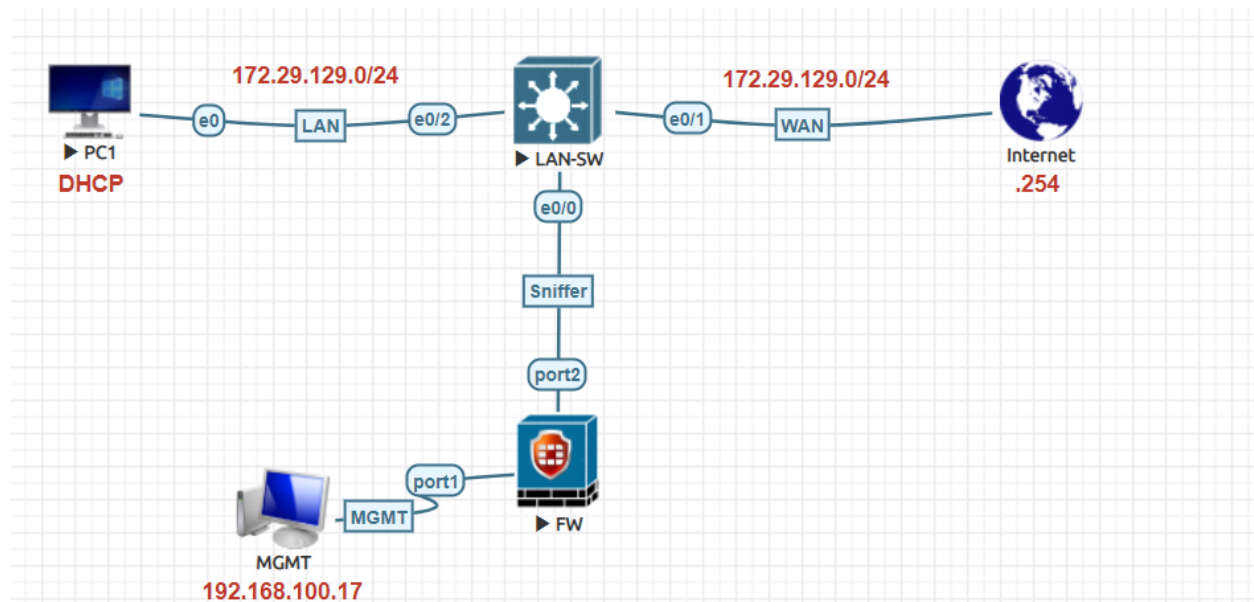
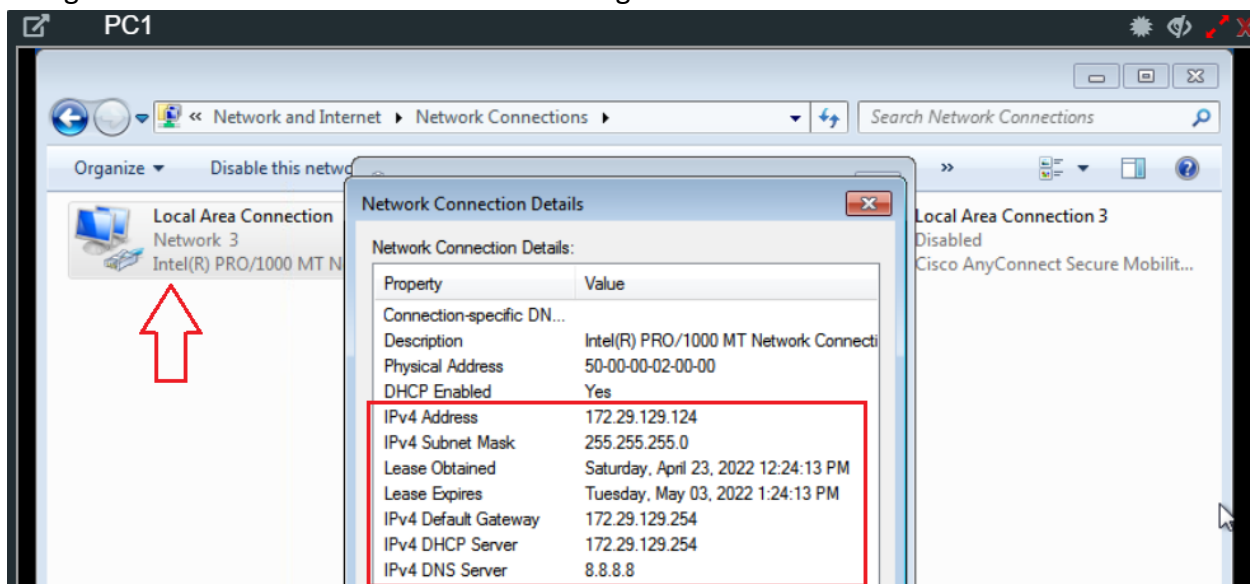


## One-Armed Sniffer Lab:



PC1 get all IP Address and related details through DHCP server from the internet cloud.



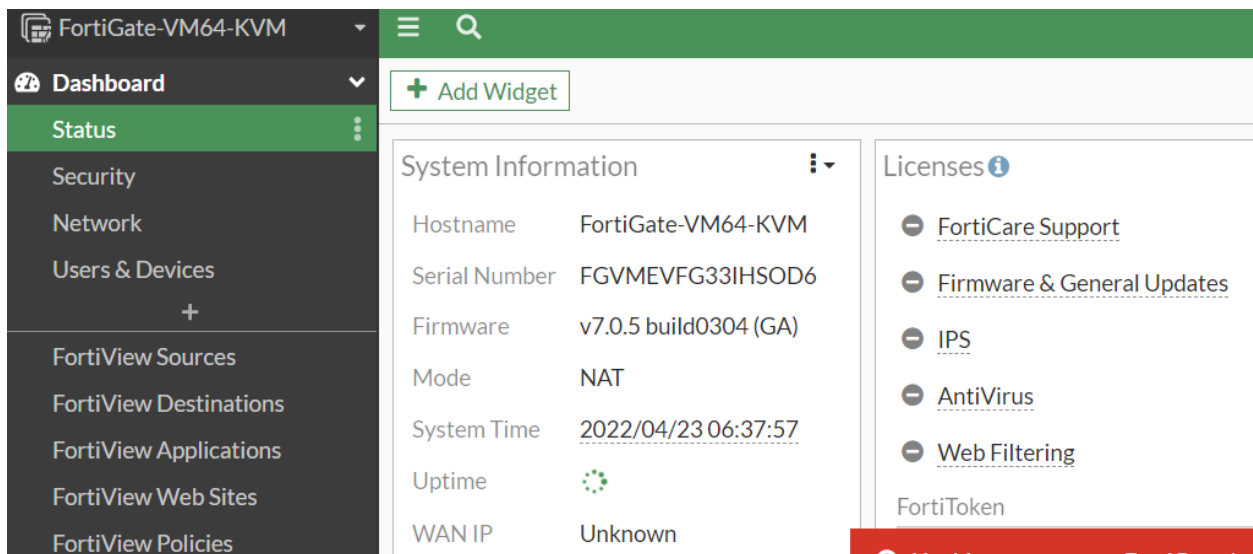
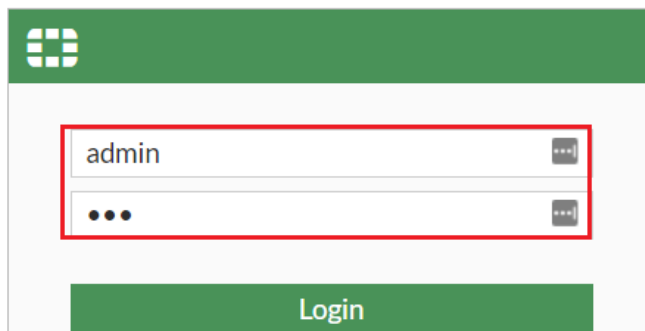
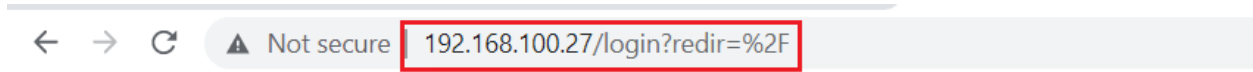
### Switch Configuration

```
Switch(config)#hostname LAN-SW
LAN-SW(config)#monitor session 1 source interface ethernet 0/2 both
LAN-SW(config)#monitor session 1 destination interface ethernet 0/0
```

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 aggregate 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
port2     static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up  disable physical enable
port3     static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up  disable physical enable
port4     static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 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.



Navigate to **Network > Interfaces** double click on port2 to configure it as a One-Arm-Sniffer.

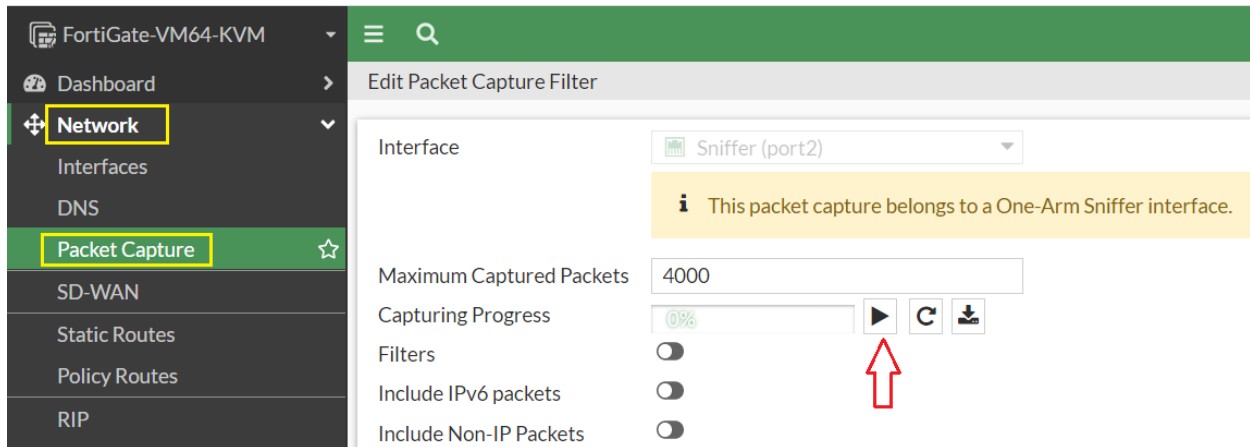
The screenshot shows the FortiGate VM64-KVM web interface. The left sidebar is expanded to 'Network > Interfaces'. The main panel is titled 'Edit Interface' and shows the configuration for 'port2'. The 'Alias' field is set to 'Sniffer'. The 'Type' is 'Physical Interface'. The 'VRF ID' is '0' and the 'Role' is 'Undefined'. The 'Dedicated Management Port' option is disabled. Under the 'Address' section, the 'Addressing mode' is set to 'One-Arm Sniffer'. The 'Maximum Captured Packets' is set to '4000'. The 'Filters' section is disabled. The 'Security Profiles' section is also disabled. The 'Logging Options' section is enabled, and 'All Sessions' is selected. The 'OK' button is highlighted with a red arrow.

Let's enable diagnose to capture Sniffer packets on port2.

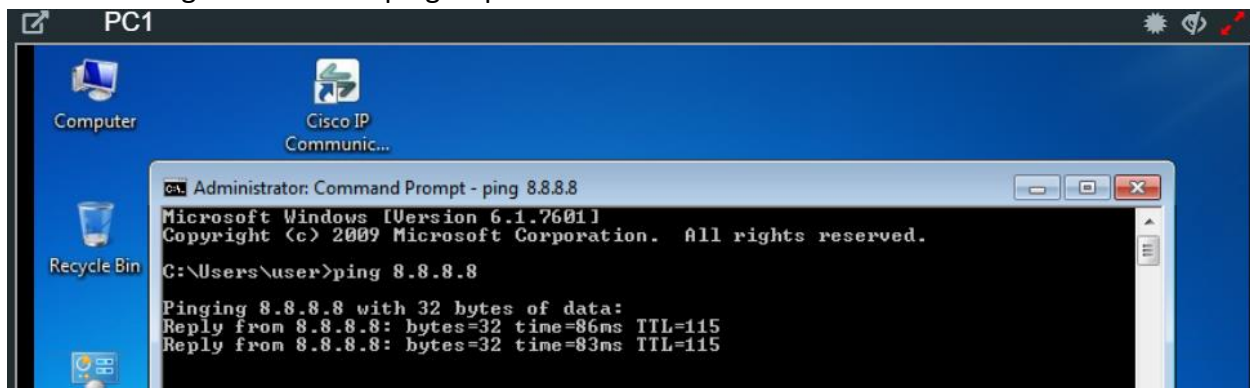
```
FW
FortiGate-VM64-KVM login: admin
Password:
Welcome!

FortiGate-VM64-KVM # diagnose sniffer packet port2
Using Original Sniffing Mode
interfaces=[port2]
filters=[none]
pcap_lookupnet: port2: no IPv4 address assigned
```

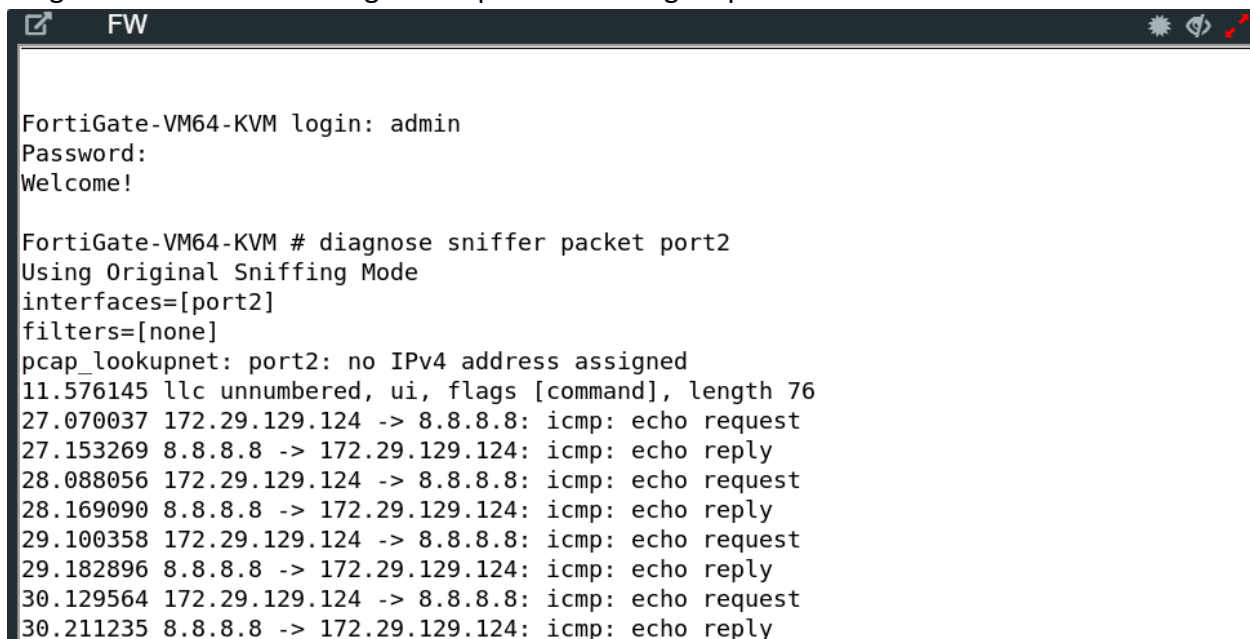
Also, let's start Packet Capture on port2 click on Play icon to start capture the packets.



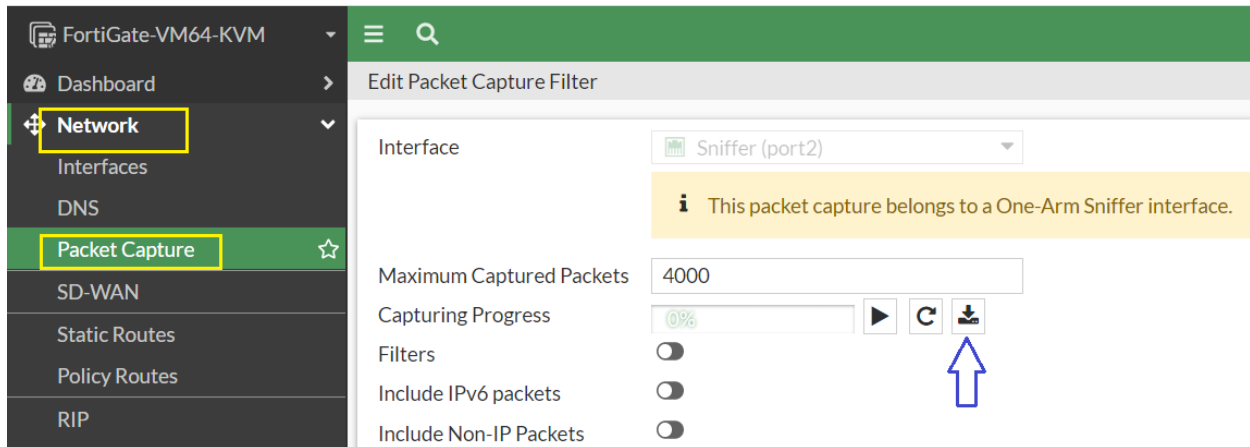
Start browsing or send ICMP ping request from PC1.



Diagnose command showing sniffer packets coming on port2.



Let's download Capture Packets click on download icon.



Packet Capture download also show ICMP request and reply.

