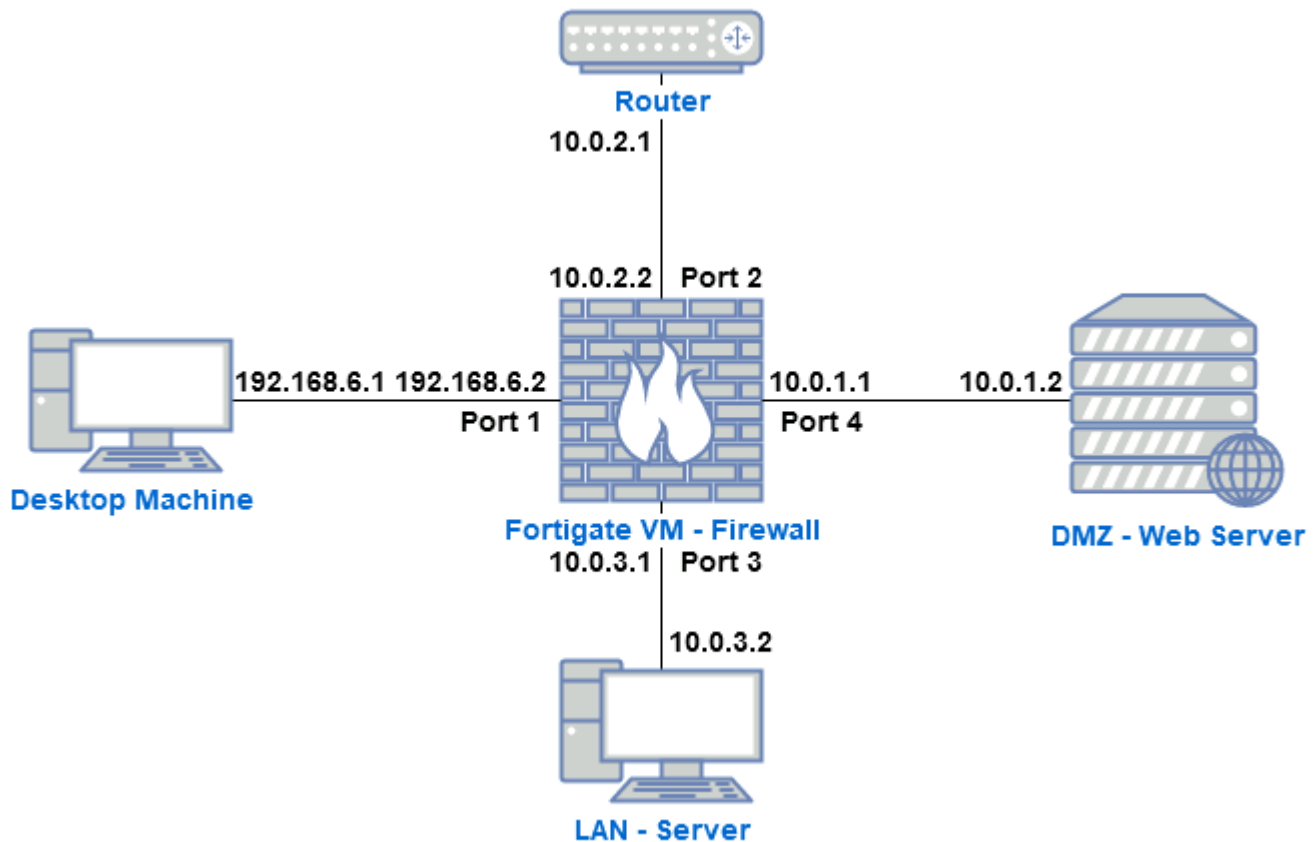


Topology



Module Description

- **Fortinet** provides intelligent and seamless protection technologies to more than 450k customers, including Fortune 500 companies, all around the world (including UofC).
- Fortinet provides their flagship **Fortigate** enterprise firewall platform in variety of sizes and form factors to accomodate their customers needs and to fit in their environments seamlessly.
- Customers have liberty of acquiring their Next-Generation Firewall solution as a **physical appliance or virtual machine** that supports various virtualization technologies.
- **FortiOS** is the OS that lies in heart of both their physical security devices and virtual machines.

→ In this module, you will be introduced to firewall policies with FortiGate VM.

Interface Configuration

- FortiGate VM offer users CLI and WEB GUI environments.
- This module will focus on WEB GUI interface, but you have the liberty of performing all tasks with command line interface via SSH if you wish so.
- Investigate the **network topology** from the menu above.
- LAN, DMZ and WAN interfaces are connected to respective ports of the FortiGate VM firewall. However, correct access permissions, interface roles, and aliases are NOT assigned to those ports yet.
- Populated ports can be viewed, edited or configured from **Network → Interfaces** of the Web GUI.
- To configure the interface, Right-click on the interface and select **Edit**.
 - **Alias** - Naming ports descriptively will allow you to navigate and make further changes easily.
 - **Interface roles** - Once the correct role is assigned, Fortigate will hide unrelated settings for that role.
 - **Administrative Access** - Allows you to grant/remove admin permissions to interfaces.
- The management interface is the backbone of this module and is used by the desktop machine to access the firewall and by the router to communicate with devices for grading purposes.

Note: Do NOT edit the management interface!

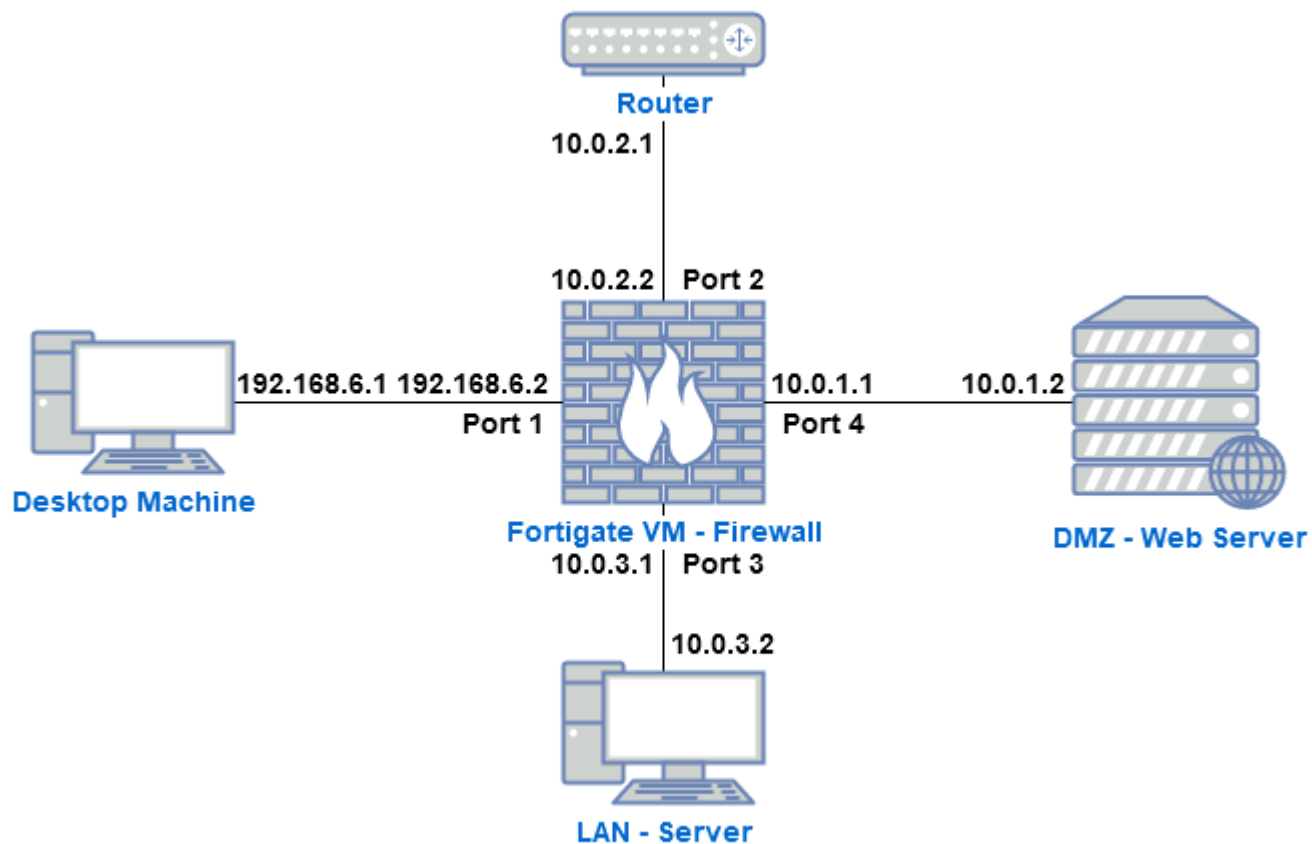
→ In this module, you will:

1. Assign correct roles and aliases to ports
2. Restrict management access from DMZ.

Objectives:

- Access to FortiGate VM.
 - Address: <https://fortigate.lab>
 - Username: **student**
 - Password: **student**
- Edit **Port 2**:
 - Set Alias to: **WAN**
 - Set Role to: **WAN**
 - Granted Administrative Access: **PING**
- Edit **Port 3**:
 - Set Alias to: **LAN**
 - Set Role to: **LAN**
 - Granted Administrative Access: **HTTPS, HTTP, SSH, PING**
- Edit **Port 4**:
 - Set Alias to: **DMZ**
 - Set Role to: **DMZ**
 - Granted Administrative Access: **None**

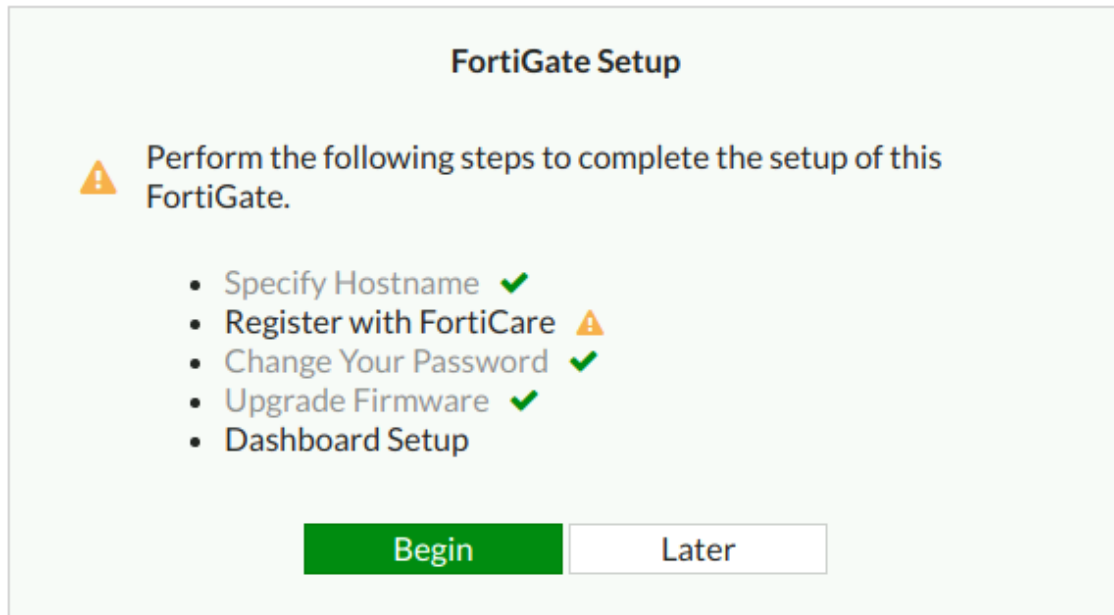
Recap of the Topology:



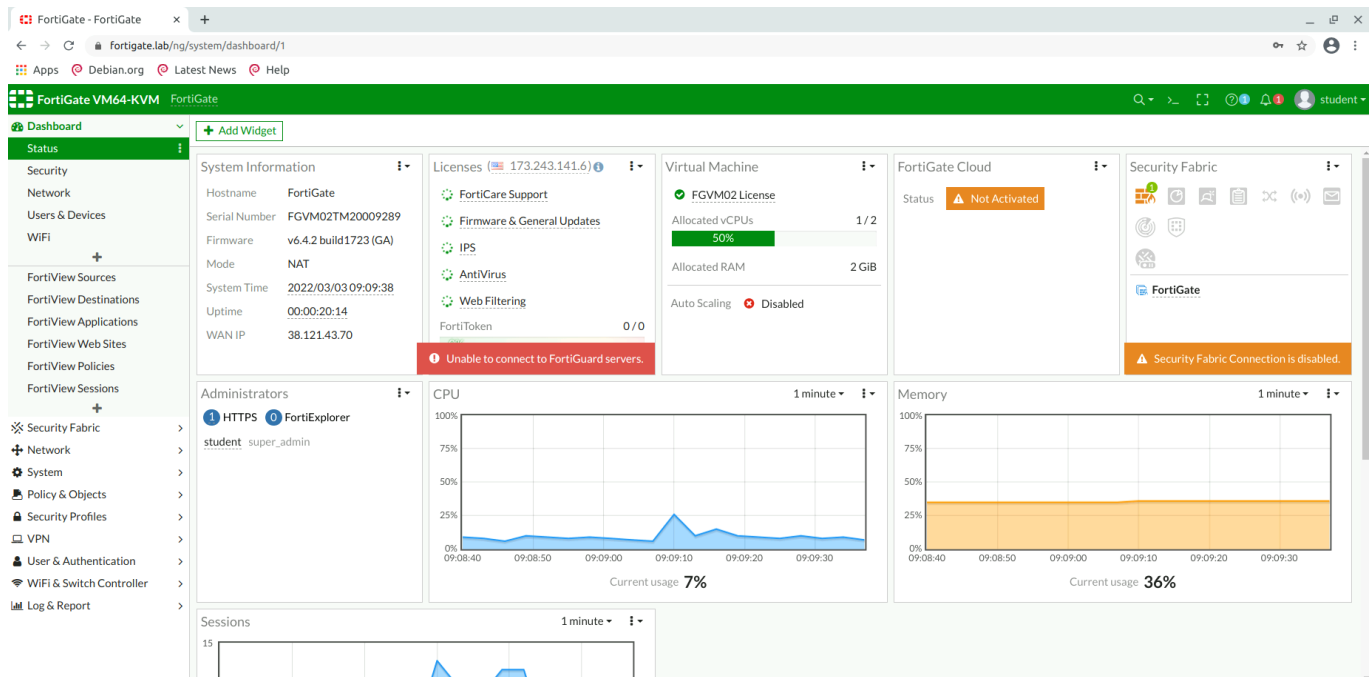
Documentation:

1. Login to the fortigate.lab link and use the given credentials.

2. Do the Fortigate Setup later.

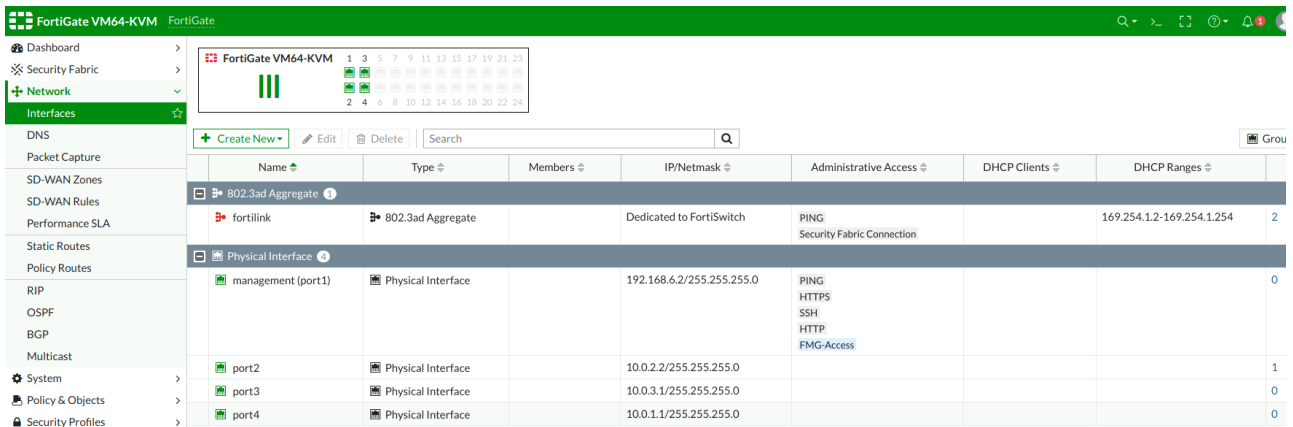


3. As you can see, this is the general overview of the Web GUI interface of the FortiGate VM.



4. How to get to modify "Port 2"?

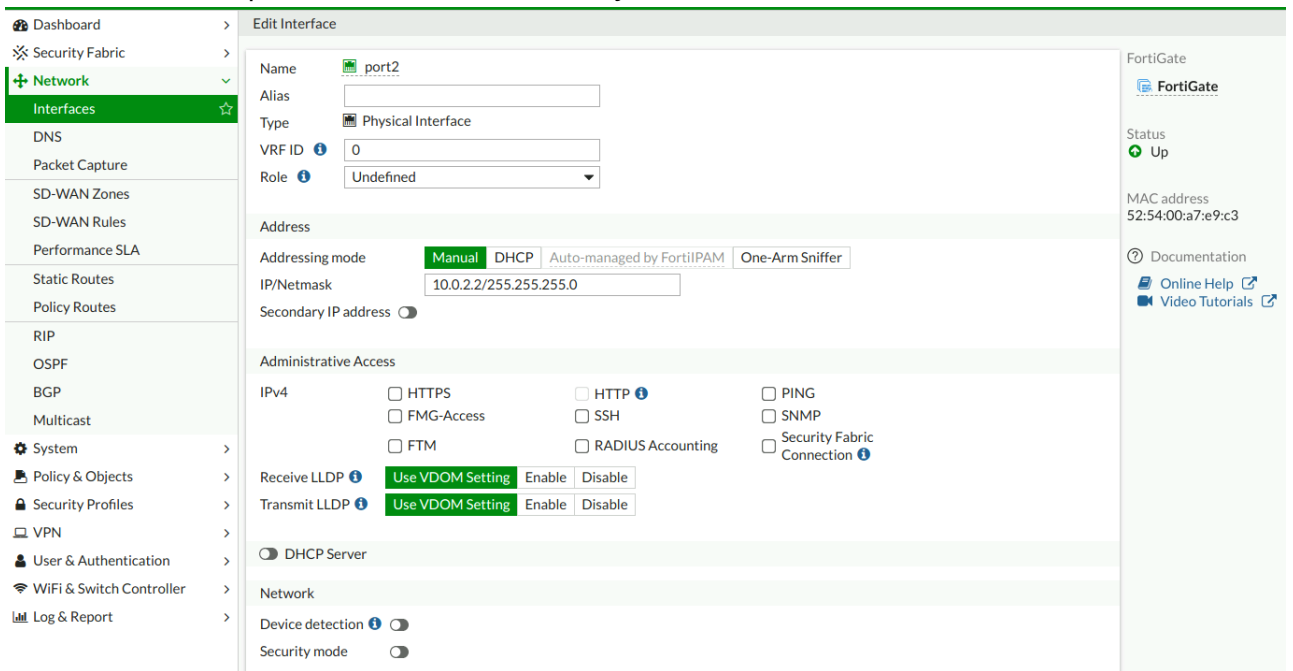
- On the left bar, go to "Network" and click it.
- Then, click on **Interfaces**. You can see this:



The screenshot shows the FortiGate VM64-KVM web interface. The left sidebar has 'Network' > 'Interfaces' selected. The main area displays a table of interfaces. At the top, there is a 'Create New' button and a search bar. The table has columns: Name, Type, Members, IP/Netmask, Administrative Access, DHCP Clients, and DHCP Ranges. The interfaces listed are: '802.3ad Aggregate' (Type: 802.3ad Aggregate, Members: Dedicated to FortiSwitch, Administrative Access: PING, Security Fabric Connection, DHCP Ranges: 169.254.1.2-169.254.1.254, DHCP Clients: 2), 'fortilink' (Type: 802.3ad Aggregate, Members: Dedicated to FortiSwitch, Administrative Access: PING, Security Fabric Connection, DHCP Ranges: 169.254.1.2-169.254.1.254, DHCP Clients: 2), 'Physical Interface' (Type: Physical Interface, Members: 192.168.6.2/255.255.255.0, Administrative Access: PING, HTTPS, SSH, HTTP, FMG-Access, DHCP Ranges: 169.254.1.2-169.254.1.254, DHCP Clients: 2), 'management (port1)' (Type: Physical Interface, Members: 192.168.6.2/255.255.255.0, Administrative Access: PING, HTTPS, SSH, HTTP, FMG-Access, DHCP Ranges: 169.254.1.2-169.254.1.254, DHCP Clients: 2), 'port2' (Type: Physical Interface, Members: 10.0.2.2/255.255.255.0, Administrative Access: PING, HTTPS, SSH, HTTP, FMG-Access, DHCP Ranges: 169.254.1.2-169.254.1.254, DHCP Clients: 2), 'port3' (Type: Physical Interface, Members: 10.0.3.1/255.255.255.0, Administrative Access: PING, HTTPS, SSH, HTTP, FMG-Access, DHCP Ranges: 169.254.1.2-169.254.1.254, DHCP Clients: 2), and 'port4' (Type: Physical Interface, Members: 10.0.1.1/255.255.255.0, Administrative Access: PING, HTTPS, SSH, HTTP, FMG-Access, DHCP Ranges: 169.254.1.2-169.254.1.254, DHCP Clients: 2).

| Name | Type | Members | IP/Netmask | Administrative Access | DHCP Clients | DHCP Ranges |
|--------------------|--------------------|--------------------------|---------------------------|--|--------------|---------------------------|
| 802.3ad Aggregate | 802.3ad Aggregate | Dedicated to FortiSwitch | | PING Security Fabric Connection | | 169.254.1.2-169.254.1.254 |
| fortilink | 802.3ad Aggregate | Dedicated to FortiSwitch | | PING Security Fabric Connection | | 169.254.1.2-169.254.1.254 |
| Physical Interface | Physical Interface | | 192.168.6.2/255.255.255.0 | PING HTTPS SSH HTTP FMG-Access | | |
| management (port1) | Physical Interface | | 192.168.6.2/255.255.255.0 | PING HTTPS SSH HTTP FMG-Access | | |
| port2 | Physical Interface | | 10.0.2.2/255.255.255.0 | | | |
| port3 | Physical Interface | | 10.0.3.1/255.255.255.0 | | | |
| port4 | Physical Interface | | 10.0.1.1/255.255.255.0 | | | |

- Double-click on "port2" to be able to modify it. You'll see this:



The screenshot shows the 'Edit Interface' page for 'port2'. The left sidebar has 'Network' > 'Interfaces' selected. The main area contains the following fields and options:

- Name:** port2
- Alias:** (empty text box)
- Type:** Physical Interface
- VRF ID:** 0
- Role:** Undefined
- Addressing mode:** Manual (selected), DHCP, Auto-managed by FortiIPAM, One-Arm Sniffer
- IP/Netmask:** 10.0.2.2/255.255.255.0
- Secondary IP address:** (toggle off)
- Administrative Access:**
 - IPv4:
 - ☐ HTTPS
 - ☐ FMG-Access
 - ☐ FTM
 - ☐ HTTP
 - ☐ SSH
 - ☐ RADIUS Accounting
 - ☐ PING
 - ☐ SNMP
 - ☐ Security Fabric Connection
- Receive LLDP:** Use VDOM Setting, Enable, Disable
- Transmit LLDP:** Use VDOM Setting, Enable, Disable
- DHCP Server:** (toggle off)
- Network:**
 - Device detection:** (toggle off)
 - Security mode:** (toggle off)

On the right side, there is a sidebar with 'FortiGate' status (Up), MAC address (52:54:00:a7:e9:c3), and links to Documentation, Online Help, and Video Tutorials.

- And then, now you can set the **Alias=WAN**, **Role=WAN** and **Permissions=+PING**. Then press **OK** at the button below.

Edit Interface

Name

port2

Alias

WAN

Type

Physical Interface

VRF ID

0

Role

WAN

Estimated bandwidth

0

0

kbps Upstream

kbps Downstream

Address

Addressing mode

Manual

DHCP

Auto-managed by FortiPAM

IP/Netmask

10.0.2.2/255.255.255.0

Secondary IP address

Administrative Access

IPv4

☐ HTTPS

☐ HTTP

☒ PING

☐ FMG-Access

☐ SSH

☐ SNMP

☐ FTM

☐ RADIUS Accounting

☐ Security Fabric Connection

Receive LLDP

Use VDOM Setting

Enable

Disable

Transmit LLDP

Use VDOM Setting

Enable

Disable

- Now, you'll see that the **port2** was definitely **modified**.

| Physical Interface 4 | | | | |
|----------------------|--------------------|--|---------------------------|--|
| management (port1) | Physical Interface | | 192.168.6.2/255.255.255.0 | PING HTTPS SSH HTTP FMG-Access |
| port3 | Physical Interface | | 10.0.3.1/255.255.255.0 | |
| port4 | Physical Interface | | 10.0.1.1/255.255.255.0 | |
| WAN (port2) | Physical Interface | | 10.0.2.2/255.255.255.0 | PING |

5. Modify "Port 3".

- Same as port2, double-click on ****Port 3****.
- This time, change ****Alias=LAN****, ****Role=LAN**** and ****Admin access=+HTTPS,HTTP,SSH,PING****. Then press ****OK**** below to save changes.

Edit Interface

Name

port3

Alias

LAN

Type

Physical Interface

VRF ID

0

Role

LAN

Addressing mode

Manual

DHCP

Auto-managed by FortiIPAM

One-Arm Sniffer

IP/Netmask

10.0.3.1/255.255.255.0

Create address object matching subnet

Secondary IP address

Administrative Access

IPv4

HTTPS

FMG-Access

FTM

HTTP

SSH

RADIUS Accounting

PING

SNMP

Security Fabric Connection

Receive LLDP

Use VDOM Setting

Enable

Disable

Transmit LLDP

Use VDOM Setting

Enable

Disable

DHCP Server

Network

Device detection

Security mode

OK

Cancel


- Result of modifying **Port 3**:

| Physical Interface 4 | | | | |
|----------------------|--------------------|--|---------------------------|--|
| LAN (port3) | Physical Interface | | 10.0.3.1/255.255.255.0 | PING HTTPS SSH HTTP |
| management (port1) | Physical Interface | | 192.168.6.2/255.255.255.0 | PING HTTPS SSH HTTP FMG-Access |
| port4 | Physical Interface | | 10.0.1.1/255.255.255.0 | |
| WAN (port2) | Physical Interface | | 10.0.2.2/255.255.255.0 | PING |

6. Modify **Port 4**:


```
- Double-click on Port 4 and modify it as such: **Alias=DMZ**,**Role=DMZ**,
**Admin access=NONE**.
```

Edit Interface

Name
 port4

Alias

DMZ

Type
 Physical Interface

VRF ID ⓘ

0

Role ⓘ

DMZ ▼

Address

Addressing mode

Manual

DHCP

Auto-managed by FortiIPAM

One-Arm Sniffer

IP/Netmask

10.0.1.1/255.255.255.0

Create address object matching subnet

☒

Secondary IP address

☐

Administrative Access

IPv4

☐ HTTPS
☐ HTTP ⓘ
☐ PING
☐ FMG-Access
☐ SSH
☐ SNMP
☐ FTM
☐ RADIUS Accounting
☐ Security Fabric Connection ⓘ

Receive LLDP ⓘ

Use VDOM Setting

Enable

Disable

Transmit LLDP ⓘ

Use VDOM Setting

Enable

Disable









Network

Device detection ⓘ

☐

→ Notice that for have NONE on the **Admin Access**, you just don't have to check on anything at all. Then, press **OK**.

Result:

| Physical Interface 4 | | | | |
|---|--------------------|---|--------------------|---------------------------|
|  | DMZ (port4) |  | Physical Interface | 10.0.1.1/255.255.255.0 |
|  | LAN (port3) |  | Physical Interface | 10.0.3.1/255.255.255.0 |
|  | management (port1) |  | Physical Interface | 192.168.6.2/255.255.255.0 |
|  | WAN (port2) |  | Physical Interface | 10.0.2.2/255.255.255.0 |

Virtual IPs

- Currently, the web server in the DMZ is NOT accessible from the outside network which prevents users outside the network from accessing the web application hosted there.
- In order to allow their communications with the web server you need to **map** from the firewall WAN interface to the DMZ.
- Virtual IPs can help you redirect http and https requests addressed to the WAN interface of your firewall machine to the web server in DMZ.
 - So technically, it goes to the router first BEFORE it goes to the DMZ but has to be redirected before the DMZ can be reachable from the outside world.
 - Also notice that the WAN/router and the DMZ are on two different VLANs. I guess in this case, the firewall acts like a "switch" as well? (not sure)
- **FortiGate Virtual IPs are similar in purpose to iptables destination NAT.**
- Virtual IPs can be created from firewall web interface by navigating to **Policy & Objects → Virtual IPs.**
- The FortiGate web GUI allows you to name the Virtual IP, choose which IP address or addresses to link, protocol, source and/or destination port or port ranges.

→ In this step, you will be creating 2 virtual IPs. One for:

1. HTTP requests and,
2. HTTPS requests

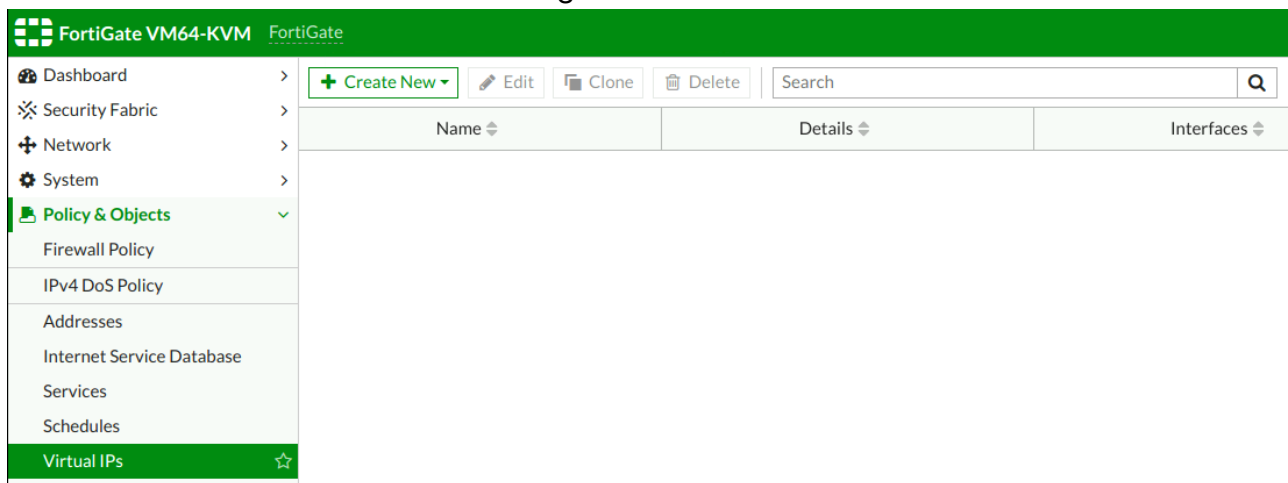
Objectives:

- Create first virtual IP:
 - Name: **web server - HTTP**
 - Interface: **WAN (port2)**
 - External IP Address: **FortiGate's WAN IP address**
 - Mapped IP Address: **Web Server's IP address**
 - Port forwarding:
 - Protocol: **TCP**
 - External service port: **80**
 - Map to port: **80**
- Create second virtual IP:
 - Name: **web server - HTTPS**
 - Interface: **WAN (port2)**
 - External IP Address: **FortiGate's WAN IP address**
 - Mapped IP Address: **Web Server's IP address**
 - Port forwarding:
 - Protocol: **TCP**
 - External service port: **443**
 - Map to port: **443**

1. Where can I find to modify and create Virtual IP?

→ On the left hand side of the Page, go to **Policy & Objects > Virtual IPs**.

- Here is what it looks like before creating a new Virtual IP:



2. Now, create the **first Virtual IP**.

Edit Virtual IP

VIP type: IPv4

Name: web server - HTTP

Comments: Write a comment... 0/255

Color: Change

Network

Interface: WAN (port2)

Type: Static NAT

External IP address/range: 10.0.2.2

Mapped IP address/range: 10.0.1.2

☐ Optional Filters

☒ Port Forwarding

Protocol: TCP UDP SCTP ICMP

External service port: 80

Map to port: 80

OK Cancel

Note: Not sure about the external IP and mapped IP address!

→ I think what is happening here is that since the router is the only thing reachable from the Internet, anyone trying to connect to the web server(DMZ) will go through the router first, then to the Firewall in which the firewall will redirect the packets to the web server! Correct! Basically we redirect packets receive from the Firewall interface to DMZ interface:

```
10.0.2.2 -> 10.0.1.2
```

Question: Wouldn't this be dangerous for the router to be at the receiving end BEFORE the firewall? Or do we assume first that the Router itself is secure and has its own software firewall activated? What are the presumptions not stated in here?

Edit Virtual IP

VIP type

IPv4

Name

web server - HTTPS

Comments

Write a comment...0/255

Color

Change

Network

Interface

WAN (port2)

Type

Static NAT

External IP address/range

10.0.2.2

Mapped IP address/range

10.0.1.2

Optional Filters

Port Forwarding

Protocol

TCPUDP SCTP ICMP

External service port

443

Map to port

443

OK

Cancel

→ Same thing happens here!

Firewall Policies

- Firewall policies are the backbone of Fortinet firewall solutions.
- All traffic going through the FortiGate VM has to be associated with a policy.
- **Firewall policies are set of instructions that control the traffic flowing through the firewall.**
- These policies control the destination of the traffic, how it is processed, whether it processed or not, and decide to allow or deny the traffic to pass through.
- By completing the previous objectives, you have assigned correct roles and access permissions to ports as well as created a link between firewall's WAN interface and a web server in the DMZ.
- That link will direct ALL HTTP and HTTPS requests made to the firewall's WAN interface IP address to the web server in the DMZ.
- However, at it's current state **firewall does NOT allow that redirection to work.**
- Furthermore, devices in LAN network cannot connect to the internet or the web server in the DMZ.

- **The reason for this is the default firewall policy that denies all traffic coming from all interfaces and destined for all interfaces.** You can observe this "Implicit Deny" policy on the:

Policy & Objects -> Firewall Policy

page.

- Furthermore, you can verify this behavior by viewing logs from the:

Log & Report -> Forward Traffic

page.

In this objective, you will create policies to:

- allow HTTP and HTTPS requests made to the WAN interface of the firewall machine to be directed to the web server in the DMZ.
- allow devices connected to the LAN interface of the Fortigate firewall to access the web server in the DMZ using its internal IP address.
- allow devices connected to the LAN interface of the Fortigate firewall to access the outside world.

WAN to DMZ

- Firewall policies can be added/edited/removed from the Web GUI via:

Policy & Objects -> Firewall Policy

" + Create New " : button from the top menu in the Firewall Policy page allows you to create new policies.

The following fields need to be specified during policy creation:

- **Name** : A descriptive name for the policy for better future management;
- **Incoming Interface** : Interface through which the traffic first enters the FortiGate firewall.
- **Outgoing Interface** : Interface through which the traffic leaves the FortiGate firewall after it has been processed.
- **Source** : Addresses from which the policy can receive the traffic. Depending on the case, you can allow everybody (by setting "all") or limit the traffic source to a branch of organization or a list of addresses.
- **Destination** : Similar concept to source addresses, but deals with destination addresses. Depending on the case, you might be interested in limiting the traffic to specific list of addresses, organization branches or allow it to all the addresses (for example, giving Internet access to LAN)
- **Service** : services that this policy deals with.

- **Action** : whether to accept or deny the traffic that matches the previously set characteristics.

→ **In this step, you will add a policy that will utilize the previously created Virtual IPs to direct (accept) HTTP and HTTPS requests to the web server.**

Note: Do NOT enable NAT. Network Address Translation for this policy is handled by the Virtual IPs that were created during previous steps. If NAT is enabled, web server will still provide services to clients. However, the web server will see Firewall's IP address as source address, hence it will lose information about users.

→ It will lose information about users because it will think that the Firewall itself made the request(s) but in reality it just redirect user's requests to the web server!

→ Note that the source of the packet will be changed if the NAT is enabled in this case and each request made by users of the web application redirected by the Firewall will come as if the Firewall itself made the requests to the web server and we do NOT want that cause otherwise, the web server will have no memory of the web app user's actions in the web application.

Objectives:

- **Create a new Firewall Policy:**
 - Policy name: **WAN to DMZ**
 - Incoming Interface: *select correct interface*
 - Outgoing Interface: *select correct interface*
 - Source: **all**
 - Destination: *both of the previously created Virtual IPs*
 - Schedule: **always**
 - Service: **HTTP, HTTPS**
 - Action: **Accept**
 - NAT: **Disabled**


Result of the new Firewall policy:

Edit Policy


Name ⓘ

WAN to DMZ


Incoming Interface

 WAN (port2) ▼



Outgoing Interface

 DMZ (port4) ▼


Source

 all ✕
+



Destination

 web server - HTTP ✕
 web server - HTTPS ✕
+

Schedule

 always ▼

Service

 HTTP ✕
 HTTPS ✕
+

Action

☒ ACCEPT ☐ DENY

Inspection Mode


☒ Flow-based ☐ Proxy-based

Firewall / Network Options

NAT

☐

Protocol Options

☒ PROT default ▼ 

Security Profiles

AntiVirus

☐

Web Filter

☐

DNS Filter

☐

Application Control

☐

OK

Cancel

Conclusion:

- This allows the users from the outside network to access your web application found in the DMZ.
- The **Incoming Interface** is where the request comes from and the **Outgoing Interface** is where the response to the request comes from.

LAN to DMZ

- Excellent. In the previous step, you allowed the users from the outside network to access your web application.
- However, currently your internal network users CANNOT access the web servre with the internal IP address of the web server. The reason for this again is the lack of a policy that would allow such traffic. Basically, the LAN part of the network cannot make any connections whatsoever. This is the default of the firewall on ANY of its interface.

- In this step, you will create a policy that will allow **ALL** LAN users to access the web server with the internal IP address of the web server in the DMZ.
- Keep in mind that more servers can be added to DMZ in the future and you would like to be able to access them **ALL** with their internal IP address.

Note: there's no necessity to create Virtual IPs for this step.

→ Same caution:

Do NOT enable NAT. For the same reason as the previous objective, the web server from the DMZ will not know the user information of the LAN users of the web application if this is the case because the Firewall itself will replace its identity as someone who passed the original request.

Objectives:

- **Create a new Firewall Policy:**
 - Name: **LAN to DMZ**
 - Incoming Interface: *select correct interface*
 - Outgoing Interface: *select correct interface*
 - Source: *select correct option*
 - Destination: *select correct option*
 - Schedule: **always**
 - Service: **HTTP, HTTPS, PING, SSH**
 - Action: **Accept**
 - NAT: **Disabled**

Hints:

1. Communications will be **entering** the firewall machine from its LAN facing interface.
2. Communications will **leave** the firewall machine from its DMZ facing interface.
3. Lab description specifies that **ALL** devices in the LAN network should be able to reach DMZ with its internal IP. Those devices are the **source** for this policy.
4. Lab description specifies the amount of servers in the DMZ can increase and LAN users should be able to reach them **ALL** with their internal IP addresses. Those DMZ servers are the **destination** of this policy.

Screenshot of the setup:

Edit Policy

Name LAN to DMZ

Incoming Interface LAN (port3) ▼

Outgoing Interface DMZ (port4) ▼

Source all ✕
+

Destination all ✕
+

Schedule always ▼

Service HTTP ✕
 HTTPS ✕
 PING ✕
 SSH ✕
+

Action ACCEPT DENY

Inspection Mode Flow-based Proxy-based

Firewall / Network Options

NAT

Protocol Options default ▼

Security Profiles

AntiVirus

Web Filter

DNS Filter

OK Cancel

LAN to WAN

- If you have completed the previous steps, LAN users can access the web server in the DMZ with its internal IP address and the outside world can browse the web application hosted in the web server with WAN IP address of the firewall machine.
- **However, currently LAN users CANNOT access the internet.** Once again, this is due to the fact that a policy allowing such traffic has NOT been created yet.
- Firewall machine is set as default gateway for the server in LAN.
- All traffic is already routed to firewall machine but dropped there.
- You can observe this from:

Log & Report -> Forward Traffic

section of the firewall web GUI.

- **Note: Enable NAT. In contrast to previously created policies, NAT must be enabled for this policy.**

→ When NAT is enabled, source IP address of the traffic is replaced with Firewall machine's WAN facing IP address.

→ This is necessary so that services in the outside world can reply back correctly since they know the router/firewall, but do NOT know the local machine!

Objectives:

- **Create a new Firewall Policy:**
 - Name: **LAN to WAN**
 - Incoming Interface: ***select correct interface***
 - Outgoing Interface: ***select correct interface***
 - Source: **all**
 - Destination: ***select correct option***
 - Schedule: **Always**
 - Service: **ALL**
 - Action: **Accept**
 - NAT: **Enabled**

Result of the setup firewall policy:

Edit Policy

Name ⓘ

LAN to WAN

Incoming Interface

LAN (port3)

Outgoing Interface

WAN (port2)

Source

all

+

Destination

all

+

Schedule

always

Service

ALL

+

Action

✓ ACCEPT

✗ DENY

Inspection Mode

Flow-based

Proxy-based

Firewall / Network Options

NAT

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Preserve Source Port

Protocol Options

PROT

default

Security Profiles

AntiVirus

Web Filter

DNS Filter

OK

Cancel

Final look for the current firewall policy for the topology:

| | | | | | | | | | | |
|---|--|--|--|--|--|--|--|--|--|--|
| FortiGate VM64-KVM FortiGate | | | | | | | | | | |
| + Create New Edit Delete Policy Lookup Search | | | | | | | | | | |
| Interface Pair View By Sequence | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |