

## Assignment Summary:

## In this capstone project, I configured and secured a network environment using a next-generation firewall. The project focused on properly segmenting the network into trusted (internal), untrusted (external), and DMZ zones, configuring interface IPs, and validating connectivity through various ping tests. Security and NAT policy rules were implemented to manage traffic flow and enforce access restrictions. Internal and DMZ hosts were granted internet access while specific external sites (e.g., Facebook, Twitter, Reddit, YouTube, and 2600.org) were successfully blocked based on URL filtering.

## I also configured firewall security profiles, including URL filtering, antivirus, DNS sinkhole, and WildFire integration. Internal users were protected from known malicious content—verified by blocking the Eicar test file and confirming WildFire logging for a simulated malware download. DNS sinkhole functionality was tested by triggering a malicious DNS request and verifying the event in the threat log. Additionally, I enabled secure access to DMZ services (FTP and SSH) for internal hosts using defined credentials, and ensured access to shared resources (like block-list.txt) over HTTP. This assignment enhanced my practical knowledge in firewall rule creation, NAT policy management, threat prevention, and secure service access configuration in a layered security architecture.

## Firewall configurations

* + - At the very beginning of the screenshots, include the complete **security policy**, **NAT policy**, **Zones**, **interfaces,** and **Security profile** configurations.

## Configure interfaces and zones (10%)

* + - Your internal hosts can ping 192.168.1.1

A screenshot of a computer

Description automatically generated

* + - From the firewall CLI, the following commands are successful:

**ping source 203.0.113.20 host 203.0.113.1**

A screenshot of a computer

Description automatically generated

**ping source 203.0.113.20 host 8.8.8.8**

A screenshot of a computer

Description automatically generated

**ping source 192.168.1.1 host 192.168.1.10**

A screenshot of a computer

Description automatically generated

**Ping source 192.168.50.1 host 192.168.50.10**

A screenshot of a computer

Description automatically generated

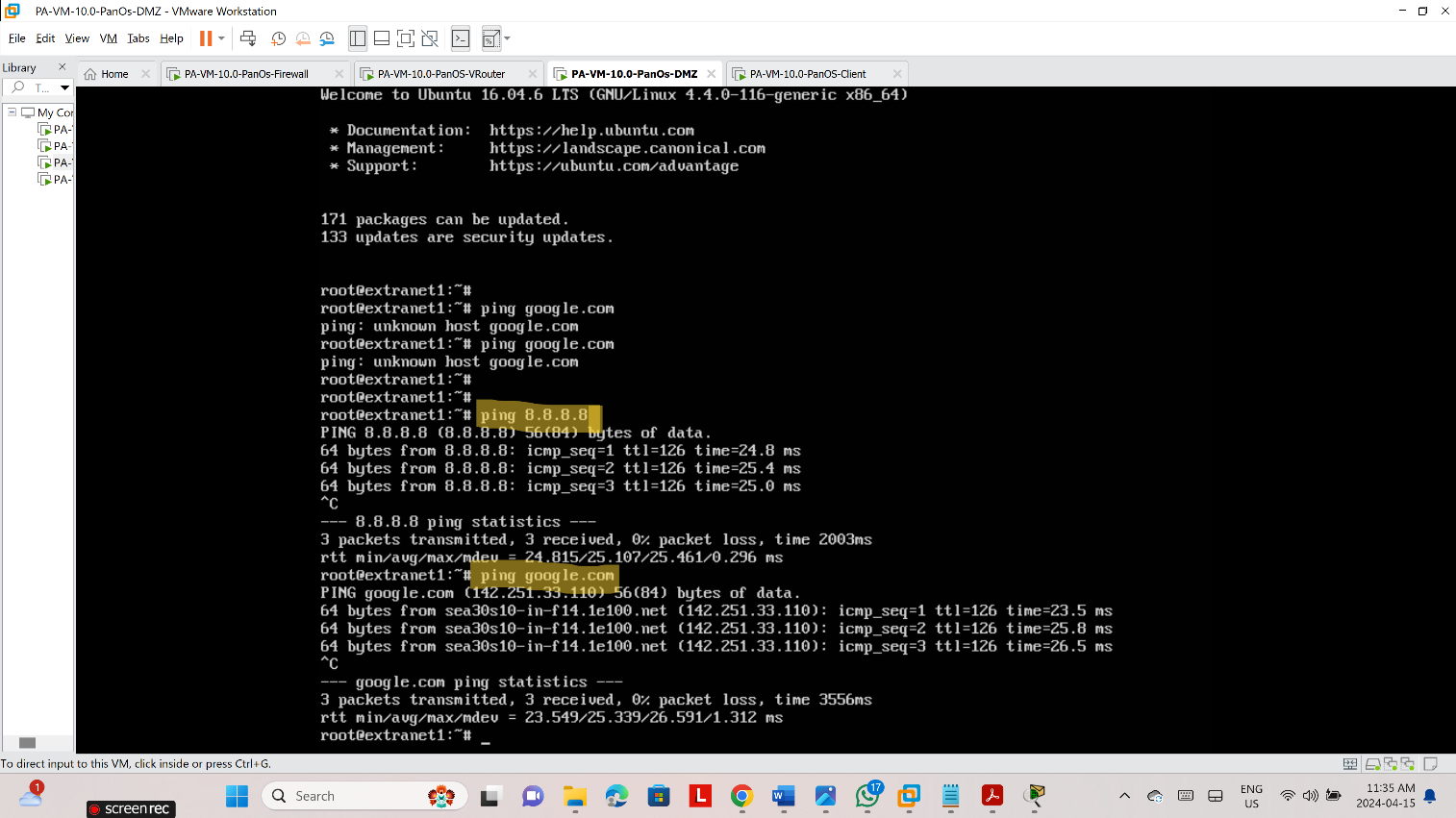
**Configure Security and NAT Policy Rules (10%)**

* + - The internal hosts can ping 8.8.8.8 and google.com.

A computer screen shot of a black and blue screen

Description automatically generated

* + - The DMZ host can ping 8.8.8.8 and google.com.



Internal hosts cannot access facebook.com, twitter.com, youtube.com, reddit.com, and 2600.org.

A screenshot of a computer

Description automatically generated

A computer screen shot of a computer

Description automatically generated

* + - The internal hosts can access <http://192.168.50.10/block-list.txt>
    - A screenshot of a computer

      Description automatically generated
    - The internal hosts can use FTP to access the DMZ host at 192.168.50.10 using the login name **lab-user** and the password **Pal0Alt0!**

A screenshot of a computer

Description automatically generated

Inernal hosts can use SSH to access the DMZ host at 192.168.50.10 using the login name **lab-user** and the password **Pal0Alt0!**

A screenshot of a computer

Description automatically generated

**Create and Apply Security Profiles (10%)**

* + - Three URL filtering configurations have been created and applied to the appropriate Security policy rule(s).

A computer screen shot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

The internal hosts cannot access twitter.com, youtube.com, reddit.com, and 2600.org.

A screenshot of a computer

Description automatically generatedA computer screen shot of a computer

Description automatically generatedA computer screen shot of a computer

Description automatically generated

* + - The DMZ host can ping box.net.

A screenshot of a computer

Description automatically generated

The internal hosts can access box.net.

A screenshot of a computer

Description automatically generated

* + - The internal hosts cannot download an eicar test virus (<http://www.virusanalyst.com/eicar.zip)> using HTTP.

A screenshot of a computer

Description automatically generated

* + - A WildFire test file (<http://wildfire.paloaltonetworks.com/publicapi/test/pe>) gets reported to the WildFire cloud when it is downloaded to the internal hosts.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

* + - A DNS request to phproxy.org initiated by an nslookup command on the internal hosts results in a sinkhole event recorded in the Threat log.

A computer screen shot of a black screen

Description automatically generated