SNMP and Syslog Configuration

Step by Step Configuration Guide

Intellectual Property

Table of Contents

1. Version Control

Version	Date	Notes	Created By	Release
1.0	15/03/2019	Initial Draft	Mazhar Minhas	Draft
1.1	21/06/2020	LAB Diagram and Document Layout Update	Farooq Zafar	Initial Release
1.2	01/04/2022	Workbook design and screenshots update	Farooq Zafar	V 2.0

2. Reference Document

Click for the Reference document

3. Assumption

- ✓ We understand that delegate already understand L2/L3, Routing.
- ✓ The delegate already knows the "***Fortray Networks – FortiGate NG Firewall"*** physical and logical connection.
- ✓ The delegate already has a basis Troubleshooting skill, such as ping and trace.
- ✓ The delegate already has access to the "***Fortray Networks – FortiGate NG Firewall"*** *Spreadsheet encompassing the Basic Layer, 2, 3 and allocated subnet information. For more details refer to the "****Student Folder".***
- ✓ This document is created to show an example for one topology only. The candidate needs to refer to his own topology and follow this step-by-step guide.
- ✓ We assume that delegate already has installed the VPN software and him/she have VPN user / Password. If any issue, contact our technical team.
- ✓ Our VPN software is supported by PC, MAC, Android, and IOS devices.
- ✓ It's also assumed that delegate has access to PC/Laptop i5 with 4GB RAM.
- ✓ For optimal connectivity, we recommend at least 10MB internet connection.
- ✓ We assume that we already have INTERNAL, DMZ, OUTISE interfaces that are already configured.

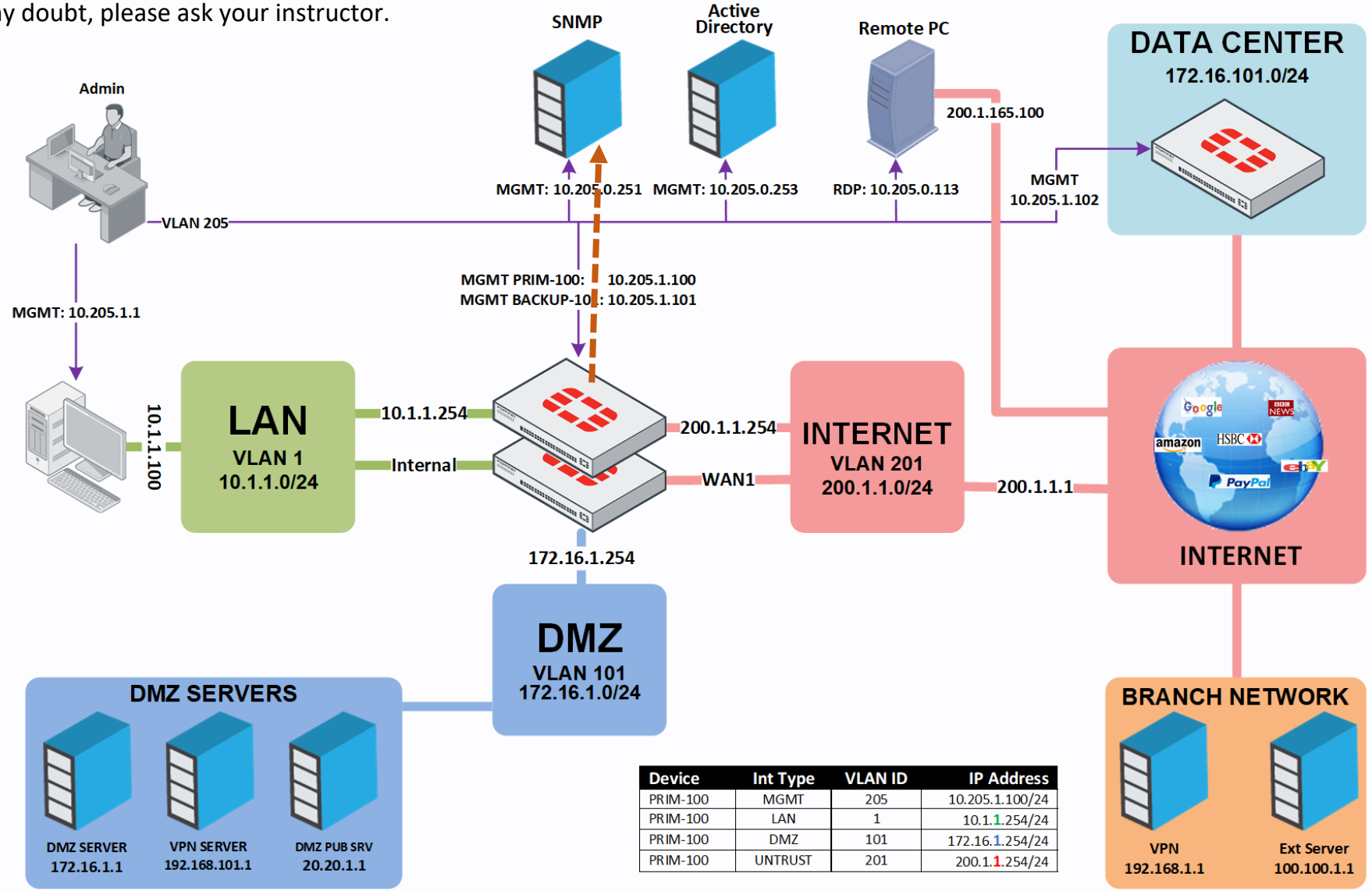
4. Fortray - Fortinet NSE4 - NOTE About Configuration Example

The configuration example is based in the "**VLAN-1**".

Please refer to "**Student Spread Sheet**" and complete your task based on your Network Topology, & Task list assigned.

5. Fortray - Fortinet NSE4 - LAB Network Topology

The below network topology is just for information purpose only. Please refer to your student folder and your designated topology.
If any doubt, please ask your instructor.



Device	Int Type	VLAN ID	IP Address
PRIM-100	MGMT	205	10.205.1.100/24
PRIM-100	LAN	1	10.1.1.254/24
PRIM-100	DMZ	101	172.16.1.254/24
PRIM-100	UNTRUST	201	200.1.1.254/24

6. Fortray - Fortinet NSE4 - LAB MGMT Access

Refer to the below table and login to Fortinet NG Firewall, and Test machine.

Each delegate has his /her own test machine, refer to the spreadsheet provided in the student shared folder

Device Name	Type	IP	Access Method	Default User	Password	New Password
FN-FORTI-PRIM-100	NG Firewall	10.205.1.100	HTTPS/SSH	admin	admin	AD/user
FN-FORTI-BACK-101	NG Firewall	10.205.1.101	HTTPS/SSH	admin	admin	AD/user
FN-FORTI-PC-01	TEST PC	10.205.1.1	RDP	administrator	cisco	N/A
FN-LAB-AD	Certificate Server Active Directory	10.205.0.253	HTTP/LDAP	<your vpn user>@fortraylab.com Password is emailed		
Remote-PC	Remote-PC	10.205.0.113	RDP	Refer to Spreadsheet		

Warning: Please don't change the above password for any devices.

7. Fortray - Fortinet NSE4 - LAB Spreadsheet

Refer to below table and login to SNMP Server:

Test-PCs, Remote-PC and SNMP Server											
VDOM / VLAN			Test PC (RDP)			Remote Test PC 10.205.0.113		SNMP & Syslog Server Parameters			
NO	VDOM	VLAN	IP Address	Username	Password	User Name	Password	Server IP Address	Community String	Username	Password
1	root	1	10.205.1.1	administrator	cisco	<your VPN user>@fortraylab.com	emailed earlier	10.205.0.251	fortraylab.com	user01	Cisco@123
2	VDOM-2	2	10.205.0.2	administrator	cisco	<your VPN user>@fortraylab.com	emailed earlier	10.205.0.251	fortraylab.com	user02	Cisco@123
3	VDOM-3	3	10.205.0.3	administrator	cisco	<your VPN user>@fortraylab.com	emailed earlier	10.205.0.251	fortraylab.com	user03	Cisco@123
4	VDOM-4	4	10.205.0.4	administrator	cisco	<your VPN user>@fortraylab.com	emailed earlier	10.205.0.251	fortraylab.com	user04	Cisco@123
5	VDOM-5	5	10.205.0.5	administrator	cisco	<your VPN user>@fortraylab.com	emailed earlier	10.205.0.251	fortraylab.com	user05	Cisco@123
6	VDOM-6	6	10.205.0.6	administrator	cisco	<your VPN user>@fortraylab.com	emailed earlier	10.205.0.251	fortraylab.com	user06	Cisco@123
7	VDOM-7	7	10.205.0.7	administrator	cisco	<your VPN user>@fortraylab.com	emailed earlier	10.205.0.251	fortraylab.com	user07	Cisco@123
8	VDOM-8	8	10.205.0.8	administrator	cisco	<your VPN user>@fortraylab.com	emailed earlier	10.205.0.251	fortraylab.com	user08	Cisco@123
9	VDOM-9	9	10.205.0.9	administrator	cisco	<your VPN user>@fortraylab.com	emailed earlier	10.205.0.251	fortraylab.com	user09	Cisco@123
10	VDOM-10	10	10.205.0.10	administrator	cisco	<your VPN user>@fortraylab.com	emailed earlier	10.205.0.251	fortraylab.com	user10	Cisco@123

8. Fortray - Fortinet NSE4 - LAB Task: SNMP and Syslog Server

Fortray Networks head office "**Security Consultant**" asked to configure SNMP and Syslog Server in FortiGate to ensure performance, health, and configuration monitoring. Please follow spreadsheet.

In the activity, we are going to learn, how to Configure SNMP Server.

Summary steps to be done by the network administrator are mentioned below: -

Steps needed to be done to accomplish this task is

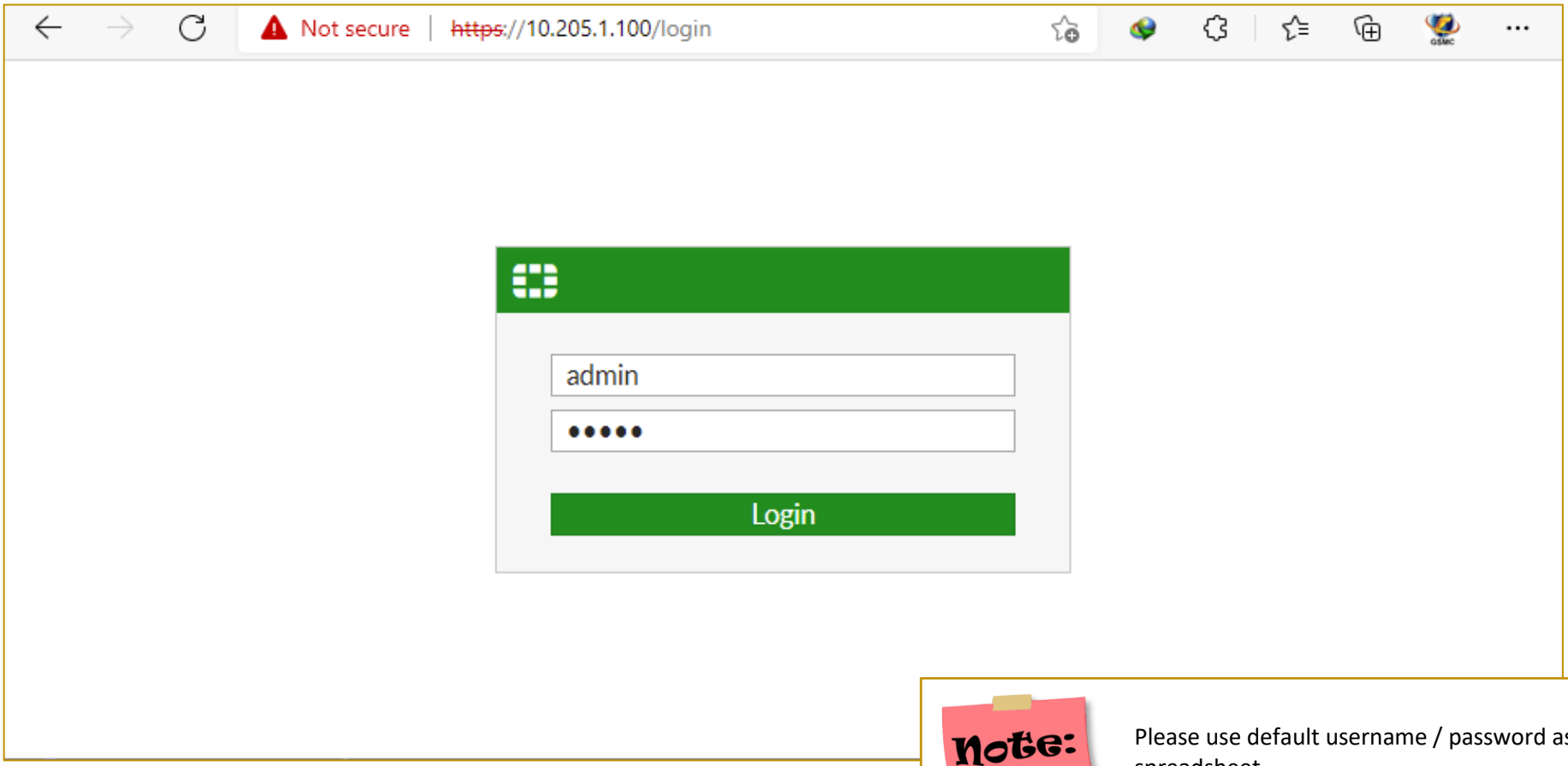
- Connecting to Fortinet Primary Firewall https://10.205.1.100/login
- Configuring SNMP Server
- Configuring Syslog Server
- Verification

9. Fortray - Fortinet NSE4 - LAB Configuration: SNMP and Syslog Server

In this section, we will configure SNMP and Syslog Server.

9.1 Step 1: Login to Fortinet Firewall

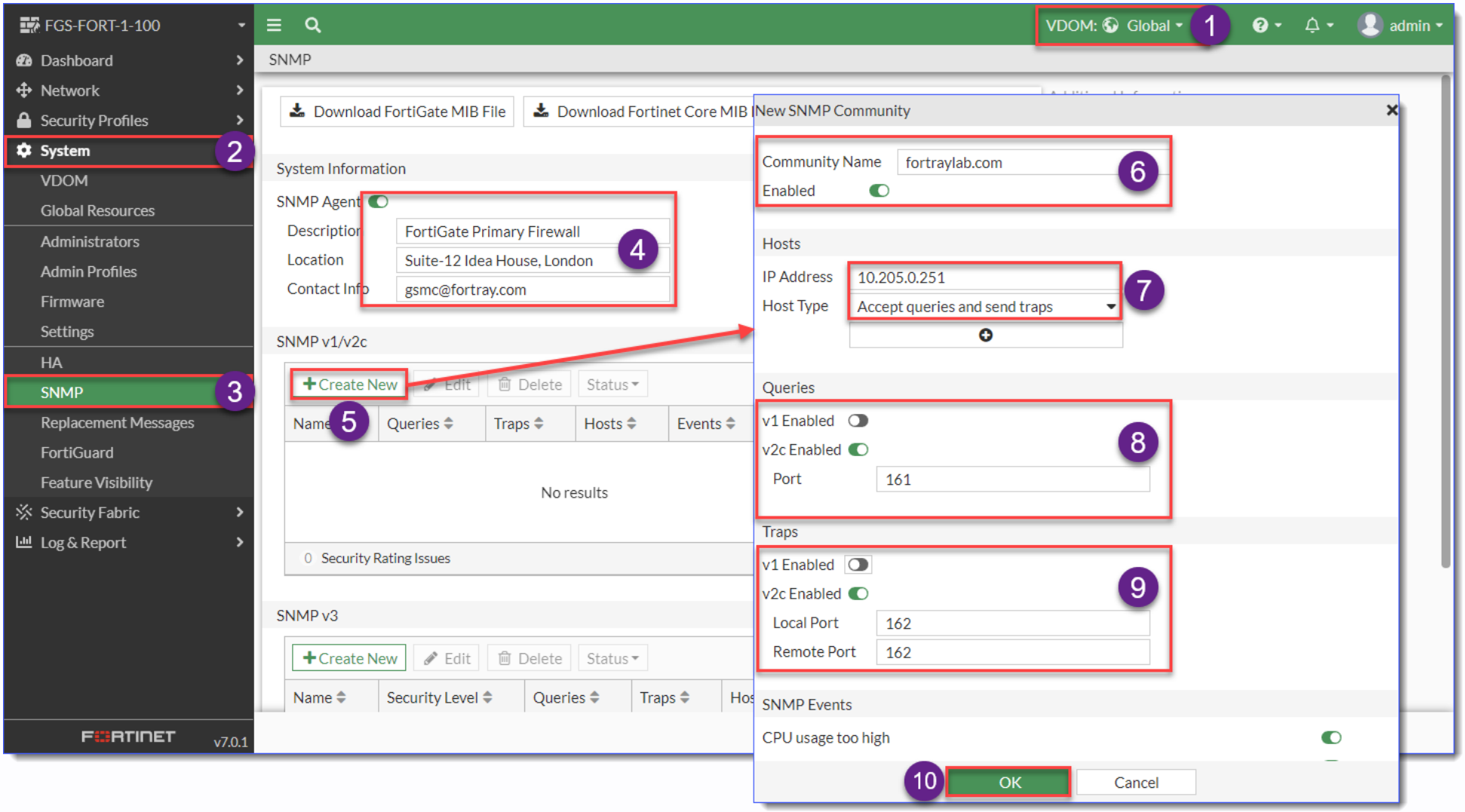
Use any browser and type https://10.205.1.100/login use the default user /password provided by the trainer. In this example, we are using Google Chrome Browser. Here is screenshot of web browser, the login page of Fortinet NG Firewall.



Note: Please use default username / password as per spreadsheet.

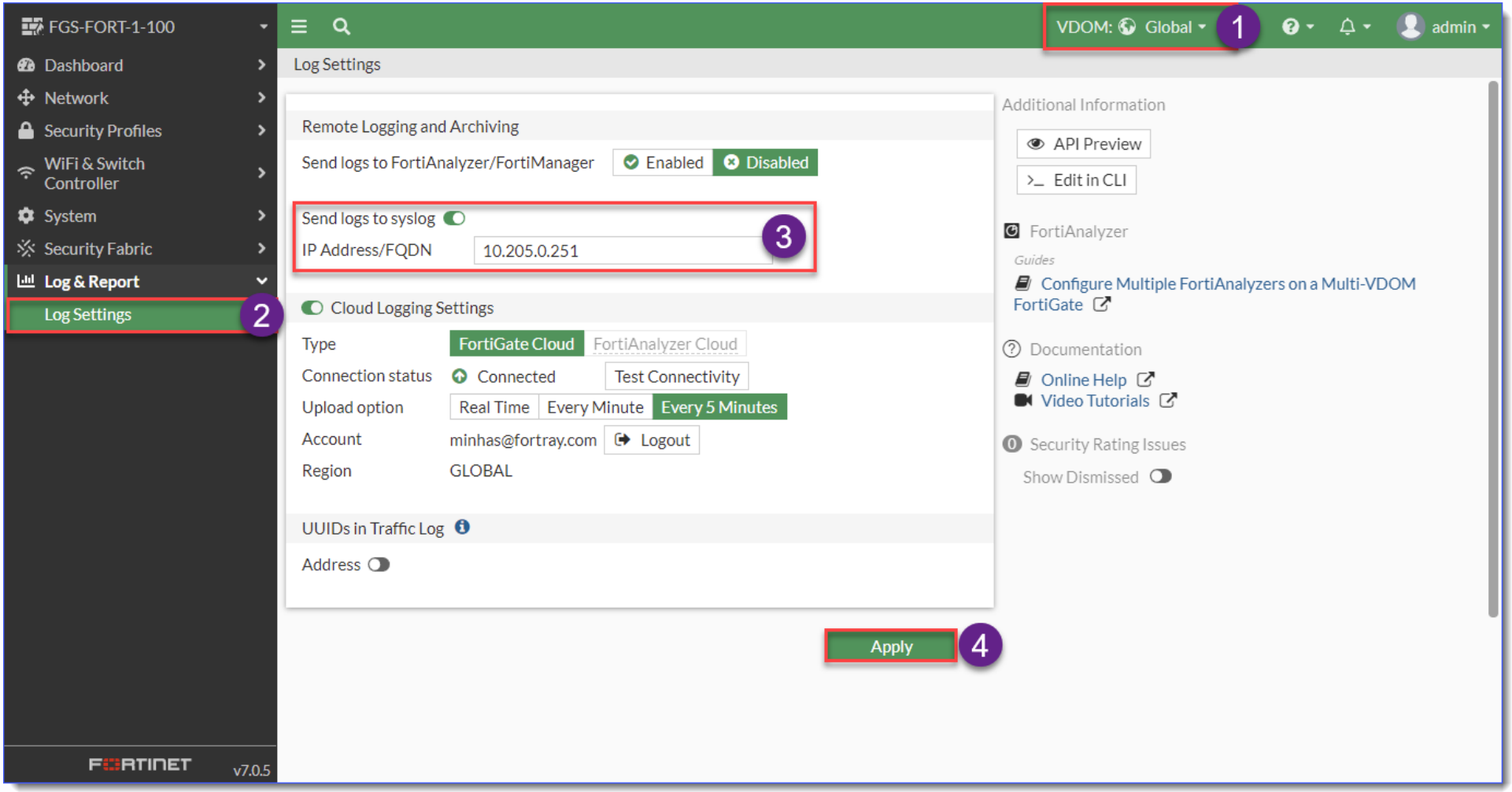
9.2 Step 2: Configuring SNMP Server

In FortiGate we can configure SNMP server as following:



9.3 Step 2: Configuring Syslog Server

In Fortinet Firewall, follow these steps to configure Syslog Server.

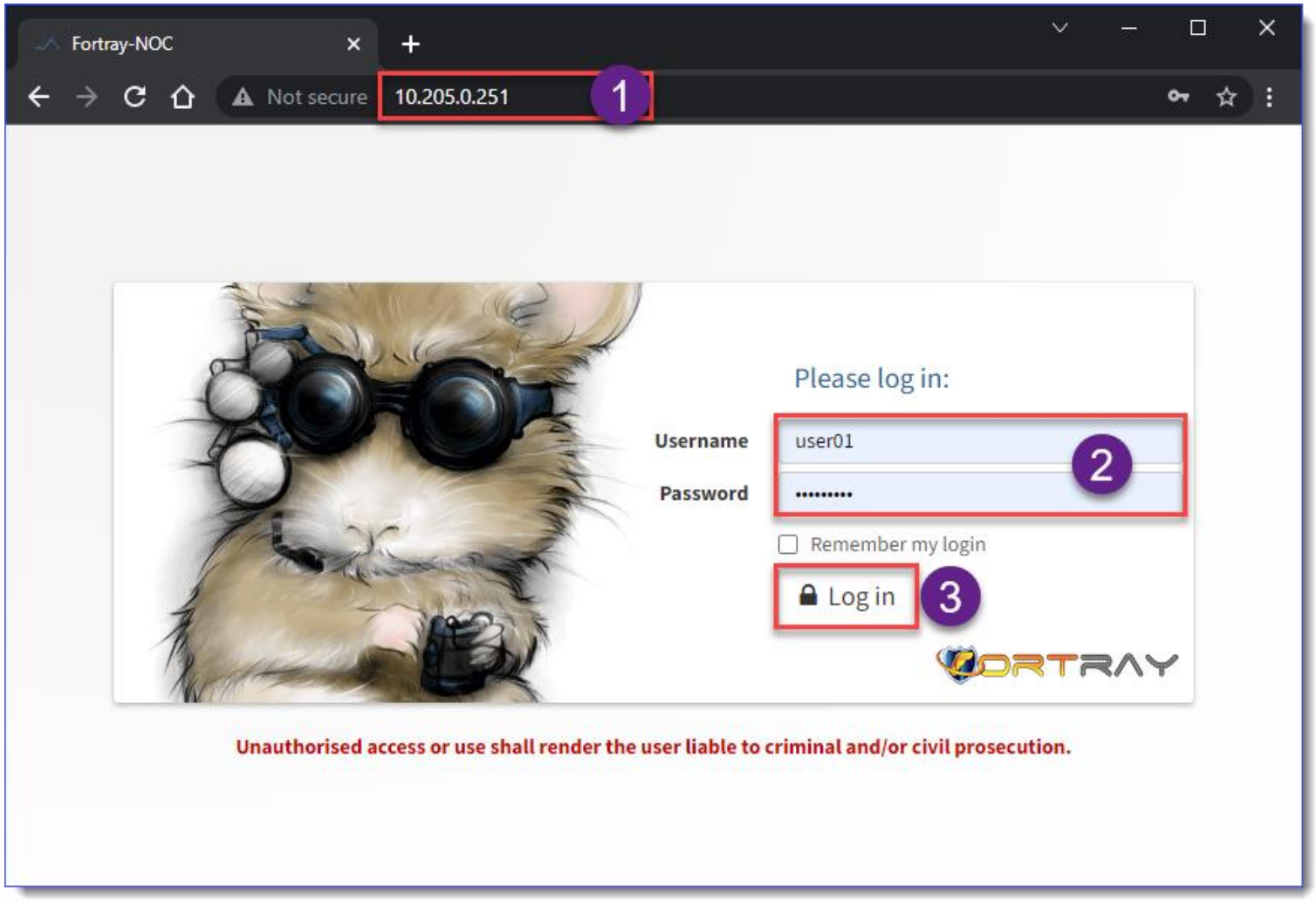


10. Fortray - Fortinet NSE4 - LAB Verification

In this section, we will verify LAB Configuration.

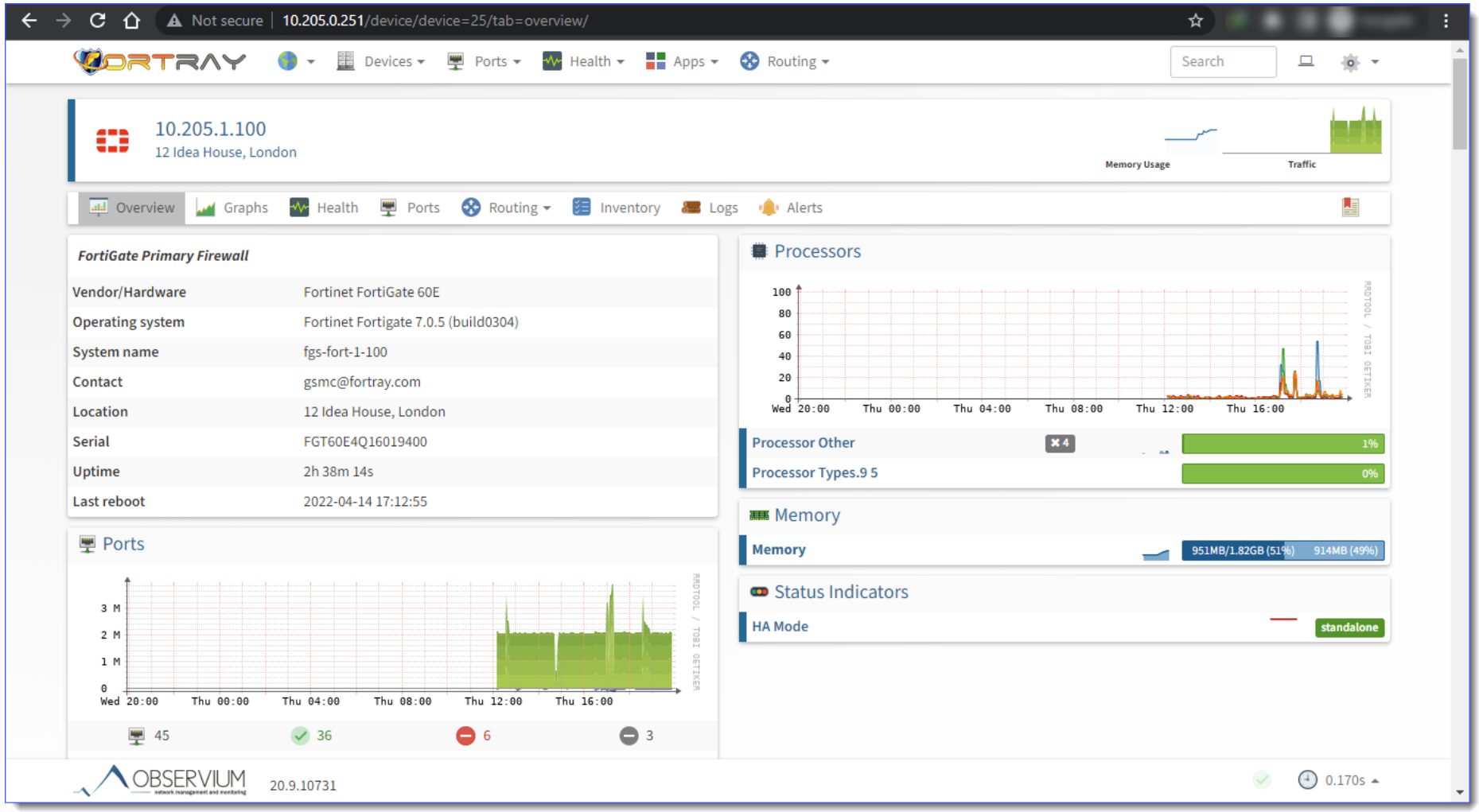
10.1 Step 1: Login to Fortray NOC Server

Open the page http://10.205.0.251 in web browser. And login using your own user/password created in previous step.



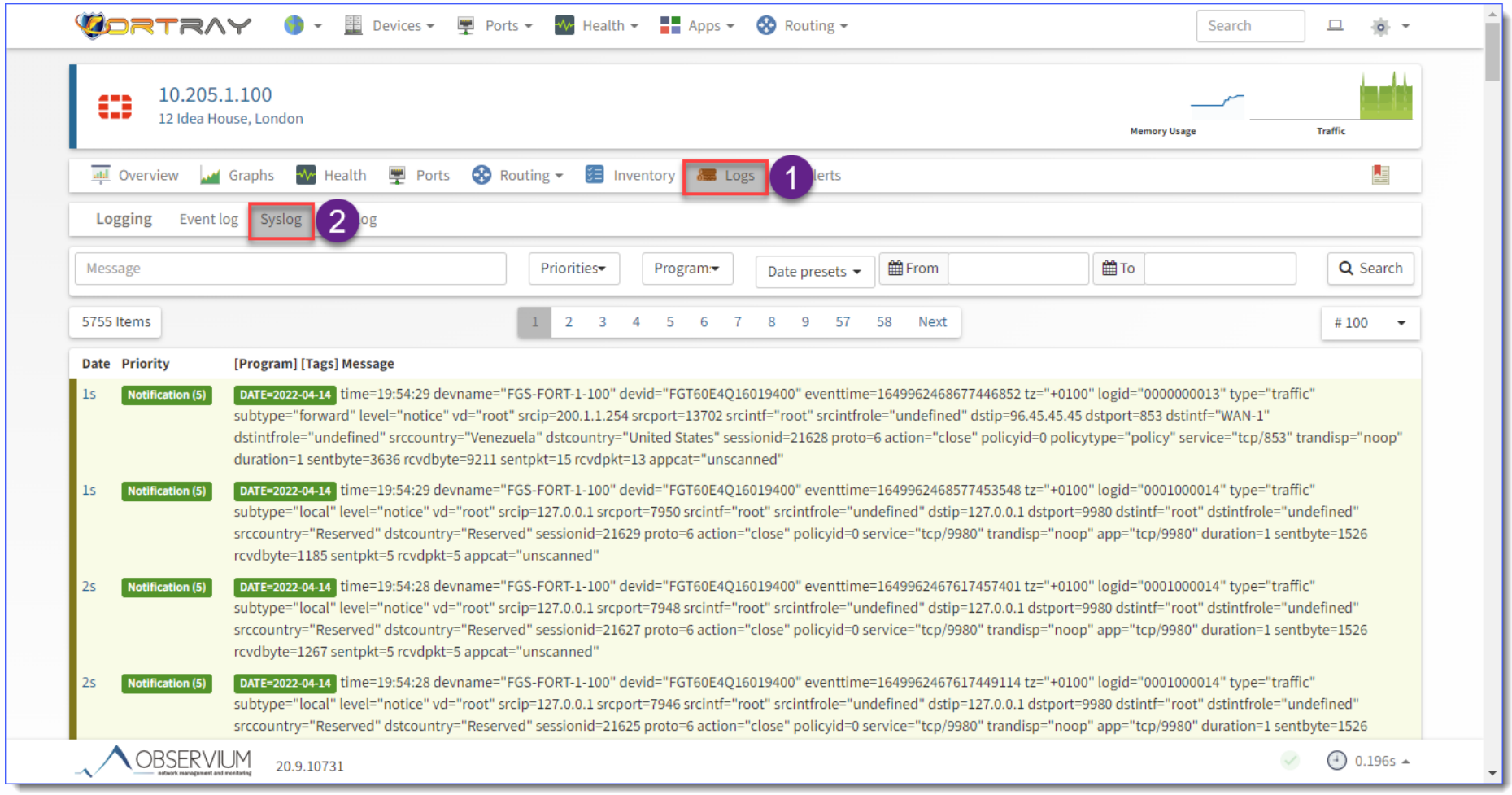
10.2 Step 2: SNMP Verification

Find device in Device List, as device is already added in this server.



10.3 Step 3: Syslog Verification

Click on Logs > Syslog



Thanks, and Good Luck