

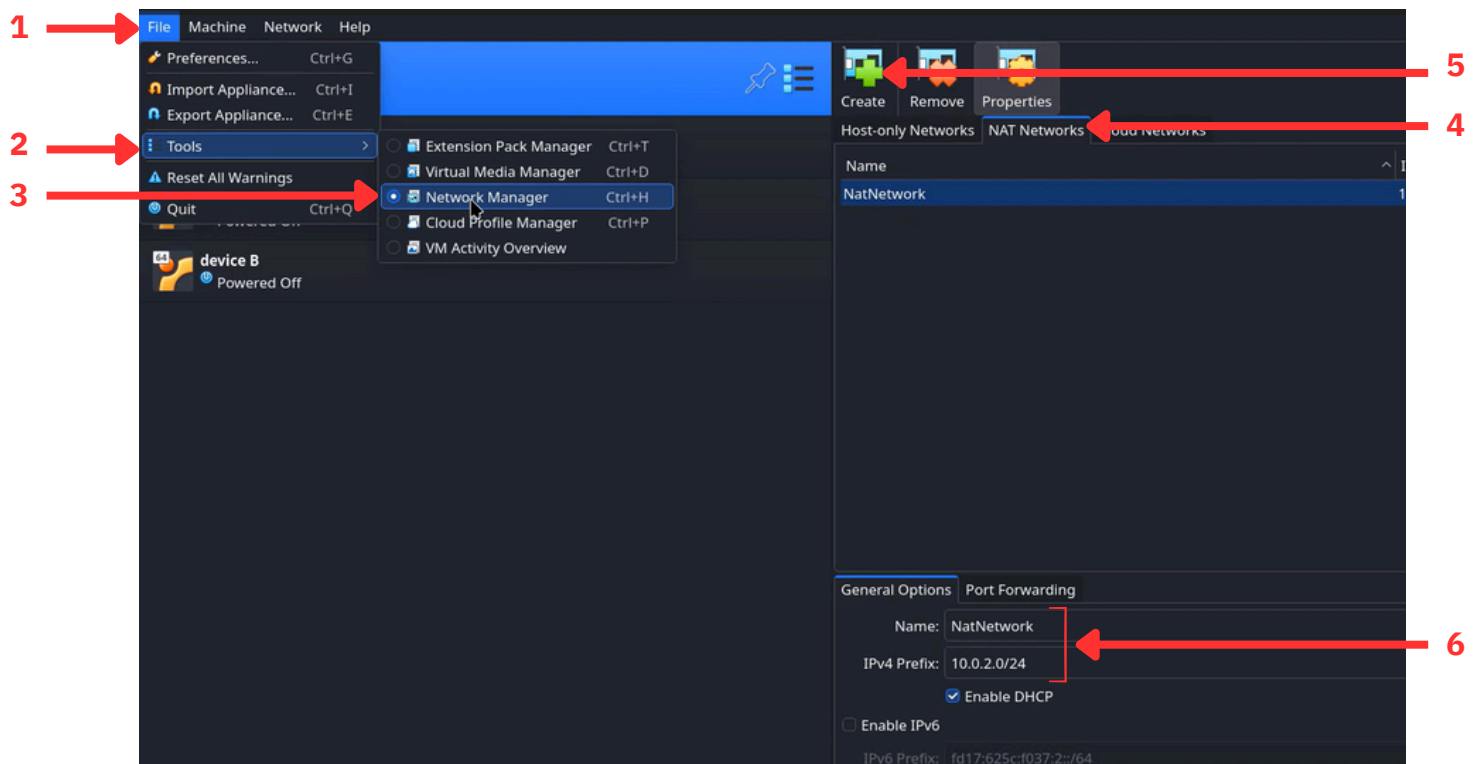
IPsec Tutorial with StrongSwan and Tshark

Introduction This guide shows how to set up an IPsec VPN tunnel between two VMs, with step-by-step commands and tips on what to check at each stage.

Commands and Steps

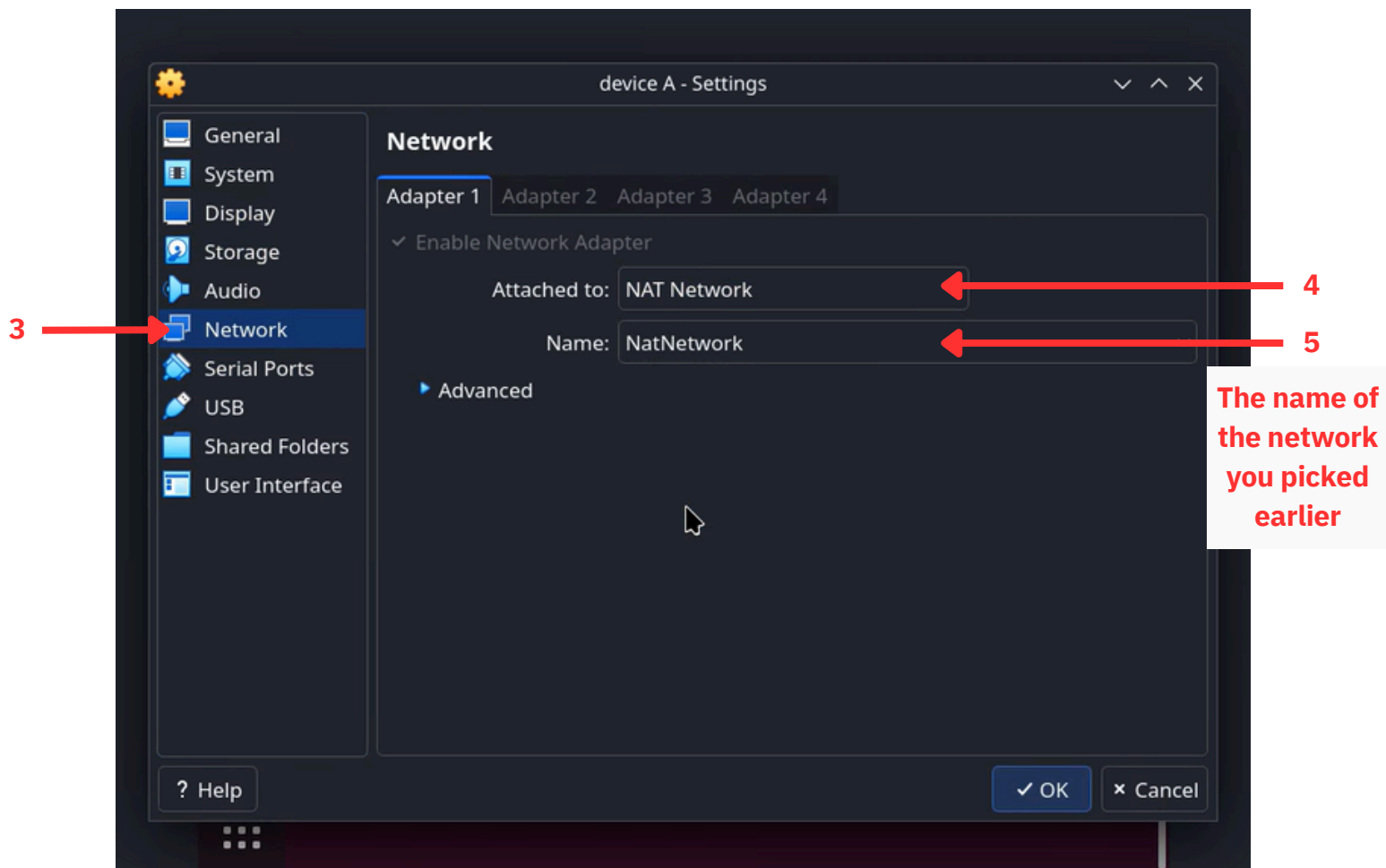
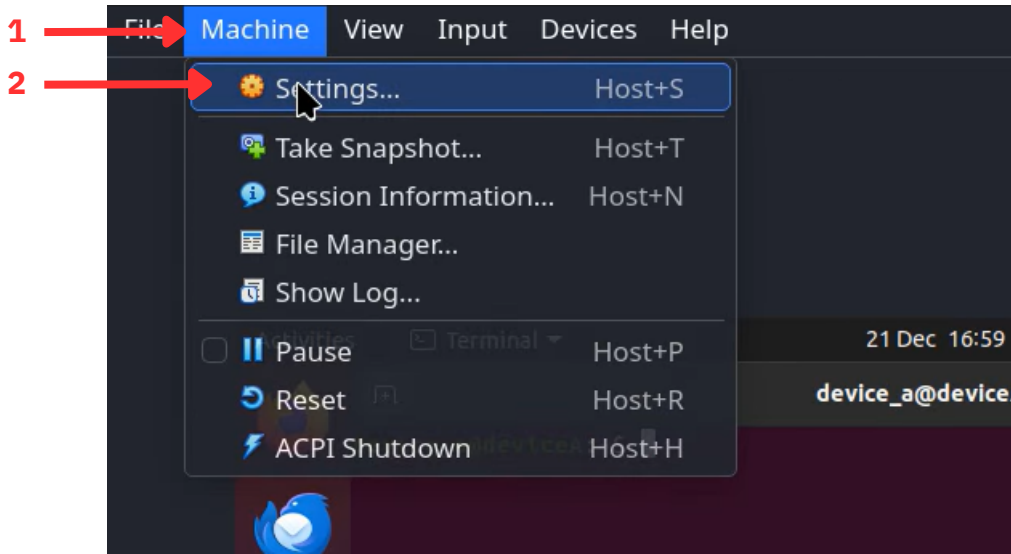
Step 1: Ensure both VMs are on the same network and assign the specified IP addresses.

1. Create the network on VirtualBox



- We chose a NAT network because it allows VM communication and internet access for installing packages, unlike a Host-Only network which lacks internet connectivity.

1. Add both VMs to the created network



- Adding both VMs to the network will automatically give them IP addresses, you can get the ip addresses by using the command:

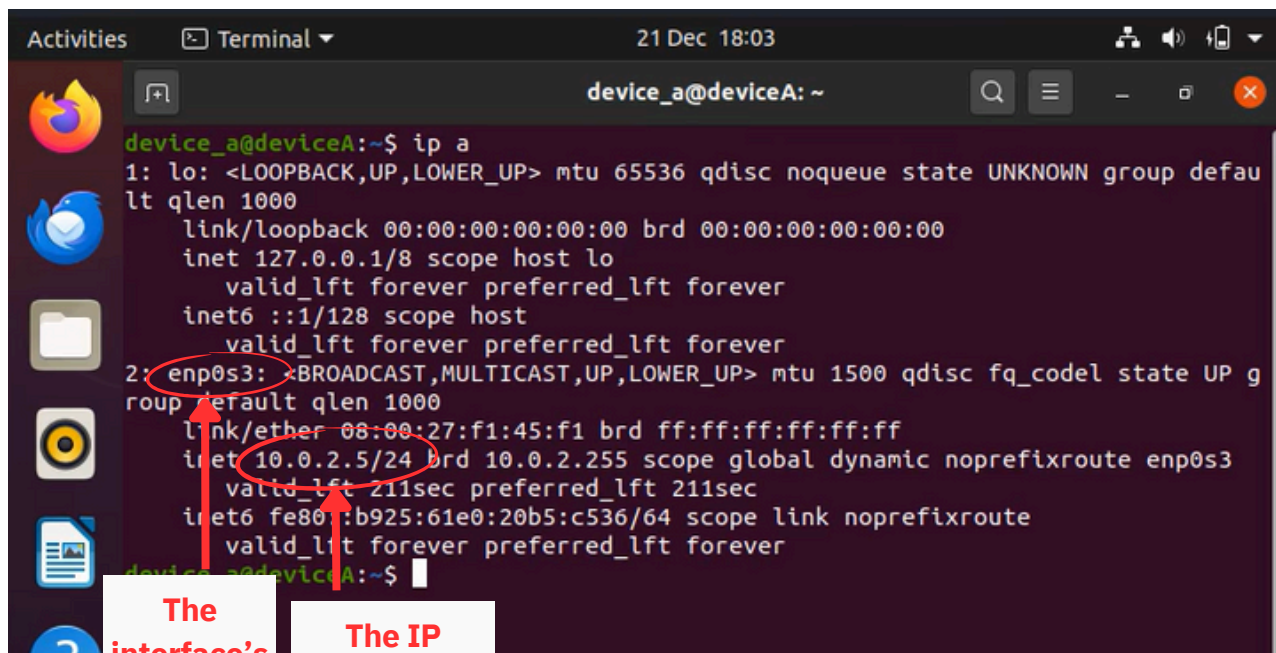
```
ip addr
```

Step 2: Identify the Network Interface

Command:

```
ip a
```

Look for the interface that has the IP address assigned in the NAT network (e.g., 10.0.2.5 or 10.0.2.15). Note the name of this interface (e.g., enp0s3) for later use.



```
device_a@deviceA:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f1:45:f1 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.5/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 211sec preferred_lft 211sec
    inet6 fe80::b925:61e0:20b5:c536/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
device_a@deviceA:~$
```

The interface's name

The IP address of the VM in the network

Step 3: Install StrongSwan

Commands:

```
sudo apt update
sudo apt install strongswan
```

Purpose: Installs StrongSwan, which is used to set up the IPsec VPN.

Execution: Run on both VMs.

Step 4: Configure IPsec

1. Edit the IPsec configuration file:

Command:

```
sudo nano /etc/ipsec.conf
```

Content for VM1:

```
config setup

    charondebug="ike 2, net 2"

conn vpn-tunnel

    left= 10.0.2.5

    leftsubnet=10.0.2.5/32

    right=10.0.2.15

    rightsubnet=10.0.2.15/32

    authby=secret

    auto=start
```

Content for VM2:

```
config setup

    charondebug="ike 2, net 2"

conn vpn-tunnel

    left=10.0.2.15

    leftsubnet=10.0.2.15/32

    right=10.0.2.5

    rightsubnet=10.0.2.5/32

    authby=secret

    auto=start
```

2. Edit the IPsec secrets file:

Command:

```
sudo nano /etc/ipsec.secrets
```

Content (same for both VMs):

```
10.0.2.5 10.0.2.15 : PSK "vpn-key"
```

Step 5: Restart IPsec and Check Status

1. Restart the IPsec service:

Command:

```
sudo ipsec restart
```

2. Check the status:

Command:

```
sudo ipsec statusall
```

What to Look For: Initially, the output should show **(0 up, 0 connecting)**, indicating no active connections. After setting up the VPN, you should see **(1 up, 0 connecting)** confirming the tunnel is established.

Step 6: Establish the VPN Tunnel

Command:

```
sudo ipsec up vpn-tunnel
```

Purpose: Initiates the VPN tunnel setup by negotiating keys and establishing secure communication.

Execution: Run on both VMs.

Step 7: Install Tshark

Commands:

```
sudo apt install tshark
```

Purpose: Installs Tshark, a command-line tool for packet analysis.

Execution: Run on both VMs.

Step 8: Analyze Traffic Using Tshark

1. Command to Capture IKE (Phase 1) Traffic:

On VM1:

```
sudo tshark -i enp0s3 -f "udp port 500"
```

Purpose: Captures packets on port 500, used during the IKE negotiation phase.

On VM2:

restart the VPN tunnel on VM2 to initiate the IKE negotiation. This will allow Tshark on VM1 to capture the packets related to the exchange of security associations (SAs) and key negotiations between the two VMs.

```
sudo ipsec restart
```

What to Look For:

Look for packets labeled ISAKMP or IKE_SA_INIT. These labels indicate that the packets are part of the exchange where security associations (SAs) and encryption keys are being negotiated during Phase 1 of the IKE protocol.



2. Command to Capture ESP (Phase 2) Traffic:

On VM1:

```
sudo tshark -i enp0s3 -f "ip proto 50"
```

Purpose: Captures packets using protocol 50 (ESP), used for encrypted data transfer.

On VM2:

execute a ping command from VM2 to VM1. This will generate encrypted traffic over the VPN tunnel, and Tshark will capture the ESP packets, which contain the encrypted data being transmitted between the two VMs.

```
ping 10.0.2.5
```

What to Look For:

Look for packets labeled ESP. This label confirms that the packets contain encrypted data being transmitted over the VPN tunnel during Phase 2 of the IPsec connection.



Although a graphical interface like **Wireshark** can be used for packet capture, we chose **Tshark** for its command-line efficiency, making it more suitable for automated and repeatable analysis in this setup.

In conclusion, this guide has provided step-by-step instructions for setting up and analyzing an IPsec VPN using StrongSwan and Wireshark. By capturing IKE and ESP traffic, you can verify the VPN's functionality, troubleshoot potential issues, and ensure secure communication. With these tools, you'll be equipped to monitor and optimize your IPsec VPN setup for both performance and security.