

FORTINET®



SNMP and Syslog Configuration

Step by Step Configuration Guide

Intellectual Property

*The Copyright in this work is vested in **Fortray Networks Limited** and the document is issued in confidence for the express purpose for which it is supplied. It must not be reproduced, in whole or in part, or be used for any other purpose without prior written consent being obtained from **Fortray Networks Limited**, and then only on the condition that this notice is included in any such reproduction. No information as to the contents or subject matter of this document or any part thereof arising directly or indirectly therefrom shall be given orally or in writing or communicated in any manner whatsoever to any third party without the prior written consent of **Fortray Networks Limited**.*

© Copyright Fortray Networks Limited 2011-2020



Table of Contents

Table of Contents.....	3
1. Version Control.....	4
2. Reference Document.....	4
3. Assumption.....	4
4. Fortray - Fortinet NSE4 - NOTE About Configuration Example	5
5. Fortray - Fortinet NSE4 - LAB Network Topology	6
6. Fortray - Fortinet NSE4 - LAB MGMT Access.....	7
7. Fortray - Fortinet NSE4 - LAB Spreadsheet.....	8
8. Fortray - Fortinet NSE4 - LAB Task: SNMP and Syslog Server.....	9
9. Fortray - Fortinet NSE4 - LAB Configuration: SNMP and Syslog Server.....	10
9.1 Step 1: Login to Fortinet Firewall.....	10
9.2 Step 2: Configuring SNMP Server.....	11
9.3 Step 2: Configuring Syslog Server	12
10. Fortray - Fortinet NSE4 - LAB Verification	13
10.1 Step 1: Login to Fortray NOC Server	13
10.2 Step 2: SNMP Verification.....	14
10.3 Step 3: Syslog Verification.....	15



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



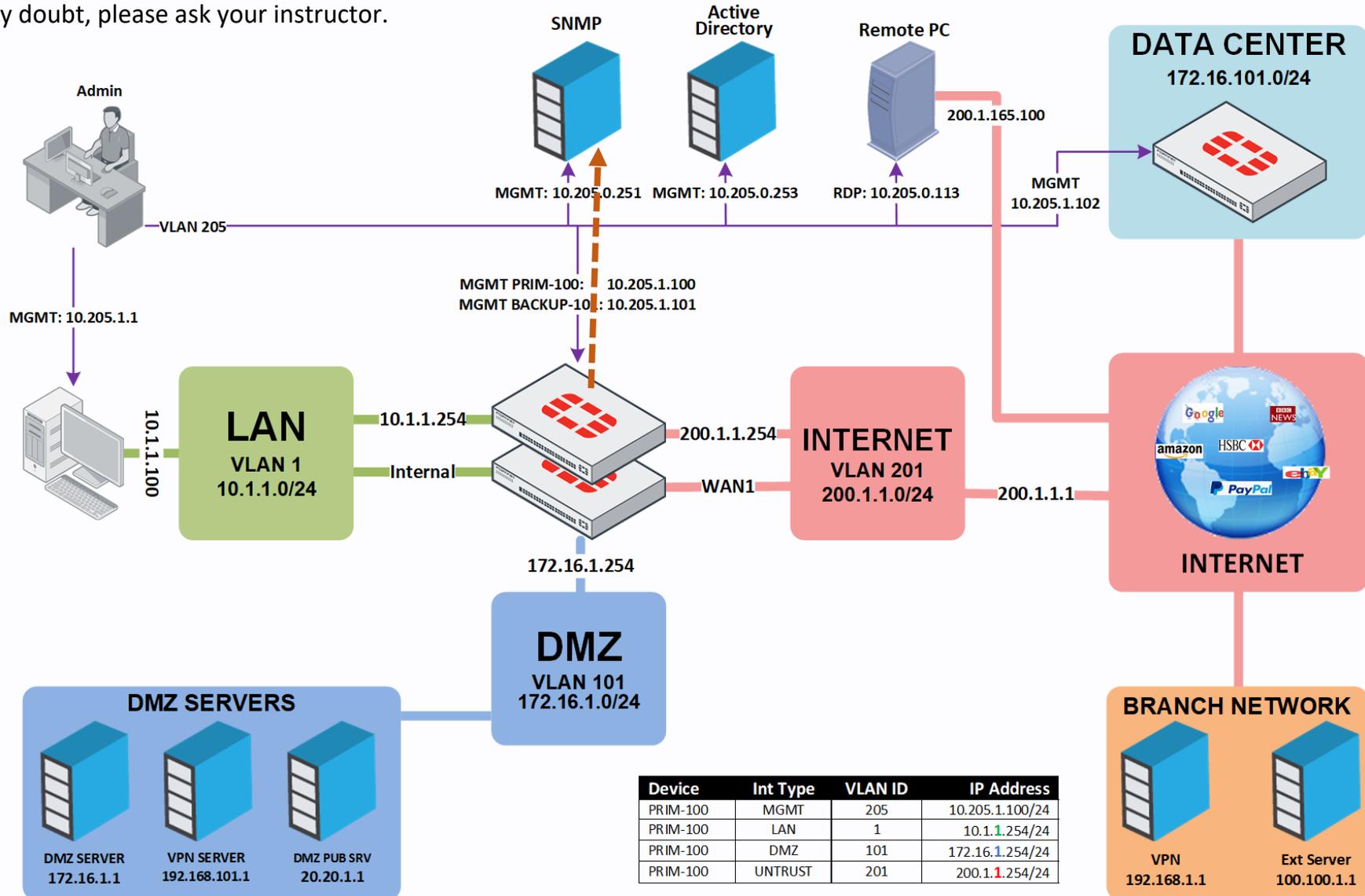
The configuration example is based in the “**VLAN-1**”.

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.



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

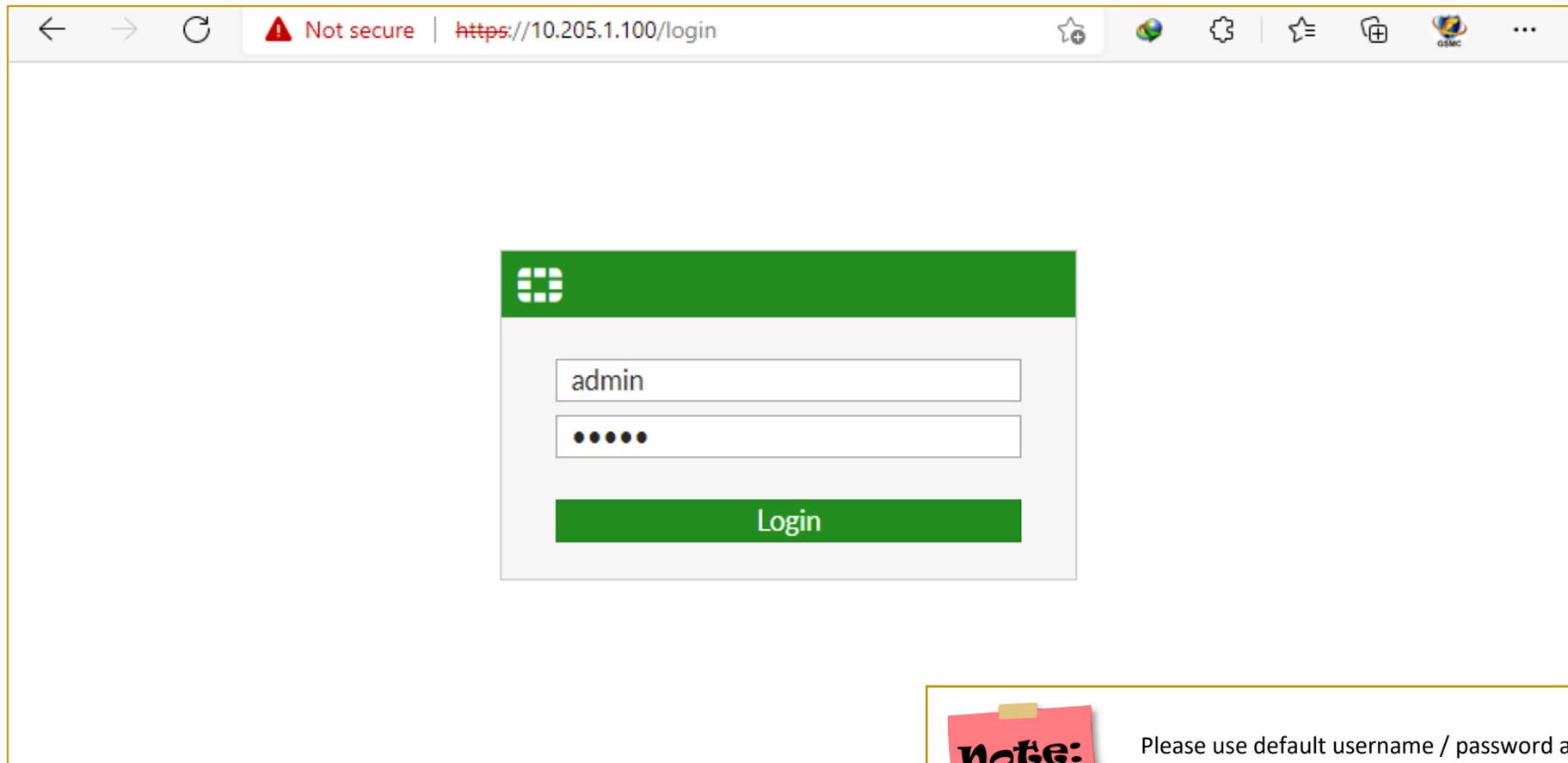
- Connecting to Fortinet Primary Firewall <https://10.205.1.100/login>
- Configuring SNMP Server
- Configuring Syslog Server
- Verification

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:

The screenshot displays the FortiGate web interface for configuring an SNMP server. The interface is divided into a sidebar on the left and a main content area. The sidebar shows the 'System' menu (2) and the 'SNMP' menu (3). The main content area shows the 'SNMP' configuration page. The 'System Information' section (4) includes fields for Description, Location, and Contact Info. The 'SNMP v1/v2c' section (5) has a '+ Create New' button. A dialog box titled 'New SNMP Community' is open, showing the following configuration steps:

- VDOM: Global (1)
- Community Name: fortraylab.com (6)
- Hosts: IP Address 10.205.0.251, Host Type: Accept queries and send traps (7)
- Queries: v1 Enabled (off), v2c Enabled (on), Port: 161 (8)
- Traps: v1 Enabled (off), v2c Enabled (on), Local Port: 162, Remote Port: 162 (9)
- SNMP Events: CPU usage too high (10)

9.3 Step 2: Configuring Syslog Server

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

The screenshot displays the Fortinet Firewall management interface for device FGS-FORT-1-100. The left sidebar shows the navigation menu with 'Log & Report' selected and 'Log Settings' highlighted. The main content area is titled 'Log Settings' and includes the following sections:

- Remote Logging and Archiving:** 'Send logs to FortiAnalyzer/FortiManager' is set to 'Enabled'. 'Send logs to syslog' is also enabled, with the 'IP Address/FQDN' field containing '10.205.0.251'.
- Cloud Logging Settings:** 'Type' is set to 'FortiGate Cloud'. 'Connection status' is 'Connected'. 'Upload option' is set to 'Every 5 Minutes'. 'Account' is 'minhas@fortray.com' and 'Region' is 'GLOBAL'.
- UIIDs in Traffic Log:** 'Address' is disabled.

Additional Information on the right includes links for 'API Preview', 'Edit in CLI', 'FortiAnalyzer Guides', 'Configure Multiple FortiAnalyzers on a Multi-VDOM FortiGate', 'Documentation', 'Online Help', 'Video Tutorials', and 'Security Rating Issues'.

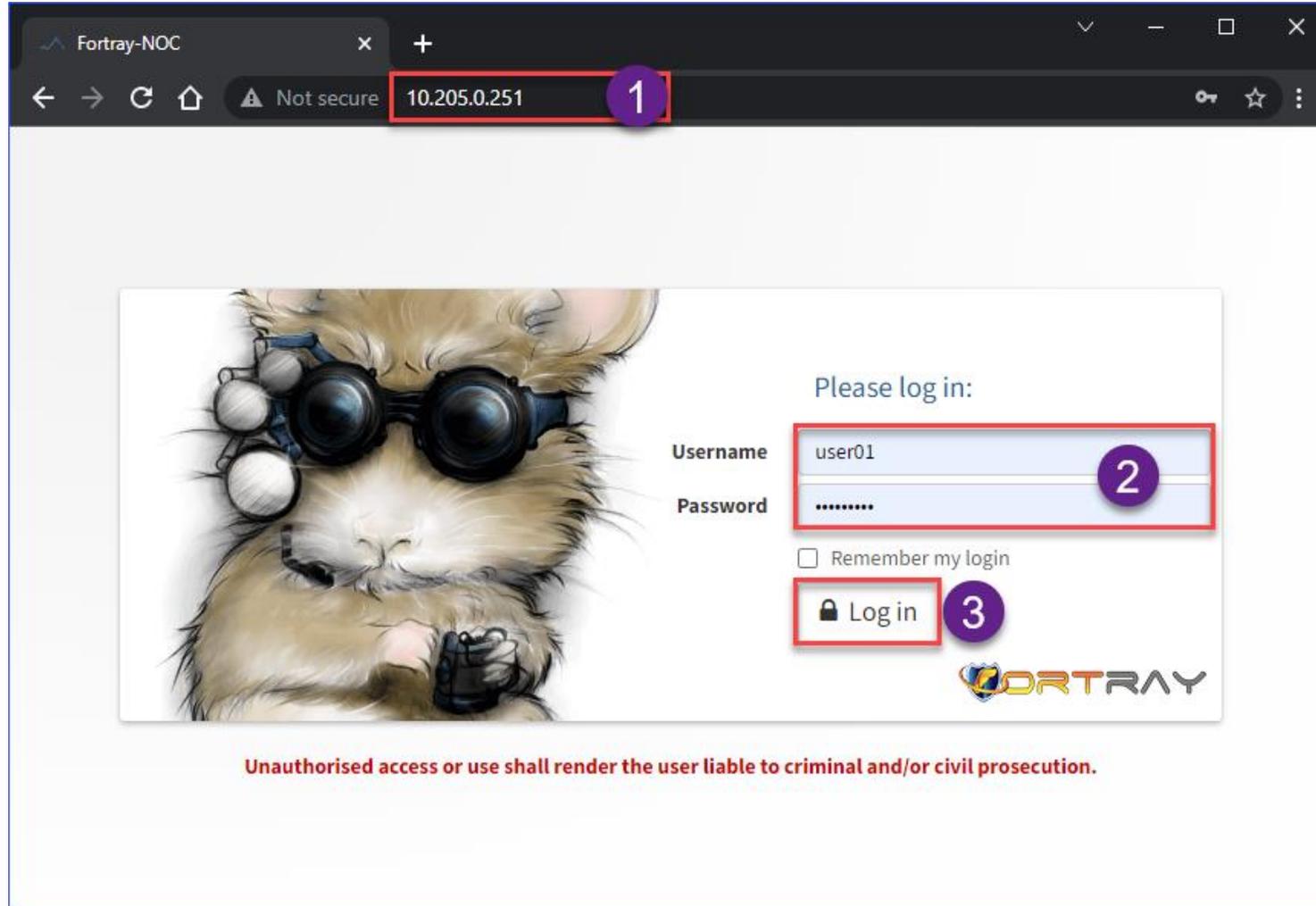
Four numbered callouts indicate the steps: 1. VDOM: Global dropdown, 2. Log Settings menu item, 3. IP Address/FQDN input field, and 4. Apply button.

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.

The screenshot displays the Fortray web interface for a FortiGate Primary Firewall. The browser address bar shows the URL `10.205.0.251/device/device=25/tab=overview/`. The interface includes a navigation menu with options like Devices, Ports, Health, Apps, and Routing. The main content area is divided into several sections:

- Device Overview:** Shows the IP address `10.205.1.100` and location `12 Idea House, London`. It includes small charts for Memory Usage and Traffic.
- FortiGate Primary Firewall Details:**

Vendor/Hardware	Fortinet FortiGate 60E
Operating system	Fortinet Fortigate 7.0.5 (build0304)
System name	fgs-fort-1-100
Contact	gsmc@fortray.com
Location	12 Idea House, London
Serial	FGT60E4Q16019400
Uptime	2h 38m 14s
Last reboot	2022-04-14 17:12:55
- Processors:** A line graph showing processor usage over time. Below the graph, a table shows processor status:

Processor Other	4	1%
Processor Types.9 5		0%
- Memory:** A bar chart showing memory usage. Below the chart, a table shows memory status:

Memory	951MB/1.82GB (51%)	914MB (49%)
--------	--------------------	-------------
- Status Indicators:** Shows the HA Mode as `standalone`.
- Ports:** A bar chart showing port activity. Below the chart, a table shows port status:

45	36	6	3
----	----	---	---

The footer of the interface includes the Observium logo and version `20.9.10731`, along with a refresh button and a loading time of `0.170s`.

10.3 Step 3: Syslog Verification

Click on Logs > Syslog

The screenshot displays the Fortray web interface for a device with IP 10.205.1.100. The navigation menu includes Overview, Graphs, Health, Ports, Routing, Inventory, Logs (1), and Alerts. Under the Logs section, the Syslog (2) option is selected. The interface shows 5755 items and a search bar. The log entries are as follows:

Date	Priority	[Program] [Tags] Message
2022-04-14 19:54:29	Notification (5)	time=19:54:29 devname="FGS-FORT-1-100" devid="FGT60E4Q16019400" eventtime=1649962468677446852 tz="+0100" logid="000000013" type="traffic" subtype="forward" level="notice" vd="root" srcip=200.1.1.254 srcport=13702 srcintf="root" srcintfrole="undefined" dstip=96.45.45.45 dstport=853 dstintf="WAN-1" dstintfrole="undefined" srccountry="Venezuela" dstcountry="United States" sessionid=21628 proto=6 action="close" policyid=0 policytype="policy" service="tcp/853"trandisp="noop" duration=1 sentbyte=3636 rcvbyte=9211 sentpkt=15 rcvdpkt=13 appcat="unscanned"
2022-04-14 19:54:28	Notification (5)	time=19:54:28 devname="FGS-FORT-1-100" devid="FGT60E4Q16019400" eventtime=1649962467617457401 tz="+0100" logid="0001000014" type="traffic" subtype="local" level="notice" vd="root" srcip=127.0.0.1 srcport=7948 srcintf="root" srcintfrole="undefined" dstip=127.0.0.1 dstport=9980 dstintf="root" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" sessionid=21627 proto=6 action="close" policyid=0 service="tcp/9980"trandisp="noop" app="tcp/9980" duration=1 sentbyte=1526 rcvbyte=1185 sentpkt=5 rcvdpkt=5 appcat="unscanned"
2022-04-14 19:54:28	Notification (5)	time=19:54:28 devname="FGS-FORT-1-100" devid="FGT60E4Q16019400" eventtime=1649962467617449114 tz="+0100" logid="0001000014" type="traffic" subtype="local" level="notice" vd="root" srcip=127.0.0.1 srcport=7946 srcintf="root" srcintfrole="undefined" dstip=127.0.0.1 dstport=9980 dstintf="root" dstintfrole="undefined" srccountry="Reserved" dstcountry="Reserved" sessionid=21625 proto=6 action="close" policyid=0 service="tcp/9980"trandisp="noop" app="tcp/9980" duration=1 sentbyte=1526 rcvbyte=1185 sentpkt=5 rcvdpkt=5 appcat="unscanned"

Thanks, and Good Luck

