SIEM Logs & Events

Ali Ali

Digitally signed by Ali Ali
DN: c=LB, st=Beirut, l=AA, o=MISC, ou=ISC, cn=Ali Ali
Date: 2024.12.16 07:34:16 +03'00'

A

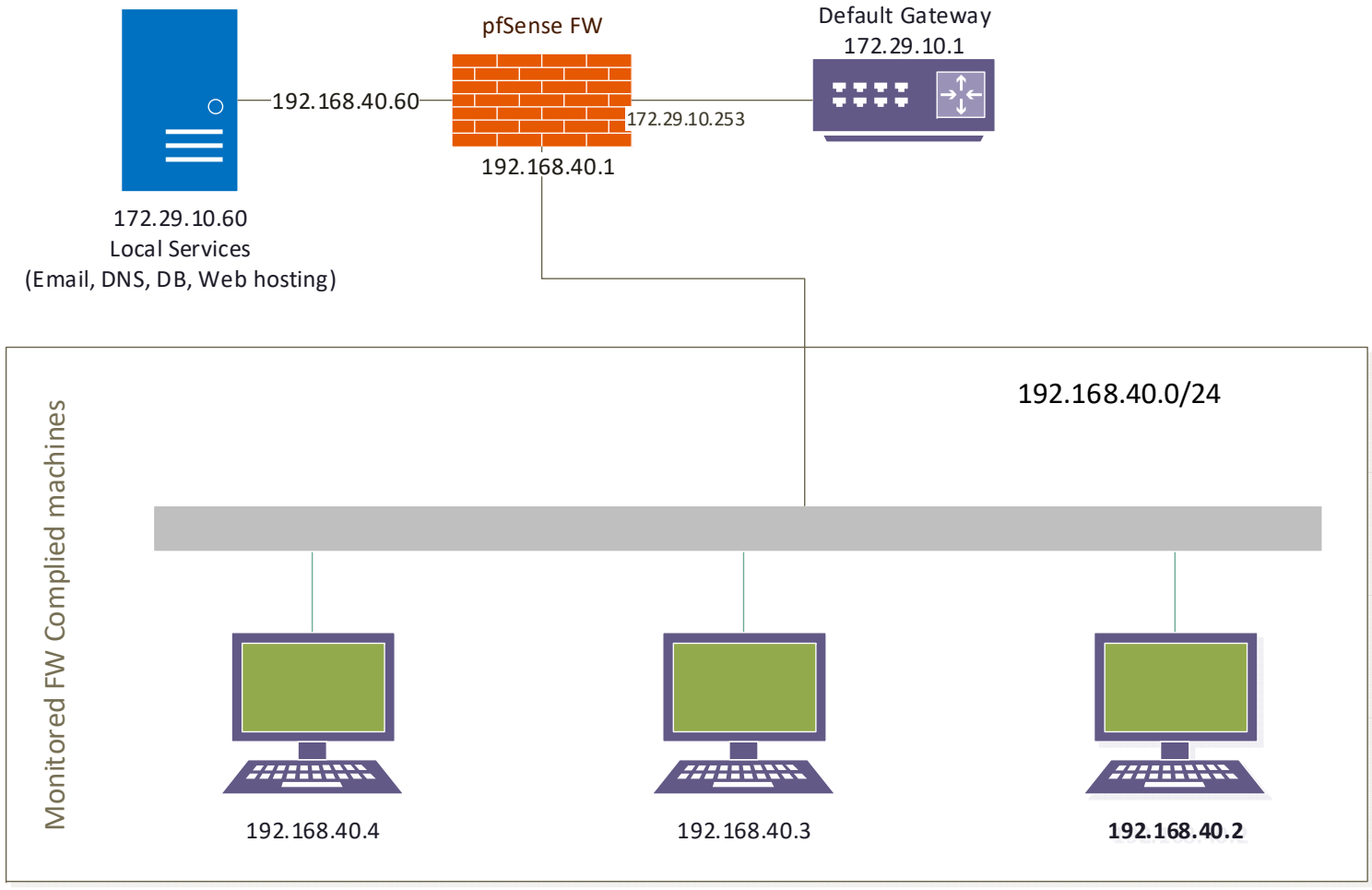
With Ali Ali

SIEM Logs & Events

Remote logging Scenario

❑ Lab Planning:

1. **Connect agentless devices to Wazuh via Syslog including:**
   - Install and configure PfSense firewall and create new network
   - Link firewall to other services (including windows and Linux machines and services)
   - Forward issued logs to Wazuh manager
2. **Planning diagram:**

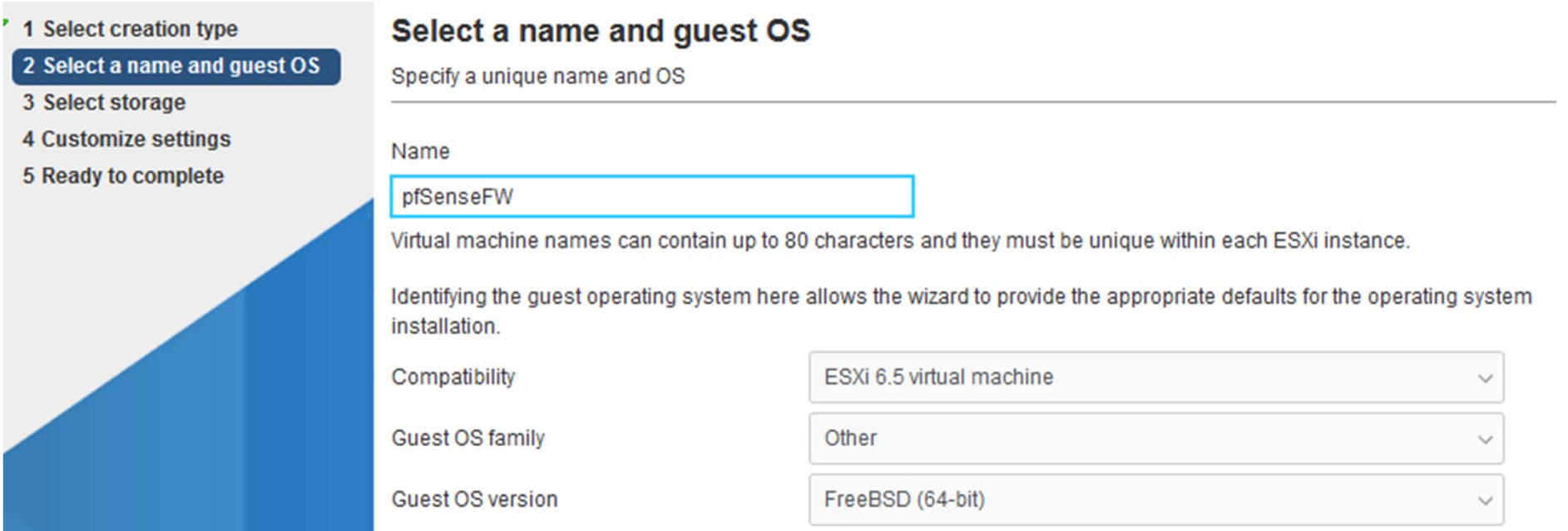


SIEM Logs & Events

Remote logging Scenario

❑ Lab Planning:

- **Install and configure PfSense firewall:**



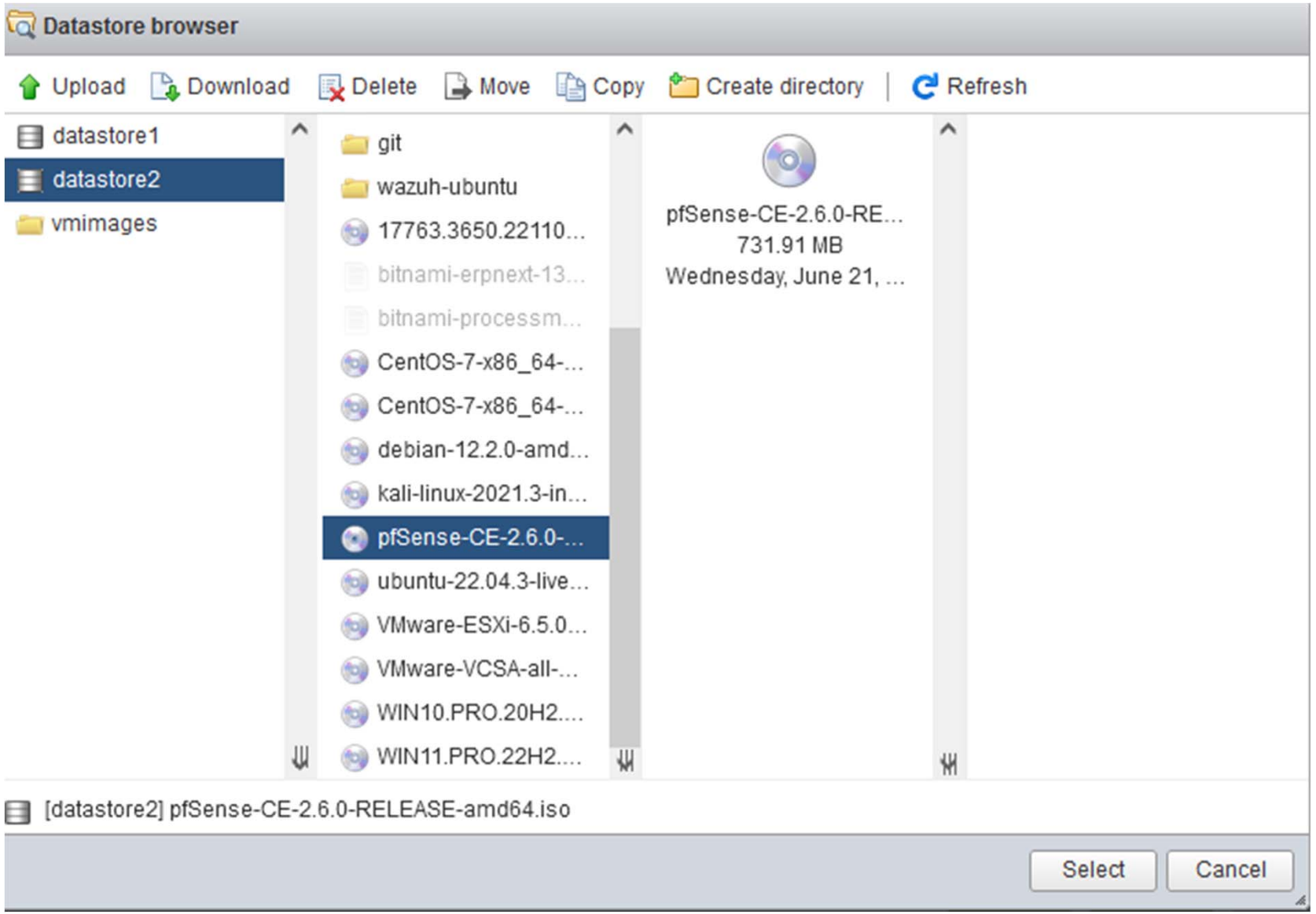
- **Prepare 2 adapters in the machine**
- **Minimum recommended requirements:**

  1 GB RAM – 1 CPU – 8 GB Storage
- **Download PfSense iso from official website upload it to datastore**

SIEM Logs & Events

Remote logging Scenario

❑ Lab Planning:

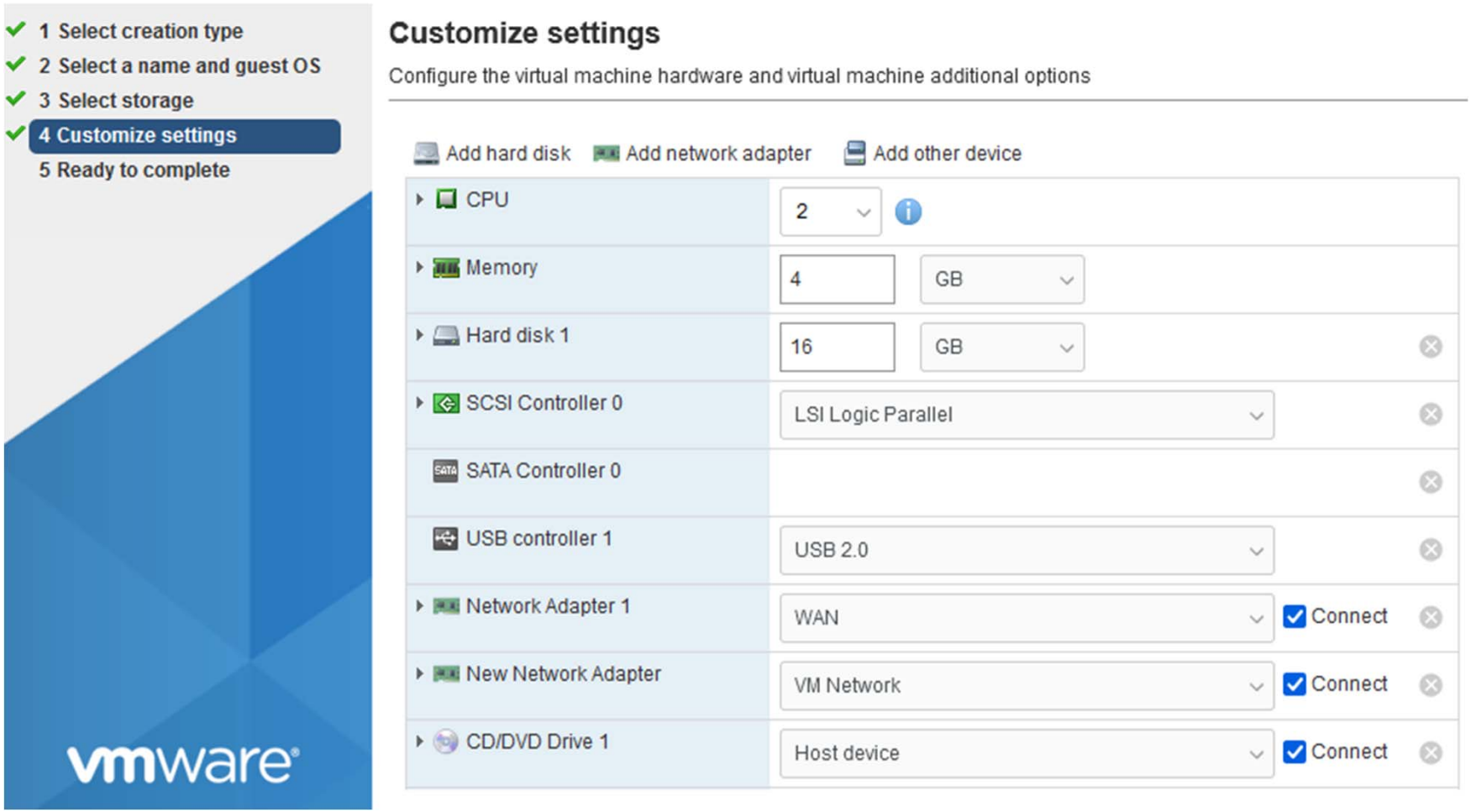


SIEM Logs & Events

Remote logging Scenario

❑ Lab Planning:

- **Review the VM requirements**

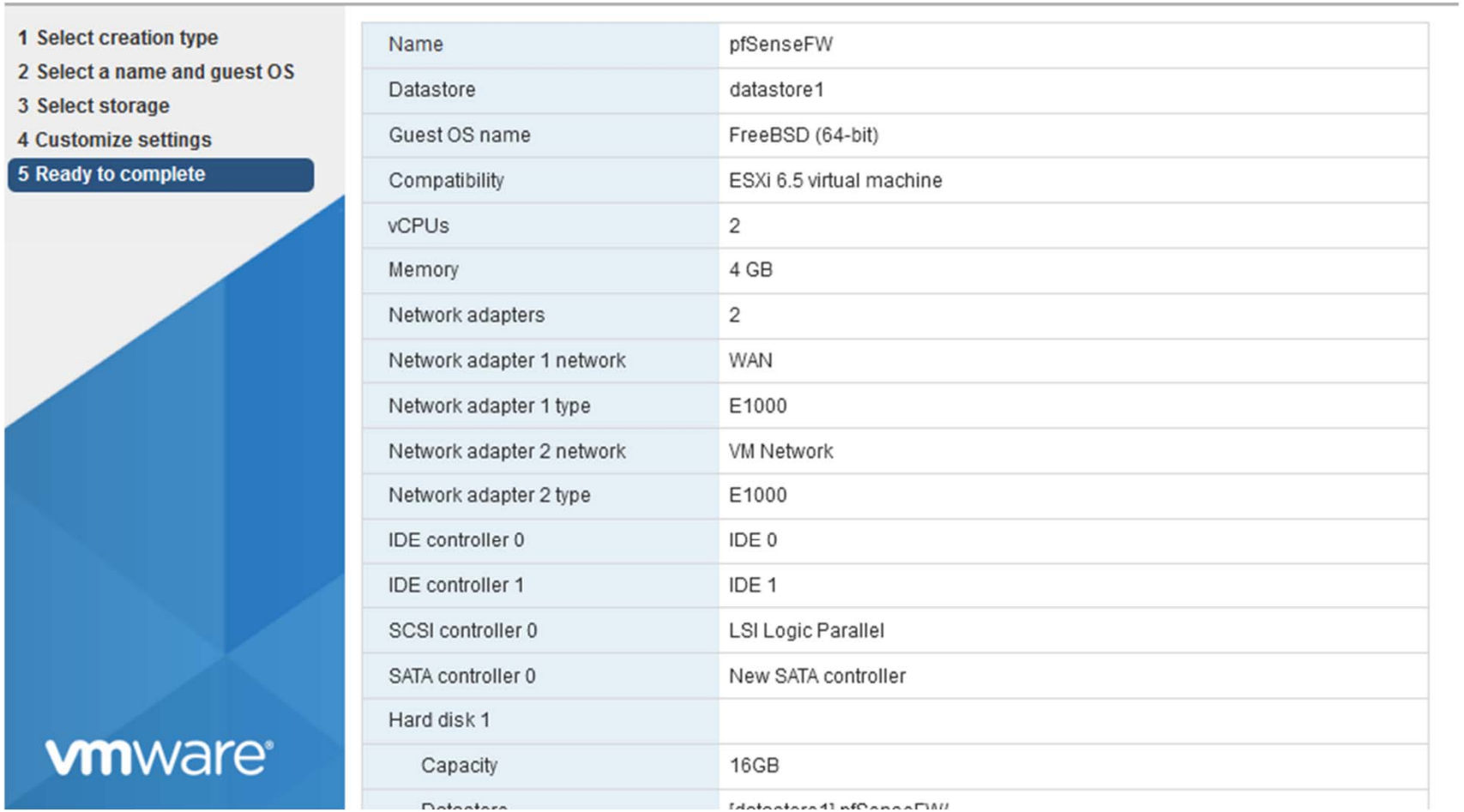


SIEM Logs & Events

Remote logging Scenario

❑ Lab Planning:

- **Review the VM requirements**



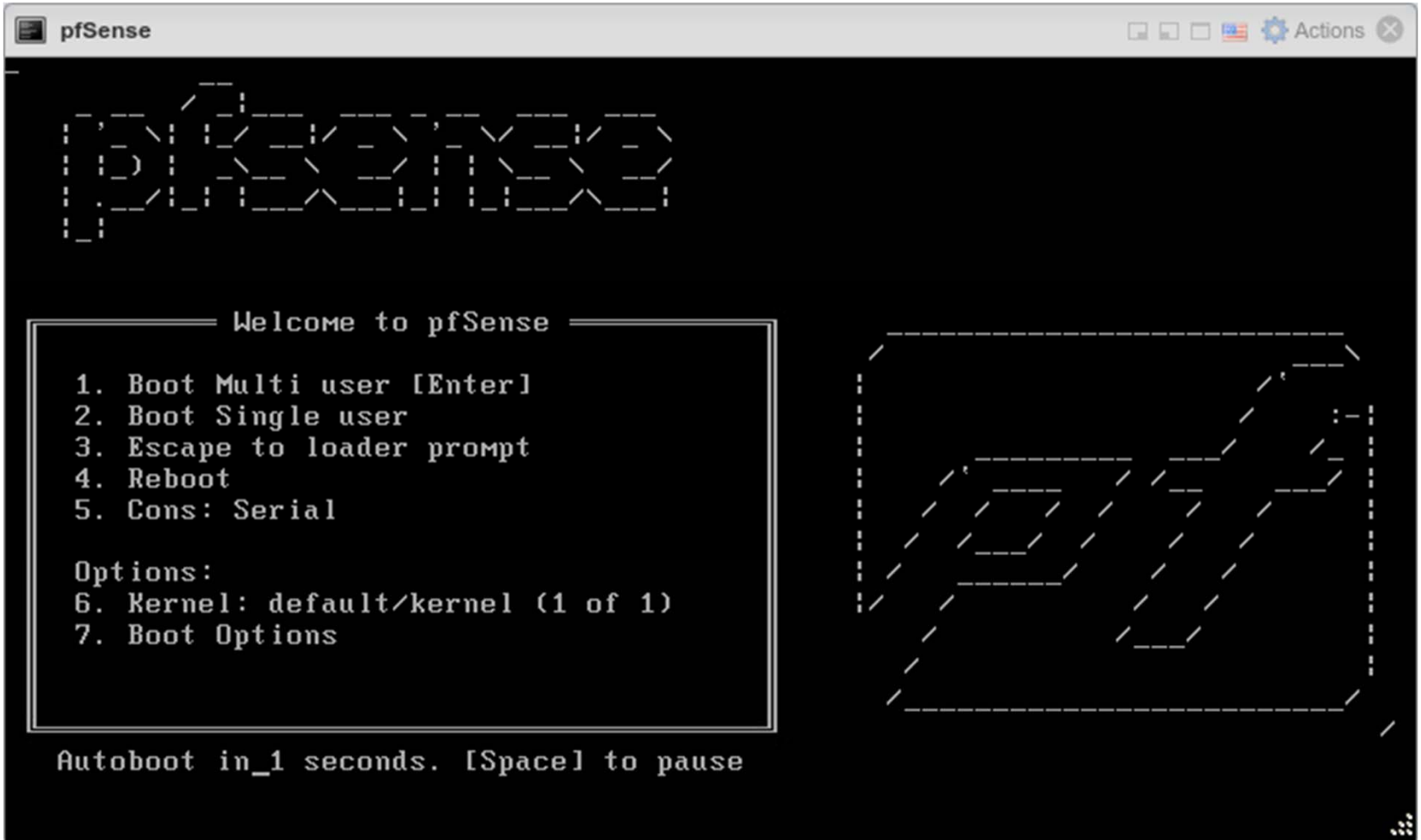
Name	pfSenseFW
Datastore	datastore1
Guest OS name	FreeBSD (64-bit)
Compatibility	ESXi 6.5 virtual machine
vCPUs	2
Memory	4 GB
Network adapters	2
Network adapter 1 network	WAN
Network adapter 1 type	E1000
Network adapter 2 network	VM Network
Network adapter 2 type	E1000
IDE controller 0	IDE 0
IDE controller 1	IDE 1
SCSI controller 0	LSI Logic Parallel
SATA controller 0	New SATA controller
Hard disk 1	
Capacity	16GB
Datastore	[datastore1] pfSenseFW/

SIEM Logs & Events

Remote logging Scenario

❑ Lab Planning:

- **Click Power on to start the VM**
- **Click inside the console window to open the console view to continue the installation**

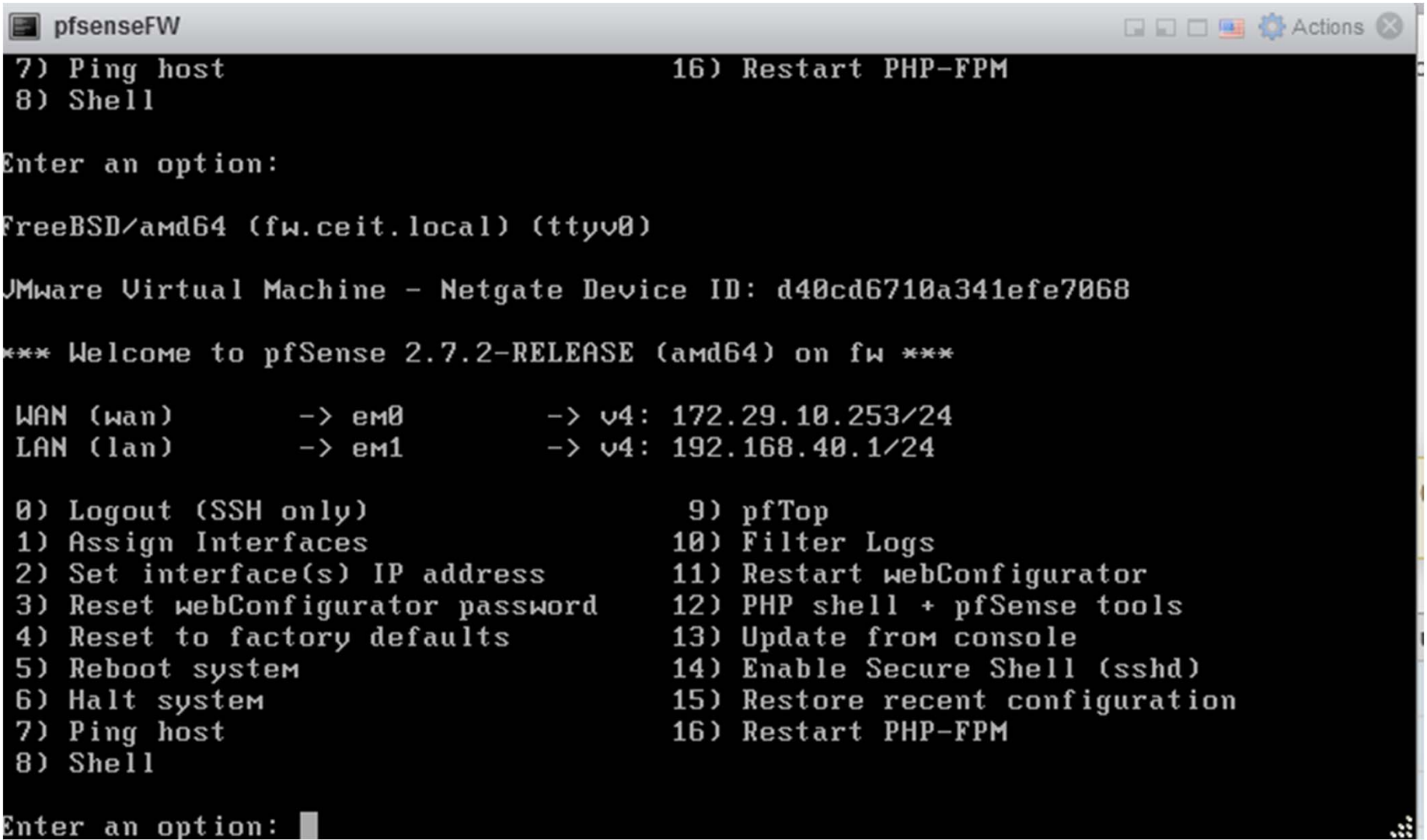


SIEM Logs & Events

Remote logging Scenario

❑ Lab Planning:

- **After assigning the interfaces the VM will complete the boot process**
- **It is now ready to configure like any other firewall running PfSense software**

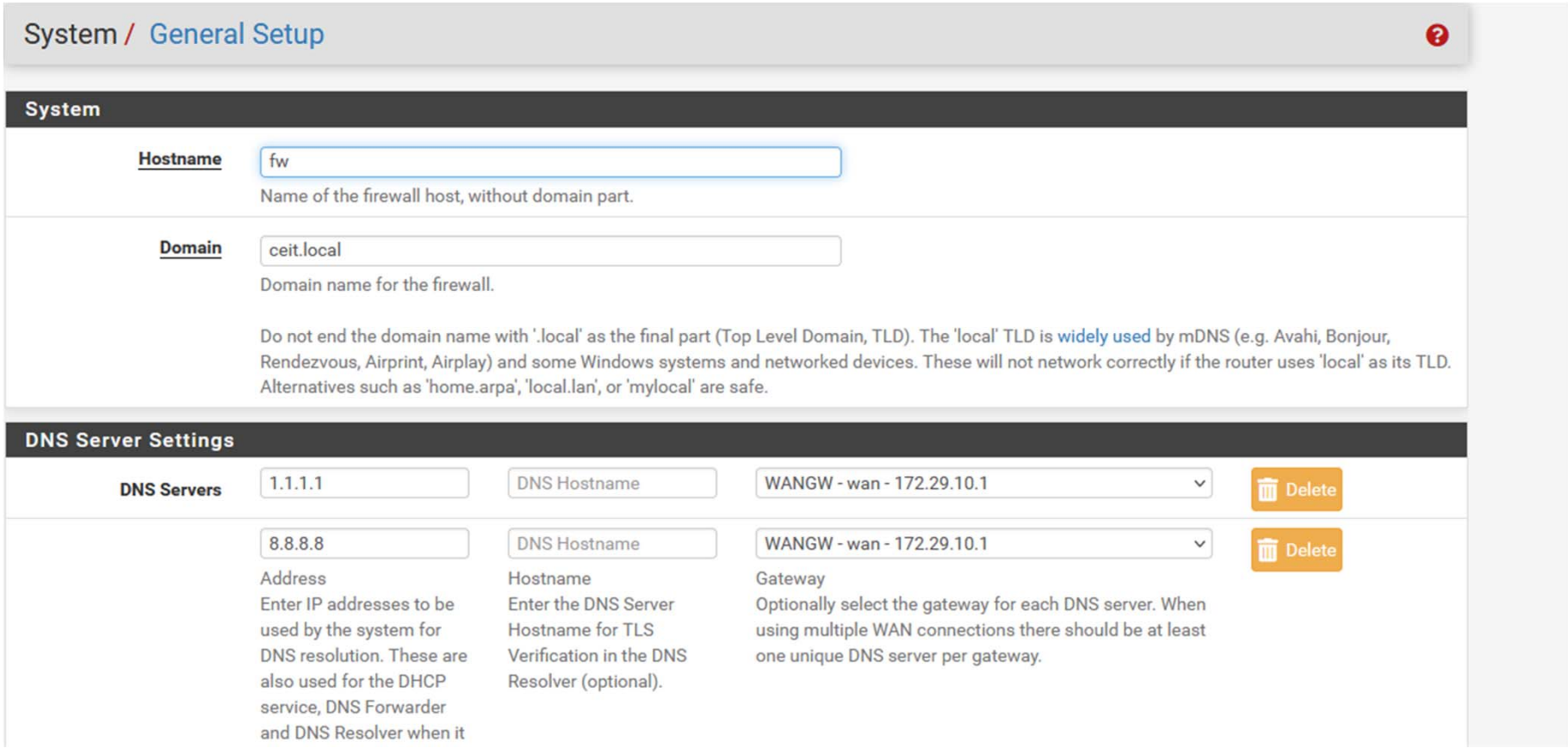


SIEM Logs & Events

Remote logging Scenario

❑ Lab Planning:

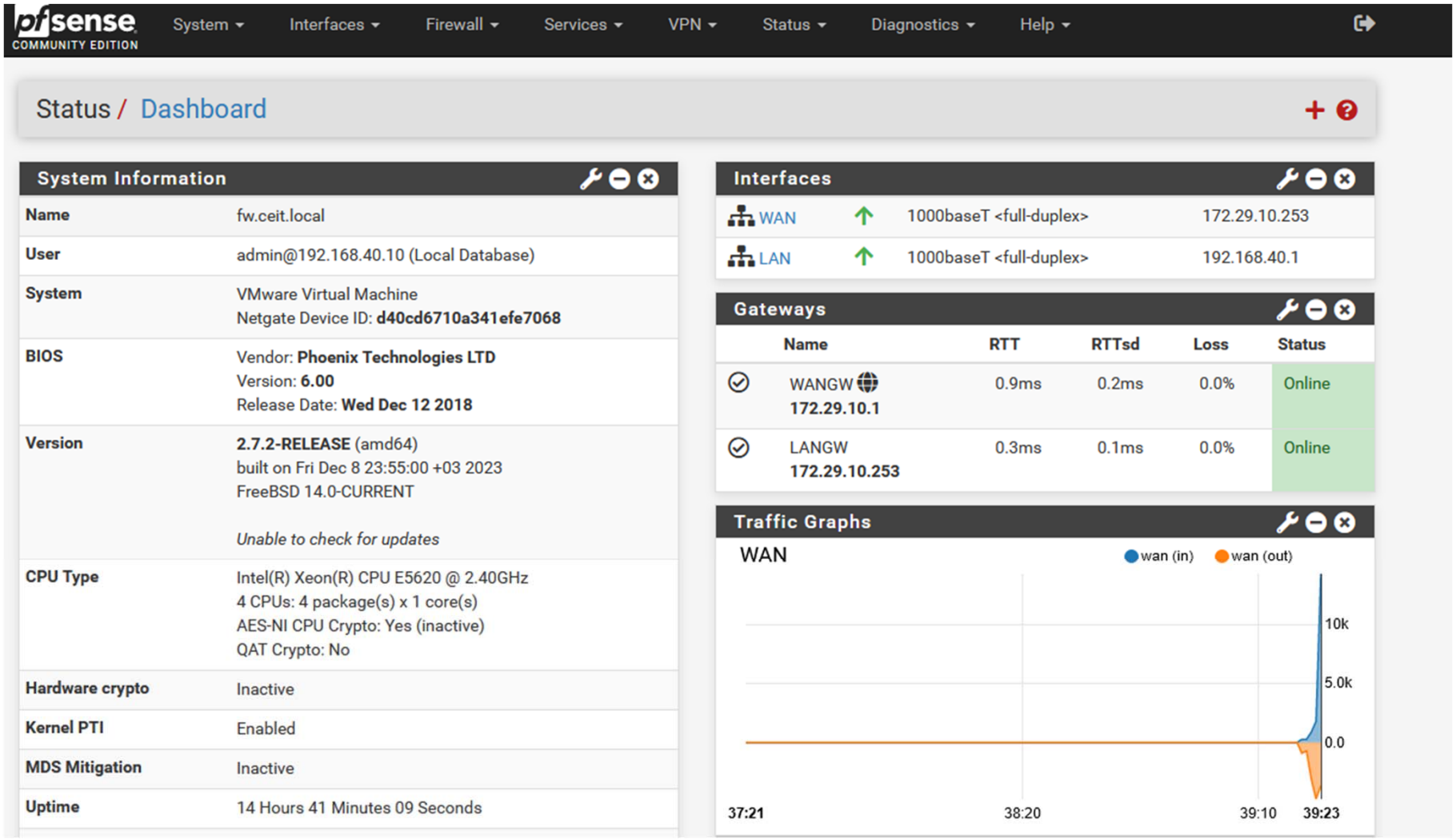
- **Apply general setup**



SIEM Logs & Events

Remote logging Scenario

❑ Lab Planning:

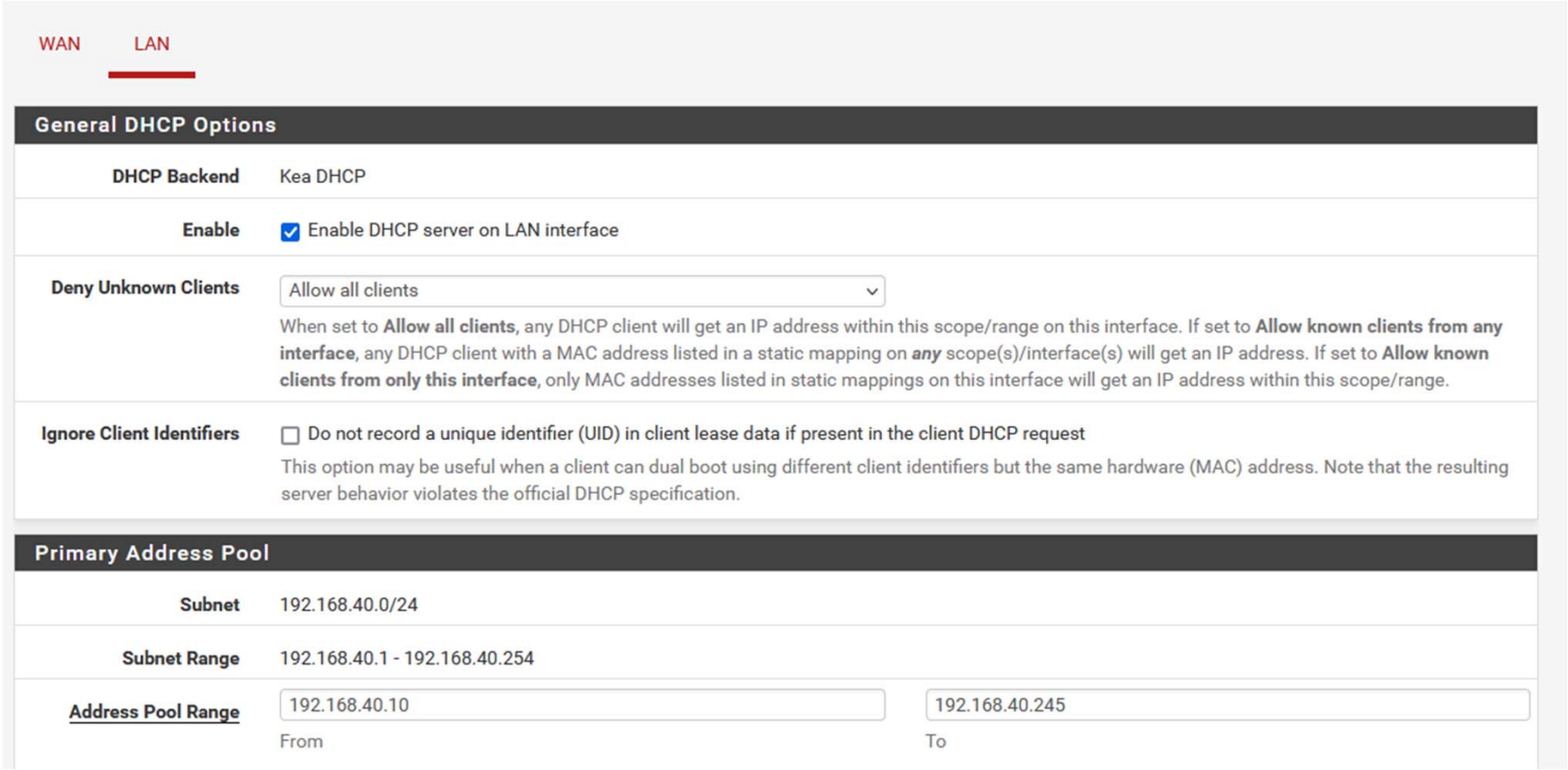


SIEM Logs & Events

Remote logging Scenario

❑ Lab Planning:

- **Enable DHCP for LAN**

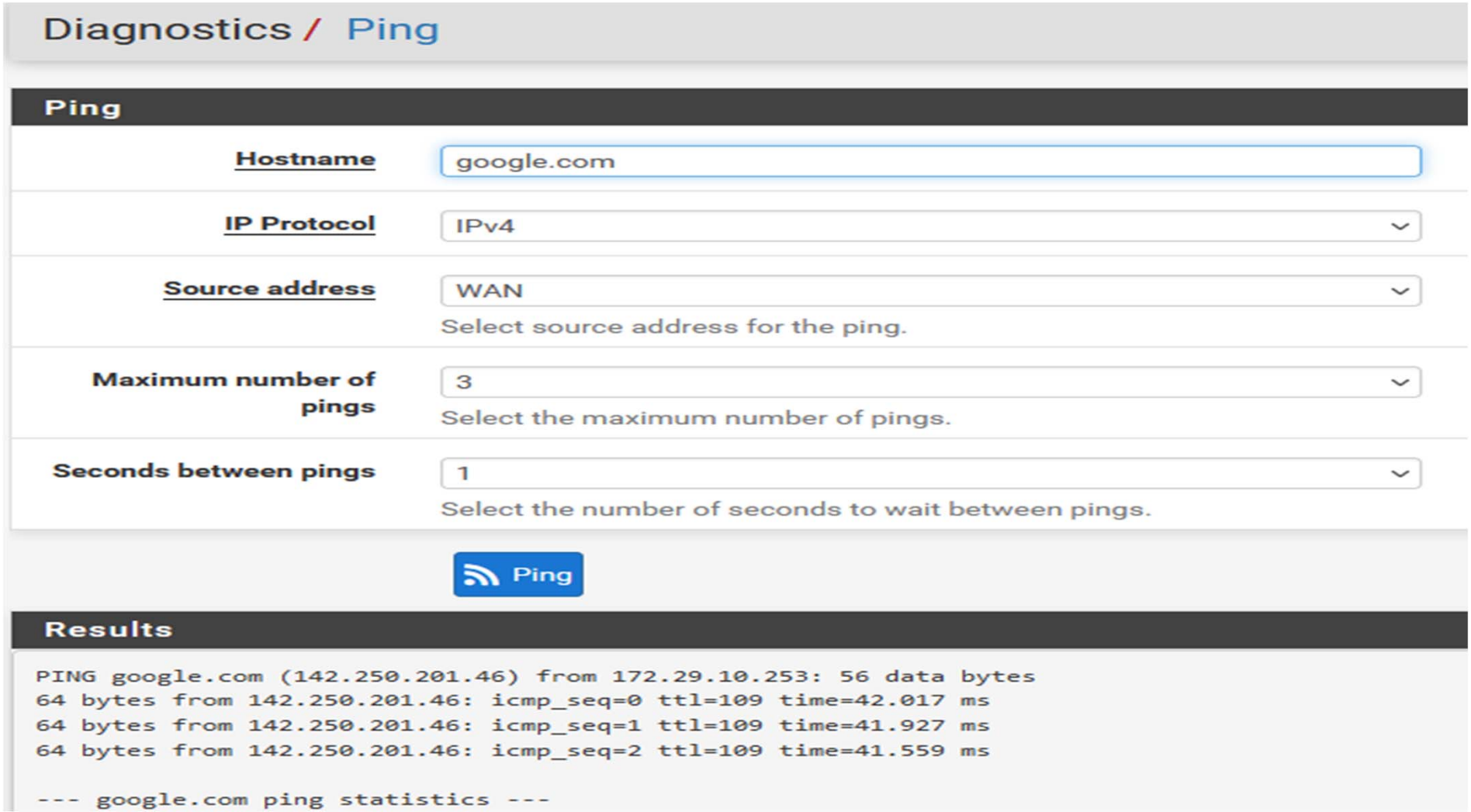


SIEM Logs & Events

Remote logging Scenario

❑ Lab Planning:

- **Checking both LAN and WAN Settings are OK**

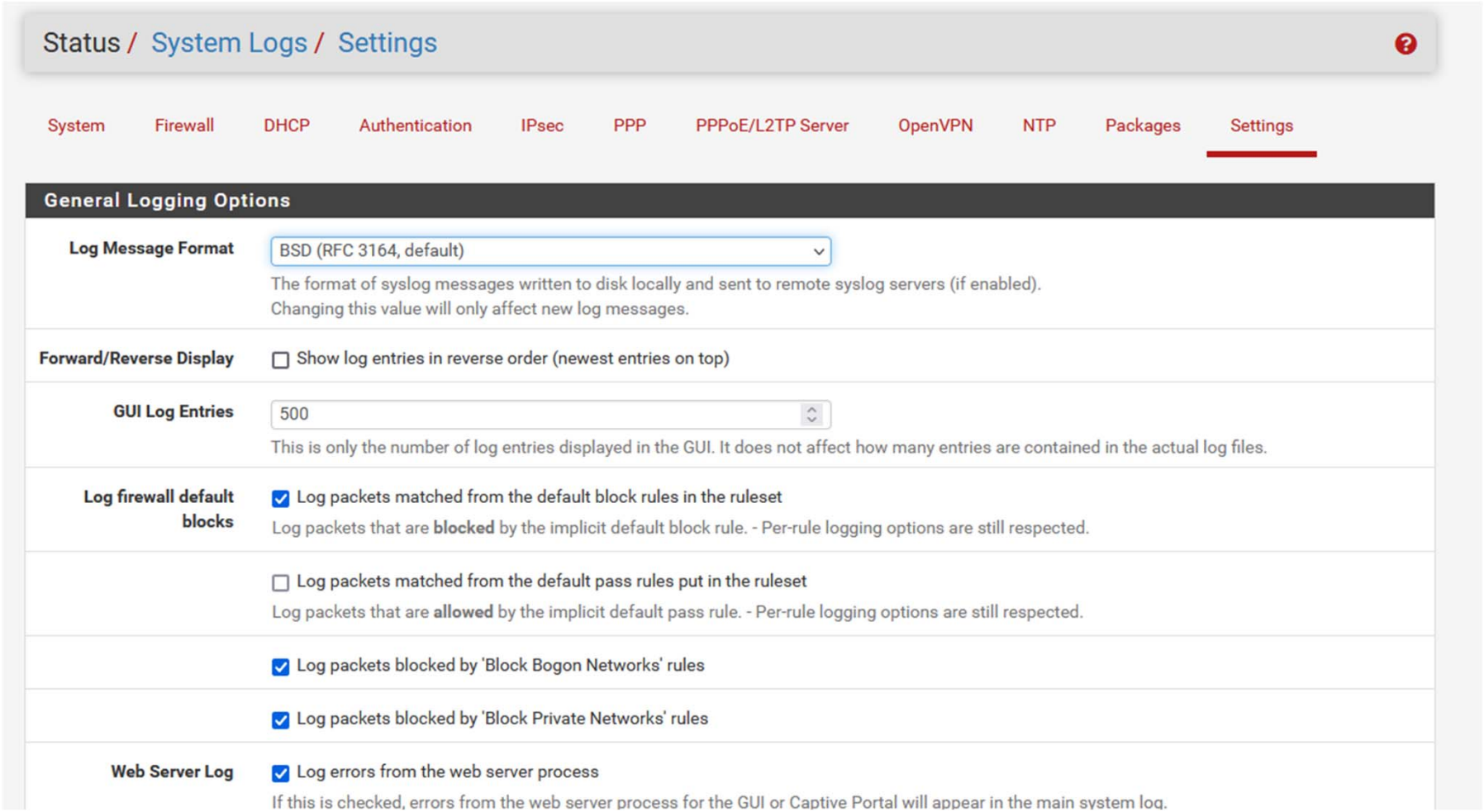


SIEM Logs & Events

Remote logging Scenario

❑ Lab Planning:

- **Enabling remote Logging:**

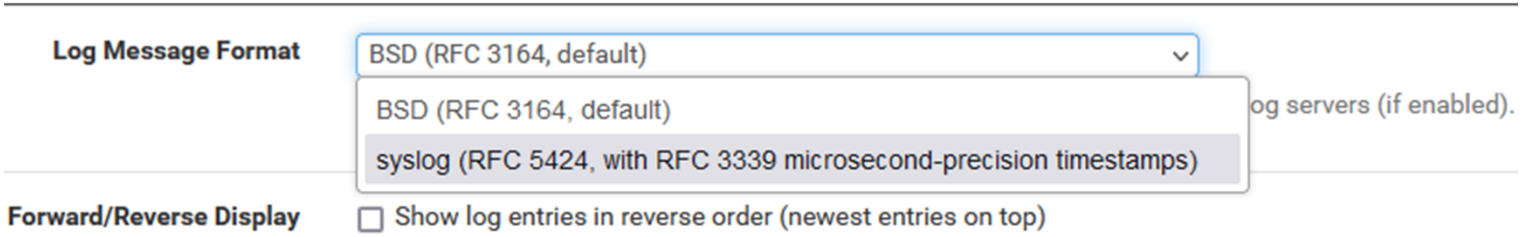


SIEM Logs & Events

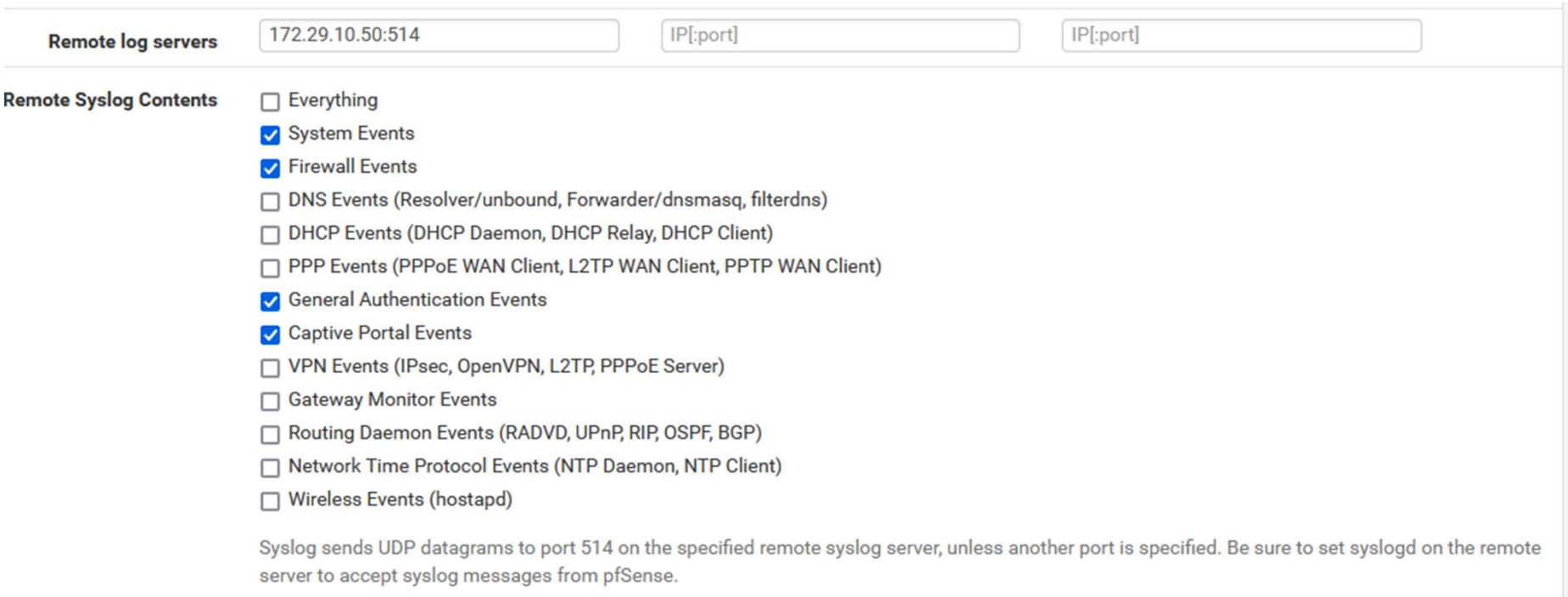
Remote logging Scenario

❑ Lab Planning:

- **Preferable Syslog format**



- **Add remote server and syslog port**
- **Select the convenient security logs based on activated service**



SIEM Logs & Events

Remote logging Scenario

❑ Lab Planning:

- **Configure Wazuh to receive the remote logs:**
- **Ssh to Wazuh manager:**

```
C:\Users\eiado>ssh root@172.29.10.50
root@172.29.10.50's password:
Linux wazuh 6.1.0-13-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.55-1 (2023-09-29) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Mar  3 00:54:52 2024 from 172.29.10.235
root@wazuh ~#
```

- **Edit /var/ossec/etc/ossec.conf as following :**
- **Create a remote section as following:**

```
<remote>
    <connection>syslog</connection>
    <port>514</port>
    <protocol>udp</protocol>
    <allowed-ips>172.29.10.0/24</allowed-ips>
    <local_ip>172.29.10.50</local_ip>
</remote>
```

SIEM Logs & Events

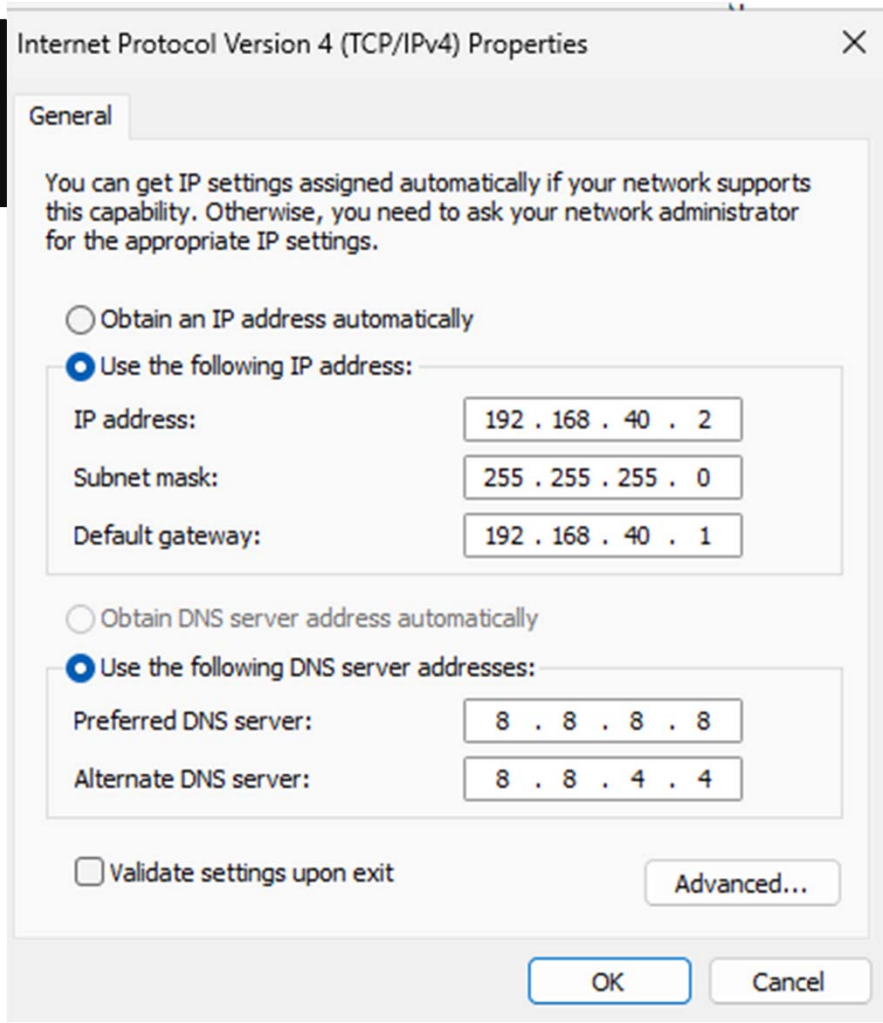
Remote logging Scenario

❑ Lab Planning:

- **All requested parameters and explanation can be found on the Local Configuration (ossec.conf)/remote section on the documentation.**
- **Restart wazuh-manager**

```
root@wazuh ~# vim /var/ossec/etc/ossec.conf
root@wazuh ~# systemctl restart wazuh-manager
```

- **Connect Windows Machine Through Firewall Gateway**



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
Santander
Alfa Romeo
SCUDERIA FERRARI
HUBLOT
WEICHAI
MAHLE
KASPERSKY
Ray-Ban
UPS

Questions

Ali Ali