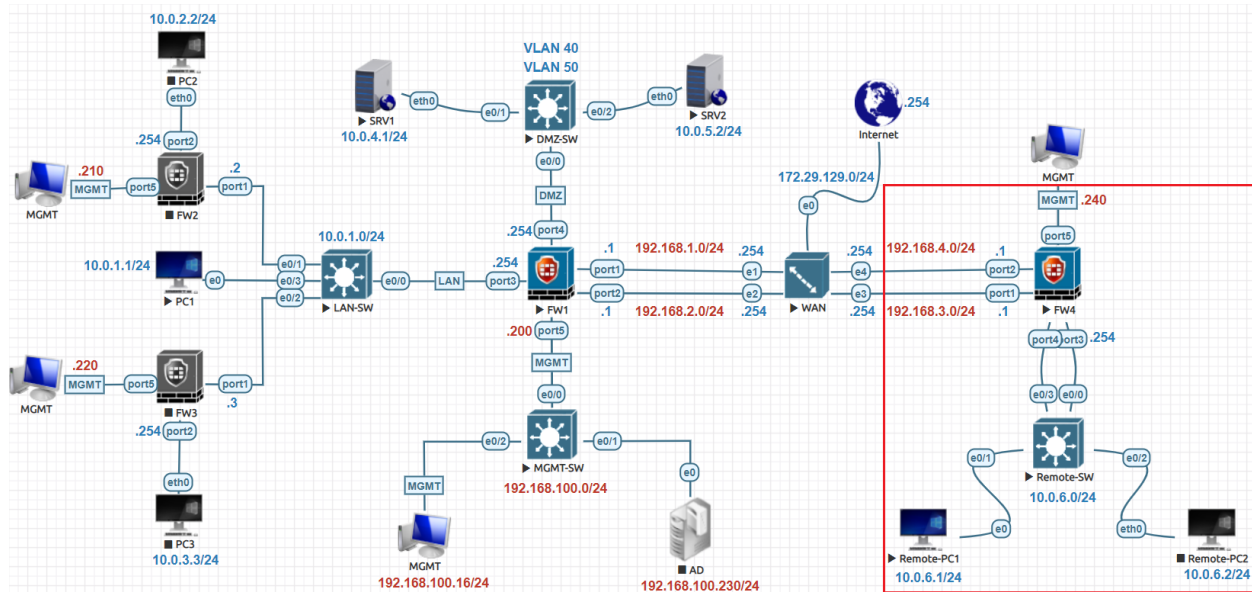


Aggregate Interfaces Lab:



Switch Configuration

```

Switch(config)#hostname Remote-SW
Remote-SW(config)#interface range e0/0,e0/3
Remote-SW(config-if-range)#switchport trunk encapsulation dot1q
Remote-SW(config-if-range)#switchport mode trunk
Remote-SW(config-if-range)#channel-protocol lacp
Remote-SW(config-if-range)#channel-group 1 mode active
Remote-SW(config-if-range)#no shutdown

Remote-SW(config)#interface port-channel 1
Remote-SW(config-if)#no shutdown

Remote-SW # show etherchannel summary
Remote-SW # show etherchannel detail
Remote-SW # show etherchannel port-channel
Remote-SW #show spanning-tree vlan 1
    
```

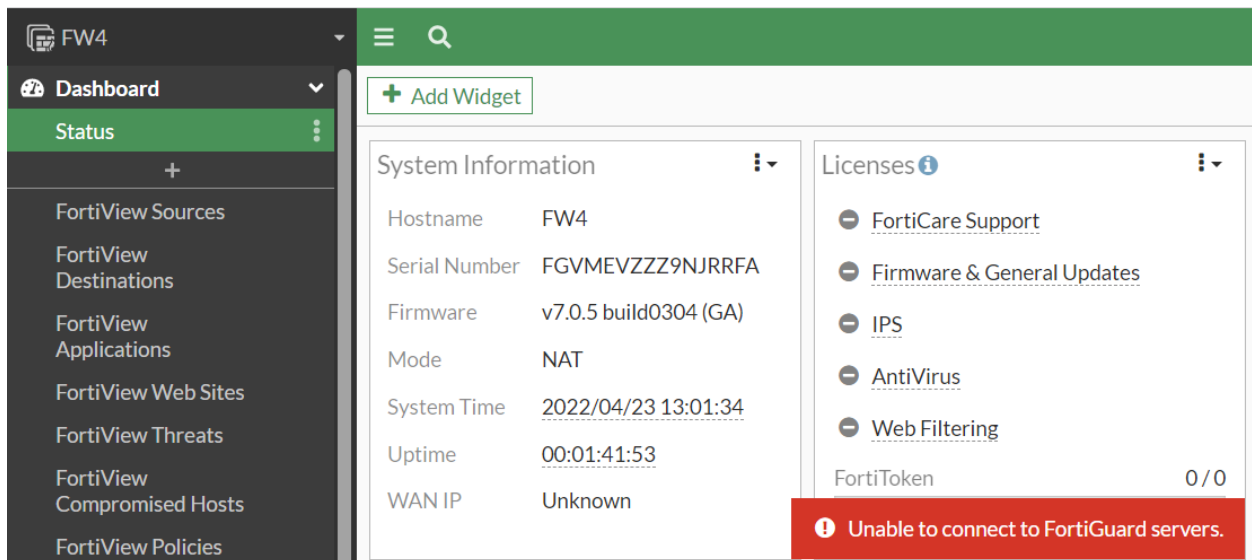
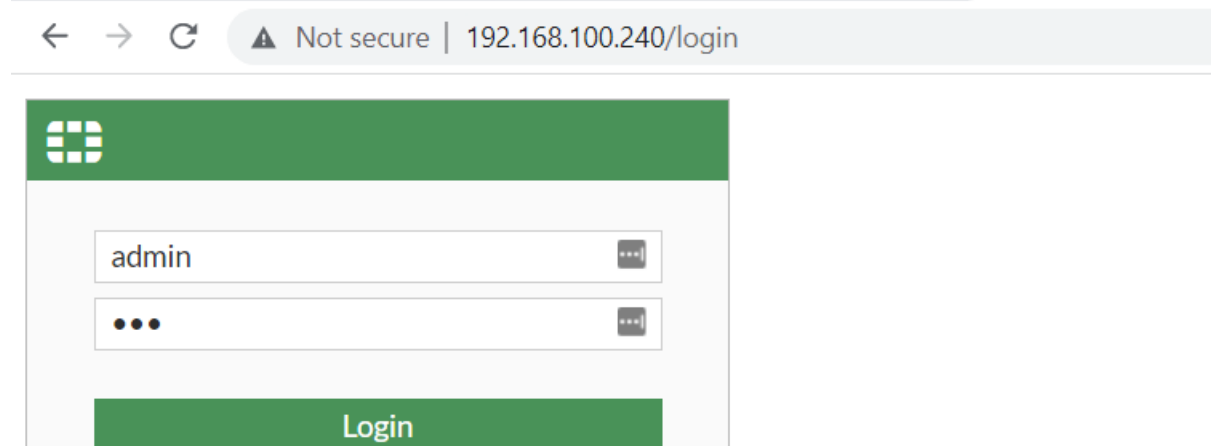
Firewall initial Configuration

```

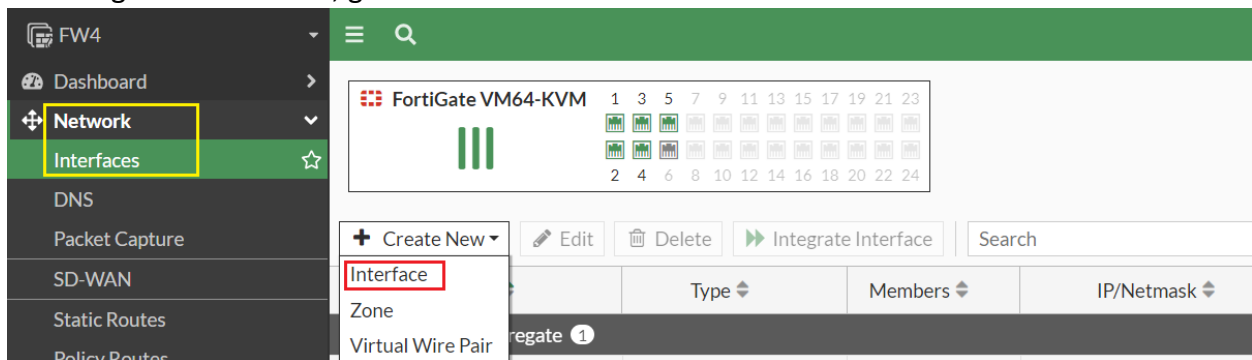
FortiGate-VM64-KVM # config system global
FortiGate-VM64-KVM (global) # set hostname FW4
FortiGate-VM64-KVM (global) # end

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 Aggregate, Assign the Gateway IP address.

The screenshot shows the 'New Interface' configuration page in FortiGate. The interface is named 'AG-1' with the alias 'Aggregate to SW'. The type is set to '802.3ad Aggregate' and the VRF ID is '0'. The role is 'LAN'. The interface members are 'LAN-1 (port3)' and 'LAN-2 (port4)'. The addressing mode is 'Manual' and the IP/Netmask is '10.0.6.254/24'. The administrative access section has 'PING' checked. The 'OK' button is highlighted with a blue arrow.

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

The screenshot shows the 'Interfaces' page in FortiGate. The interface 'Aggregate to SW (AG-1)' is highlighted with a red box. It is an '802.3ad Aggregate' type with members 'LAN-1 (port3)' and 'LAN-2 (port4)' and IP/Netmask '10.0.6.254/255.255.255.0'.

Name	Type	Members	IP/Netmask
Aggregate to SW (AG-1)	802.3ad Aggregate	LAN-1 (port3) LAN-2 (port4)	10.0.6.254/255.255.255.0
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch
Physical Interface 4			
ISP-1 (port1)	Physical Interface		192.168.3.11/255.255.255.0
ISP-2 (port2)	Physical Interface		0.0.0.0/0.0.0.0
MGMT (port5)	Physical Interface		192.168.114.240/255.255.255.0

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'. Under 'DNS servers', the 'Use FortiGuard Servers' option is selected, and the 'Specify' button is active. The 'Primary DNS server' is set to 8.8.8.8 with a response time of 70 ms, and the 'Secondary DNS server' is set to 8.8.4.4 with a response time of 90 ms. The 'Local domain name' field is empty. Under 'DNS Protocols', 'DNS (UDP/53)' is enabled, while 'TLS (TCP/853)' and 'HTTPS (TCP/443)' are disabled.

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 shows the following configuration: 'Automatic gateway retrieval' is disabled. The 'Destination' is set to 'Subnet' with the value '0.0.0.0/0.0.0.0'. The 'Gateway Address' is set to 'Specify' with the value '192.168.3.254'. The 'Interface' is set to 'ISP-1 (port1)'. The 'Administrative Distance' is set to 10. The 'Status' is 'Enabled'.

The screenshot shows the 'Static Routes' table in the FortiGate web interface. The table has columns for 'Destination', 'Gateway IP', and 'Interface'. There is one entry with the following values:

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 Aggregate, outgoing Interface ISP-1 click OK.

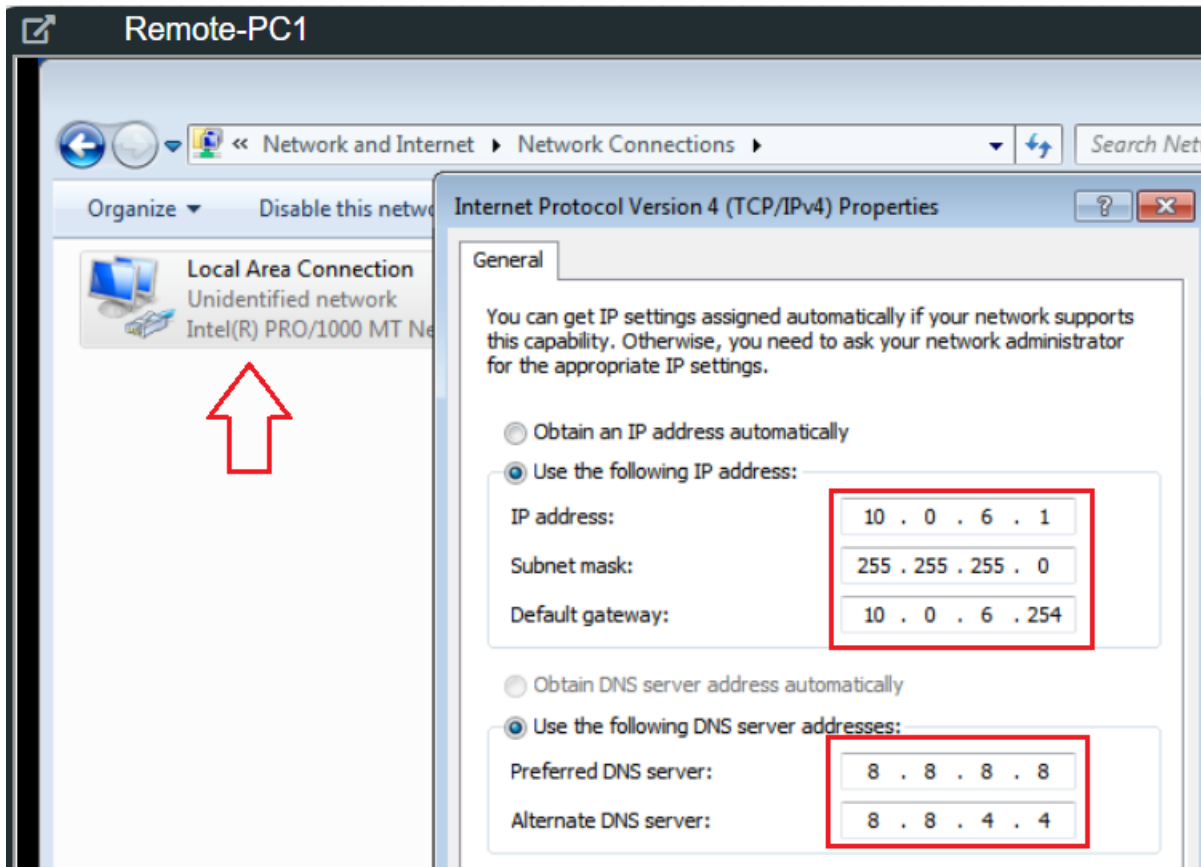
The screenshot shows the configuration for a new firewall policy. The configuration details are as follows:

- Name:** Allow LAN to Internet
- Incoming Interface:** Aggregate to SW (AG-1)
- Outgoing Interface:** ISP-1 (port1)
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY (unchecked)
- Inspection Mode:** Flow-based (selected), Proxy-based (unselected)
- Firewall / Network Options:** NAT (checked)

The screenshot shows the list of firewall policies. The table below represents the data shown in the interface:

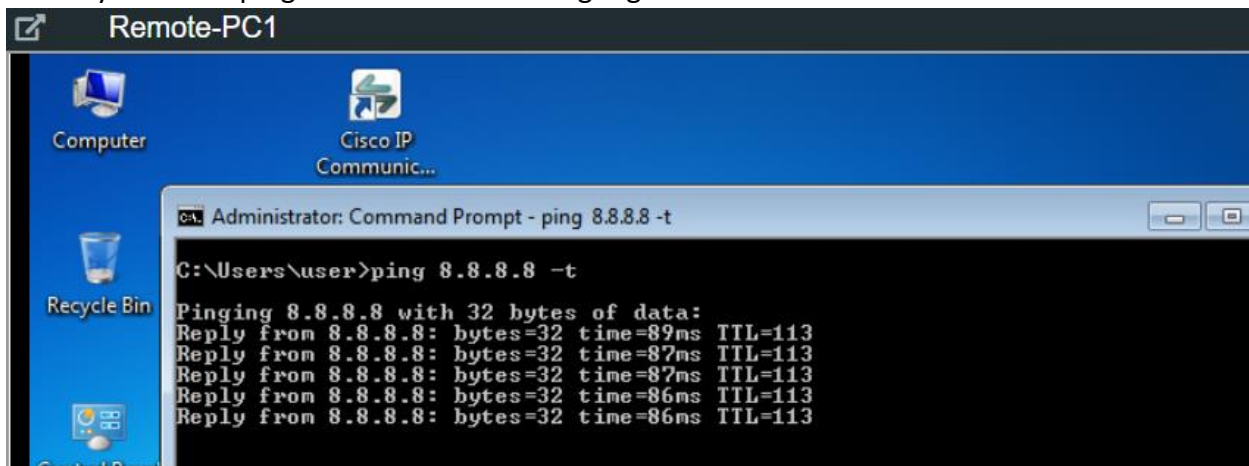
Name	Source	Destination	Schedule	Service	Action
Aggregate to SW (AG-1) → ISP-1 (port1)					
Allow LAN to Internet	all	all	always	ALL	ACCEPT
Implicit					

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



Test and Verification:

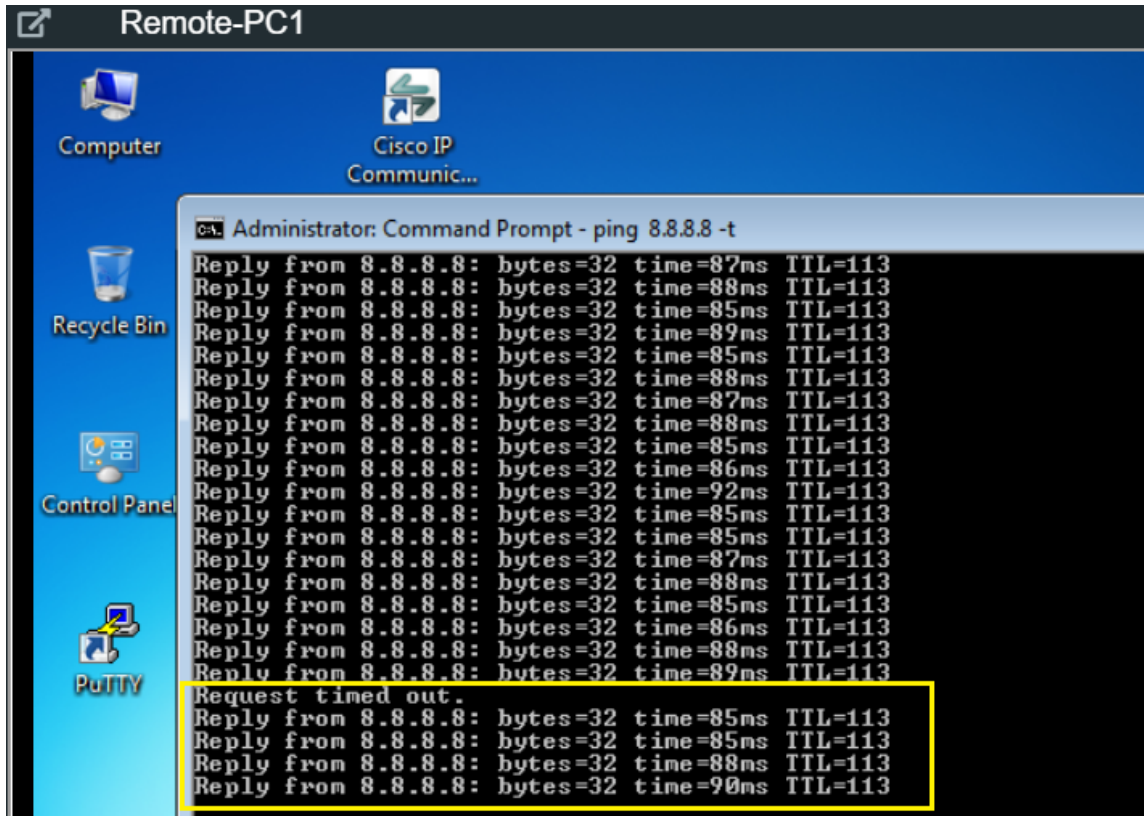
Let's try continue ping from Remote-PC1 to google DNS 8.8.8.8



Shutdown Switch interface

```
Remote-SW(config)#interface e0/3  
Remote-SW(config-if)#shutdown
```

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



Shutdown FW interface

```
Remote-SW(config)#interface e0/3  
Remote-SW(config-if)#no shutdown
```

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

