

# Project Whiptail Appendix: Configuration Document

---

ORIGINAL AND IMPROVED VIRTUAL NETWORK SETUP GUIDES

Mink Jo, Gary Khodayari, Michael Klym

PROJECT WHIPTAIL | INDUSTRIAL NETWORK CYBERSECURITY | BCIT | MAY 26, 2021

## TABLE OF CONTENTS

Config Tables.....	6
Original Network Config Tables .....	6
Improved Network Config Tables .....	7
Accounts & Logon .....	9
Network Preparation (Original and Improved).....	10
VMware Virtual Network Setup.....	10
'Public' Network Setup .....	10
'IT Net' Network Setup .....	10
'OT Net' Network Setup.....	10
'Bridge Net' Network Setup.....	11
Screenshot of Correctly Configured VMnets (Public, IT Net, OT Net, Bridge Net) .....	11
Kali-Linux (Attacker Machine).....	12
Section 1: Installing Kali .....	12
Section 2: Installing Tools .....	12
Modbus-cli.....	12
Scapy.....	12
Smod.....	12
Section 3: Finishing Up .....	12
Modbus-Server (Kubuntu) .....	13
Section 1: Installing Kubuntu .....	13
Section 2: Configuring Settings.....	13
Section 3: Installing Python Modbus Server .....	13
Section 4: Finishing Up .....	14
Original Network Setup .....	16
GW-FW (pfSense Firewall).....	16
Section 1: Creating the Virtual Machine.....	16
Section 2: Installing pfSense .....	16
Section 3: Configuring Interfaces.....	16
Section 4: Configuring the Firewall.....	18

Main-Wkstn (Windows 7) .....	21
Section 1: Installing Windows.....	21
Section 2: Installing Office .....	21
Eng-Wkstn (Windows 7) .....	21
Improved Network Setup .....	23
GW-FW (pfSense Firewall) .....	23
Section 1: Creating the Virtual Machine.....	23
Section 2: Installing pfSense .....	23
Section 3: Configuring Interfaces.....	23
Section 4: Configuring the Firewall.....	25
Configuring the Setup Wizard .....	25
Fixing DNS Resolutions .....	26
Naming the Interfaces .....	26
Creating Aliases .....	26
Adding the IDMZ Gateway .....	27
Setting Static Routes.....	28
Creating Firewall Rules .....	28
IDMZ-FW (pfSense Firewall) .....	30
Section 1: Creating the Virtual Machine.....	30
Section 2: Installing pfSense .....	30
Section 3: Configuring Interfaces.....	30
Section 4: Configuring the Firewall.....	31
Configuring the Setup Wizard .....	32
Fixing DNS Resolutions .....	33
Naming the Interfaces .....	33
Creating Aliases .....	33
Editing the Gateway .....	34
Setting A Static Route .....	35
Creating Firewall Rules .....	35
Windows Server 2019.....	38

Section 1: Creating the Virtual Machine.....	38
Section 2: Installing Windows Server .....	38
Section 3: Configuring.....	38
Basic Settings.....	38
VMWare Tools .....	39
Section 4: Adding Server Roles .....	39
Active Directory Domain Services (AD DS) Role .....	39
Promote to Domain Controller.....	39
Finishing Up .....	40
Section 5: Creating Groups and Users .....	40
Create a Group .....	40
Create a User .....	40
Logon as a Domain user .....	41
Section 6: Group Policy (Firewall Rule).....	41
Section 7: Joining the Domain .....	41
Main-Wkstn (Windows 10) .....	43
Mon-Wkstn (Windows 10).....	43
Eng-Wkstn (Windows 10) .....	44
Honeypot (Kubuntu) .....	45
Section 1: Installing Kubuntu .....	45
Section 2: Configuring Settings.....	45
Section 3: Installing Conpot .....	45
Section 4: Creating a Start Script .....	46
Section 5: Finishing Up .....	47
Splunk .....	48
Section 1: Installing Splunk .....	48
Section 2: Setting up Splunk .....	48
Section 3: Setting up Splunk Alerts.....	50
Section 4: Perform Splunk Alert Simulation .....	51
Section 5: Finishing Up .....	51

Sec-Orion (Security Onion SIEM).....	52
Section 1: Creating the Virtual Machine.....	52
Section 2: Installing Security Onion .....	52
Section 3: Setting up Wazuh.....	53
Getting the Installers .....	53
Allowing Agent Connections.....	54
Adding an Agent (Windows).....	54
Adding an Agent (Linux) .....	54
Section 3: Setting up Osquery .....	55
Getting the Packages.....	55
Allowing Osquery Connections.....	55
Adding an Agent (Windows).....	55
Adding an Agent (Linux) .....	55
Section 4: Setting up Syslog.....	56
Allowing Connections .....	56
Enabling Syslog on the Firewalls (GW-FW & IDMZ-FW) .....	56
Section 5: Finishing Up .....	56

# CONFIG TABLES

## ORIGINAL NETWORK CONFIG TABLES

Table 1 Original Network Machine Configurations

Machine	Image	CPUs	RAM	HDD	NIC 1	NIC 2
Kali-Linux	<a href="#">kali-linux-2021.1-vmware-amd64</a>	4	2 GB	80 GB	<b>Public</b> 192.168.50.50 /24	-
GW-FW	<a href="#">pfSense-CE-2.5.1-RELEASE-amd64</a>	2	512 MB	20 GB	<b>Public</b> 192.168.50.10 /24	<b>IT Net</b> 10.10.10.2 /24
Main-Wkstn	<a href="#">IE11.Win7.VMWare Microsoft Office Standard 2007</a>	2	2 GB	40 GB	<b>IT Net</b> 10.10.10.200 /24	-
Eng-Wkstn	<a href="#">IE11.Win7.VMWare</a>	2	2 GB	40 GB	<b>IT Net</b> 10.10.10.201 /24	<b>OT Net</b> 172.16.0.20 /24
Modbus-Server	<a href="#">kubuntu-20.04.2.0-desktop-amd64</a>	2	2 GB	20 GB	<b>OT Net</b> 172.16.0.101 /24	-

Table 2 Original Network Addressing Scheme

Addressing Scheme – Original			
Virtual Network	Network Address	Subnet Mask	Default Gateway + DNS
Public	192.168.50.0	255.255.255.0	192.168.50.1
IT Net	10.10.10.0	255.255.255.0	10.10.10.2
OT Net	172.16.0.0	255.255.255.0	-

## IMPROVED NETWORK CONFIG TABLES

Table 3 Improved Network Machine Configurations

Machine	Image	CPUs	RAM	HDD	NIC 1	NIC 2	NIC 3	NIC 4
Kali-Linux	<a href="#">kali-linux-2021.1-vmware-amd64</a>	4	2 GB	80 GB	<b>Public</b> 192.168.50.50 /24	-	-	-
GW-FW	<a href="#">pfSense-CE-2.5.1-RELEASE-amd64</a>	2	512 MB	20 GB	<b>Public</b> 192.168.50.10 /24	<b>IT Net</b> 10.10.10.2 /24	<b>Bridge Net</b> 10.11.11.2 /29	-
IDMZ-FW	<a href="#">pfSense-CE-2.5.1-RELEASE-amd64</a>	2	512 MB	20 GB	<b>Bridge Net</b> 10.11.11.3 /29	<b>IDMZ</b> 10.10.20.2 /24	<b>OT Net</b> 172.16.0.2 /24	-
Win-Server	<a href="#">17763.737.190906-2324.rs5_release_svc_refresh_SERVER_EVAL_x64FRE_en-us_1</a>	2	2 GB	60 GB	<b>IDMZ</b> 10.10.20.252 /24	-	-	-
Main-Wkstn	<a href="#">MSEdge.Win10.VMware</a>	2	2 GB	40 GB	<b>IT Net</b> 10.10.10.200 /24	-	-	-
Mon-Wkstn	<a href="#">MSEdge.Win10.VMware</a>	2	2 GB	40 GB	<b>IDMZ</b> 10.10.20.200 /24	-	-	-
Eng-Wkstn	<a href="#">MSEdge.Win10.VMware</a>	2	2 GB	40 GB	<b>OT Net</b> 172.16.0.200 /24	-	-	-
Modbus-Server	<a href="#">kubuntu-20.04.2.0-desktop-amd64</a>	2	2 GB	20 GB	<b>OT Net</b> 172.16.0.101 /24	-	-	-
Honeypot	<a href="#">kubuntu-20.04.2.0-desktop-amd64</a>	2	2 GB	20 GB	<b>IDMZ</b> 10.10.20.25 /24	-	-	-
Sec-Onion	<a href="#">securityonion-2.3.50.iso</a>	8	12 GB	150 GB	<b>IDMZ</b> 10.10.20.253 /24	<b>IDMZ</b> (no IP)	<b>IT Net</b> (no IP)	<b>OT Net</b> (no IP)

**Table 4 Improved Network Addressing Scheme**

Network Addressing Scheme – Improved				
Virtual Network	Network Address	Subnet Mask	Default Gateway	DNS
Public	192.168.50.0	255.255.255.0	192.168.50.1	192.168.50.1
IT Net	10.10.10.0	255.255.255.0	10.10.10.2	10.10.20.252
Bridge Net	10.11.11.0	255.255.255.248	10.11.11.2	10.10.20.252
IDMZ	10.10.20.0	255.255.255.0	10.10.20.2	10.10.20.252
OT Net	172.16.0.0	255.255.255.0	172.16.0.2	10.10.20.252



# ACCOUNTS & LOGON

Machine	Username	Password
Kali-Linux	kali	kali
GW-FW	admin	pfsense
IDMZ-FW	admin	pfsense
Win-Server ( <i>Local Account</i> )	Administrator	ServerPassw0rd!
Win-Server ( <i>Domain Account</i> )	iacsadmin	Passw0rd!
Sec-Onion	seconion	seconion
Security Onion Dashboard	<a href="mailto:admin@iacsplant.com">admin@iacsplant.com</a>	iacsplantadmin
Honeypot	honeypot	honeypot
Splunk Dashboard	honeypot	honeypot
Main-Wkstn (Win 10) ( <i>Local Account</i> )	IEUser	Passw0rd!
Mon-Wkstn (Win 10) ( <i>Local Account</i> )	IEUser	Passw0rd!
Eng-Wkstn (Win 10) ( <i>Local Account</i> )	IEUser	Passw0rd!
Main-Wkstn (Win 10) ( <i>Domain Account</i> )	mattmain	Passw0rd!
Mon-Wkstn (Win 10) ( <i>Domain Account</i> )	mariamon	Passw0rd!
Eng-Wkstn (Win 10) ( <i>Domain Account</i> )	edeng	Passw0rd!
Modbus-Server	modbus	modbus
Main-Wkstn (Win 7)	IEUser	Passw0rd!
Eng-Wkstn (Win 7)	IEUser	Passw0rd!

# NETWORK PREPARATION (ORIGINAL AND IMPROVED)

## VMWARE VIRTUAL NETWORK SETUP

1. In VMware, choose 'Edit' -> 'Virtual Network Editor...'.  
2. Click 'Change Settings' near the bottom right corner of the new window and approve the admin prompt.

### 'Public' Network Setup

1. Click 'Add Network...' and select an unused network option (e.g., VMnet10) and click 'OK'.
2. Select the newly created network in the list and choose 'Rename Network...'.
3. Name the network 'Public' and click 'OK'.
4. Ensure 'Connect a host virtual adapter to this network' is enabled.
5. Leave 'Use local DHCP service to distribute IP addresses to VMs' enabled.
6. Change the Subnet IP to 192.168.50.0 and the Subnet mask to 255.255.255.0.
7. Select the radial next to 'NAT (shared host's IP address with VMs)'.  
*Note: If another network is already set up as NAT, VMware may prompt that only one NAT network may exist at a time. Change the other network to 'Bridged' or 'Host-only' to continue.*
8. Click 'NAT Settings...' to bring up the NAT Settings dialog box.
9. Set the 'Gateway IP' to 192.168.50.1.
10. Ensure 'Enable IPv6' is not checked.
11. Click 'DNS Settings...' to bring up the Domain Name Server (DNS) dialog box.
12. Uncheck the 'Auto-detect available DNS servers' box.
13. Set the Preferred DNS server to 1.1.1.1 and the Alternate DNS server 1 to 1.0.0.1 and click 'OK'.

### 'IT Net' Network Setup

1. Click 'Add Network...' and select an unused network option (e.g., VMnet11) and click 'OK'.
2. Select the newly created network in the list and choose 'Rename Network...'.
3. Name the network 'IT Net' and click 'OK'.
4. Ensure 'Connect a host virtual adapter to this network' is disabled.
5. Deselect 'Use local DHCP service to distribute IP addresses to VMs'.
6. Change the Subnet IP to 10.10.10.0 and the Subnet mask to 255.255.255.0.
7. Select the radial next to 'Host-only (connect VMs internally in a private network)'.

### 'OT Net' Network Setup

1. Click 'Add Network...' and select an unused network option (e.g., VMnet12) and click 'OK'.

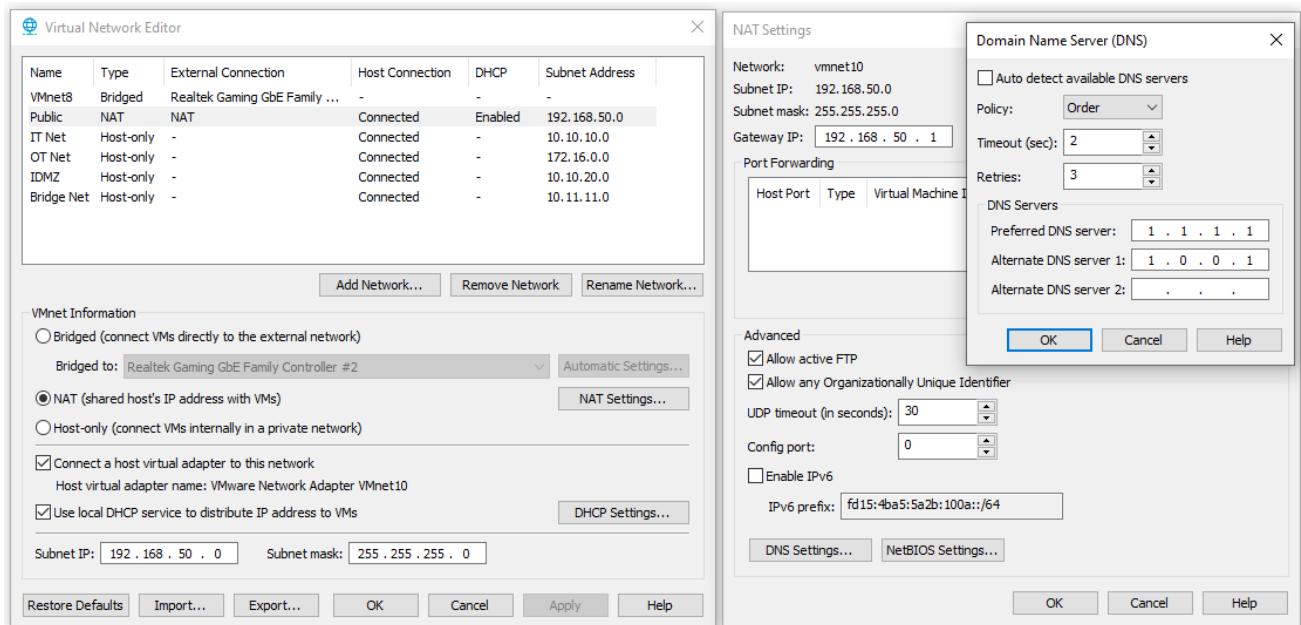
2. Select the newly created network in the list and choose 'Rename Network...'.
3. Name the network 'OT Net' and click 'OK'.
4. Ensure 'Connect a host virtual adapter to this network' is disabled.
5. Deselect 'Use local DHCP service to distribute IP addresses to VMs'.
6. Change the Subnet IP to 172.16.0.0 and the Subnet mask to 255.255.255.0.
7. Select the radial next to 'Host-only (connect VMs internally in a private network)'.

## 'Bridge Net' Network Setup

*Note: This network is not technically required for the 'Original' setup, but it is recommended to set it up now.*

1. Click 'Add Network...' and select an unused network option (e.g., VMnet13) and click 'OK'.
2. Select the newly created network in the list and choose 'Rename Network...'.
3. Name the network 'Bridge Net' and click 'OK'.
4. Ensure 'Connect a host virtual adapter to this network' is disabled.
5. Deselect 'Use local DHCP service to distribute IP addresses to VMs'.
6. Change the Subnet IP to 10.11.11.0 and the Subnet mask to 255.255.255.248.
7. Select the radial next to 'Host-only (connect VMs internally in a private network)'.

## Screenshot of Correctly Configured VMnets (Public, IT Net, OT Net, Bridge Net)



# KALI-LINUX (ATTACKER MACHINE)

## Section 1: Installing Kali

*Reference: Original Network Config Tables or Improved Network Config Tables (both are the same).*

1. Unzip the kali-linux-2021.1-vmware-amd64.7z file and copy the extracted folder to where you would like to store the virtual machine.
2. In VMware, click File > Scan for Virtual Machines...
3. Point VMware at the directory where the machine is stored and complete the wizard to add it.
4. Edit the virtual machine settings.
5. Boot the machine for the first time, and when prompted, click 'I Copied It'.
6. Enter the username 'kali' and the password 'kali' to log in.
7. Adjust the Display settings to an appropriate resolution.
8. Change the power settings so the machine does not go to sleep or turn off the display automatically.
9. Change the time zone to PST.
10. Set static IP addressing for the system.

## Section 2: Installing Tools

### MODBUS-CLI

1. `sudo apt update`
2. `sudo gem install modbus-cli`

### SCAPY

1. `sudo apt install python3-pip`
2. `sudo pip3 install --pre scapy[basic]`

### SMOD

1. `cd`
2. `git clone https://github.com/trouat/smod`

## Section 3: Finishing Up

1. Shutdown machine.
2. Take a snapshot of the current state.

# MODBUS-SERVER (KUBUNTU)

*Reference: Original Network Config Tables or Improved Network Config Tables (Default Gateway and DNS server varies).*

## Section 1: Installing Kubuntu

1. Open the *New Virtual Machine Wizard* in VMware and select the *kubuntu-20.04.2.0-desktop-amd64.iso* image file.
2. VMware should detect the image as based on Ubuntu 64-bit 20.04.2.0 and offer 'Easy Install'.
3. Set the *Personalize Linux* options to the following:
  - a. Full name: modbus
  - b. Username: modbus
  - c. Password: modbus
  - d. Confirm: modbus

4. On the next screen, set the virtual machine name to 'Modbus-Server'.
5. Leave the default HDD space at 20.0 GB.
6. Customize the hardware.

*Note: For now, connect a NAT network adapter for the install process so VMware is able to connect to the internet and automate the process. We will also need this to install the Python Modbus server in Section 3 below. Once finished setting up the Modbus server, change the NIC to match the network being set up (Original or Improved).*

7. Finish the setup wizard and boot the machine to let VMware take care of the install. [wait]
8. If you have issues with the automated installer, delete the machine and repeat steps 1 – 6. Before booting this time, remove the 2 drives VMware adds to facilitate the auto-install process.

## Section 2: Configuring Settings

1. Change power options so the machine does not go to sleep or shut off the display automatically.
2. Ensure time and time zone settings are correct.
3. Set the system hostname to 'modbus-server' by running 'sudo hostnamectl set-hostname modbus-server' and then restarting the system.

## Section 3: Installing Python Modbus Server

1. Open a terminal and run the following commands to update the package database and install pyModbus and its dependencies:
  - a. `sudo apt update`
  - b. `sudo apt install python3-pip`
  - c. `sudo pip3 install pyModbus twisted cryptography bcrypt pyasn1`

2. Create a file on the Desktop called 'Modbus\_server.py' containing the following:

*Note: Double-check the formatting as copy-pasting from a Word doc / PDF can introduce issues. It may be a good idea to paste into Notepad first, and then copy-paste from there into the VM.*

```
#!/usr/bin/env python
'''
Asynchronous Modbus Server Built in Python using the pyModbus module
'''

# Import the libraries we need
from pymodbus.server.asynchronous import StartTcpServer
from pymodbus.device import ModbusDeviceIdentification
from pymodbus.datastore import ModbusSequentialDataBlock
from pymodbus.datastore import ModbusSlaveContext, ModbusServerContext

# Create a datastore and populate it with test data
store = ModbusSlaveContext(
    di = ModbusSequentialDataBlock(0, [17]*100), # Discrete Inputs initializer
    co = ModbusSequentialDataBlock(0, [17]*100), # Coils initializer
    hr = ModbusSequentialDataBlock(0, [17]*100), # Holding Register initializer
    ir = ModbusSequentialDataBlock(0, [17]*100)) # Input Registers initializer
context = ModbusServerContext(slaves=store, single=True)

# Populate the Modbus server information fields, these get returned as
# response to identity queries
identity = ModbusDeviceIdentification()
identity.VendorName = 'PyModbus Inc.'
identity.ProductCode = 'PM'
identity.VendorUrl = 'https://github.com/riptideio/pyModbus'
identity.ProductName = 'Modbus Server'
identity.ModelName = 'PyModbus'
identity.MajorMinorRevision = '1.0'

# Start the listening server
print("Starting Modbus server...")
StartTcpServer(context, identity=identity, address=("0.0.0.0", 502))
```

3. Using a terminal, navigate to the desktop and run the file using Python3 to start the Modbus server:
  - a. `cd /home/modbus/Desktop/`
  - b. `sudo python3 Modbus_server.py`
4. Stop the server using the key combination: Ctrl + C.

## Section 4: Finishing Up

1. Shut down the system.
2. Change the NIC from the NAT adapter to one on the OT Net.
3. Reboot the system.

4. Set static IP addressing based on the network environment you are setting up (Original or Improved).  
***Note: If setting up on the Improved network, set the DNS server to DC1 (10.10.20.252).***
5. Shut down the system once more and take a snapshot of the current state.

# ORIGINAL NETWORK SETUP

## GW-FW (PFSENSE FIREWALL)

*Reference: Original Network Config Tables.*

### Section 1: Creating the Virtual Machine

1. Open New Virtual Machine Wizard in VMware.
2. Select Typical config.
3. Set Installer disc image file to: pfSense-CE-2.5.1-RELEASE-amd64.iso.
4. Name the firewall (e.g., 'GW-FW').
5. Set maximum disk size to 20.0 GB.
6. Select Customize Hardware and change appropriately.
7. Finish the wizard.

### Section 2: Installing pfSense

1. Boot the firewall appliance. [wait]
2. At the *Copyright and distribution notice* screen press 'Enter' to accept.
3. Press 'Enter' to Install.
4. Press 'Enter' to accept the default keymap (US).
5. Press 'Enter' to accept the default *Auto (UFS) BIOS* disk partition option. [wait]
6. At the *Manual Configuration* screen press 'Enter' to choose No.
7. Press 'Enter' to Reboot the firewall appliance. [wait]

### Section 3: Configuring Interfaces

1. Once the restart is complete, you should see a screen like the one below.

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.5.1-RELEASE amd64 Mon Apr 12 07:50:14 EDT 2021
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: c8a2b13269ab673d07ba

*** Welcome to pfSense 2.5.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      ->
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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: █
```



2. Select option 1 to assign interfaces manually.
3. Sample sub-steps follow:
  - a. Take notice of the MAC addresses listed for the valid interfaces (em0 and em1).  
*Note: These steps will assume em0 is associated with the Public LAN Adapter and em1 the IT LAN Adapter.*
  - b. Type 'n' and press 'Enter' to disable VLAN configuration.
  - c. Type 'em0' and press 'Enter' when prompted for the WAN interface name.
  - d. Type 'em1' and press 'Enter' when prompted for the LAN interface name.
  - e. Type 'y' and press 'Enter' to confirm the choices and proceed. [wait]
4. Select option 2 to set the WAN (Public) interface IP address:
  - a. Type '1' and press 'Enter' to set the WAN interface addressing.
  - b. Type 'n' and press 'Enter' to decline IPv4 DHCP configuration.
  - c. Input the static IPv4 address 192.168.50.10 and press 'Enter'.
  - d. Type '24' for the subnet bit count and press 'Enter'.
  - e. Set the Default Gateway address to 192.168.50.1 and press 'Enter'.  
***Note: VMware Virtual Network Editor steps must be completed for this Gateway address to be valid.***
  - f. Type 'n' and press 'Enter' to decline IPv6 DHCP configuration.
  - g. Leave the field blank and press 'Enter' to skip IPv6 addressing.
  - h. Type 'n' and press 'Enter' to decline reverting to HTTP for the web configurator. [wait]
  - i. Press 'Enter' to continue when prompted.
5. Select option 2 again to set up the LAN (IT Net) interface this time:
  - a. Type '2' and press 'Enter' to set the LAN interface addressing.
  - b. Input the static IPv4 address 10.10.10.2 and press 'Enter'.
  - c. Type '24' for the subnet bit count and press 'Enter'.
  - d. Press 'Enter' to skip upstream gateway address configuration.
  - e. Press 'Enter' to skip assigning an IPv6 address.
  - f. Type 'n' and press 'Enter' to disable the DHCP server on the interface.
  - g. Type 'n' and press 'Enter' to decline reverting to HTTP for the web configurator. [wait]
  - h. Press 'Enter' to continue when prompted.

6. Once addressing is set, your display should look similar to the one below.

```
The IPv4 LAN address has been set to 10.10.10.2/24
You can now access the webConfigurator by opening the following URL in your web
browser:
      https://10.10.10.2/

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: c8a2b13269ab673d07ba

*** Welcome to pfSense 2.5.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.50.10/24
LAN (lan)      -> em1      -> v4: 10.10.10.2/24

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: █
```

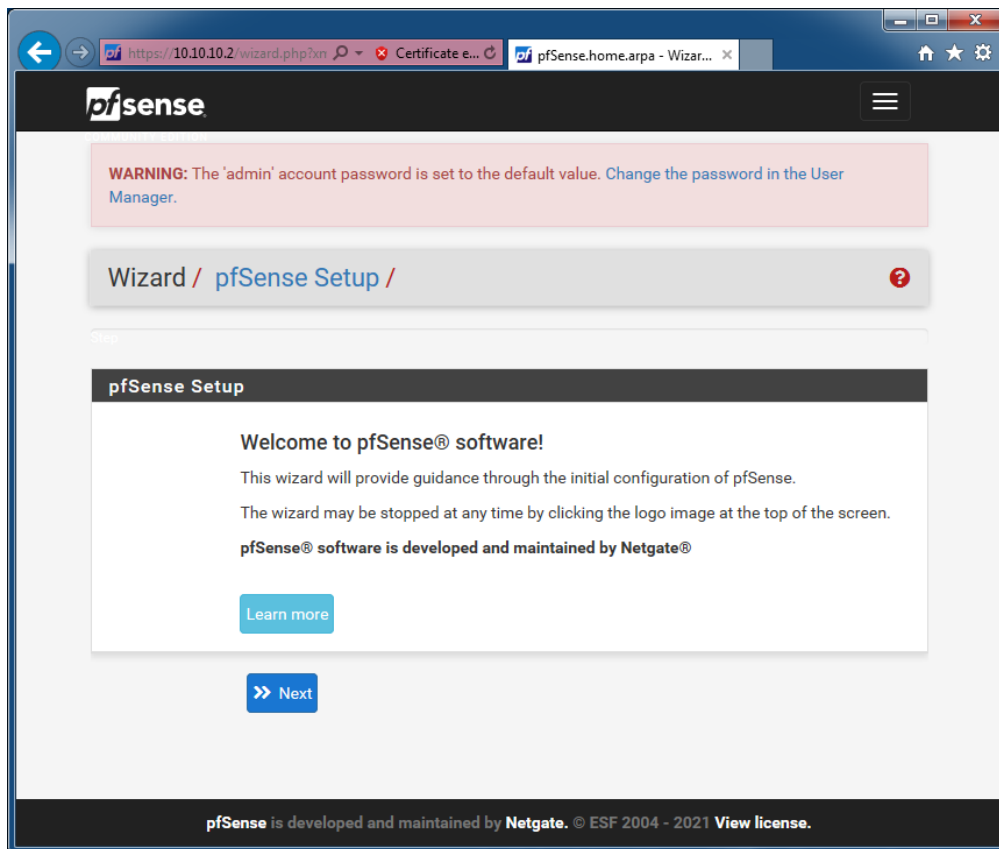
## Section 4: Configuring the Firewall

**Note:** The following steps assume VMware Virtual Networks are configured.

1. Start a virtual machine that resides on the same subnet as the LAN interface of the pfSense firewall and open a web browser to the interface address assigned (e.g., <https://10.10.10.2>).

*Note: If you don't yet have a VM on this subnet, you can install the Main-Wkstn (Windows 7) machine and then come back to complete this Firewall configuration.*

2. Accept the security risk and continue to the webpage if prompted.
3. Enter the default username ('admin') and password ('pfsense') to login to the firewall.
4. You should be presented with a screen that looks like the one below.



5. Click 'Next' to get started.
6. Click 'Next again'.
7. Make the following changes on the *General Information* screen:
  - a. Change the Hostname to 'GW-FW'.
  - b. Change the Domain to 'iacsplant.arpa'.
  - c. Set the Primary DNS Server to 192.168.50.1.
  - d. Keep the Override DNS setting enabled.
8. Click 'Next'.
9. Change the time zone to 'Canada/Pacific' and click 'Next'.
10. On the *Configure WAN Interface* page **DISABLE** "Block RFC1918 Private Networks" and click 'Next'.  
*Note: This is required as our WAN interface resides on a private network subnet.*
11. Click 'Next' to accept the LAN interface addressing (completed in Section 3: Configuring Interfaces).
12. Change the Admin Password to something else if you wish or enter 'pfsense' in both boxes to retain the default. Click 'Next'.
13. Click 'Reload' to confirm the changes.
14. From the *Services* menu along the top of the page navigate to *DNS Resolver*, and in the *General Settings* area of the page, uncheck the 'Enable DNS resolver' box. Scroll down to the bottom of the page and click the blue 'Save' button, followed by the green 'Apply Changes' button at the top of the page (this will appear after saving).

15. Next, go to the *Services* → *DNS Forwarder* page and enable the DNS forwarder. Also tick the following boxes in the *DNS Query Forwarding* section:
  - a. Query DNS servers sequentially.
  - b. Do not forward private reverse lookups.
16. Scroll down to the bottom of the page and click the 'Save' button, followed by the 'Apply Changes' button as done in the previous section.
17. Finally, click the pfSense logo on the top left of the page to be taken to the Dashboard. The system should now be able to check for updates and perform public internet name resolutions. Your screen should look similar to the one below.

The screenshot shows the pfSense Dashboard. At the top, there is a navigation bar with the pfSense logo and menu items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. A warning message is displayed: "WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager." Below this, the "Status / Dashboard" section is active. The main content area is divided into two columns. The left column, titled "System Information", contains a table with the following data:

Name	GW-FW.iacsplant.arpa
User	admin@10.10.10.200 (Local Database)
System	VMware Virtual Machine Netgate Device ID: bff1879b05423d2d30c9
BIOS	Vendor: <b>Phoenix Technologies LTD</b> Version: <b>6.00</b> Release Date: <b>Wed Jul 22 2020</b>
Version	<b>2.5.1-RELEASE</b> (amd64) built on Mon Apr 12 07:50:14 EDT 2021 FreeBSD 12.2-STABLE  The system is on the latest version. Version information updated at Sun May 9 10:22:42 PDT 2021
CPU Type	AMD Ryzen 7 3800X 8-Core Processor 2 CPUs: 2 package(s) x 1 core(s) AES-NI CPU Crypto: Yes (inactive)
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	00 Hour 26 Minutes 08 Seconds
Current date/time	Sun May 9 10:48:21 PDT 2021
DNS server(s)	• 127.0.0.1 • 1.1.1.1 • 1.0.0.1
Last config change	Sun May 9 10:45:02 PDT 2021
State table size	0% (5/45000) <a href="#">Show states</a>

The right column, titled "Netgate Services And Support", contains information about support resources. It includes a section for "NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES" with text about community support and a link to the "NETGATE RESOURCE LIBRARY". Below this, there are links for "Upgrade Your Support", "Community Support Resources", "Netgate Global Support FAQ", "Official pfSense Training by Netgate", "Netgate Professional Services", and "Visit Netgate.com". A red box at the bottom of this section contains a warning: "If you decide to purchase a Netgate Global TAC Support subscription, you **MUST** have your **Netgate Device ID (NDI)** from your firewall in order to validate support for this unit. Write down your NDI and store it in a safe place. You can purchase TAC support [here](#)."

At the bottom of the dashboard, there is an "Interfaces" section showing a table of network interfaces:

WAN	1000baseT <full-duplex>	192.168.50.10
LAN	1000baseT <full-duplex>	10.10.10.2

18. Shut the machine down and take a snapshot of the current state.

## MAIN-WKSTN (WINDOWS 7)

*Reference: Original Network Config Tables.*

*Note: The GW-FW machine should be running before installing (for network access).*

### Section 1: Installing Windows

1. Open IE11-Win7-VMWare.ovf in VMware (Ignore error regarding OVF inspection failure).
2. Change hardware configuration.
3. Boot machine and install VMware Tools and restart.
4. Change screen resolution (optional).
5. Ensure system date, time and time zone are set appropriately.
6. Change power settings to prevent system from sleeping automatically.
7. Disable automatic Windows updates.
8. Disable the Windows Firewall.
9. Disable IPv6 on the network adapter.
10. Set static IPv4 addressing.
11. Verify host is able to access the public internet (via pfSense gateway).
12. Shutdown the machine.
13. Take a snapshot of the initial configuration.

### Section 2: Installing Office

1. Boot the system and use the virtual CD/DVD drive to attach the 'Microsoft Office Standard 2007.iso' image file.
2. Run the setup when prompted or start it manually by accessing the drive in Windows Explorer.
3. Leave the product key field blank and click 'Continue'.
4. Click 'No' when prompted about entering a product key now.
5. Accept the license terms and click 'Continue'.
6. Click 'Install Now'. [wait]
7. Click 'Close' when the installer finishes and disconnect the disc image from the VM.
8. Shutdown the machine and take a snapshot.

## ENG-WKSTN (WINDOWS 7)

*Reference: Original Network Config Tables.*

*Note: The GW-FW machine should be running before installing (for network access).*

1. Open IE11-Win7-VMWare.ovf in VMware (Ignore error regarding OVF inspection failure).
2. Change hardware configuration.
3. Boot machine and install VMware Tools and restart.
4. Change screen resolution (optional).

5. Ensure system date, time and time zone are set appropriately.
6. Change power settings to prevent system from sleeping automatically.
7. Disable automatic Windows updates.
8. Disable the Windows Firewall.
9. Disable IPv6 on both network adapters.
10. Set static IPv4 addressing on appropriate NICs.
11. Verify host is able to access the public internet (via pfSense gateway).
12. Shutdown the machine.
13. Take a snapshot of the initial configuration.

# IMPROVED NETWORK SETUP

## GW-FW (PFSENSE FIREWALL)

*Reference: Improved Network Config Tables.*

### Section 1: Creating the Virtual Machine

1. Open New Virtual Machine Wizard in VMware.
2. Select Typical config.
3. Set Installer disc image file to: pfSense-CE-2.5.1-RELEASE-amd64.iso.
4. Name the firewall (e.g., 'GW-FW').
5. Set maximum disk size to 20.0 GB.
6. Select Customize Hardware and change appropriately.
7. Finish the wizard.

### Section 2: Installing pfSense

1. Boot the firewall appliance. [wait]
2. At the *Copyright and distribution notice* screen press 'Enter' to accept.
3. Press 'Enter' to Install.
4. Press 'Enter' to accept the default keymap (US).
5. Press 'Enter' to accept the default *Auto (UFS) BIOS* disk partition option. [wait]
6. At the *Manual Configuration* screen press 'Enter' to choose No.
7. Press 'Enter' to Reboot the firewall appliance. [wait]

### Section 3: Configuring Interfaces

1. Select option 1 to assign interfaces manually:
  - a. Take notice of the MAC addresses listed for the valid interfaces (em0, em1, and em2).  
*Note: These steps will assume em0 is associated with the Public LAN Adapter, em1 the IT LAN Adapter, and em2 the Bridge Net adapter.*
  - b. Type 'n' and press 'Enter' to disable VLAN configuration.
  - c. Type 'em0' and press 'Enter' when prompted for the WAN interface name.
  - d. Type 'em1' and press 'Enter' when prompted for the LAN interface name.
  - e. Type 'em2' and press 'Enter' when prompted for the Optional 1 interface name.
  - f. Type 'y' and press 'Enter' to confirm the choices and proceed. [wait]
2. Select option 2 to set the WAN (Public) interface IP address:
  - a. Type '1' and press 'Enter' to set the WAN interface addressing.
  - b. Type 'n' and press 'Enter' to decline IPv4 DHCP configuration.
  - c. Input the static IPv4 address 192.168.50.10 and press 'Enter'.
  - d. Type '24' for the subnet bit count and press 'Enter'.

- e. Set the Default Gateway address to 192.168.50.1 and press 'Enter'.  
**Note: VMware Virtual Network Editor steps must be completed for this Gateway address to be valid.**
  - f. Type 'n' and press 'Enter' to decline IPv6 DHCP configuration.
  - g. Leave the field blank and press 'Enter' to skip IPv6 addressing.
  - h. Type 'n' and press 'Enter' to decline reverting to HTTP for the web configurator. [wait]
  - i. Press 'Enter' to continue when prompted.
3. Select option 2 again to set up the LAN (IT Net) interface this time:
    - a. Type '2' and press 'Enter' to set the LAN interface addressing.
    - b. Input the static IPv4 address 10.10.10.2 and press 'Enter'.
    - c. Type '24' for the subnet bit count and press 'Enter'.
    - d. Press 'Enter' to skip upstream gateway address configuration.
    - e. Press 'Enter' to skip assigning an IPv6 address.
    - f. Type 'n' and press 'Enter' to disable the DHCP server on the interface.
    - g. Type 'n' and press 'Enter' to decline reverting to HTTP for the web configurator. [wait]
    - h. Press 'Enter' to continue when prompted.
  4. Select option 2 once more to set up the OPT1 (Bridge Net) interface:
    - a. Type '3' and press 'Enter' to set the OPT1 interface addressing.
    - b. Input the static IPv4 address 10.11.11.2 and press 'Enter'.
    - c. Type '29' for the subnet bit count and press 'Enter'.
    - d. Press 'Enter' to skip upstream gateway address configuration.
    - e. Press 'Enter' to skip assigning an IPv6 address.
    - f. Type 'n' and press 'Enter' to disable the DHCP server on the interface.
    - g. Type 'n' and press 'Enter' to decline reverting to HTTP for the web configurator. [wait]
    - h. Press 'Enter' to continue when prompted.
  5. Once addressing is set, your display should look similar to the one below.

```

Reloading filter...
Reloading routing configuration...

The IPv4 OPT1 address has been set to 10.11.11.2/29

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: faf407daf5cb497ef452

*** Welcome to pfSense 2.5.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.50.10/24
LAN (lan)      -> em1      -> v4: 10.10.10.2/24
OPT1 (opt1)    -> em2      -> v4: 10.11.11.2/29

 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: █

```

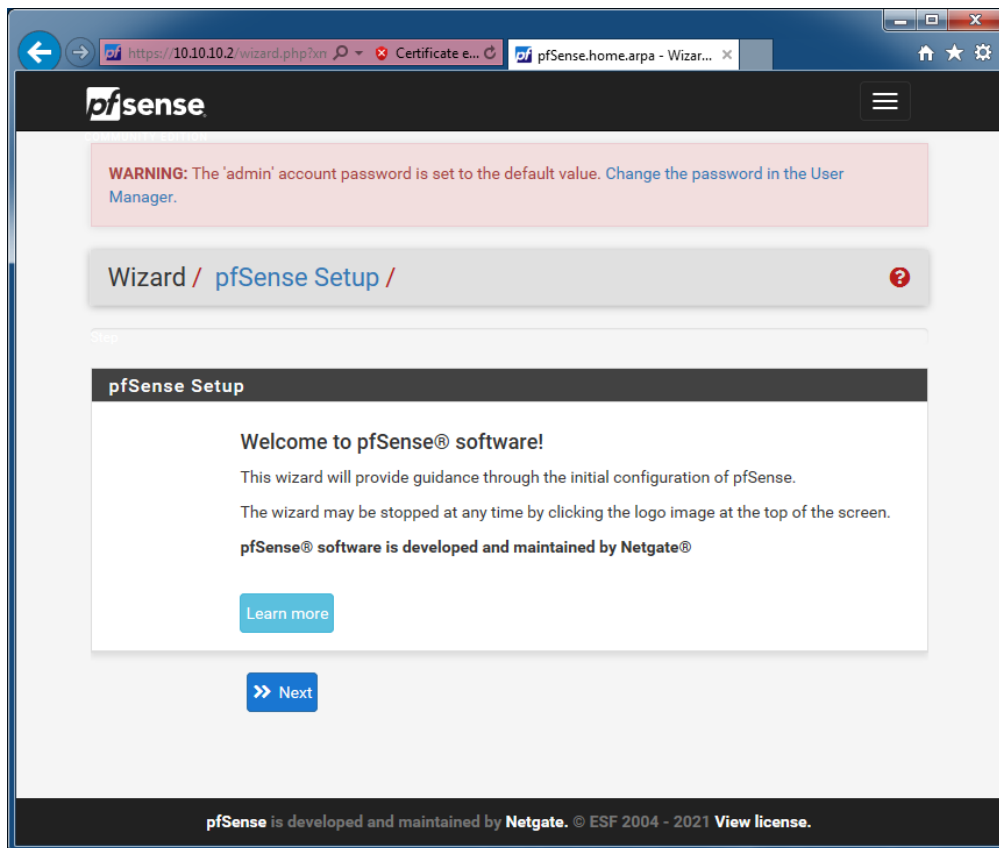


## Section 4: Configuring the Firewall

**Note:** The following steps assume VMware Virtual Networks are configured.

### CONFIGURING THE SETUP WIZARD

1. Start a virtual machine that resides on the same subnet as the LAN interface of the pfSense firewall and open a web browser to the interface address assigned (e.g., <https://10.10.10.2>).
2. Accept the security risk and continue to the webpage if prompted.
3. Enter the default username ('admin') and password ('pfsense') to login to the firewall.
4. You should be presented with a screen that looks similar to the one below.



5. Click 'Next' to get started.
6. Click 'Next' again.
7. Make the following changes on the *General Information* screen:
  - a. Change the Hostname to 'GW-FW'.
  - b. Change the Domain to 'iacsplant.arpa'.
  - c. Set the Primary DNS Server to 192.168.50.1.
  - d. Keep the Override DNS setting enabled.
8. Click 'Next'.
9. Change the time zone to 'Canada/Pacific' and click 'Next'.
10. On the *Configure WAN Interface* page **DISABLE** "Block RFC1918 Private Networks" and click 'Next'.

*Note: This is required as our WAN interface resides on a private network subnet.*

11. Click 'Next' to accept the LAN interface addressing.
12. Change the Admin Password to something else if you wish or enter 'pfsense' in both boxes to retain the default. Click 'Next'.
13. Click 'Reload' to confirm the changes.
14. Click the pfSense logo on the top left of the page to be taken to the Dashboard.

## FIXING DNS RESOLUTIONS

1. From the *Services* menu along the top of the page navigate to *DNS Resolver*, and in the *General Settings* area of the page, uncheck the 'Enable DNS resolver' box. Scroll down to the bottom of the page and click the blue 'Save' button, followed by the green 'Apply Changes' button at the top of the page (this will appear after saving).
2. Next, go to the *Services* → *DNS Forwarder* page and enable the DNS forwarder. Also tick the following boxes in the *DNS Query Forwarding* section:
  - a. Query DNS servers sequentially.
  - b. Do not forward private reverse lookups.
3. Scroll down to the bottom of the page and click the 'Save' button, followed by the 'Apply Changes' button as done in the previous section.

## NAMING THE INTERFACES

1. Go to Interfaces → LAN.
2. Change the Description to 'IT', scroll to the bottom of the page and click 'Save'.
3. If you get an error message about The Router Advertisements Server being active on the interface, do the following:
  - a. On the same page, change the IPv6 Configuration Type to 'Static IPv6'.
  - b. Set the Static IPv6 address to ':::1'.
  - c. Click the 'Save' button at the bottom of the page.
  - d. Navigate to Services → DHCPv6 Server & RA → Router Advertisements and set the Router mode selector to 'Disabled'.
  - e. Click the 'Save' button at the bottom of the page.
  - f. Go back to Interfaces → LAN (or IT if it renamed) and change the IPv6 Configuration Type back to 'None'.
  - g. Now set the Description to 'IT' (if it is still showing as LAN) and click 'Save' and then 'Apply Changes'.
4. Use the same procedure to set the OPT1 interface description to 'BRIDGE'.

## CREATING ALIASES

1. Navigate to Firewall → Aliases.
2. Under the IP section of the page, click 'Add'.
3. Use the following table to add IP Aliases and when done click 'Apply Changes'.

Name	Description	Type	Network/Host
------	-------------	------	--------------

Bridge_Network	Connects GW-FW to IDMZ-FW	Network	10.11.11.0/29
DomainController	Domain Controller	Host	10.10.20.252
Honeypot	Honeypot	Host	10.10.20.25
IDMZ_Network	IDMZ LAN	Network	10.10.20.0/24
IT_Network	Enterprise Network LAN	Network	10.10.10.0/24
OT_Network	Industrial Zone LAN	Network	172.16.0.0/24
SecurityOnion	Security Onion	Host	10.10.20.253

- Under the Ports section of the page, click 'Import'.
- Use the following table to add Port Aliases and when done click 'Apply Changes'.

Alias Name	Description	Aliases to Import
ADDS_Ports	Microsoft Server 2019 Domain Access Ports	53 dns 88 kerberos-sec 135 msrpc 139 netbios-ssn 389 ldap 445 microsoft-ds and smb 464 kpasswd5 593 http-rpc-epmap 636 ldapssl 3268 globalcatLDAP 3269 globalcatLDAPssl 5357 wsdapi 5985 wsman 9389 adws 49152:65535 dynamic port range
SecOnion_Ports	Security Onion Wazuh and Osquery Ports	1514 Wazuh Agent (TCP/UDP) 1515 Wazuh Registration Service TCP 55000 Wazuh API (TCP) 8090 Osquery Endpoint (TCP)
Web_Ports	HTTP and HTTPS Ports	80 HTTP 443 HTTPS

## ADDING THE IDMZ GATEWAY

- Navigate to System → Advanced → Networking and check the 'Prefer IPv4 over IPv6' box.
- Scroll to the bottom of the page and click the 'Save' button.
- Navigate to System → Routing → Gateways.
- Change the Default gateway IPv6 dropdown box to 'None' and click 'Save', then 'Apply Changes'.
- Under the Gateways list, click 'Add'.
- Set the Interface to 'BRIDGE' and the Name to 'IDMZGWFW'.
- Set the Gateway IP address to 11.11.11.3 and click the 'Save' button.
- Click 'Apply Changes' when redirected back to the Gateways page.

## SETTING STATIC ROUTES

1. Navigate to System → Routing → Static Routes and click 'Add'.
2. In the Destination network box, start typing 'IDMZ\_Network' – the system should offer to complete the alias for the network.
3. Change the Gateway to 'IDMZGWFW – 10.11.11.3'.
4. Set the Description to 'IDMZ Routing' and click 'Save'.
5. Click to add another static route.
6. Set the Destination network field to 'OT\_Network'.
7. Change the Gateway to 'IDMZGWFW – 10.11.11.3'.
8. Set the Description to 'OT Routing' and click 'Save'.
9. Apply the changes. Your static routes should look like the ones below (you may have aliases in place of the network addressing):

System / Routing / Static Routes

Gateways

Static Routes

Gateway Groups

Static Routes

	Network	Gateway	Interface	Description	Actions
✓	10.10.20.0/24	IDMZFW - 10.11.11.3	BRIDGE	IDMZ Routing	<div><div></div><div></div><div></div></div>
✓	172.16.0.0/24	IDMZFW - 10.11.11.3	BRIDGE	OT Net Routing	<div><div></div><div></div><div></div></div>

+

Add

## CREATING FIREWALL RULES

### IT Interface Rules

1. Navigate to Firewall → Rules → IT.
2. Using the Add to Top, Add to End, Delete, Save, and Separator options, create rules that match the following screenshot:

*Note:*

*The 'Interface' for all these rules should be 'IT'.*

*Use the Aliases defined previously to make this process easier.*

*Use the 'Block' Action for the 'Block to OT Net' rule.*

*Click the green tick-mark on the far left of the 'Default allow LAN to any rule' to disable the rule.*

Floating	WAN	IT	BRIDGE
----------	-----	----	--------

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 8.43 MiB	*	*	*	IT Address	443 80	*	*		Anti-Lockout Rule	
Allow Everything [Testing and Configuration ONLY]											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 *	IT net	*	*	*	*	none		Default allow LAN to any rule	
OT Net Block											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 120 B	IPv4 *	*	*	OT_Network	*	*	none		Block to OT Net	
Windows Server AD DS											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 238 B	IPv4 TCP/UDP	IT net	*	DomainController	ADDS_Ports	*	none		Access AD DS	
Security Onion											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 1 / 382 B	IPv4 TCP/UDP	IT net	*	SecurityOnion	SecOnion_Ports	*	none		Send Wazuh and Osquery	
Allow Public											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 1 / 12 KiB	IPv4 TCP/UDP	IT net	*	*	Web_Ports	*	none		Web Access	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 296 B	IPv4 UDP	IT net	*	*	123 (NTP)	*	none		Network Time Protocol	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 960 B	IPv4 ICMP any.	IT net	*	*	*	*	none		Ping Anyone	

Add
 Add
 Delete
 Save
 Separator

### BRIDGE Interface Rules

1. While still on the Firewall → Rules → IT page, click the 'Copy' button (2 buttons right of the anchor looking button) on the 'Default allow LAN to any rule'.
2. Uncheck 'Disabled' and change the Interface to 'BRIDGE'.
3. Change the Source dropdown box to 'any'.
4. Change the Description to 'Pass Between Firewalls' and click the 'Save' button.
5. Apply the changes.
6. Optionally, add a separator that says 'Allow Communication Between Firewalls' and place it above the rule:

Floating	WAN	IT	BRIDGE
----------	-----	----	--------

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
Allow Communication Between Firewalls											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 3 / 135 KiB	IPv4 *	*	*	*	*	*	none		Pass Between Firewalls	

Add
 Add
 Delete
 Save
 Separator

7. Shut the machine down and take a snapshot of the current state.

# IDMZ-FW (PFSENSE FIREWALL)

*Reference: Improved Network Config Tables.*

## Section 1: Creating the Virtual Machine

1. Open New Virtual Machine Wizard in VMware.
2. Select Typical config.
3. Set Installer disc image file to: pfSense-CE-2.5.1-RELEASE-amd64.iso.
4. Name the firewall (e.g., 'IDMZ-FW').
5. Set maximum disk size to 20.0 GB.
6. Select Customize Hardware and change appropriately.
7. Finish the wizard.

## Section 2: Installing pfSense

*Note: The GW-FW machine should be running before installing (for network access).*

1. Boot the firewall appliance. [wait]
2. At the *Copyright and distribution notice* screen press 'Enter' to accept.
3. Press 'Enter' to Install.
4. Press 'Enter' to accept the default keymap (US).
5. Press 'Enter' to accept the default *Auto (UFS) BIOS* disk partition option. [wait]
6. At the *Manual Configuration* screen press 'Enter' to choose No.
7. Press 'Enter' to Reboot the firewall appliance. [wait]

## Section 3: Configuring Interfaces

1. Select option 1 to assign interfaces manually:
  - a. Take notice of the MAC addresses listed for the valid interfaces (em0, em1, and em2).  
*Note: These steps will assume em0 is associated with the Bridge Net Adapter, em1 the IDMZ Adapter, and em2 the OT Net adapter.*
  - b. Type 'n' and press 'Enter' to disable VLAN configuration.
  - c. Type 'em0' and press 'Enter' when prompted for the WAN interface name.
  - d. Type 'em1' and press 'Enter' when prompted for the LAN interface name.
  - e. Type 'em2' and press 'Enter' when prompted for the Optional 1 interface name.
  - f. Type 'y' and press 'Enter' to confirm the choices and proceed. [wait]
2. Select option 2 to set the WAN (Bridge Net) interface IP address:
  - a. Type '1' and press 'Enter' to set the WAN interface addressing.
  - b. Type 'n' and press 'Enter' to decline IPv4 DHCP configuration.
  - c. Input the static IPv4 address 10.11.11.3 and press 'Enter'.
  - d. Type '29' for the subnet bit count and press 'Enter'.
  - e. Set the Default Gateway address to 10.11.11.2 and press 'Enter'.

- f. Type 'n' and press 'Enter' to decline IPv6 DHCP configuration.
  - g. Leave the field blank and press 'Enter' to skip IPv6 addressing.
  - h. Type 'n' and press 'Enter' to decline reverting to HTTP for the web configurator. [wait]
  - i. Press 'Enter' to continue when prompted.
3. Select option 2 again to set up the LAN (IDMZ) interface this time:
  - a. Type '2' and press 'Enter' to set the LAN interface addressing.
  - b. Input the static IPv4 address 10.10.20.2 and press 'Enter'.
  - c. Type '24' for the subnet bit count and press 'Enter'.
  - d. Press 'Enter' to skip upstream gateway address configuration.
  - e. Press 'Enter' to skip assigning an IPv6 address.
  - f. Type 'n' and press 'Enter' to disable the DHCP server on the interface.
  - g. Type 'n' and press 'Enter' to decline reverting to HTTP for the web configurator. [wait]
  - h. Press 'Enter' to continue when prompted.
4. Select option 2 once more to set up the OPT1 (OT Net) interface:
  - a. Type '3' and press 'Enter' to set the OPT1 interface addressing.
  - b. Input the static IPv4 address 172.16.0.2 and press 'Enter'.
  - c. Type '24' for the subnet bit count and press 'Enter'.
  - d. Press 'Enter' to skip upstream gateway address configuration.
  - e. Press 'Enter' to skip assigning an IPv6 address.
  - f. Type 'n' and press 'Enter' to disable the DHCP server on the interface.
  - g. Type 'n' and press 'Enter' to decline reverting to HTTP for the web configurator. [wait]
  - h. Press 'Enter' to continue when prompted.
5. Once addressing is set, your display should look similar to the one below.

```

Reloading filter...
Reloading routing configuration...

The IPv4 OPT1 address has been set to 172.16.0.2/24

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 028d11ee72838f02c74c

*** Welcome to pfSense 2.5.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 10.11.11.3/29
LAN (lan)      -> em1      -> v4: 10.10.20.2/24
OPT1 (opt1)    -> em2      -> v4: 172.16.0.2/24

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: █

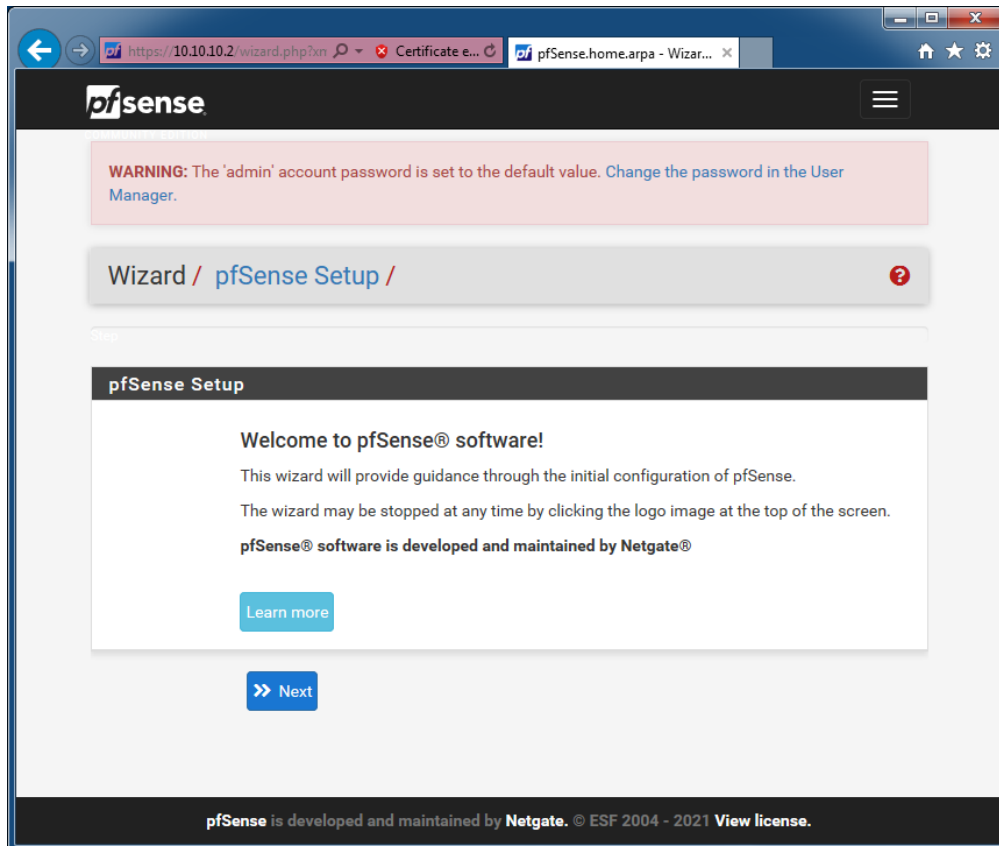
```

## Section 4: Configuring the Firewall

**Note:** The following steps assume VMware Virtual Networks are configured.

## CONFIGURING THE SETUP WIZARD

1. Start a virtual machine that resides on the same subnet as the LAN interface of the pfSense firewall and open a web browser to the interface address assigned (e.g., <https://10.10.20.2>).
2. Accept the security risk and continue to the webpage if prompted.
3. Enter the default username ('admin') and password ('pfsense') to login to the firewall.
4. You should be presented with a screen that looks like the one below.



5. Click 'Next' to get started.
6. Click 'Next' again.
7. Make the following changes on the *General Information* screen:
  - a. Change the Hostname to 'IDMZ-FW'.
  - b. Change the Domain to 'iacsplant.arpa'.
  - c. Set the Primary DNS Server to 10.11.11.2.
  - d. Keep the Override DNS setting enabled.
8. Click 'Next'.
9. Change the time zone to 'Canada/Pacific' and click 'Next'.
10. On the *Configure WAN Interface* page **DISABLE** "Block RFC1918 Private Networks" **AND** "Block bogon networks" and click 'Next'.

*Note: This is required as our WAN interface resides on a private network subnet.*
11. Click 'Next' to accept the LAN interface addressing.



12. Change the Admin Password to something else if you wish or enter 'pfsense' in both boxes to retain the default. Click 'Next'.
13. Click 'Reload' to confirm the changes.
14. Click the pfSense logo on the top left of the page to be taken to the Dashboard.

## FIXING DNS RESOLUTIONS

1. From the *Services* menu along the top of the page navigate to *DNS Resolver*, and in the *General Settings* area of the page, uncheck the 'Enable DNS resolver' box. Scroll down to the bottom of the page and click the blue 'Save' button, followed by the green 'Apply Changes' button at the top of the page (this will appear after saving).
2. Next, go to the *Services* → *DNS Forwarder* page and enable the DNS forwarder. Also tick the following boxes in the *DNS Query Forwarding* section:
  - a. Query DNS servers sequentially.
  - b. Do not forward private reverse lookups.
3. Scroll down to the bottom of the page and click the 'Save' button, followed by the 'Apply Changes' button as done in the previous section.

## NAMING THE INTERFACES

1. Go to *Interfaces* → *WAN*.
2. Change the Description to 'BRIDGE', scroll to the bottom of the page and click 'Save'.
3. If you get an error message about The Router Advertisements Server being active on the interface, do the following:
  - a. On the same page, change the IPv6 Configuration Type to 'Static IPv6'.
  - b. Set the Static IPv6 address to ':::1'.
  - c. Click the 'Save' button at the bottom of the page.
  - d. Navigate to *Services* → *DHCPv6 Server & RA* → *Router Advertisements* and set the Router mode selector to 'Disabled'.
  - e. Click the 'Save' button at the bottom of the page.
  - f. Go back to *Interfaces* → *WAN* (or *BRIDGE* if it renamed) and change the IPv6 Configuration Type back to 'None'.
  - g. Now set the Description to 'BRIDGE' (if it is still showing as *WAN*) and click 'Save' and then 'Apply Changes'.
4. Use the same procedure to set the LAN interface description to 'IDMZ' and the OPT1 interface description to 'OT'.

## CREATING ALIASES

1. Navigate to *Firewall* → *Aliases*.
2. Under the IP section of the page, click 'Add'.
3. Use the following table to add IP Aliases and when done click 'Apply Changes'.

Name	Description	Type	Network/Host
Bridge_Network	Connects GW-FW to IDMZ-FW	Network	10.11.11.0/29
DomainController	Domain Controller	Host	10.10.20.252
Honeypot	Honeypot	Host	10.10.20.25
IDMZ_Network	IDMZ LAN	Network	10.10.20.0/24
IT_Network	Enterprise Network LAN	Network	10.10.10.0/24
OT_Network	Industrial Zone LAN	Network	172.16.0.0/24
SecurityOnion	Security Onion	Host	10.10.20.253

- Under the Ports section of the page, click 'Import'.
- Use the following table to add Port Aliases and when done click 'Apply Changes'.

Alias Name	Description	Aliases to Import
ADDS_Ports	Microsoft Server 2019 Domain Access Ports	53 dns 88 kerberos-sec 135 msrpc 139 netbios-ssn 389 ldap 445 microsoft-ds and smb 464 kpasswd5 593 http-rpc-epmap 636 ldapssl 3268 globalcatLDAP 3269 globalcaLDAPssl 5357 wsdapi 5985 wsman 9389 adws 49152:65535 dynamic port range
SecOnion_Ports	Security Onion Wazuh and Osquery Ports	1514 Wazuh Agent (TCP/UDP) 1515 Wazuh Registration Service TCP 55000 Wazuh API (TCP) 8090 Osquery Endpoint (TCP)
Web_Ports	HTTP and HTTPS Ports	80 HTTP 443 HTTPS

## EDITING THE GATEWAY

- Navigate to System → Advanced → Networking and check the 'Prefer IPv4 over IPv6' box.
- Scroll to the bottom of the page and click the 'Save' button.
- Navigate to System → Routing → Gateways.
- Change the Default gateway IPv6 dropdown box to 'None' and click 'Save', then 'Apply Changes'.
- Click 'Apply Changes' when redirected back to the Gateways page.

## SETTING A STATIC ROUTE

1. Navigate to System → Routing → Static Routes and click 'Add'.
2. In the Destination network box, start typing 'IT\_Network' – the system should offer to complete the alias for the network.
3. Set the Gateway to 'IDMZGFW – 10.11.11.2'.
4. Set the Description to 'IT Net Routing' and click 'Save'.
5. Apply the changes. Your static route should look like the one below:

System / Routing / Static Routes				
Gateways   Static Routes   Gateway Groups				
Static Routes				
	Network	Gateway	Interface	Description
<input checked="" type="checkbox"/>	it_network	WANGW - 10.11.11.2	BRIDGE	IT Net Routing
+ Add				

## CREATING FIREWALL RULES

### BRIDGE Interface Rules

1. Navigate to Firewall → Rules → BRIDGE.
2. Create a new rule to match the screenshot below and apply changes:

Floating   BRIDGE   IDMZ   OT											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>										Allow Communication Between Firewalls	
<input checked="" type="checkbox"/>	✓	0 / 2.33 MIB	IPv4 *	*	*	*	*	*	none	Pass Between Firewalls	
↑ Add   ↓ Add   Delete   Save   + Separator											

### IDMZ Interface Rules

1. Navigate to Firewall → Rules → IDMZ.
2. Using the Add to Top, Add to End, Delete, Save, and Separator options, create rules that match the following screenshot:

*Note:*

*The 'Interface' for all these rules should be 'IDMZ'.*

*Use the Aliases defined previously to make this process easier.*






























Use the 'Block' Action for the 'Block to OT Net' rule.

Click the green tick-mark on the far left of the 'Default allow LAN to any rule' to disable the rule.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 / 1.86 MiB	*	*	*	IDMZ Address	443 80	*	*		Anti-Lockout Rule	
Allow Everything [Testing and Configuration ONLY]											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 *	IDMZ net	*	*	*	*	none		Default allow LAN to any rule	
OT Net Block											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 *	*	*	OT net	*	*	none		Block to OT Net	
Windows Server (AD DS)											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 1 / 1 KiB	IPv4 TCP/UDP	DomainController	*	*	53 (DNS)	*	none		DNS Resolve	
Allow Public											
<input type="checkbox"/>	<input checked="" type="checkbox"/> 5 / 61.62 MiB	IPv4 TCP/UDP	IDMZ net	*	*	Web_Ports	*	none		Web Access	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 UDP	IDMZ net	*	*	123 (NTP)	*	none		Network Time Protocol	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 73 KiB	IPv4 TCP	Honeypot	*	*	587 (SUBMISSION)	*	none		Honeypot Email Alerts	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0 / 0 B	IPv4 ICMP any	IDMZ net	*	*	*	*	none		Ping Anyone	
							Add	Add	Delete	Save	Separator

## OT Interface Rules

1. Navigate to Firewall → Rules → OT.
2. Using the Add to Top, Add to End, Delete, Save, and Separator options, create rules that match the following screenshot:

Floating BRIDGE IDMZ <b>OT</b>											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0 / 0 B	IPv4 *	OT net	*	*	*	none		Default allow LAN to any rule	   
AD DS											
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP/UDP	OT net	*	DomainController	ADDS_Ports	*	none	Access AD DS	    
Security Onion											
<input type="checkbox"/>	✓	0 / 0 B	IPv4 TCP/UDP	OT net	*	SecurityOnion	SecOnion_Ports	*	none	Send Wazuh and Osquery	    
ICMP											
<input type="checkbox"/>	✓	0 / 0 B	IPv4 ICMP any	OT net	*	172.16.0.2	*	*	none	Ping Local Gateway	    
<input type="checkbox"/>	✓	0 / 0 B	IPv4 ICMP any	OT net	*	IDMZ net	*	*	none	Ping IDMZ	    
							 Add	 Add	 Delete	 Save	 Separator

3. Shut the machine down and take a snapshot of the current state.

# WINDOWS SERVER 2019

*Reference: Improved Network Config Tables.*

## Section 1: Creating the Virtual Machine

1. Open New Virtual Machine Wizard in VMware.
2. Select Typical config.
3. Select 'I will install the operating system later'.
4. For Guest Operating System type, choose Microsoft Windows, Windows Server 2019.
5. Name the machine (e.g., 'Win-Server').
6. Set maximum disk size to 60 GB.
7. Select Customize Hardware and change appropriately.
8. Finish the wizard.

## Section 2: Installing Windows Server

*Note: Both the GW-FW and IDMZ-FW machines should be running before installing (for network access).*

1. Click 'Edit virtual machine settings' and add the 17763.737.190906-2324.rs5\_release\_svc\_refresh\_SERVER\_EVAL\_x64FRE\_en-us\_1.iso image to the CD/DVD connection.
2. Power on the virtual machine and press any key when prompted to load the installer.
3. Leave the install language set to English (United States).
4. Change the time and currency format to English (Canada).
5. Leave the keyboard input method as US.
6. Click 'Next' and then 'Install now'.
7. Select the fourth install option for the operating system – Windows Server 2019 Datacenter Evaluation (Desktop Experience) – and then click 'Next'.
8. Accept the license terms and continue.
9. Choose the custom install option.
10. Select the single empty drive volume and press 'Next'. [wait]
11. Once the initial install is complete, you should be presented with the 'Customize settings' page.
12. Set the Administrator password to 'ServerPassw0rd!' and click 'Finish'.

## Section 3: Configuring

### BASIC SETTINGS

1. Logon to the machine by right clicking on the VM tab and selecting 'Send Ctrl + Alt + Del', or by pressing Ctrl + Alt + Ins on your keyboard.
2. Enter the password set previously to logon.
3. Change the screen resolution to something appropriate (optional).
4. Set the power options so the screen does not turn off automatically.
5. In the Local Server section of the Server Manager window, do the following:

- a. Configure the IPv4 static addressing.  
*Note: The first DNS server should be the server itself (127.0.0.1). The second will be the subnet's default gateway.*
  - b. Disable IPv6 networking.
  - c. Ensure the system date, time and time zone are set properly.
  - d. Change the computer name to 'DC1' and reboot to apply the change.
6. Logon once the system reboots.

## VMWARE TOOLS

1. Right-click on the VM tab and select Install VMware Tools.
2. Run the VMware tools installer and choose Typical installation. Finish and reboot the system when prompted.

## Section 4: Adding Server Roles

### ACTIVE DIRECTORY DOMAIN SERVICES (AD DS) ROLE

1. Logon once more, and on the *Server Manager Dashboard*, click 'Add roles and features'.
2. Click 'Next' to acknowledge the first screen.
3. Leave 'Role-based or feature-based installation selected and click 'Next'.
4. Leave the current local server selected (DC1) and click 'Next'.
5. Select the box next to 'Active Directory Domain Services' (AD DS) and then click 'Add Features' on the pop-up window that appears (leave 'Include management tools selected). Click 'Next'.
6. Click 'Next' again to skip the Features page.
7. On the AD DS page, click 'Next' to acknowledge the notes about ideally having at least two domain controllers on a network and that a DNS server will be required.
8. Check the box at the top of the next page, 'Restart the destination server automatically if required' and then click 'Install'.
9. Click the 'Close' button to dismiss the progress window.

### PROMOTE TO DOMAIN CONTROLLER

1. Once the AD DS role install completes, there should be a yellow caution triangle visible next to the flag icon on the top right of the *Server Manager* window.
2. Click the flag to view the 'Post-deployment Configuration' task and click on the link to 'Promote this server to a domain controller'.
3. On the *Deployment Configuration* window, choose the option to 'Add a new forest', specify the root domain as 'iacsplant.arpa', and click 'Next'.
4. Leave the forest and domain function levels at their defaults (Windows Server 2016), as well as the domain controller capabilities selections (Domain Name System (DNS) server and Global Catalog (GC) selected).
5. Set the Directory Services Restore Mode (DSRM) password to 'ServerPassw0rd!' and continue.
6. On the DNS Options page, ignore the warning banner and click 'Next'.

7. Verify the NetBIOS domain name has been set to 'IACSPLANT' and click 'Next'.
8. Leave the AD DS database, log files, and SYSVOL paths at their defaults and continue.
9. Review the configuration options and click 'Next'.
10. Once the Prerequisites Check is complete, click 'Install'. [wait]
11. The system will automatically reboot once the promotion is complete. [wait]

## FINISHING UP

1. When the server finishes rebooting, logon to the newly created domain administrator account (IACSPLANT\Administrator) using the same password as before ('ServerPassw0rd!').
2. Open a command prompt window and do a ping test to verify connectivity between the server and the subnet default gateway. Also test a public name resolution (i.e.: [www.google.ca](http://www.google.ca)). Both should be working at this point.  
*Note: You may have to reconfigure the second DNS server (IDMZ subnet gateway address).*
3. Shutdown the server and take a snapshot of the initial configuration.

## Section 5: Creating Groups and Users

Domain Users				
Group	First Name	Last Name	Logon Name	Password
Domain Admins	IACS	Admin	iacsadmin	Passw0rd!
Business	Matt	Main	mattmain	Passw0rd!
SOC	Maria	Monitor	mariamon	Passw0rd!
Engineers	Ed	Engineer	edeng	Passw0rd!

### CREATE A GROUP

*Note: The 'Domain Admins' group is already present in Windows Server and does not need to be created.*

1. From the *Server Manager* window, click Tools → Active Directory Users and Computers.
2. Expand the 'iacsplant.arpa' tree and click on the 'Users' folder.
3. Right-click in an empty space in the right-hand panel and choose New → Group.
4. Name the group.
5. Leave the scope set to Global and the type set to Security and click 'OK'.

### CREATE A USER

1. From the *Server Manager* window, click Tools → Active Directory Users and Computers.
2. Expand the 'iacsplant.arpa' tree and click on the 'Users' folder.
3. Right-click in an empty space in the right-hand panel and choose New → User.
4. Fill out the *New Object – User* dialog box.



5. Click 'Next'.
6. Set the user password and ensure only the 'Password never expires' option box is ticked.
7. Click 'Next' and then 'Finish'.
8. Right-click on the newly created user and select 'Add to a group'.
9. Type the name of the group to add them to in the *Enter the object names to select* field and then click 'Check Names'. The named group object should become underlined.
10. Click 'OK' to add the user to this group.
11. Acknowledge the pop-up dialog verifying the operation was completed successfully.

## LOGON AS A DOMAIN USER

1. Restart the system and logon to the server with the newly created 'iacsadmin' domain account.
2. At the logon screen choose the 'Other user' option at the bottom left corner of the display.
3. Type the username of the domain account to logon as (i.e.: 'iacsadmin').
4. Fill in the password and press 'Enter'.
5. You should now be logged on as the domain user on the iacsplant.arp domain.

## Section 6: Group Policy (Firewall Rule)

1. From the *Server Manager* window, click Tools → Group Policy Management.
2. Expand the tree Forest: iacsplant.arp → Domains → iacsplant.arp.
3. Right-click on Starter GPOs and select 'New'.
4. Name the Starter GPO 'Allow ICMP Echo/Reply' and click 'OK'.
5. Right-click on the just created 'Firewall Rules' Starter GPO and choose 'Edit'.
6. Expand the tree Computer Configuration → Administrative Templates → Network → Network Connections → Windows Defender Firewall → Domain Profile.
7. Double-click on the Setting 'Windows Defender Firewall: Allow ICMP exceptions'.
8. Select 'Enabled' and tick the box next to 'Allow inbound echo request'.
9. Click 'OK' and close the *Group Policy Starter GPO Editor* window.
10. Right-click on the 'Firewall Rules' Starter GPO and select 'New GPO From Starter GPO'.
11. Name the GPO 'Allow ICMP Echo/Reply' and click 'OK'.
12. Expand the 'Group Policy Objects' tree. The 'Allow ICMP Echo/Reply' GPO should be visible there.
13. Right-click on 'iacsplant.arp' and select 'Link an Existing GPO'.
14. From the Group Policy objects list, choose the 'Allow ICMP Echo/Reply' and click 'OK'.
15. Shut the machine down and take a snapshot of the current state.

## Section 7: Joining the Domain

1. Logon to the Windows 10 machine (i.e.: main-wkstn) normally.
2. Open the Control Panel and navigate to System and Security → System and click 'Change settings' on the right-hand side of the window.
3. Click the 'Change...' button to rename the computer or change its domain or workgroup.
4. Change the Computer name (i.e.: 'main-wkstn').

5. Set the Member of selection radial to Domain, and enter 'iacsplant.arpa'.
6. Click 'OK'.
7. Use the recently created IACS Admin account to join the computer to the domain (username: 'iacsadmin', password: 'Passw0rd!').  
*Note: You must use an administrator account to join a machine to a domain.*
8. Click 'OK' on the dialog box welcoming you to the new domain.
9. Click 'Restart Now' on the next pop-up box.
10. On reboot, use the 'Other user' option to logon as the IACS Admin user and confirm addition. [wait]
11. Repeat these steps for the remaining Windows 10 workstation machines using the same naming scheme (e.g.: mon-wkstn, eng-wkstn).

## MAIN-WKSTN (WINDOWS 10)

*Reference: Improved Network Config Tables.*

*Note: The GW-FW, IDMZ-FW, and Win-Server machines should be running before installing (for network and domain access).*

1. Open MSEdge-Win10-VMware.ovf in VMware.
2. Change the hardware configuration.
3. Boot machine and install VMware Tools and restart.
4. Change screen resolution (optional).
5. Ensure system date, time and time zone are set appropriately.
6. Change power settings to prevent system from sleeping automatically.
7. Disable automatic Windows updates (for now).
8. Disable IPv6 on the network adapter.
9. Set static IPv4 addressing.
10. Connect to the iacsplant domain (Windows Server 2019 → Section 7: Joining the Domain).
11. Reboot and logon to the system using the Business user account.
12. Verify the host is able to ping the GW-FW firewall (default gateway) and reach the internet.
13. Install the 'new' Edge web browser (based on Chromium).
14. Shut the machine down and take a snapshot of the current state.

## MON-WKSTN (WINDOWS 10)

*Reference: Improved Network Config Tables.*

*Note: The GW-FW, IDMZ-FW, and Win-Server machines should be running before installing (for network and domain access).*

1. Open MSEdge-Win10-VMware.ovf in VMware.
2. Change the hardware configuration.
3. Boot machine and install VMware Tools and restart.
4. Change screen resolution (optional).
5. Ensure system date, time and time zone are set appropriately.
6. Change power settings to prevent system from sleeping automatically.
7. Disable automatic Windows updates (for now).
8. Disable IPv6 on the network adapter.
9. Set static IPv4 addressing.
10. Connect to the iacsplant domain (Windows Server 2019 → Section 7: Joining the Domain).
11. Reboot and logon to the system using the SOC user account.
12. Verify the host is able to ping the IDMZ-FW firewall (default gateway) and reach the internet.

13. Install the 'new' Edge web browser (based on Chromium) so that Security Onion and Splunk Dashboards will load with full functionality later on.
14. Shut the machine down and take a snapshot of the current state.

## ENG-WKSTN (WINDOWS 10)

*Reference: Improved Network Config Tables.*

*Note: The GW-FW, IDMZ-FW, and Win-Server machines should be running before installing (for network and domain access).*

1. Open MSEdge-Win10-VMware.ovf in VMware.
2. Change the hardware configuration.
3. Boot machine and install VMware Tools and restart.
4. Change screen resolution (optional).
5. Ensure system date, time and time zone are set appropriately.
6. Change power settings to prevent system from sleeping automatically.
7. Disable automatic Windows updates (for now).
8. Disable IPv6 on the network adapter.
9. Set static IPv4 addressing.
10. Connect the machine to the plant domain – See Windows Server 2019 → Section 7: Joining the Domain.
11. Reboot and logon to the system using the Engineer user account.
12. Verify the host is able to ping the IDMZ-GW firewall (default gateway).
13. Shut the machine down and take a snapshot of the current state.

# HONEYPOT (KUBUNTU)

*Reference: Improved Network Config Tables.*

## Section 1: Installing Kubuntu

*Note: Both the GW-FW and IDMZ-FW machines should be running before installing (for network access).*

1. Open the *New Virtual Machine Wizard* in VMware and select the *kubuntu-20.04.2.0-desktop-amd64.iso* image file.
2. VMware should detect the image as based on Ubuntu 64-bit 20.04.2.0 and offer 'Easy Install'.
3. Set the *Personalize Linux* options to the following:
  - a. Full name: honeypot
  - b. Username: honeypot
  - c. Password: honeypot
  - d. Confirm: honeypot

4. On the next screen, set the virtual machine name to 'Honeypot'.
5. Leave the default HDD space at 20.0 GB.
6. Customize the hardware.

*Note: For now, connect a NAT network adapter for the install process so VMware is able to connect to the internet and automate the process. Once finished setting up the Honeypot, change the NIC to the OT Net.*

7. Finish the setup wizard and boot the machine to let VMware take care of the install. [wait]
8. If you have issues with the automated installer, delete the machine and repeat steps 1 – 6. Before booting this time, remove the 2 drives VMware adds to facilitate the auto-install process.

## Section 2: Configuring Settings

1. Change power options so the machine does not go to sleep or shut off the display automatically.
2. Ensure time and time zone settings are correct.
3. Set static IPv4 addressing.
4. Set the system hostname to 'honeypot' by running 'sudo hostnamectl set-hostname honeypot' and then restarting the system.

## Section 3: Installing Conpot

1. Open a terminal and run the following commands to update the package database and install dependencies before installing Conpot:
  - a. `sudo apt update`
  - b. `sudo apt install python3-pip`
  - c. `sudo apt install python3-virtualenv`
  - d. `sudo apt install git libsmi2ldbl smistrip libxslt1-dev python3.6-dev libevent-dev default-libmysqlclient-dev`

*Note: If there is an error that 'python3.6-dev' is not found, you need to update ppa and then update the system again to install python3.6.*

- i. `sudo add-apt-repository ppa:deadsnakes/ppa`
  - ii. `sudo apt update`
  - iii. `sudo apt install python3.6`
2. After the installation of all the dependencies, create isolated Python environment named 'conpot'. Then, activate the created environment:
  - a. `virtualenv --python=python3.6 conpot`
  - b. `source conpot/bin/activate`
3. Upgrade basic tools and install Conpot from PyPI:
  - a. `pip3 install --upgrade pip`
  - b. `pip3 install --upgrade setuptools`

*Note: If there is an error that 'pycrypto is not found, you need to uninstall pycrypto and install pycryptodome*

    - iv. `pip3 uninstall pycrypto`
    - v. `pip3 install pycryptodome`
  - c. `pip3 install cffi`
  - d. `pip3 install conpot`

*Note: If there is an error that 'stix distribution is not found', you need to install sphinx-rtd-theme.*

    - i. `pip3 install sphinx-rtd-theme`
4. Start Conpot:
  - a. `conpot -f --template default`

*Note: default is the template which contains HTTP, MODBUS, S7COMM, and SNMP. There are other templates available such as "proxy" which demonstrates the proxy feature.*

*Note: if there is a Permission error that Conpot cannot reach conpot.log file, use chmod command to modify file permission.*

    - i. `sudo chmod -R a+rw /usr/local/lib/python3.8`

## Section 4: Creating a Start Script

1. Create a new file called startconpot.sh in the home directory and open it for editing:
  - a. `cd ~/`
  - b. `touch startconpot.sh`
  - c. `nano startconpot.sh`
2. Paste / type the following:

```
#!/bin/bash
source conpot/bin/activate
conpot -f --template default
```

3. Save the file and add the executable property:
  - a. Ctrl + X
  - b. 'y'
  - c. 'Enter'
  - d. `chmod +x startconpot.sh`
4. To start Conpot from now on, open a terminal to the home directory and run the script:
  - a. `./startconpot.sh`

## Section 5: Finishing Up

1. Shut the machine down and take a snapshot of the current state.

# SPLUNK

## Section 1: Installing Splunk

*Note: Both the GW-FW and IDMZ-FW machines should be running before installing (for network access).*

1. Start the Honeypot (Kubuntu) machine in VMware.
2. Install the wget command and download Splunk:
  - a. `sudo apt install wget`
  - b. `wget -O splunk-8.2.0-e053ef3c985f-linux-2.6-amd64.deb 'https://www.splunk.com/bin/splunk/DownloadActivityServlet?architecture=x86_64&platform=linux&version=8.2.0&product=splunk&filename=splunk-8.2.0-e053ef3c985f-linux-2.6-amd64.deb&wget=true'`
  - c. Install and start Splunk by accepting the license.
  - d. `sudo dpkg -i <splunk_package_name>.deb` (i.e.: `sudo dpkg -i splunk-8.2.0-e053ef3c985f-linux-2.6-amd64.deb`)

```
root@ubuntu:/home/modbus# dpkg -i splunk-8.2.0-e053ef3c985f-linux-2.6-amd64.d
Selecting previously unselected package splunk.
(Reading database ... 174448 files and directories currently installed.)
Preparing to unpack splunk-8.2.0-e053ef3c985f-linux-2.6-amd64.deb ...
Unpacking splunk (8.2.0) ...
Setting up splunk (8.2.0) ...
/var/lib/dpkg/info/splunk.postinst: line 74: curl: command not found
cp: cannot stat '/opt/splunk/etc/regid.2001-12.com.splunk-Splunk-Enterprise.s
complete
```

*Note: ignore the error that there is no file or directory.*

- e. `sudo /opt/splunk/bin/splunk start --accept-license`
3. Provide an administrator username for Splunk (i.e.: honeypot)
  4. Provide a password for Splunk (i.e.: honeypot)

```
Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

Waiting for web server at http://127.0.0.1:8000 to be available..... Done

If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://ubuntu:8000
```

## Section 2: Setting up Splunk

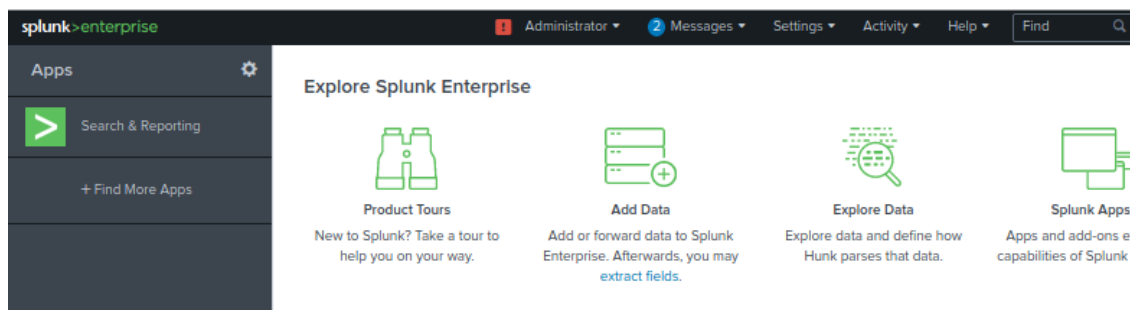
1. Open Firefox and access the Splunk web interface (ubuntu:8000 or 127.0.0.1:8000).
2. Login with the administrator username and password (i.e.: honeypot).
3. Go to the Settings and select Licensing under System.
4. To use full features of Splunk, click 'Change license group'.



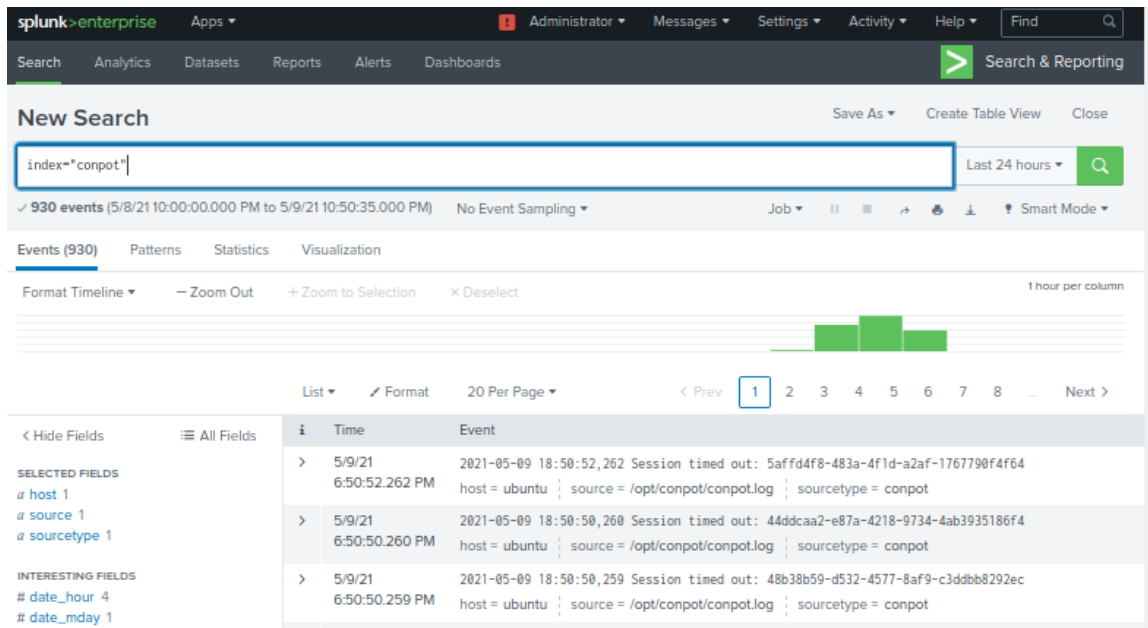
5. Make sure 'Enterprise Trial License' is selected at the bottom of the page.

**Note: Do not change the license if 'Enterprise Trial license' is already selected. If you switch to another license, you cannot return to the trial.**

6. Go to the Settings and under Data select Indexes to add new index.
7. Click 'New Index' green button on top right of the page.
8. Provide the index name 'conpot' and leave other parts as default. Click 'Save'.
9. Go to Splunk main page and click the 'Add Data' icon.



10. Click the 'Monitor' icon and select 'Files & Directories'.
11. Provide the conpot.log file location (i.e.: /opt/conpot/conpot.log or /home/honeypot/conpot.log) and then click 'Next'.
12. On the Set Source Type page, verify the log file timestamps are recognized and click 'Next'.
13. Set the Save Source Type name to 'conpot log' and click 'Save'.
14. Change the index value on the Input Settings page to 'conpot' and leave other fields as default.
15. Click 'Review' and then 'Submit'.
16. Return to the Splunk main page and click 'Search & Reporting' to search data by index.
17. Type the target index (i.e.: index="conpot") in the search box and check if the real time honeypot data is connected to Splunk.



## Section 3: Setting up Splunk Alerts

1. Search by index and keywords based on the table below. For example, search 'index="conpot" "FTP"' and then create alerts.

Protocol	Alert Title	Email - Severity	Triggered - Alert Severity	Search
Modbus	Conpot Modbus Traffic	Highest	Critical	Index="conpot" "Modbus traffic from"
HTTP	Conpot HTTP GET Request	High	High	Index="conpot" "HTTP GET request"
SNMP	Conpot SNMP Session	Normal	Medium	Index="conpot" "SNMP session from"
FTP	Conpot FTP Traffic	Low	Low	Index="conpot" "FTP"



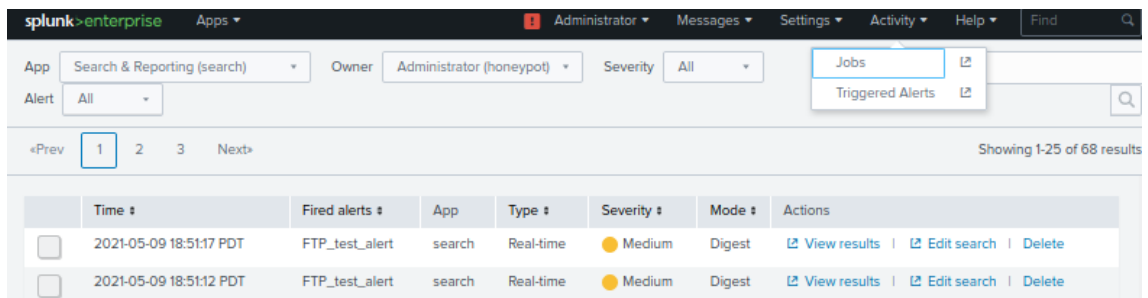
2. Provide the title and change alert type to 'Real-time'.
3. Select 'Per-Result' to trigger alerts whenever the search returns a result.
4. Add two trigger actions:
  - a. Add 'ADD to Triggered Alerts' and provide severity based on the table.
  - b. Add 'Send email' and enter an email address in the 'To' field. Also, provide severity based on the table and leave other fields as default. (i.e.: incswhiptail@gmail.com)

*Note: For this project, we created a Gmail account. If you use a personal email, you might get a security alert from Gmail.*

5. Save the alerts.
6. Go to Settings and select Server Settings under System.
7. Click 'Email settings' and provide the following information:
  - a. Mail host: smtp.gmail.com:587
  - b. Email security: Enable TLS
  - c. Username: [incswhiptail@gmail.com](mailto:incswhiptail@gmail.com)
  - d. Password: [REDACTED]
  - e. Leave other fields as default, but you can customize the email format later.
8. Click 'Save' at the bottom of the page.

## Section 4: Perform Splunk Alert Simulation

1. As a test, run Nmap to generate FTP logs and check 'Triggered Alerts'.



The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items like 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. Below this, there's a search bar and filters for 'App' (Search & Reporting (search)), 'Owner' (Administrator (honeypot)), and 'Severity' (All). A dropdown menu for 'Alert' is set to 'All'. On the right, a 'Jobs' dropdown menu is open, showing 'Triggered Alerts'. Below the filters, a table displays triggered alerts. The table has columns: Time, Fired alerts, App, Type, Severity, Mode, and Actions. Two alerts are listed, both for 'FTP\_test\_alert' triggered at 2021-05-09 18:51:17 PDT and 2021-05-09 18:51:12 PDT. Each alert has links for 'View results', 'Edit search', and 'Delete'.

	Time	Fired alerts	App	Type	Severity	Mode	Actions
<input type="checkbox"/>	2021-05-09 18:51:17 PDT	FTP_test_alert	search	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>
<input type="checkbox"/>	2021-05-09 18:51:12 PDT	FTP_test_alert	search	Real-time	Medium	Digest	<a href="#">View results</a>   <a href="#">Edit search</a>   <a href="#">Delete</a>

2. Also, login to the administrator email:
  - a. Go to the gmail.com
  - b. Username: [incswhiptail@gmail.com](mailto:incswhiptail@gmail.com) / password: [REDACTED]
  - c. Check if you got the alert email from Splunk.



3. At this point you may also login to the Splunk Dashboard from the Mon-Wkstn by navigating to 10.10.20.25:8000 in the Microsoft Edge browser (username 'honeypot', password 'honeypot').

## Section 5: Finishing Up

1. Shut the machine down and take a snapshot of the current state.

# SEC-ONION (SECURITY ONION SIEM)

*Reference: Improved Network Config Tables.*

## Section 1: Creating the Virtual Machine

1. Open New Virtual Machine Wizard in VMware.
2. Select Typical config.
3. Set Installer disc image file to: securityonion-2.3.50.iso.
4. For Guest Operating System type, choose Linux, CentOS 7 64-bit.
5. Name the machine (e.g., 'Sec-Onion').
6. Set maximum disk size to 150 GB.
7. Select Customize Hardware and change appropriately.
8. Finish the wizard.

## Section 2: Installing Security Onion

*Note: Both the GW-FW and IDMZ-FW machines should be running before installing (for network access).*

1. Boot the machine. [wait]
2. At the warning screen type 'yes' and press 'Enter' to continue the installation.
3. Set the administrative username to 'seconion'.
4. Set and confirm the administrative account password as 'seconion'.
5. Wait for the initial install to complete and press 'Enter' when prompted to reboot.
6. At the 'localhost login' prompt, login using the administrative account credentials set earlier.
7. At the *Welcome to Security Onion Setup* screen, choose 'Yes' to continue.
8. Select the 'STANDALONE' Install option.
9. Type 'AGREE', and press 'Enter' at the next screen to accept the Elastic License.
10. Select the 'Standard' manager installation type.
11. If you allocated less than 12 GB of RAM for the machine, you will now see a warning about 12 GB being the minimum requirement. Select 'Yes' to continue.
12. Set the hostname to 'sec-onion'.
13. Leave the description box blank.
14. When selecting the management NIC, be sure to choose the first one that resides in the IDMZ network. If you added the interfaces in the same order as in the Improved Network Config Tables, this should be the lowest number link in the list. If you know how, you can verify this by opening the .vmx file associated with the virtual machine (do not edit this file while the machine is running).
15. Choose 'STATIC' as the IPv4 addressing type for the management interface.
16. Enter the IPv4 address for the IDMZ management interface.
17. Enter the gateway IPv4 address for the IDMZ network.
18. Enter the DNS server address for the IDMZ network.
19. For the DNS search domain, enter 'iacsplant.arpa'.

20. Choose 'Ok' at the next screen to initialize networking.
21. Choose 'Direct' as the method to connect to the internet.
22. Select all 3 remaining NICs as monitoring interfaces.
23. Leave updates set to automatic.
24. For home networks, enter all networks to be monitored (i.e.: IT Net, OT Net, IDMZ) using CIDR notation.
25. Select the 'BASIC' manager type to install.
26. Choose 'Zeek' for metadata generation.
27. Set the IDS ruleset to 'ETOPEN' (Emerging Threats Open).
28. Acknowledge the screen about enabling services and RAM usage.
29. Leave all components selected to install.
30. Select 'Yes' to keep the default Docker IP range.
31. Enter an email address for the admin account web logon (i.e.: 'admin@iacsplant.com').
32. Enter a password for the admin account (i.e.: 'iacsplantadmin') and confirm it on the next screen.
33. For access to the web interface, choose to use an IP address.
34. Select 'Ok' to set a password for the soremote user.
35. Set the soremote user password (i.e.: 'soremoteadmin').
36. Select the 'BASIC' configuration type to use.
37. Set the number of zeek processes to 1 (sufficient for loads under 200Mbps).
38. Set the number of Suricata processes to 1 (sufficient for loads under 200Mbps).
39. Select 'Yes' when asked if you would like to configure NTP servers.
40. Accept the default NTP servers listed.
41. Select 'NODEBASIC' as the config type to use.
42. Select 'Yes' to run 'so-allow' to allow access to web tools.
43. Allow the IDMZ subnet (i.e.: 10.10.20.0/24) access to the web tools.
44. On the summary screen, select 'Yes' to confirm and install. [wait]
45. Once the install is complete, press 'Enter' to reboot the system.

## Section 3: Setting up Wazuh

### References:

- <https://docs.securityonion.net/en/2.3/wazuh.html#adding-agents>
- <https://documentation.wazuh.com/3.13/user-manual/registering/command-line-registration.html>

### GETTING THE INSTALLERS

1. Using the Mon-Wkstn running Windows 10, access the Security Onion web interface (10.10.20.253).
2. Click on the Downloads section in the left-hand menu to view available packages customized for this Security Onion installation.
3. Download Wazuh Agents for Windows and Debian based Linux and copy them to your host machine.

## ALLOWING AGENT CONNECTIONS

1. On the Mon-Wkstn machine, open PowerShell and SSH to the Security Onion box ([ssh seconion@10.10.20.253](ssh:seconion@10.10.20.253)).
2. If prompted, type 'yes' to accept the key fingerprint and continue connecting.
3. Enter the password for the seconion user to login ('seconion').
4. Run the 'sudo so-allow' command (confirm password if required).
5. Type 'w' to setup the Wazuh agent role on TCP/UDP port 1514.
6. Enter the network address range to allow agent collection on (i.e.: 10.10.20.0/24 (IDMZ)).
7. Repeat steps 8 through 10 for the IT and OT network address ranges.
8. Use the 'sudo docker exec -it so-wazuh dpkg -l | grep wazuh' command to check the current version of the Wazuh Agent manager on the Security Onion installation (v3.13.1 as of writing).
9. Use the 'sudo so-wazuh-agent-manage' command to bring up the Wazuh Agent Manager.
10. Select the 'Add an agent' option.
11. Provide a name for the new agent (i.e.: 'mon-wkstn').
12. Enter the IP address of the new agent (i.e.: 10.10.20.200).
13. Confirm adding of the new agent.
14. Select the 'Extract key for an agent' option.
15. Enter the ID number of the agent to extract a key for (i.e.: 002).
16. Copy the key and use it to authenticate the new agent when setting up the installer package as outlined in the following section.
17. Repeat steps 9 through 16 for each new agent to be added.

## ADDING AN AGENT (WINDOWS)

1. Copy the wazuh-agent-3.13.1-1.msi file to the Windows host.
2. Run the MSI Wazuh Agent installer on the host machine.
3. Agree to the license agreement and continue the installation.
4. Check the 'Run Agent configuration interface' box and click 'Finish'.
5. In the 'Manager IP' field, enter the Security Onion management interface IP (i.e.: 10.10.20.253).
6. In the 'Authentication key' box paste the code copied in the previous section (*Allowing Agent Connections – Step 16*) for this specific agent.
7. Click 'Save' and then 'OK' to confirm adding the key for the new agent.
8. Click Manage → Restart to start the agent service with the updated settings.
9. Click the 'Refresh' button to verify the status as running.
10. Repeat these steps to add the agent service to the remaining Windows-based host machines.  
*Windows machines that should be added: Win-Server, Mon-Wkstn, Main-Wkstn, Eng-Wkstn.*

## ADDING AN AGENT (LINUX)

1. Copy the wazuh-agent\_3.13.1-1\_amd64.deb file to the Linux host.
2. Run the .deb Wazuh Agent installer on the host machine.
3. Click 'Install Package' and enter the system password.

4. Open a terminal window and run 'sudo /var/ossec/bin/manage\_agents -i <key>', replacing <key> with the appropriate agent key copied in the previous section (*Allowing Agent Connections – Step 16*). Enter the system password when prompted.
5. Confirm addition of the new agent.
6. Next, edit the file at '/var/ossec/etc/ossec.conf', replacing 'MANAGER\_IP' in the <client><server> section with the Security Onion management interface IP (i.e.: 10.10.20.253). Save the edited file.
7. Finally, restart the Wazuh agent using the command, 'sudo systemctl restart wazuh-agent.service'.
8. Repeat these steps to add the agent service to the remaining Linux-based host machines.  
*Linux machines that should be added: Honeypot, Modbus-Server.*

## Section 3: Setting up Osquery

Reference: <https://docs.securityonion.net/en/2.3/osquery.html#agents-deployment>

### GETTING THE PACKAGES

1. Using the Mon-Wkstn running Windows 10, access the Security Onion web interface (10.10.20.253).
2. Click on the Downloads section in the left-hand menu to view available packages customized for this Security Onion installation.
3. Download Osquery Packages and Configs for Windows and Debian based Linux and copy them to your host machine.

### ALLOWING OSQUERY CONNECTIONS

1. On the Mon-Wkstn machine, open PowerShell and SSH to the Security Onion box (ssh [seconion@10.10.20.253](mailto:seconion@10.10.20.253)).
2. If prompted, type 'yes' to accept the key fingerprint and continue connecting.
3. Enter the password for the seconion user to login ('seconion').
4. Run the 'sudo so-allow' command (confirm password if required).
5. Type 'o' to setup access on TCP port 8090 for Osquery endpoints.
6. Enter the network address range to allow agent collection on (i.e.: 10.10.20.0/24 (IDMZ)).
7. Repeat steps 8 through 10 for the IT and OT network address ranges.

### ADDING AN AGENT (WINDOWS)

1. Copy the Osquery msi-launcher.msi and launcher-msi.flags.txt files to the Windows host.
2. Run the Osquery MSI launcher file.

*Windows machines that should be added: Win-Server, Mon-Wkstn, Main-Wkstn, Eng-Wkstn.*

### ADDING AN AGENT (LINUX)

1. Copy the Osquery deb-launcher.deb and launcher.flags.txt files to the Linux host.
2. Run the .deb Wazuh Agent installer on the host machine.
3. Click 'Install Package' and enter the system password.

*Linux machines that should be added: Honeypot, Modbus-Server.*

## Section 4: Setting up Syslog

### ALLOWING CONNECTIONS

1. On the Mon-Wkstn machine, open PowerShell and SSH to the Security Onion box (ssh [seconion@10.10.20.253](mailto:seconion@10.10.20.253)).
2. If prompted, type 'yes' to accept the key fingerprint and continue connecting.
3. Enter the password for the seconion user to login ('seconion').
4. Run the 'sudo so-allow' command (confirm password if required).
5. Type 's' to setup access on TCP/UDP port 514 for Syslog devices.
6. Enter 10.10.20.2 as the IP address to allow (IDMZ interface of the IDMZ-FW firewall). [wait]
7. Repeat steps 4 and 5, and this time enter 10.11.11.2 as the allowed IP address (Bridge Net interface of the GW-FW firewall). [wait]

### ENABLING SYSLOG ON THE FIREWALLS (GW-FW & IDMZ-FW)

#### *IDMZ-FW*

1. Login to the IDMZ-FW web management interface from the Mon-Wkstn.
2. Navigate to Status → System Logs → Settings.
3. At the top of the page, change the Log Message Format selector to syslog.
4. Scroll to the bottom of the page and tick the box to 'Enable Remote Logging'.
5. Change the Source Address box to 'IDMZ' (this will use the 10.10.20.2 IP address allowed earlier).
6. Leave the IP Protocol box set to IPv4.
7. Set the first remote log server box to 10.10.20.253 (Security Onion IP address).
8. Check the 'Everything' box next to Remote Syslog Contents to send all log messages to the SIEM.
9. Click the 'Save' button at the bottom of the page.

#### *GW-FW*

1. Login to the GW-FW web management interface from the Main-Wkstn.
2. Navigate to Status → System Logs → Settings.
3. At the top of the page, change the Log Message Format selector to syslog.
4. Scroll to the bottom of the page and tick the box to 'Enable Remote Logging'.
5. Change the Source Address box to 'BRIDGE' (this will use the 10.11.11.2 IP address allowed earlier).
6. Leave the IP Protocol box set to IPv4.
7. Set the first remote log server box to 10.10.20.253 (Security Onion IP address).
8. Check the 'Everything' box next to Remote Syslog Contents to send all log messages to the SIEM.
9. Click the 'Save' button at the bottom of the page.

## Section 5: Finishing Up

1. Shut the machine down and take a snapshot of the current state.