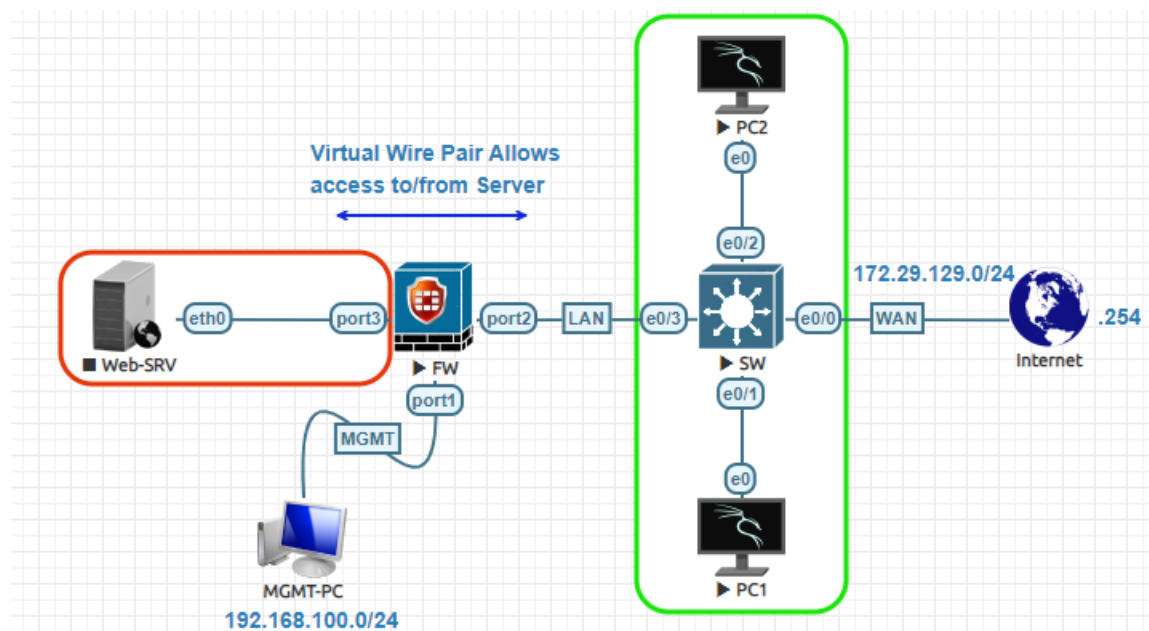


## Virtual Wire Pair Lab:

- o Two interfaces that do not have IP addressing & are treated similar to a transparent mode.
- o All traffic received by one interface in virtual wire pair can only be forwarded out the other.
- o In FortiGate Unit Firewall provided that a virtual wire pair firewall policy allows this traffic.
- o Virtual wire pairs are useful for topologies where MAC addresses do not behave normally.
- o Virtual Wire Pairing can be used for FortiGate in both the NAT and Transparent modes.



Let's login to Fortigate Firewall default username is **admin** and there is no password we need to set new password in this case the password is **123**.

FortiGate-VM64-KVM login: **admin**

Password:

You are forced to change your password. Please input a new password.

New Password:

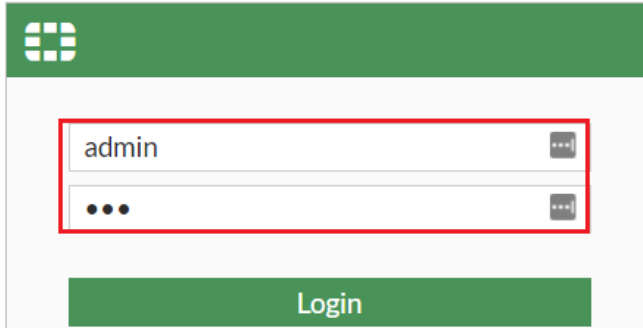
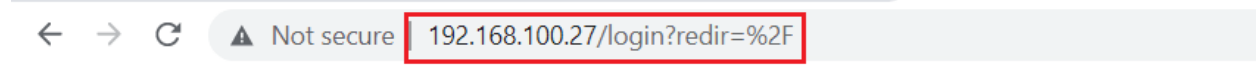
Confirm Password:

Welcome!

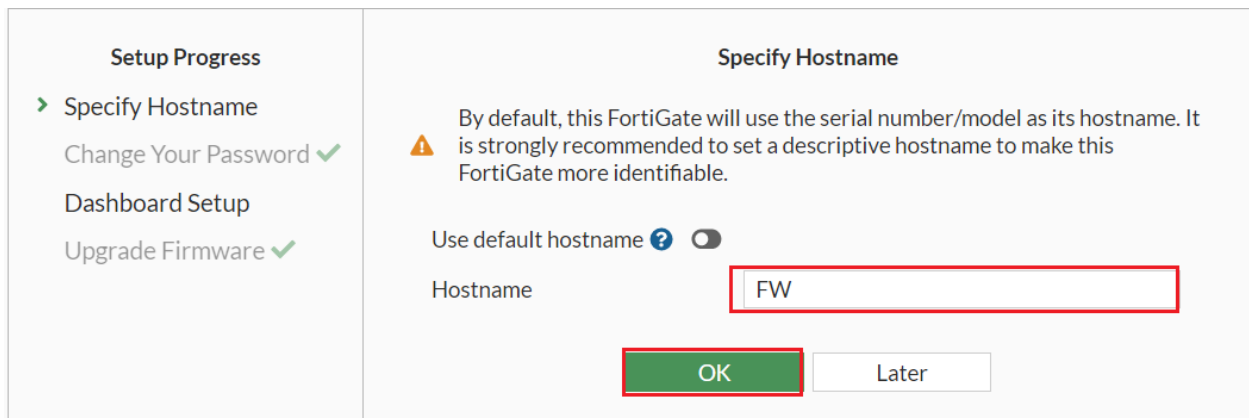
Fortigate Firewall get Management IP address through DHCP automatically.

```
FW
FortiGate-VM64-KVM # show system interface
name      Name.
fortilink static  0.0.0.0 0.0.0.0 10.255.1.1 255.255.255.0 up  disable  aggrega
te enable
l2t.root  static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up  disable  tunnel  enable
naf.root  static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up  disable  tunnel  disable
port1     dhcp   0.0.0.0 0.0.0.0 192.168.100.27 255.255.255.0 up  disable  physical
enable
```

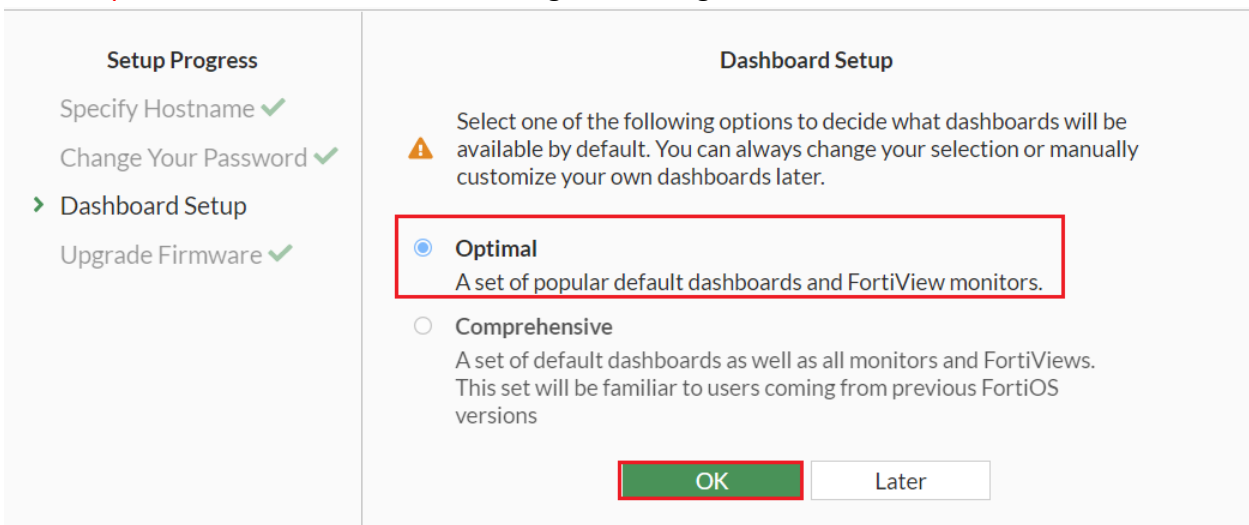
Let's browse Fortigate Firewall IP address in the browser <http://192.168.100.27> login with default username **admin** and password set initially which is **123**.



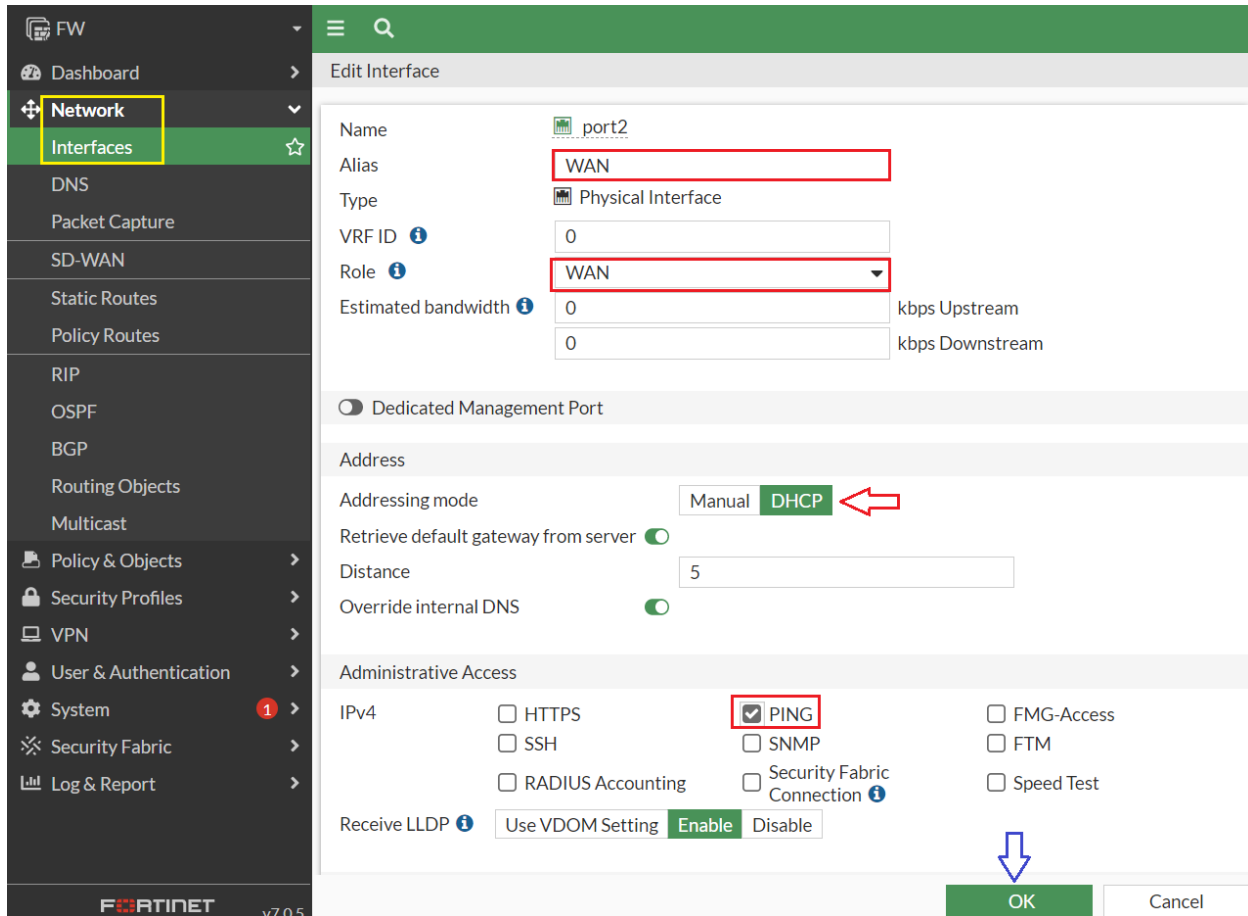
Set the **hostname** in this case FW and click **OK** to continue.



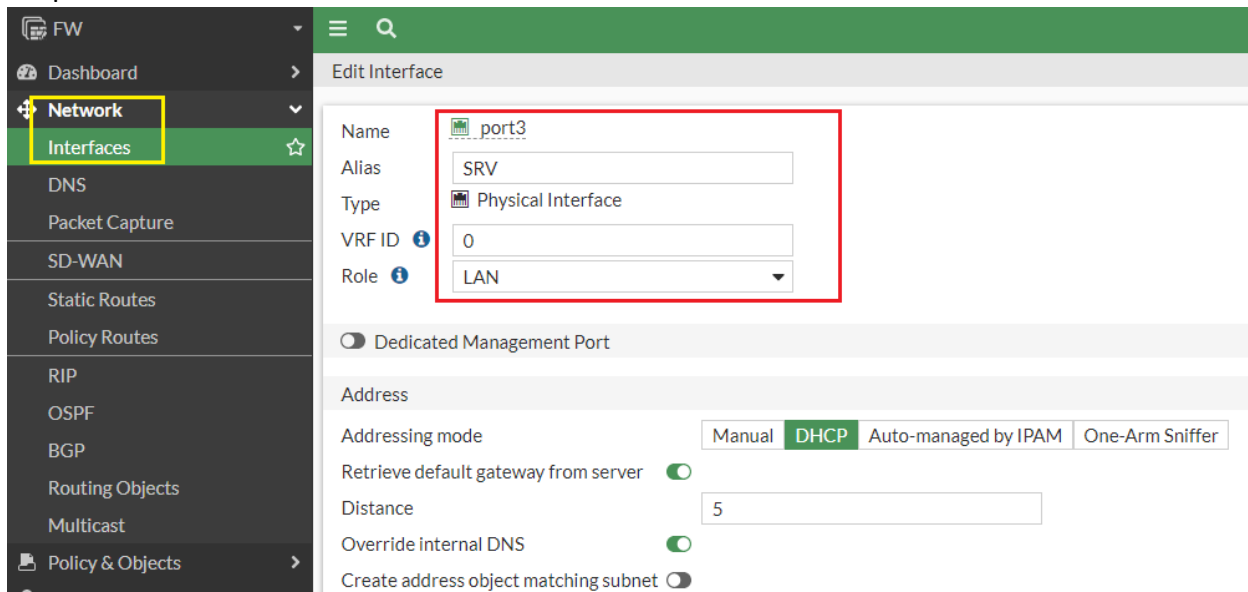
Select **Optimal** and click **OK** to continue log in to Fortigate Firewall dashboard.



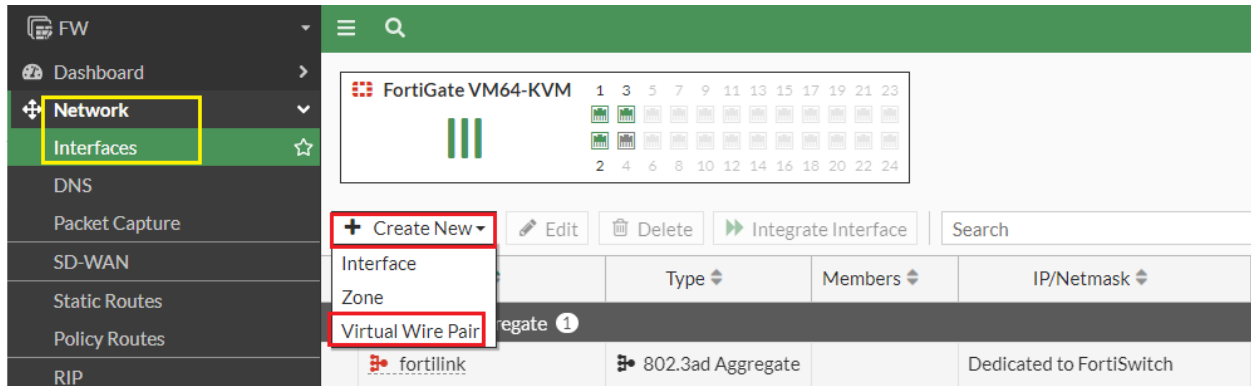
Navigate to **Network > Interfaces** double click on **port2** to configure it as WAN interface type the Alias **WAN**, choose the Role **WAN** change the Addressing Mode to **Manual** click **OK**.



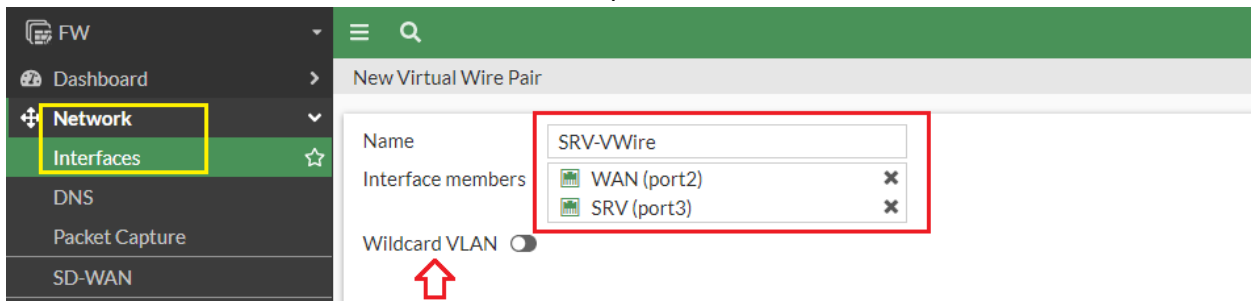
Change the other interfaces Alias names and Role set **Port3** Alias to **SRV**, besides this set Alias for **port1** **MGMT** and Click **OK**.



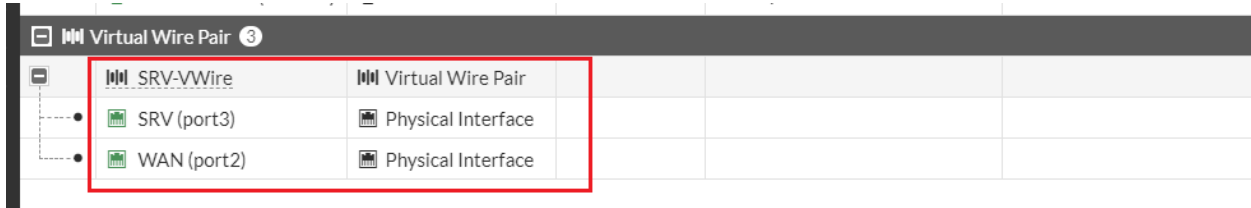
Navigate to **Network > Interfaces** and select **Create New > Virtual Wire Pair**.



Select the interfaces to add to the virtual wire pair. If desired, enable Wildcard VLAN. Select **OK**.



After created Virtual Wire Pair look like below in interfaces.



Go to **Policy & Objects > IPv4 Virtual Wire Pair Policy**, Select **Create New**. Select the direction that traffic is allowed to flow. Allow users on the internal network to connect to the server. Select the direction that traffic is allowed to flow (from port2 to port3). Configure the other firewall options as desired. Select **OK**.

The screenshot shows the 'New Policy' configuration window. The left sidebar has 'Policy & Objects' selected, with 'Firewall Virtual Wire Pair Policy' highlighted. The main configuration area is titled 'LAN-to-Server Access'. It includes the following settings:

- Name:** LAN-to-Server Access
- Virtual Wire Pair:** SRV-VWire
- Direction:** port2 → port3 (SRV-VWire)
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY
- Inspection Mode:** Flow-based (selected), Proxy-based
- Firewall / Network Options:** NAT is turned off.

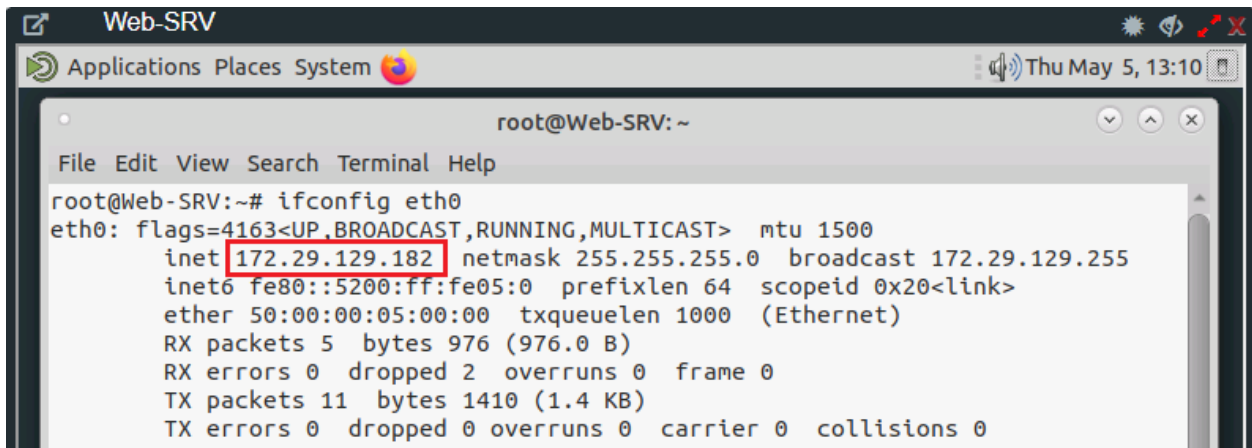
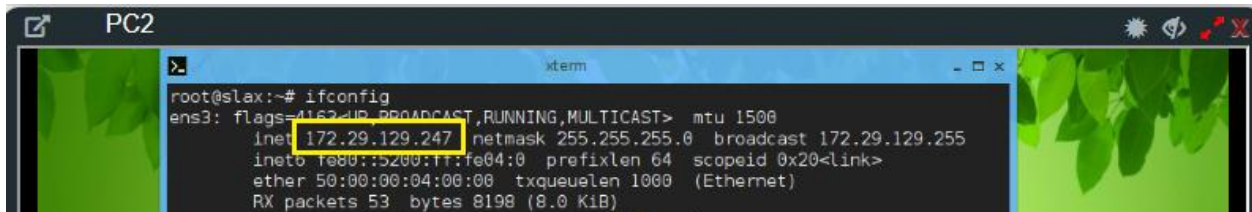
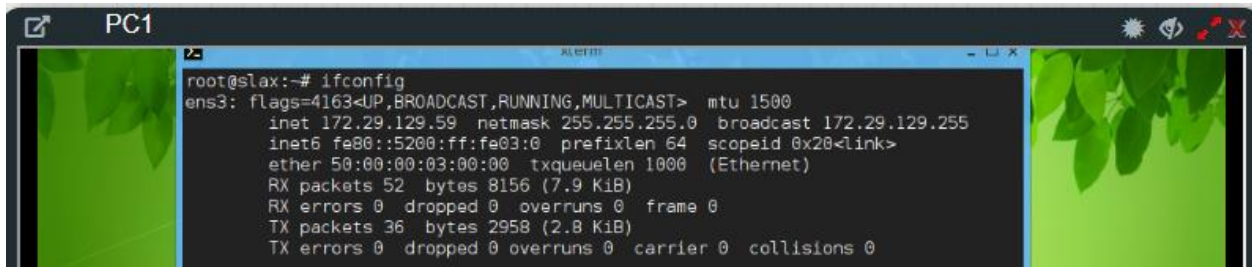
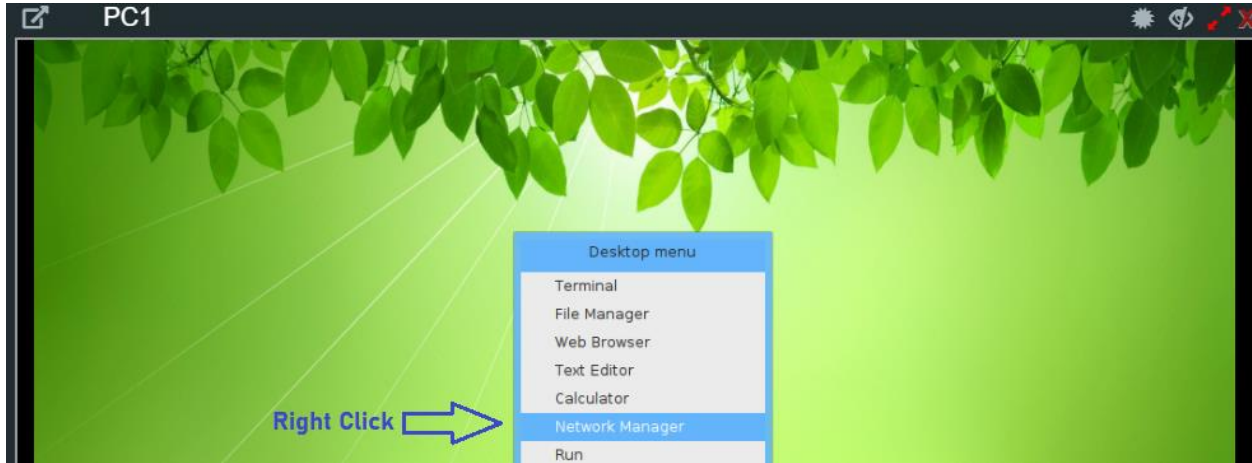
Create a second virtual wire pair policy allowing traffic from port3 to exit out of port2. This policy allows the server to connect to the Internet, in order to download updates.

The screenshot shows the 'New Policy' configuration window for a second policy. The left sidebar is the same as in the first screenshot. The main configuration area is titled 'SRV-Internet Access'. It includes the following settings:

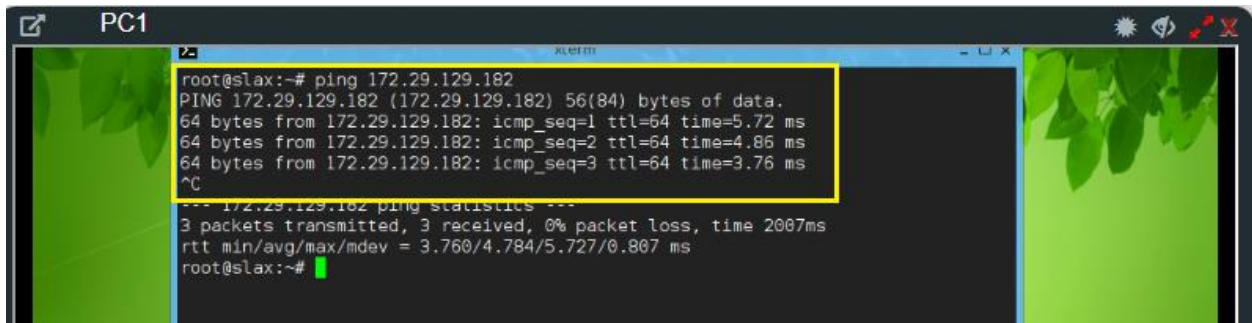
- Name:** SRV-Internet Access
- Virtual Wire Pair:** SRV-VWire
- Direction:** port3 (SRV-VWire) ← port2
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY
- Inspection Mode:** Flow-based (selected), Proxy-based
- Firewall / Network Options:** NAT is turned on.

## Testing and Verification:

To test both virtual wire pair policies, connect to the web server from a PC on the internal network, and also connect to the Internet from the web server. Right click to get Desktop Menu click on **Network Manager** click refresh to get IP address.

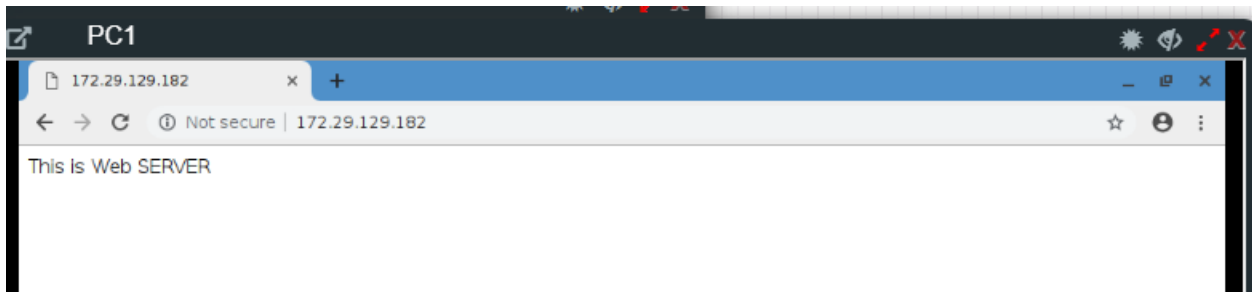


Let's try to ping from LAN PC1 to Web-Server, It is working.

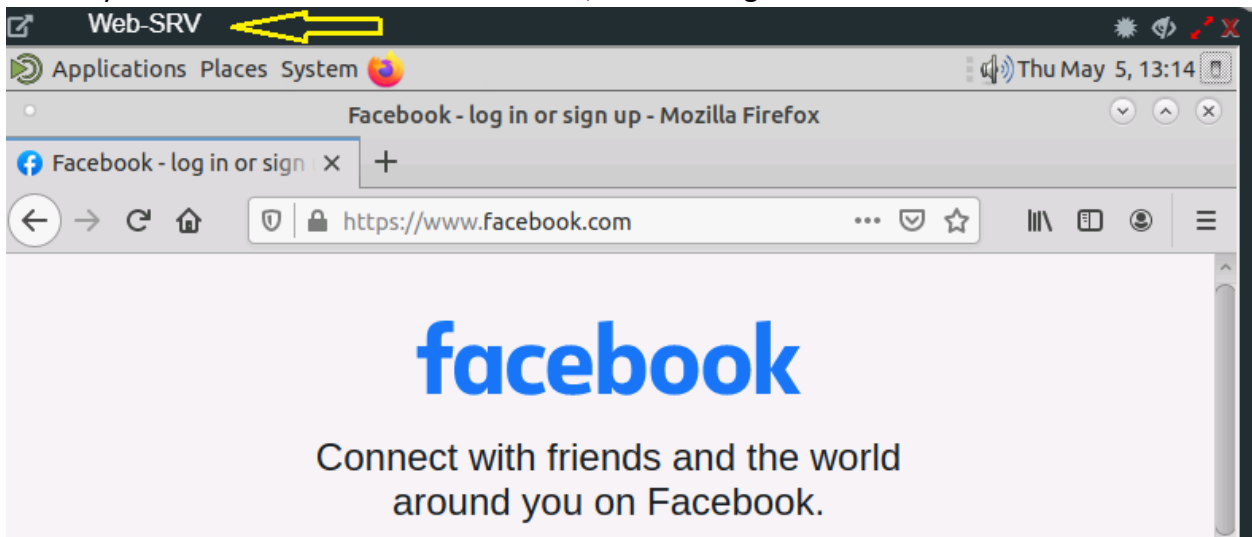


```
root@slax:~# ping 172.29.129.182
PING 172.29.129.182 (172.29.129.182) 56(84) bytes of data:
64 bytes from 172.29.129.182: icmp_seq=1 ttl=64 time=5.72 ms
64 bytes from 172.29.129.182: icmp_seq=2 ttl=64 time=4.86 ms
64 bytes from 172.29.129.182: icmp_seq=3 ttl=64 time=3.76 ms
^C
--- 172.29.129.182 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 3.760/4.784/5.727/0.867 ms
root@slax:~#
```

Let's try to Access Web-Server from Internal LAN PC1, it is accessible.



Let's Try to access Internet from Web-Server, It is working.



FW

- Dashboard
- Status
- Security
- Network
- Users & Devices
- +
- FortiView Sources
- FortiView Destinations
- FortiView Applications
- FortiView Web Sites
- FortiView Policies

FortiView Sources by Bytes

+ Add Filter

Source	Device	Bytes
172.29.129.182	50:00:00:05:00:00	36.06 kB
172.29.129.59		700 B

FW

- Dashboard
- Status
- Security
- Network
- Users & Devices
- +
- FortiView Sources
- FortiView Destinations
- FortiView Applications
- FortiView Web Sites
- FortiView Policies
- FortiView Sessions

FortiView Destinations by Bytes

+ Add Filter

Destination	Application	Bytes
www.facebook.com (179.60.192.36)	TCP/443	14.60 kB
firefox.settings.services.mozilla.com (143.204.98...)	TCP/443	6.72 kB
push.services.mozilla.com (34.218.121.180)	TCP/443	6.51 kB
content-signature-2.cdn.mozilla.net (143.204.98...)	TCP/443	6.18 kB
classify-client.services.mozilla.com (34.98.75.36)	TCP/443	3.69 kB
8.8.8.8	UDP/53	3.33 kB
172.29.129.182	TCP/80	804 B

FW

- Dashboard
- Status
- Security
- Network
- Users & Devices
- +
- FortiView Sources
- FortiView Destinations
- FortiView Applications
- FortiView Web Sites
- FortiView Policies

FortiView Policies by Bytes

+ Add Filter

Policy	Policy Type	Source Interface	Destination Interface	Bytes
SRV-Internet Access (2)	Firewall	SRV (port3)	WAN (port2)	15.16 kB
LAN-to-Server Access (1)	Firewall	WAN (port2)	SRV (port3)	908 B