

# SIEM Logs & Events



A



With Ali Ali

# SIEM Logs & Events

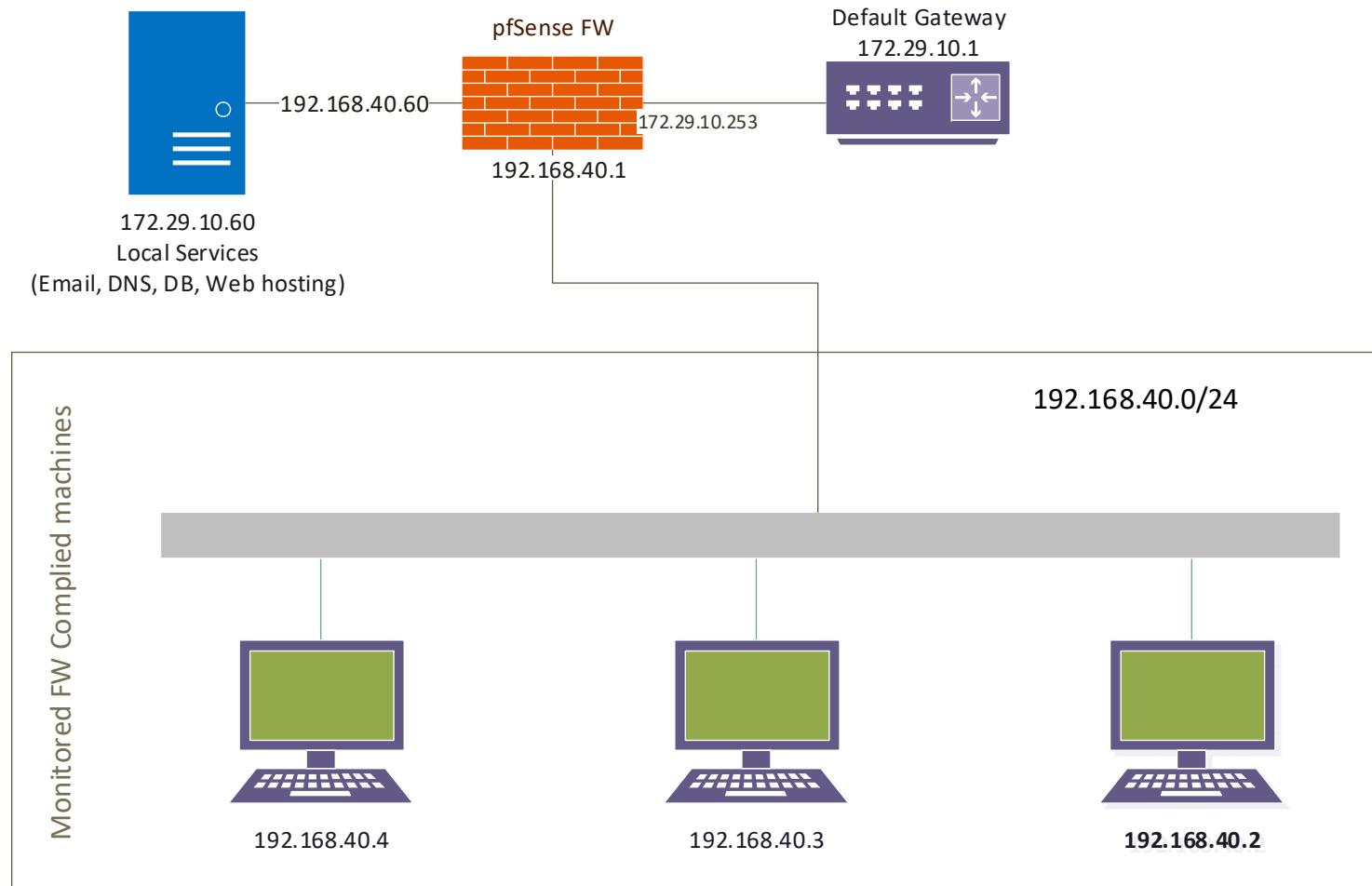
## Remote logging Scenario

### ☐ 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:**

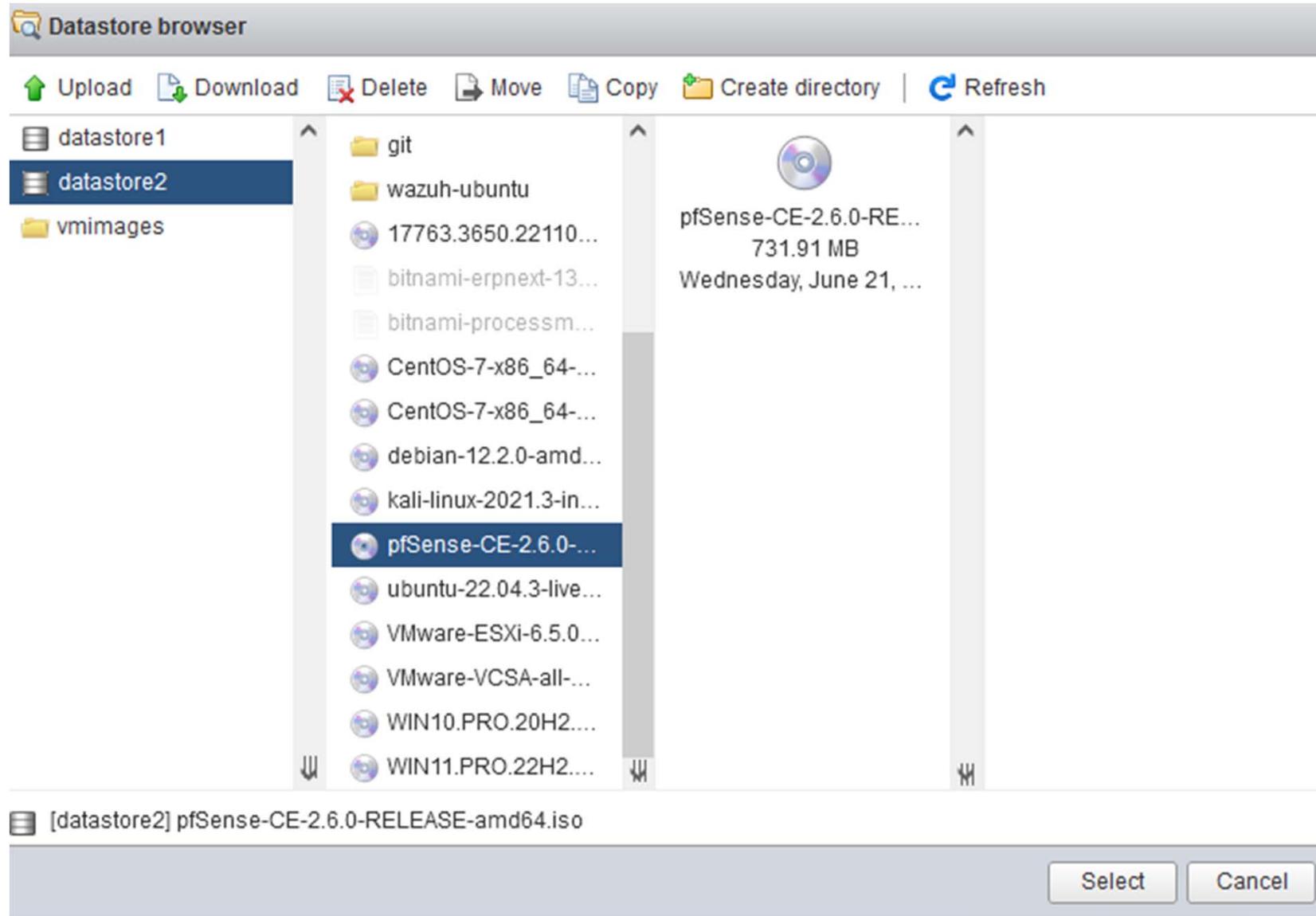
The screenshot shows a wizard interface for creating a virtual machine. The left sidebar lists steps: 1 Select creation type, 2 Select a name and guest OS (which is highlighted in blue), 3 Select storage, 4 Customize settings, and 5 Ready to complete. The main area is titled "Select a name and guest OS" with the sub-instruction "Specify a unique name and OS". A text input field contains "pfSenseFW". Below it, a note says: "Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance." Another note states: "Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation." To the right are three dropdown menus: "Compatibility" set to "ESXi 6.5 virtual machine", "Guest OS family" set to "Other", and "Guest OS version" set to "FreeBSD (64-bit)".

- **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

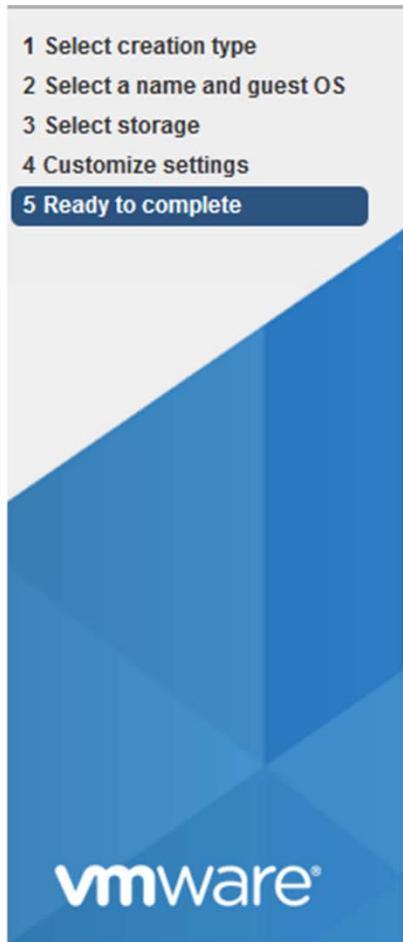


# SIEM Logs & Events

## Remote logging Scenario

### □ Lab Planning:

- Review the VM requirements



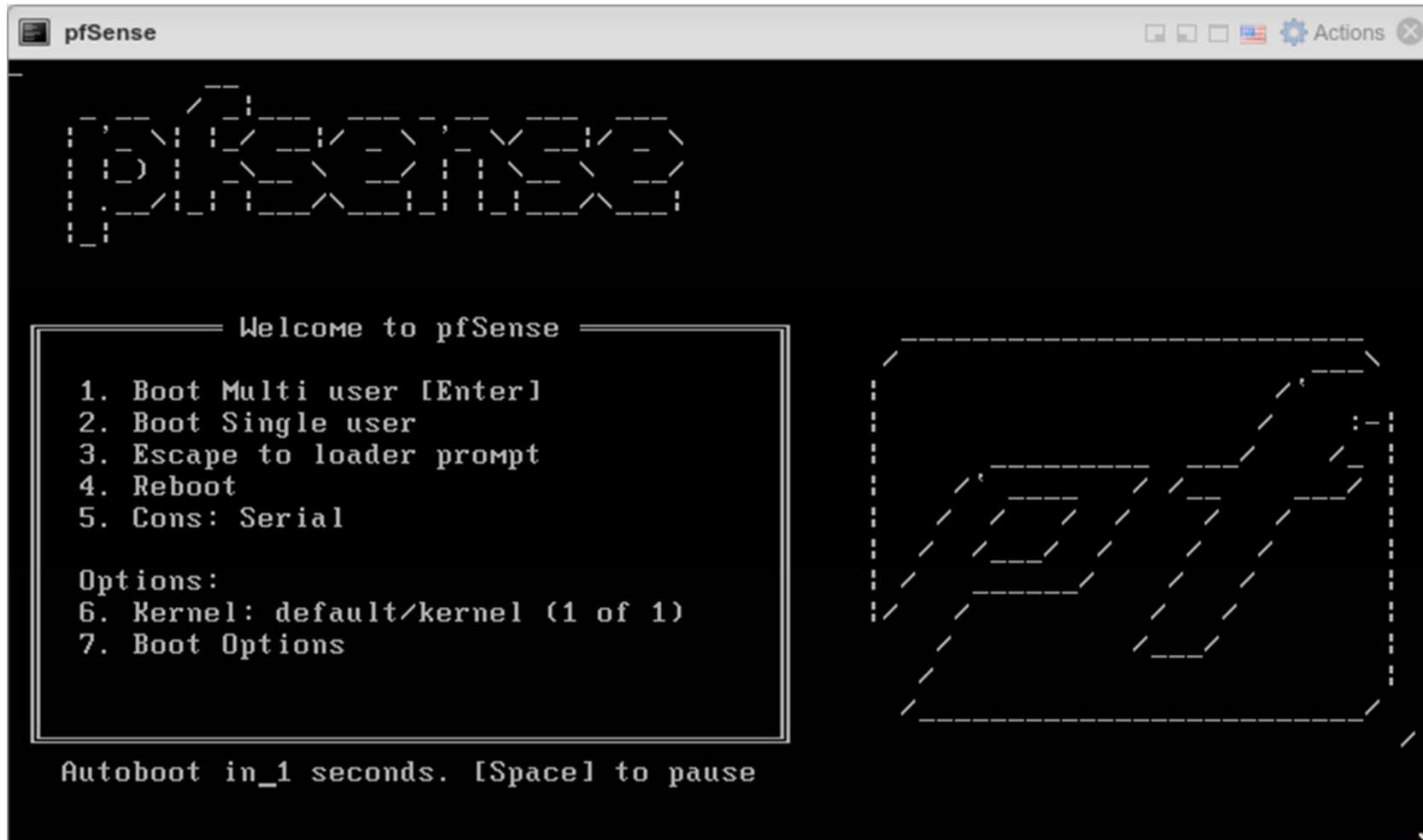
Name	pfSenseFW
Datastore	datastore1
Guest OS name	FreeBSD (64-bit)
Compatibility	ESXi 6.5 virtual machine
vCPUs	2
Memory	4 GB
Network adapters	2
Network adapter 1 network	WAN
Network adapter 1 type	E1000
Network adapter 2 network	VM Network
Network adapter 2 type	E1000
IDE controller 0	IDE 0
IDE controller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

# 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

The screenshot shows a terminal window titled "pfSenseFW". The window contains the following text:

```
7) Ping host          16) Restart PHP-FPM
8) Shell

Enter an option:

FreeBSD/amd64 (fw.ceit.local) (ttyv0)

VMware Virtual Machine - Netgate Device ID: d40cd6710a341efe7068

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on fw ***

WAN (wan)      -> em0      -> v4: 172.29.10.253/24
LAN (lan)      -> em1      -> v4: 192.168.40.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: [
```

# SIEM Logs & Events

## Remote logging Scenario

### ☐ Lab Planning:

- Apply general setup

System / General Setup ?

**System**

<u>Hostname</u>	fw	Name of the firewall host, without domain part.
<u>Domain</u>	ceit.local	Domain name for the firewall.  Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is <a href="#">widely used</a> by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

**DNS Server Settings**

DNS Servers	DNS Hostname	Gateway	
1.1.1.1	WANGW - wan - 172.29.10.1	WANGW - wan - 172.29.10.1	<span style="color: orange;">Delete</span>
8.8.8.8	WANGW - wan - 172.29.10.1	WANGW - wan - 172.29.10.1	<span style="color: orange;">Delete</span>

Address  
Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it

Hostname  
Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).

Gateway  
Optional select the gateway for each DNS server. When using multiple WAN connections there should be at least one unique DNS server per gateway.

# SIEM Logs & Events

## Remote logging Scenario

### Lab Planning:

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Status / Dashboard + ?

System Information	
Name	fw.ceit.local
User	admin@192.168.40.10 (Local Database)
System	VMware Virtual Machine Netgate Device ID: d40cd6710a341efe7068
BIOS	Vendor: Phoenix Technologies LTD Version: 6.00 Release Date: Wed Dec 12 2018
Version	2.7.2-RELEASE (amd64) built on Fri Dec 8 23:55:00 +03 2023 FreeBSD 14.0-CURRENT  Unable to check for updates
CPU Type	Intel(R) Xeon(R) CPU E5620 @ 2.40GHz 4 CPUs: 4 package(s) x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	14 Hours 41 Minutes 09 Seconds

Interfaces				
WAN	↑	1000baseT <full-duplex>	172.29.10.253	
LAN	↑	1000baseT <full-duplex>	192.168.40.1	

Gateways				
Name	RTT	RTTsd	Loss	Status
WANGW 172.29.10.1	0.9ms	0.2ms	0.0%	Online
LANGW 172.29.10.253	0.3ms	0.1ms	0.0%	Online

Traffic Graphs				
WAN				
wan (in)	wan (out)	10k	5.0k	0.0
37:21	38:20	39:10	39:23	

# SIEM Logs & Events

## Remote logging Scenario

### Lab Planning:

- Enable DHCP for LAN

The screenshot shows a network configuration interface with two tabs at the top: 'WAN' and 'LAN'. The 'LAN' tab is selected, indicated by a red underline.

**General DHCP Options**

- DHCP Backend: Kea DHCP
- Enable:  Enable DHCP server on LAN interface
- Deny Unknown Clients: Allow all clients
  - When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed in a static mapping on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed in static mappings on this interface will get an IP address within this scope/range.
- Ignore Client Identifiers:  Do not record a unique identifier (UID) in client lease data if present in the client DHCP request
  - This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

**Primary Address Pool**

- Subnet: 192.168.40.0/24
- Subnet Range: 192.168.40.1 - 192.168.40.254
- Address Pool Range: From 192.168.40.10 To 192.168.40.245

# SIEM Logs & Events

## Remote logging Scenario

### □ Lab Planning:

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

Diagnostics / Ping

**Ping**

<u>Hostname</u>	google.com
<u>IP Protocol</u>	IPv4
<u>Source address</u>	WAN Select source address for the ping.
<u>Maximum number of pings</u>	3 Select the maximum number of pings.
<u>Seconds between pings</u>	1 Select the number of seconds to wait between pings.

 Ping

**Results**

```
PING google.com (142.250.201.46) from 172.29.10.253: 56 data bytes
64 bytes from 142.250.201.46: icmp_seq=0 ttl=109 time=42.017 ms
64 bytes from 142.250.201.46: icmp_seq=1 ttl=109 time=41.927 ms
64 bytes from 142.250.201.46: icmp_seq=2 ttl=109 time=41.559 ms

--- google.com ping statistics ---
```

# SIEM Logs & Events

## Remote logging Scenario

### Lab Planning:

- Enabling remote Logging:

Status / System Logs / Settings ?

System Firewall DHCP Authentication IPsec PPP PPPoE/L2TP Server OpenVPN NTP Packages **Settings**

#### General Logging Options

**Log Message Format**  The format of syslog messages written to disk locally and sent to remote syslog servers (if enabled). Changing this value will only affect new log messages.

**Forward/Reverse Display**  Show log entries in reverse order (newest entries on top)

**GUI Log Entries**  This is only the number of log entries displayed in the GUI. It does not affect how many entries are contained in the actual log files.

**Log firewall default blocks**  Log packets matched from the default block rules in the ruleset  
Log packets that are **blocked** by the implicit default block rule. - Per-rule logging options are still respected.  
  
 Log packets matched from the default pass rules put in the ruleset  
Log packets that are **allowed** by the implicit default pass rule. - Per-rule logging options are still respected.  
  
 Log packets blocked by 'Block Bogon Networks' rules  
  
 Log packets blocked by 'Block Private Networks' rules

**Web Server Log**  Log errors from the web server process  
If this is checked, errors from the web server process for the GUI or Captive Portal will appear in the main system log.

# SIEM Logs & Events

## Remote logging Scenario

### Lab Planning:

- Preferable Syslog format

Log Message Format

BSD (RFC 3164, default)

syslog (RFC 5424, with RFC 3339 microsecond-precision timestamps)

Forward/Reverse Display

Show log entries in reverse order (newest entries on top)

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

Remote log servers

172.29.10.50:514

IP[:port]

IP[:port]

Remote Syslog Contents

Everything

System Events

Firewall Events

DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)

DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)

PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)

General Authentication Events

Captive Portal Events

VPN Events (IPsec, OpenVPN, L2TP, PPPoE Server)

Gateway Monitor Events

Routing Daemon Events (RADVD, UPnP, RIP, OSPF, BGP)

Network Time Protocol Events (NTP Daemon, NTP Client)

Wireless Events (hostapd)

Syslog sends UDP datagrams to port 514 on the specified remote syslog server, unless another port is specified. Be sure to set syslogd on the remote server to accept syslog messages from pfSense.

# 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

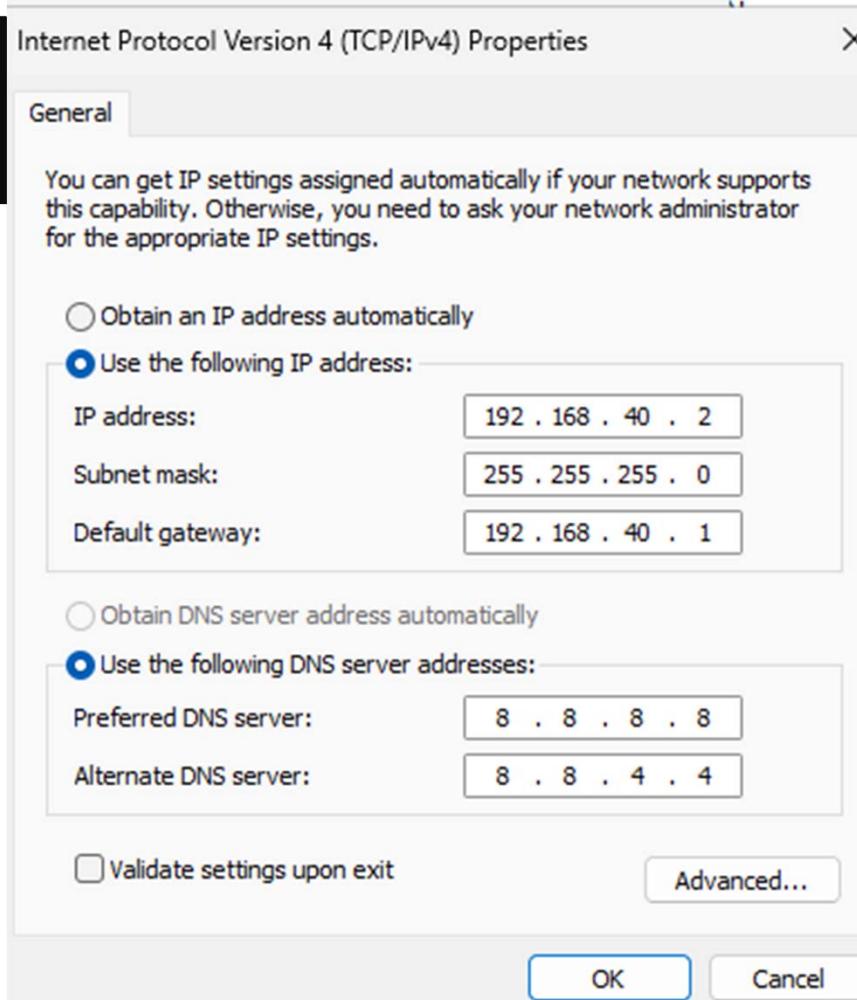
## Remote logging Scenario

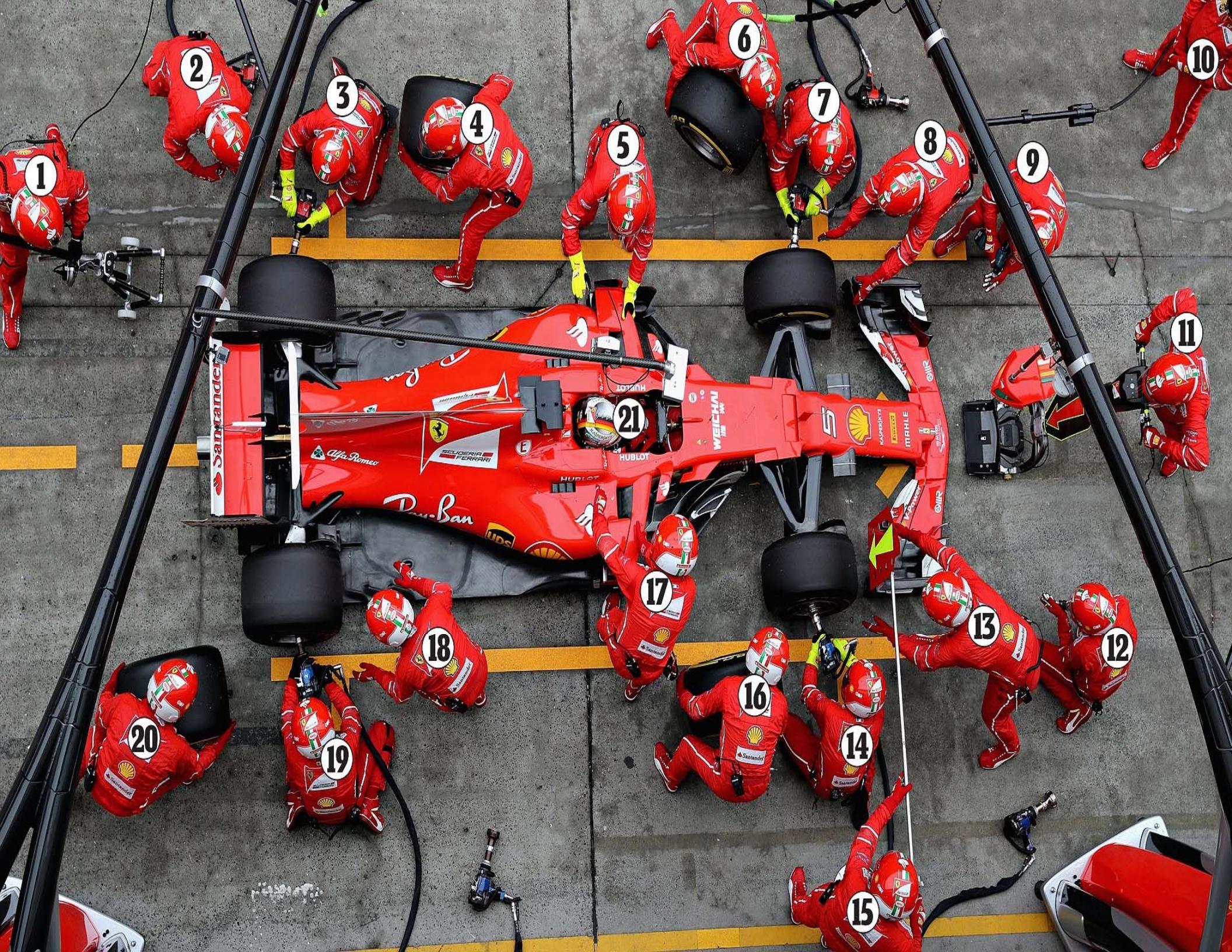
### Lab Planning:

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

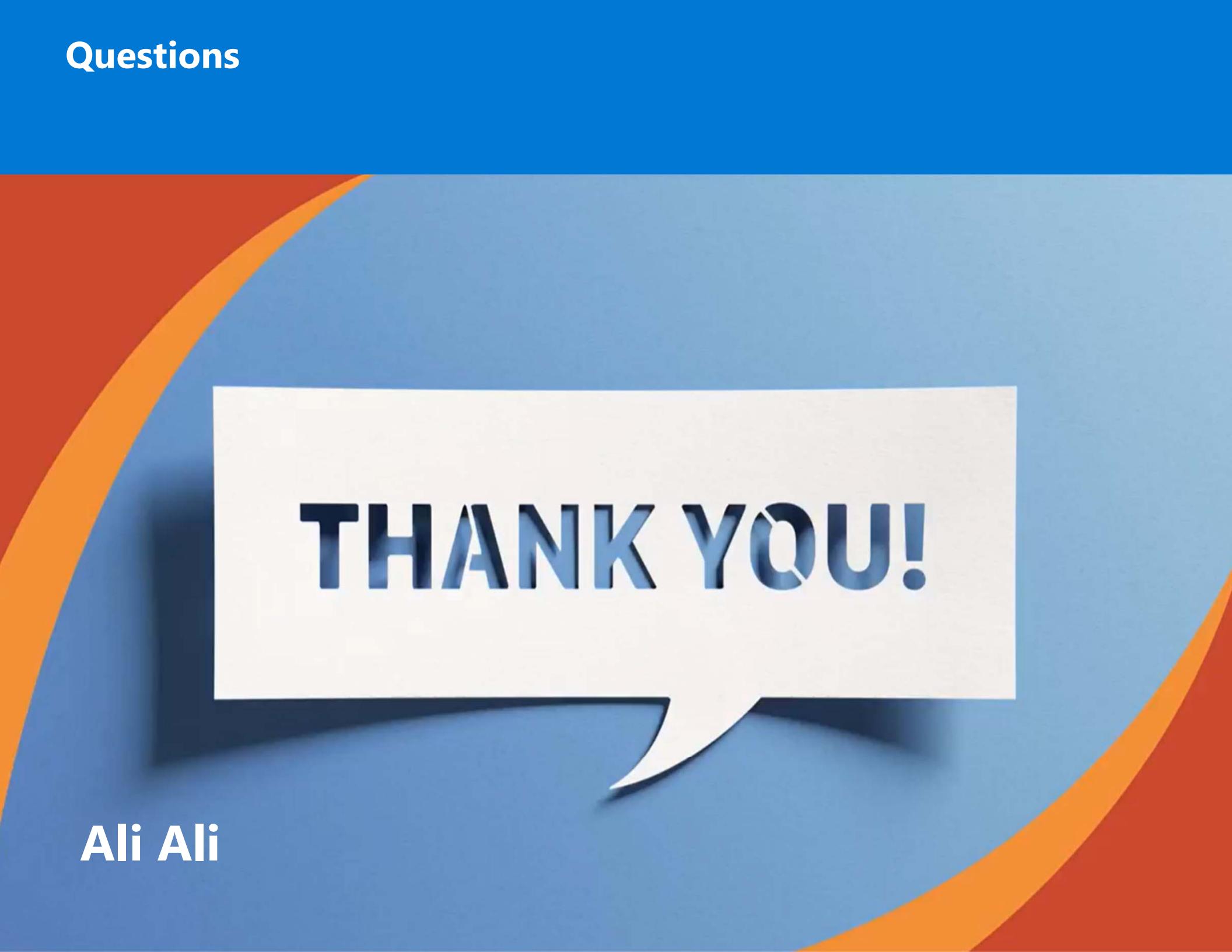
```
root@wazuh ~# vim /var/ossec/etc/ossec.conf
root@wazuh ~# systemctl restart wazuh-manager
```

- Connect Windows Machine Through Firewall Gateway





## Questions



**THANK YOU!**

Ali Ali