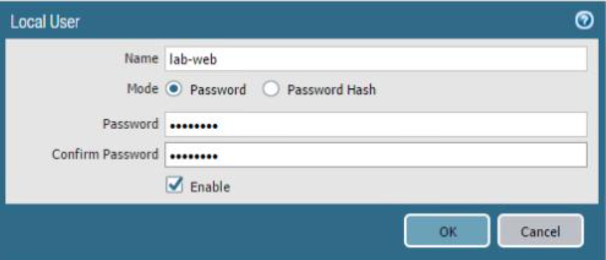
* Testing Process:

(Detailed Information about the traffic!)

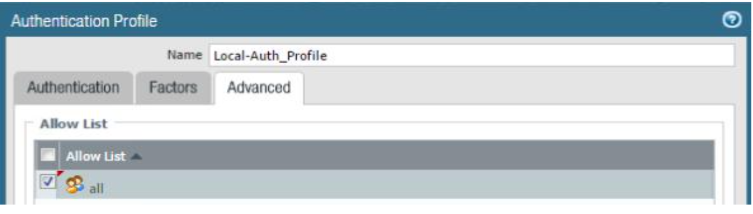
Module 1B (Lab 2): Configuring Authentication

Summary:

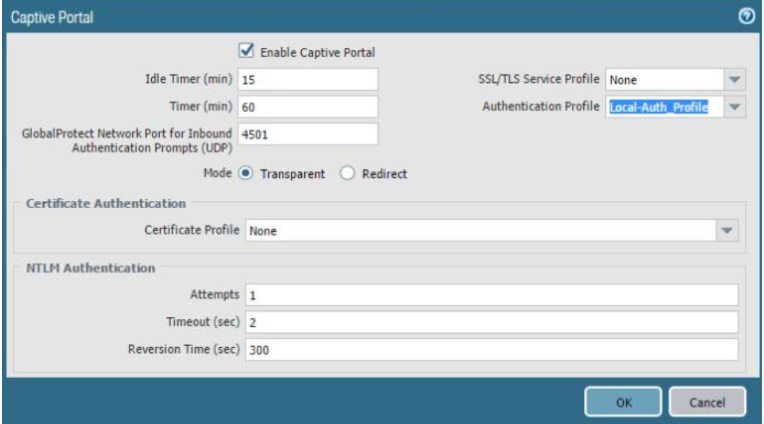
I implemented a captive portal gateway for accessing web services in Palo Alto Firewall. I also created local user authentication for security and monitoring. We also analysed logs of the user.

****

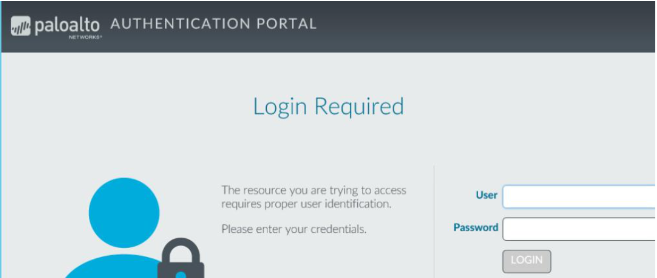
* Creating a Local User Account:

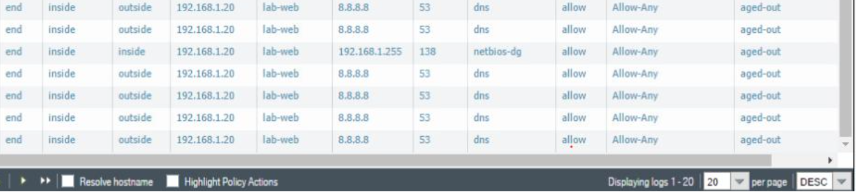


* Creating an Authentication Profile:



* Captive Portal Configurations
* Firewall Rules Configurations

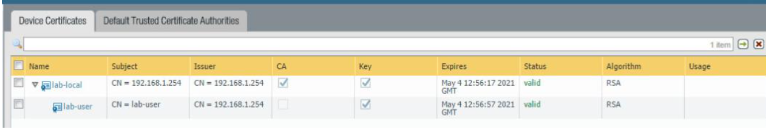


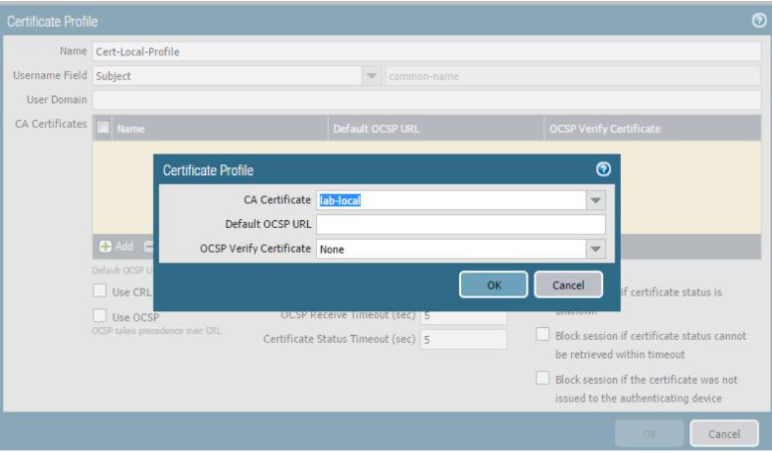
* After logging in:
* We can monitor the user’s activity.

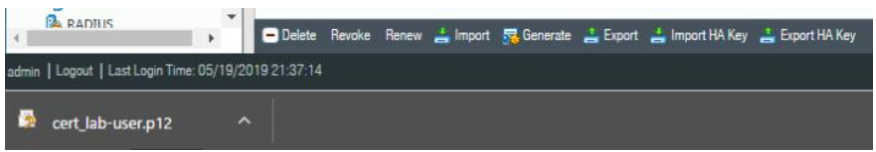
Module 2A (Lab 3): Using 2FA to secure the firewall:

Summary:

In this module, I enabled two factor authentication for Palo Alto Firewall using a digital certificate.



* Creating an account
* Creating Certificate Profile

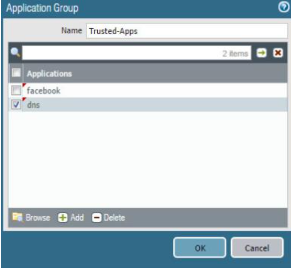


* Downloading Certificate for the user

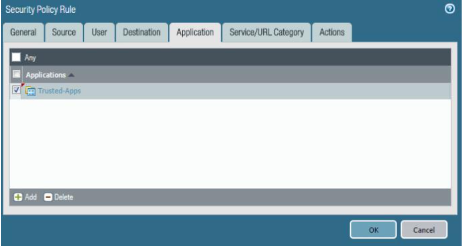
Module 2B (Lab 4): Allowing only Trusted Applications

Summary:

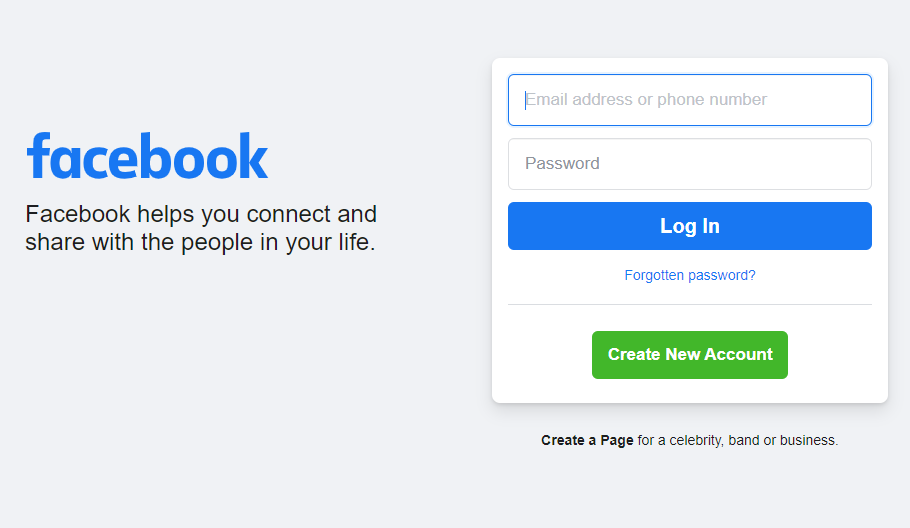
In this module, I configured my firewall to allow traffic from and to selected apps. First, I made an application group and added the websites to it. Then I configured security policy rule for the same. Then I tested it and observed the results.



* Application Group Configurations



* Security Policy Rule Configurations

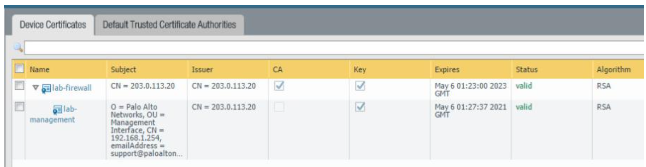


* Testing rules and configurations.

Module 3A (Lab 5): Managing Certificates

Summary:

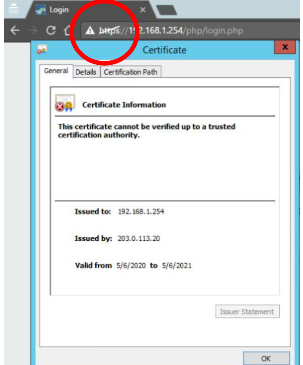
In this module, we generated a digital certificate for the inbound management traffic. After that we exported, tested and verified it.



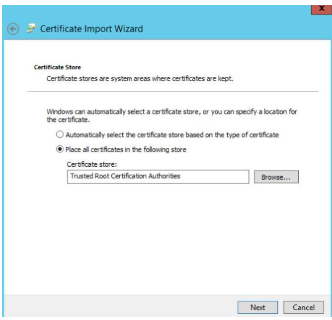
* Certificate Generation



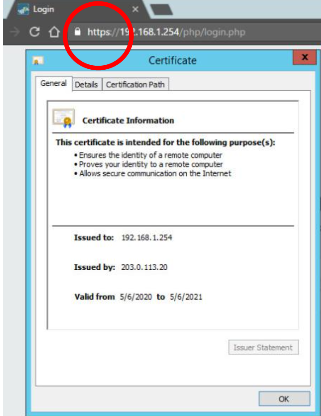
* Exporting Certificate



* Testing it and we can see that it is not verified.



* After downloading it locally, I imported it to certificates.msc utility.

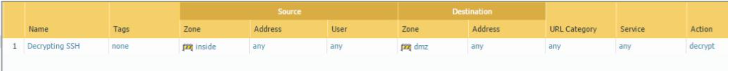


* Now we can observe that it is verified.

Module 3B (Lab 6&7): Decrypting SSH Traffic

Summary:

In this module, I decrypted some SSH packets. First, I created a policy for decryption from inside zone to DMZ. Then I generated SSH traffic towards DMZ. After that, I decrypted it using the same policy.



* Creation of the Policy



* Decrypting traffic in logs.



Project Introduction

In this project, I will configure the wire for a zero-trust environment.



November 29, 2020

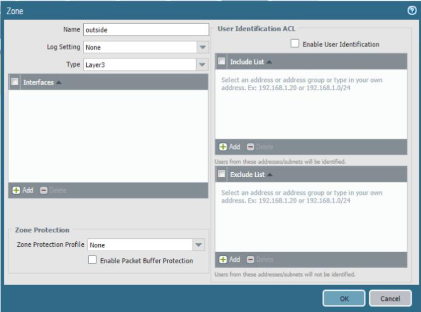
KIIT UNIVERSITY

Siddhant Kumar (1705348)

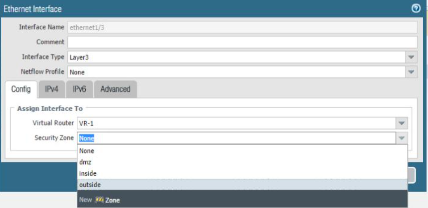
Objectives:

1. Create zones and associate the zones to interfaces.
2. Create a security policy rule.
3. Create a NAT policy.

Screenshots:



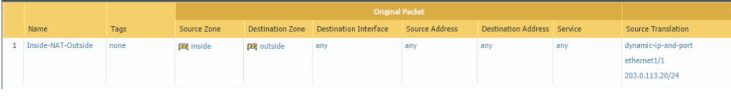
* Creating Zones



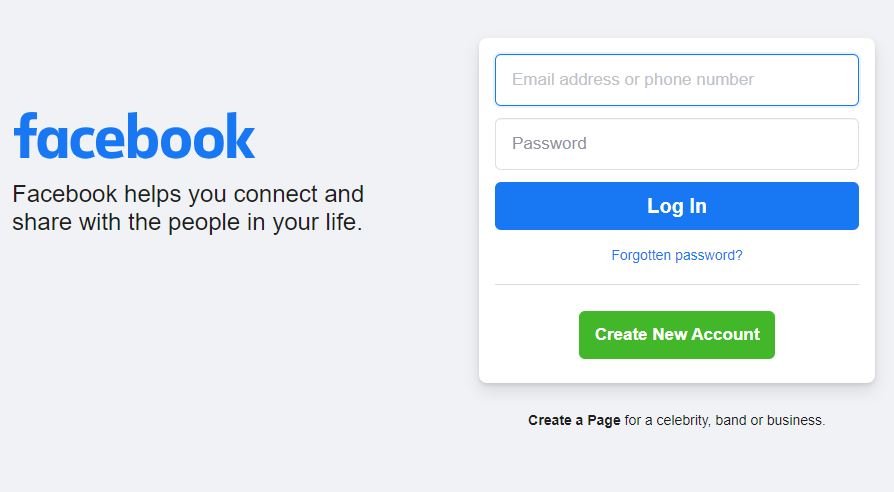
* Configuring Ethernet Interfaces



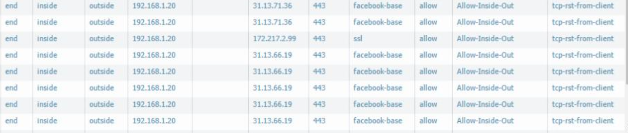
* Creation of Rules



* NAT Configurations



* Testing Facebook.com



* Detailed information about the traffic in logs.

----------------------------Siddhant Kumar 1705348------------------------------------------