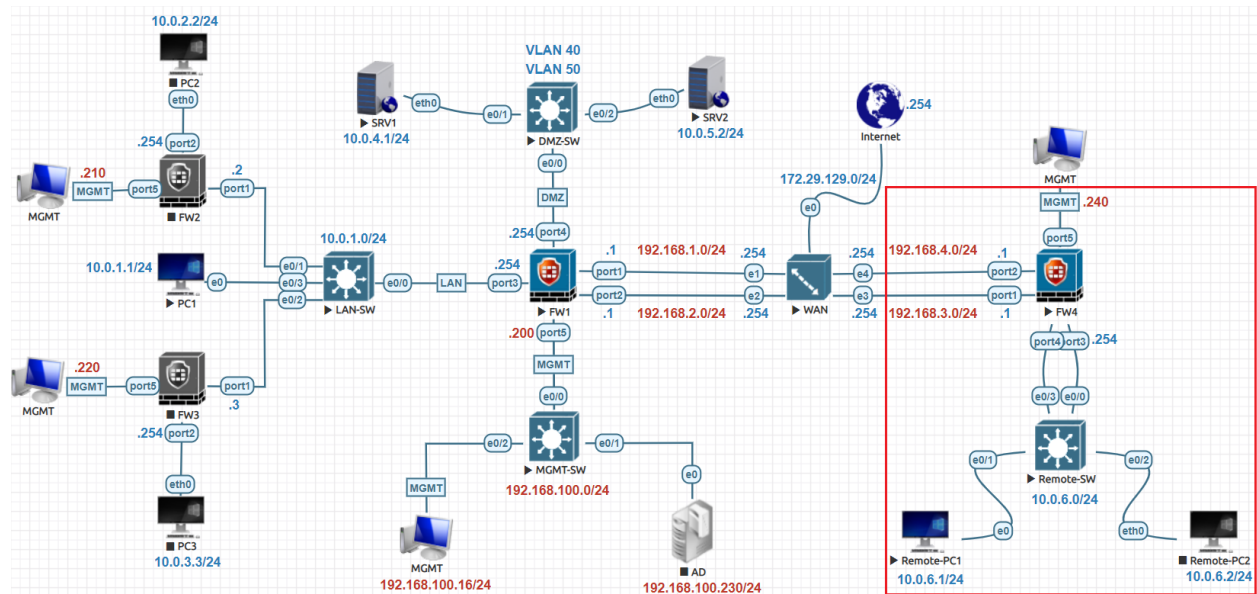


Redundant Interfaces Lab:



Switch Configuration

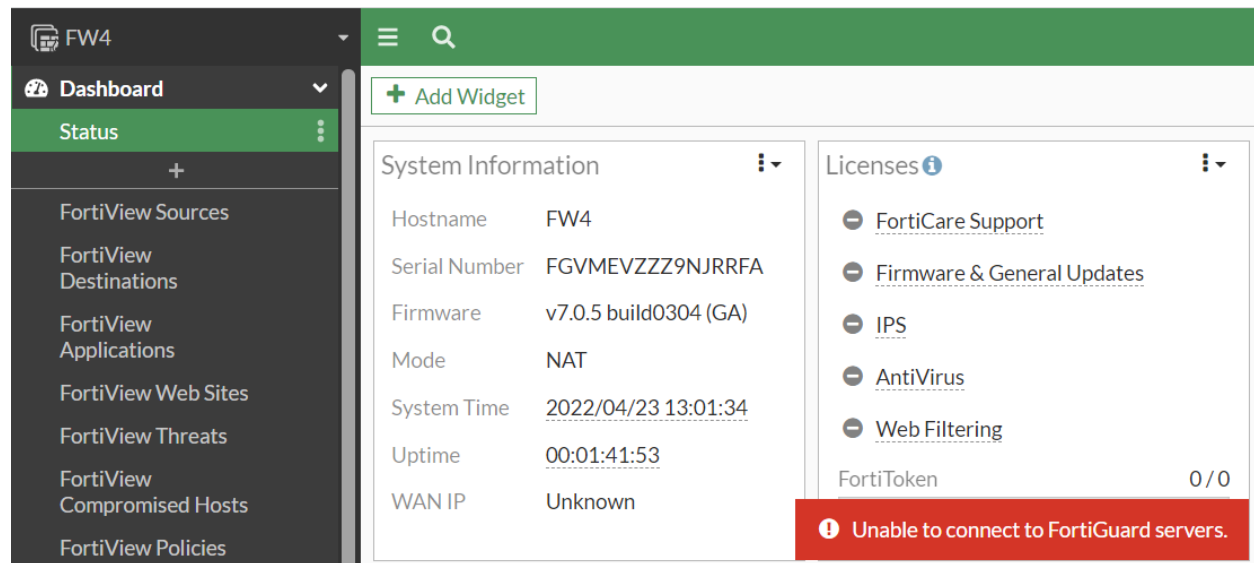
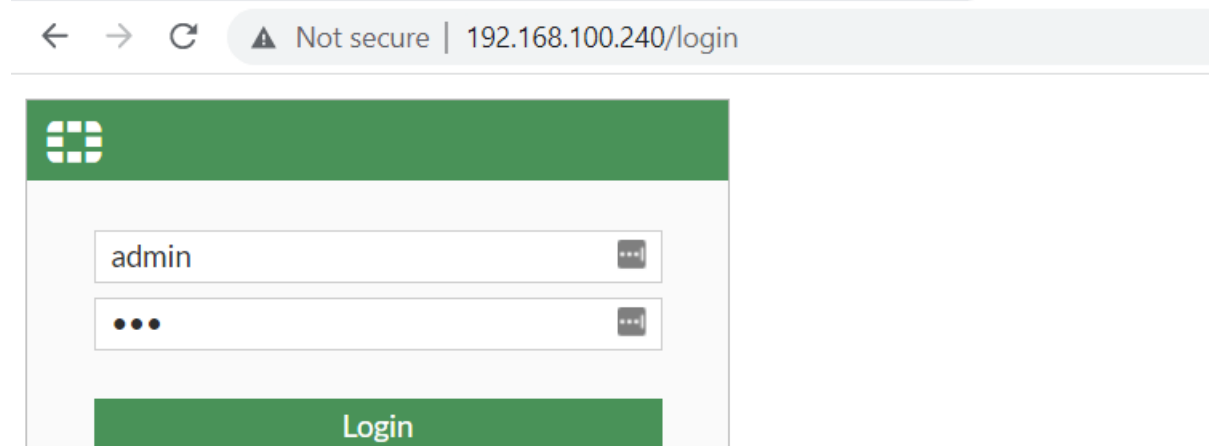
```
Switch(config)#hostname Remote-SW
Remote-SW(config)#interface range ethernet 0/0,e0/3
Remote-SW(config-if-range)#switchport trunk encapsulation dot1q
Remote-SW(config-if-range)#switchport mode trunk
```

Firewall initial Configuration

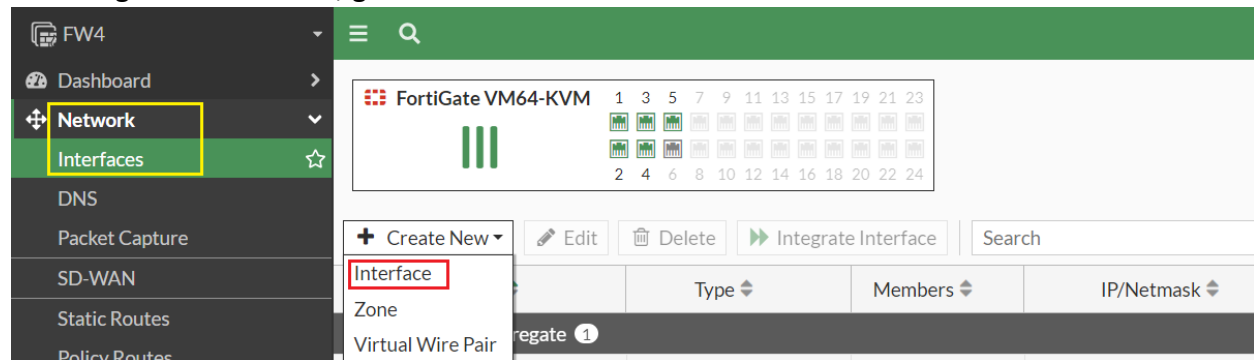
```
FortiGate-VM64-KVM # config system global
FortiGate-VM64-KVM (global) # set hostname FW4
FortiGate-VM64-KVM (global) # end

FW4 # config system interface
FW4 (interface) # edit port5
FW4 (port5) # set mode static
FW4 (port5) # set ip 192.168.100.240/24
FW4 (port5) # set allowaccess https http ping ssh telnet
FW4 (port5) # end
```

Login to FortiGate Firewall type <http://192.168.100.240> in any browser.



To configure an interface, go to **Network > Interfaces** Click **Create New > Interface**.



Type the name, Alias, select Interface type Redundant interface, Assign the Gateway IP address.

Finally, Redundant interface has been configured combine Port3 and Port4.

Name	Type	Members	IP/Netmask	Adminis
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security
Physical Interface 4				
ISP-1 (port1)	Physical Interface		192.168.3.11/255.255.255.0	PING
ISP-2 (port2)	Physical Interface		0.0.0.0/0.0.0.0	PING
MGMT (port5)	Physical Interface		192.168.100.240/255.255.255.0	PING HTTPS SSH HTTP TELNET
port6	Physical Interface		0.0.0.0/0.0.0.0	
Redundant Interface 1				
Redundant-IF	Redundant Interface	LAN-1 (port3) LAN-2 (port4)	10.0.6.254/255.255.255.0	PING

Go to **Network > DNS** Set DNS Servers to **Specify**, Configure the primary and secondary DNS servers as needed. Configure additional DNS settings as needed Click Apply.

The screenshot shows the FortiGate web interface for configuring DNS settings. The left sidebar has 'Network' and 'DNS' highlighted. The main panel is titled 'DNS Settings' and includes the following fields:

- DNS servers:** A dropdown menu set to 'Specify'.
- Primary DNS server:** A text box containing '8.8.8.8' with a '70 ms' response time indicator.
- Secondary DNS server:** A text box containing '8.8.4.4' with a '90 ms' response time indicator.
- Local domain name:** An empty text box with a '+' icon below it.
- DNS Protocols:** A section with three toggle switches:
 - DNS (UDP/53):
 - TLS (TCP/853):
 - HTTPS (TCP/443):

Create a new default route, go to **Network > Static Routes**.

The screenshot shows the 'Edit Static Route' configuration page. The left sidebar has 'Network' and 'Static Routes' highlighted. The main panel includes the following fields:

- Automatic gateway retrieval:** A toggle switch set to 'Off'.
- Destination:** A dropdown menu set to 'Subnet' with a text box containing '0.0.0.0/0.0.0.0'.
- Gateway Address:** A dropdown menu set to 'Specify' with a text box containing '192.168.3.254'.
- Interface:** A dropdown menu set to 'ISP-1 (port1)'.
- Administrative Distance:** A text box containing '10'.
- Comments:** A text box containing 'Write a comment...'.
- Status:** A dropdown menu set to 'Enabled'.

The screenshot shows the 'Static Routes' table in the FortiGate web interface. The table has the following columns and data:

Destination	Gateway IP	Interface
0.0.0.0/0	192.168.3.254	ISP-1 (port1)

Create a firewall policy, go to **Policy & Objects > Firewall Policy**, and click **Create New**. Type the name of the Policy, choose incoming Interface Redundant-IF, outgoing Interface ISP-1 click OK.

Edit Policy

Name: Allow LAN to Internet

Incoming Interface: Redundant-IF

Outgoing Interface: ISP-1 (port1)

Source: all

Destination: all

Schedule: always

Service: ALL

Action: ACCEPT DENY

Inspection Mode: Flow-based Proxy-based

Firewall / Network Options

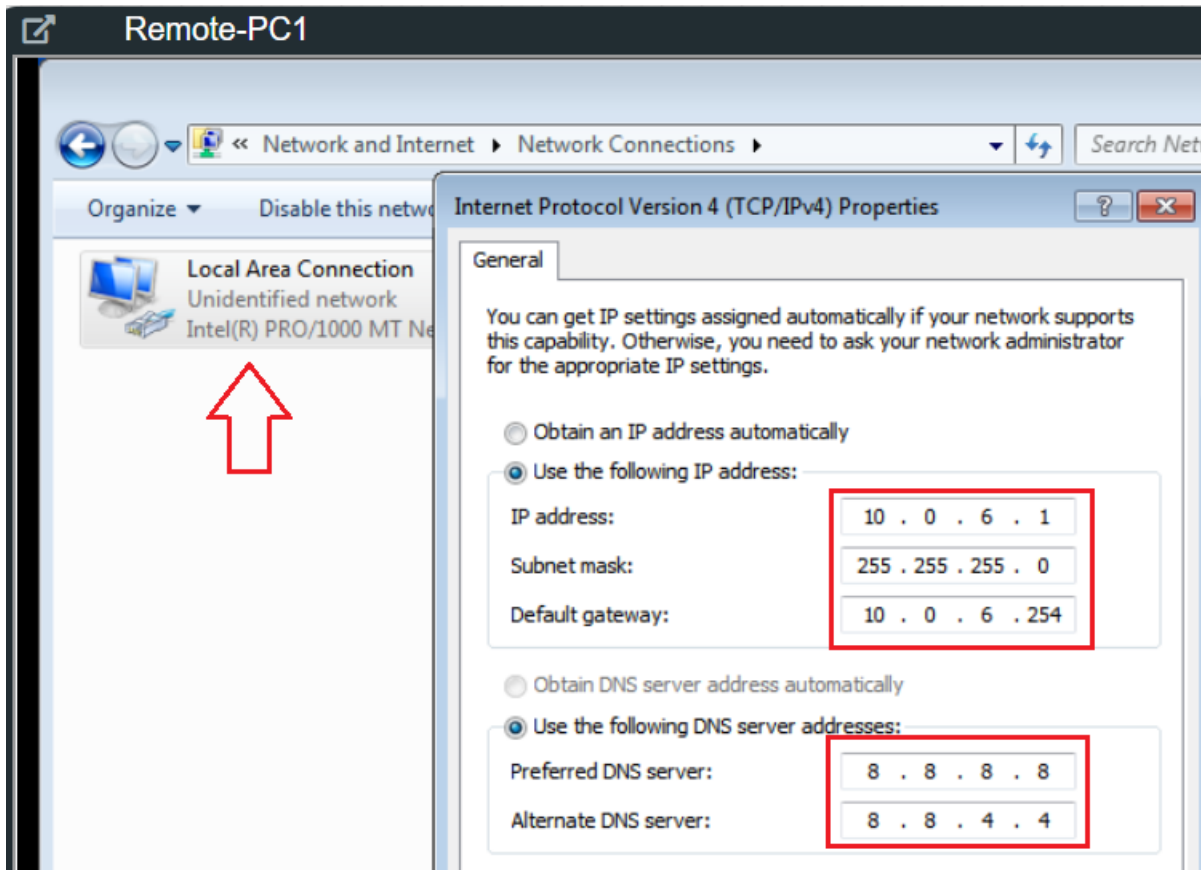
NAT:

Policy & Objects

Firewall Policy

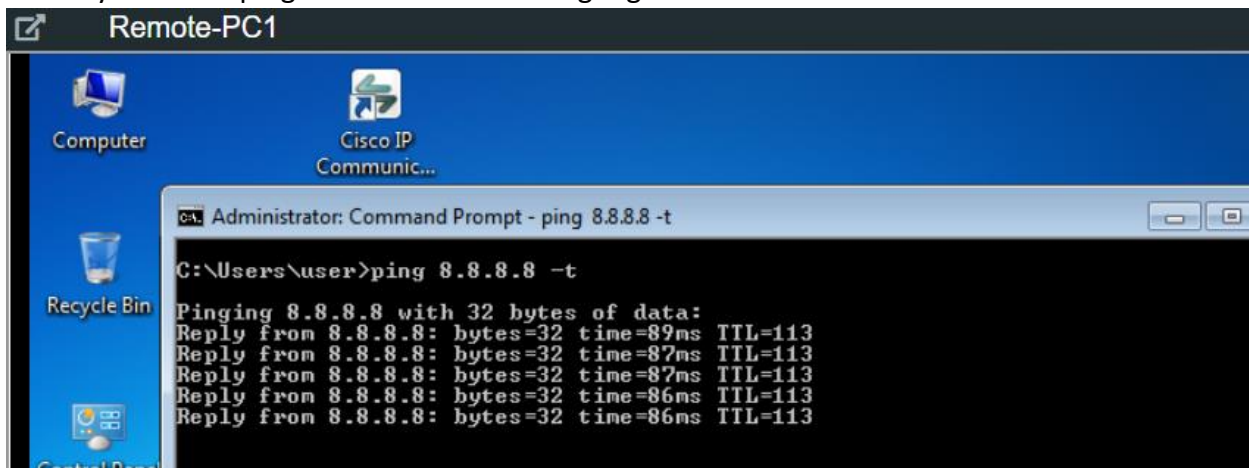
Name	Source	Destination	Schedule	Service	Action
Redundant-IF → ISP-1 (port1)					
Allow LAN to Internet	all	all	always	ALL	ACCEPT
Implicit					

Assign IP address to Remote-PC1 10.0.6.1 with subnet mask 255.255.255.0.



Test and Verification:

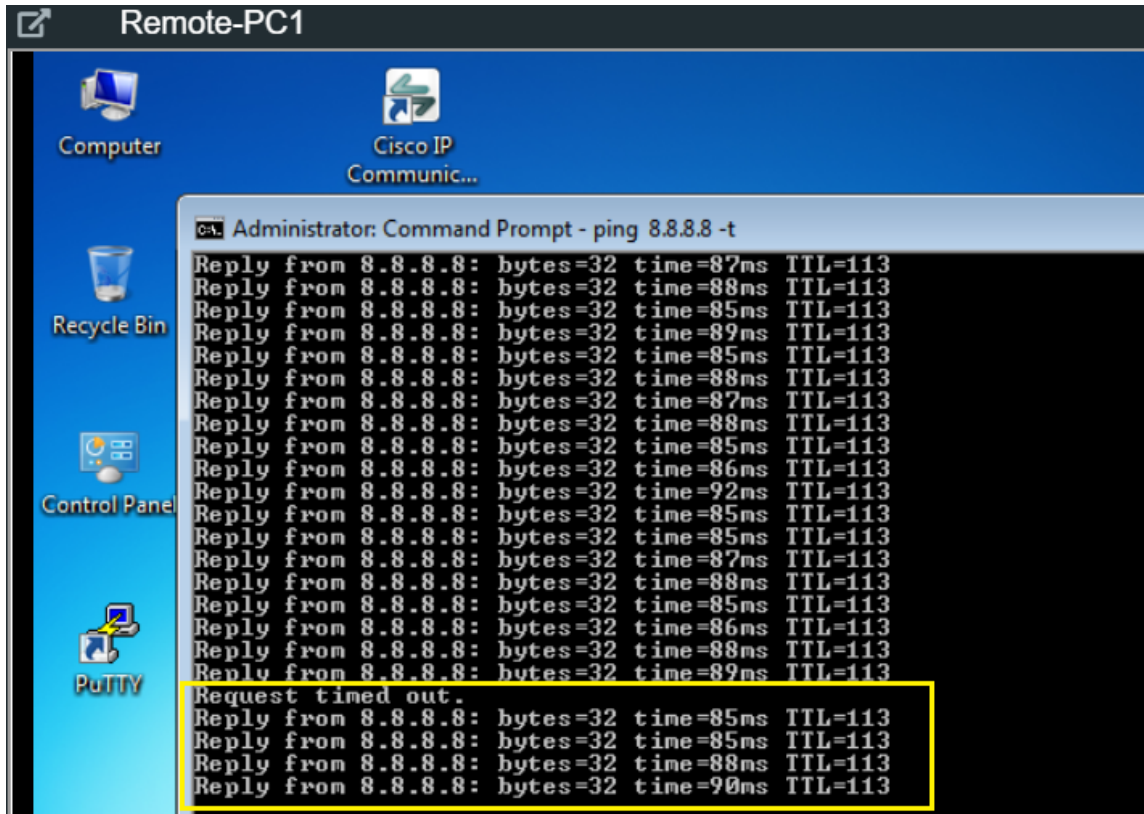
Let's try continue ping from Remote-PC1 to google DNS 8.8.8.8



Shutdown FW interface

```
FW4 # config system interface
FW4 (interface) # edit port3
FW4 (port3) # set status down
FW4 (port3) # end
```

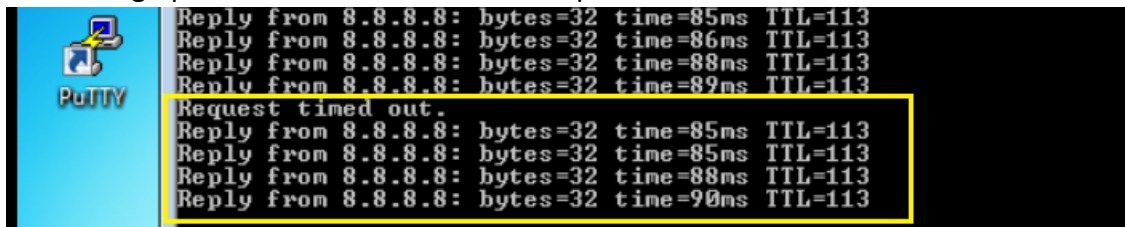
After shutdown the interface there is one drop the interface switchover.



Shutdown FW interface

```
FW4 # config system interface
FW4 (interface) # edit port3
FW4 (port3) # set status up
FW4 (port3) # end
```

After bring up the interface there is one drop the interface switchover.



Down and UP port3 and port4 of Fortigate Firewall to see the traffic switchover to other port.

The top screenshot shows traffic on port3 with the following data:

No.	Time	Source	Destination	Protocol	Length	Info
1342	498.951829604	8.8.8.8	10.0.6.2	ICMP	98	Echo (ping) reply id=0x
1343	499.831895060	10.0.6.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x
1344	499.907861094	8.8.8.8	10.0.6.2	ICMP	98	Echo (ping) reply id=0x

The bottom screenshot shows traffic on port4 with the following data:

No.	Time	Source	Destination	Protocol	Length	Info
93	50.044560937	8.8.8.8	10.0.6.2	ICMP	98	Echo (ping) reply id=0x
95	50.973859612	10.0.6.2	8.8.8.8	ICMP	98	Echo (ping) request id=0x
98	51.052501690	8.8.8.8	10.0.6.2	ICMP	98	Echo (ping) reply id=0x

Priority-Override is enable when port3 is back it will be used again.

```
FW4 #
FW4 # diagnose netlink redundant name red
status: up
npu: n
flush: n
asic helper: y
ports: 2
link-up-delay: 50ms
priority-override: enable
MAC addr: 50:00:00:04:00:02
current slave: port3

slave: port3
  index: 0
  link status: up
  link failure count: 2
  permanent MAC addr: 50:00:00:04:00:02

slave: port4
  index: 1
  link status: up
  link failure count: 1
  permanent MAC addr: 50:00:00:04:00:03
```