TRAINING SESSION NAME

Firewall

Tables of content

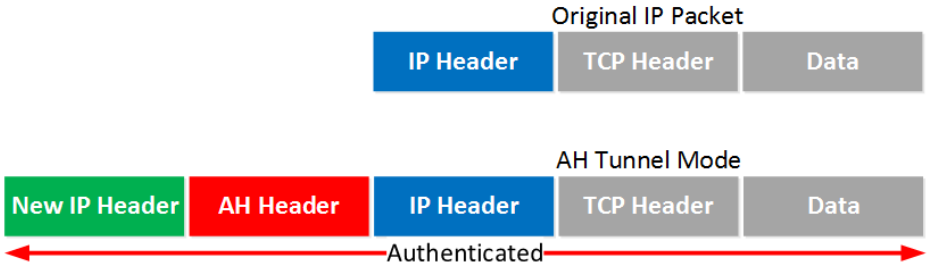
A.1 IPsec

1. Concept

- IPsec (Internet Protocol Security) is a secure network protocol suite that authenticates and encrypts packets of data to provide secure encrypted communication between two computers over an Internet Protocol network.
- As a part of the IPv4 enhancement, IPsec is a layer 3 OSI model or internet layer end-to-end security scheme.

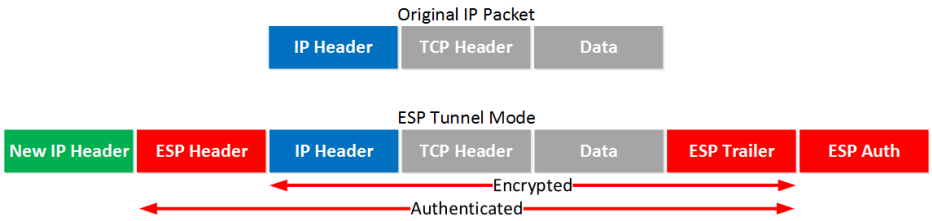
1.1 Component

- Authentication Headers (AH): ensures that data packets are from a trusted source and that the data has not been tampered with



IP packet with AH tunnel mode. Source: IPsec (Internet Protocol Security) (networklessons.com)

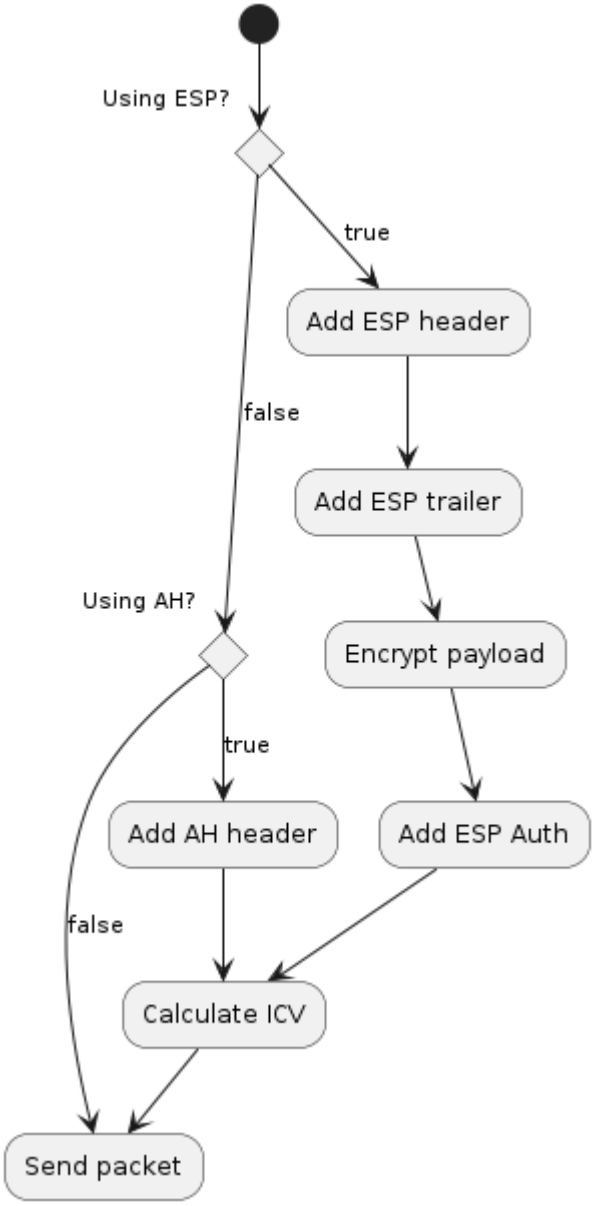
- Encapsulating Security Payload (ESP): encrypts the IP header and the payload for each packet. ESP adds its own header and a trailer to each data packet.



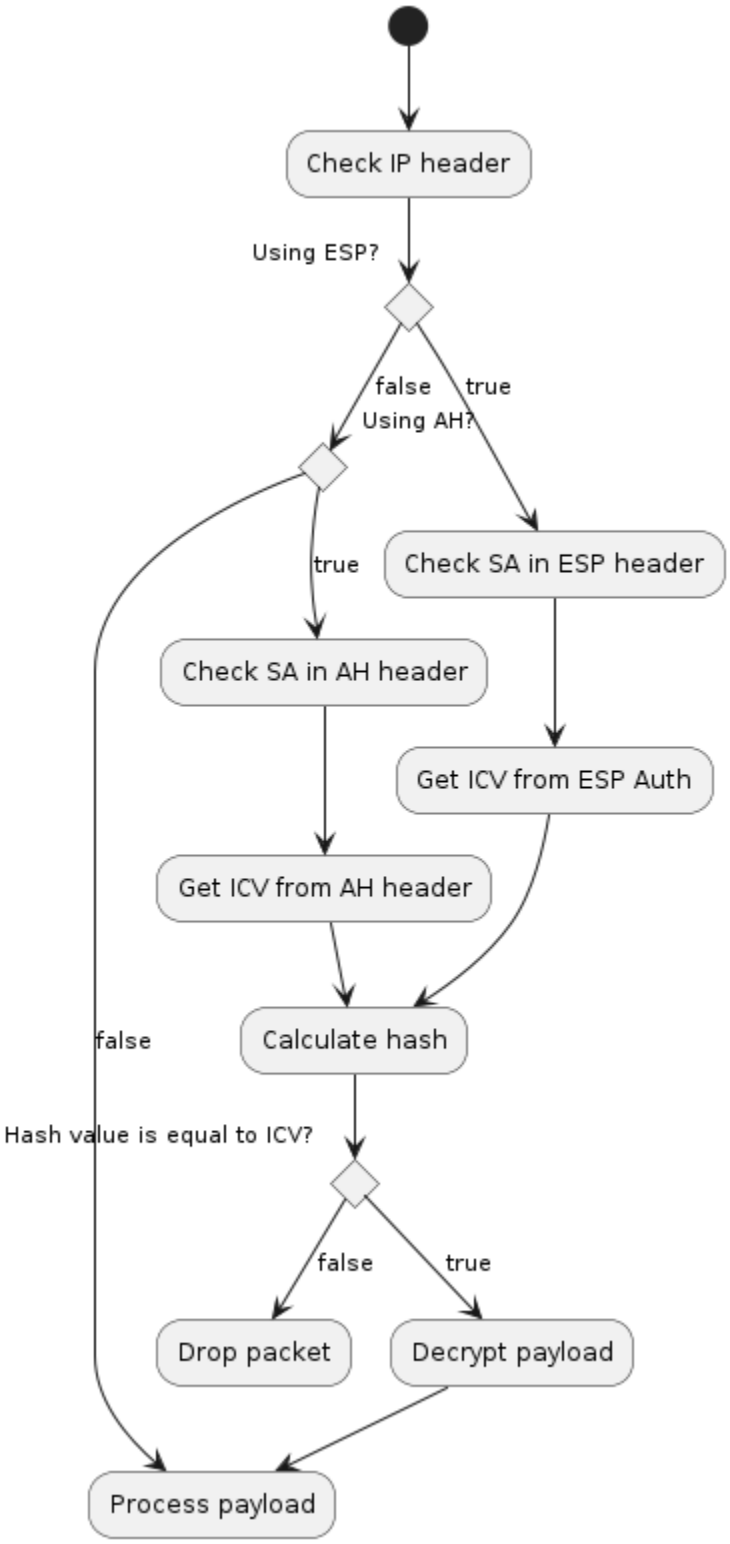
IP packet with ESP tunnel mode. Source: [IPsec (Internet Protocol Security) (networklessons.com)]

- Security Association (SA): SA refers to a number of protocols used for negotiating encryption keys and algorithms. One of the most common SA protocols is Internet Key Exchange (IKE).

Transmitter

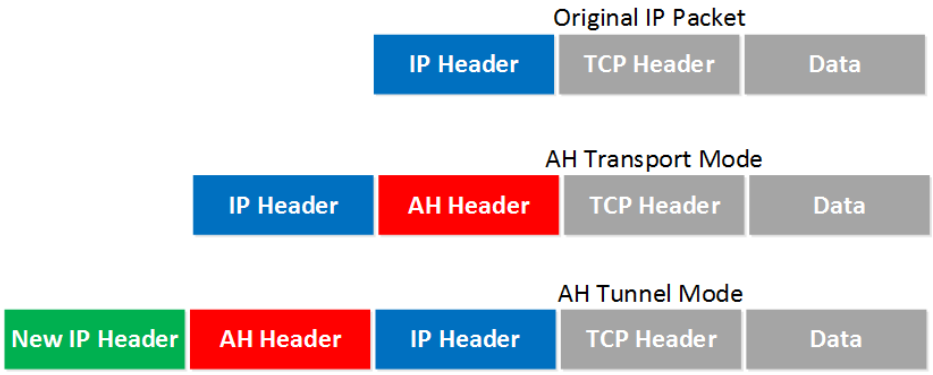

Using ESP?
true
Add ESP header
false
Add ESP trailer
Using AH?
Encrypt payload
true
Add AH header
Add ESP Auth
false
Calculate ICV
Send packet

Receiver



1.2 Modes of operation

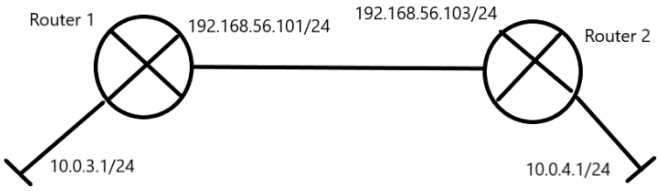
- Tunnel mode: the original IP header containing the final destination of the packet is encrypted, in addition to the packet payload. To tell intermediary routers where to forward the packets, IPsec adds a new IP header. At each end of the tunnel, the routers decrypt the IP headers to deliver the packets to their destinations.
- Transport mode: the payload of each packet is encrypted, but the original IP header is not. Intermediary routers are thus able to view the final destination of each packet.



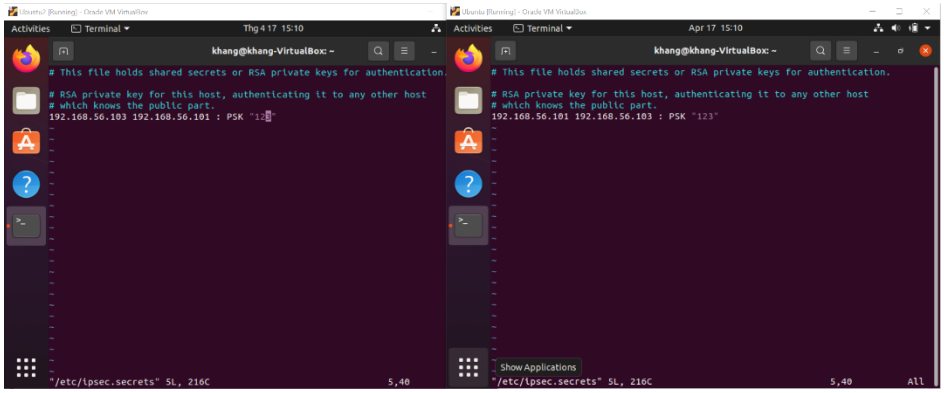
IP packet in transport mode and tunnel mode. Source: [IPsec (Internet Protocol Security) (networklessons.com)]

2. Demo

Connect server 1 (Ubuntu) with IP 10.0.3.1 to server 2 (Ubuntu2) with IP 10.0.4.1.

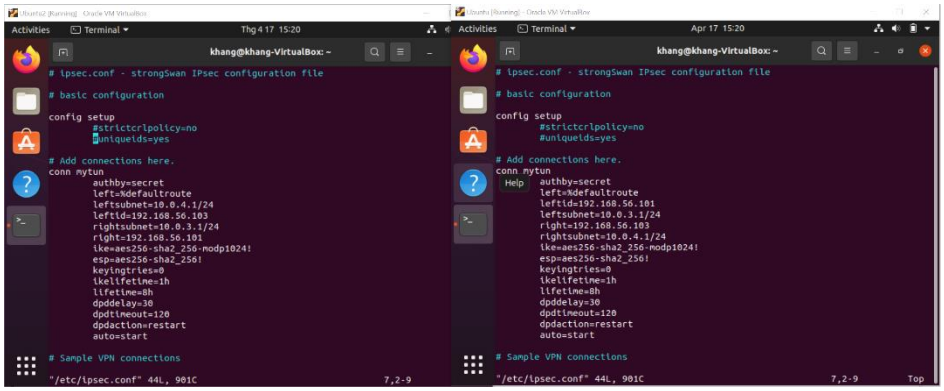


2.1 Add key between 2 public addresses

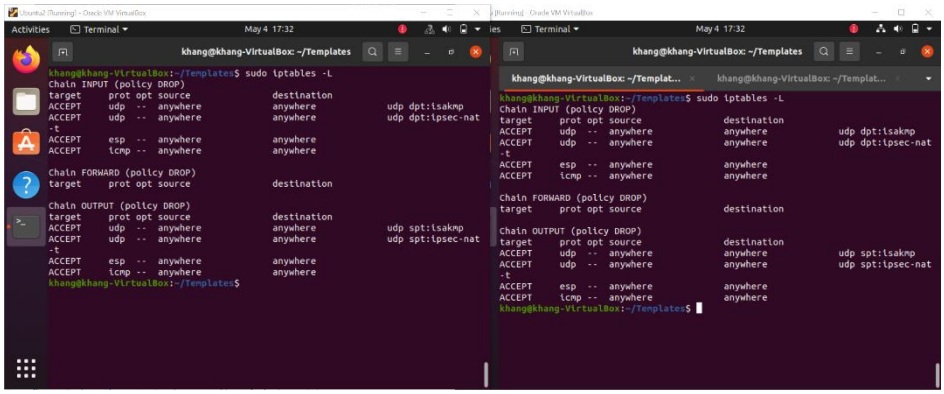


2.2 Add new connection config

Example: mytun
left ip: source ip
right ip: destination ip



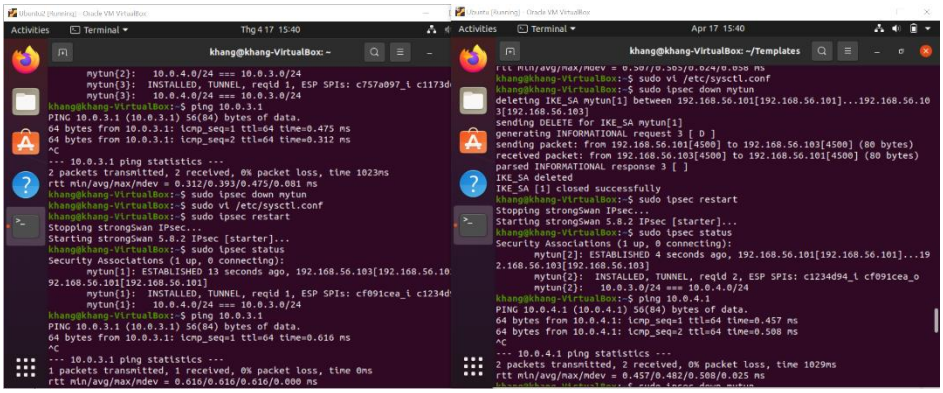
2.3 Add iptables rules



2.4 Check connection

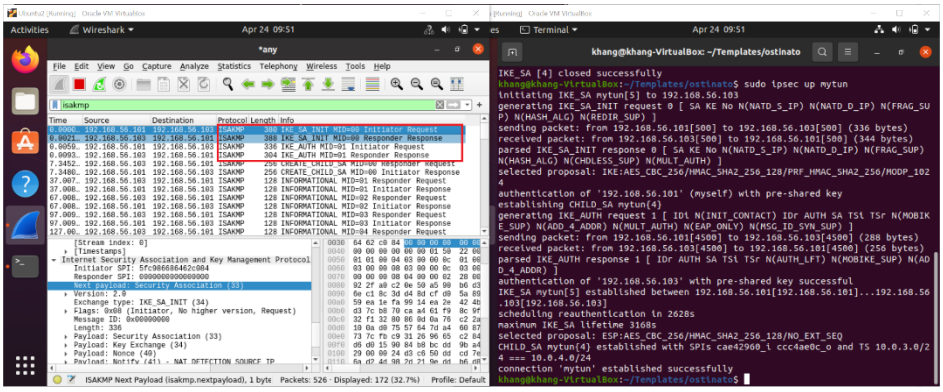
ipsec status or *ipsec statusall*

If connection has not been set up, try using command *ipsec reload* or *ipsec restart*.
If connection has been set up, ping between 2 ip.

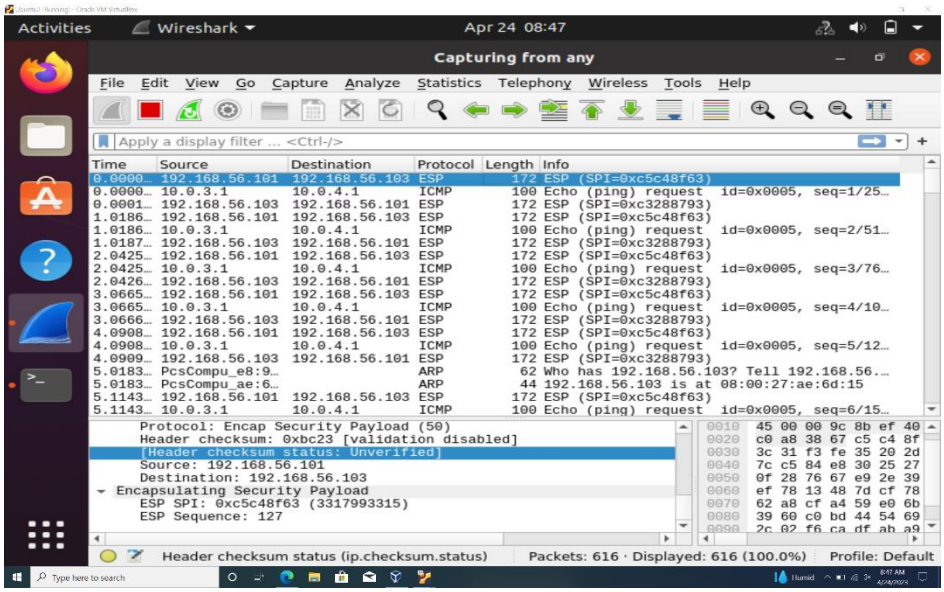


2.5 Capture packets by wireshark

When the tunnel is initialized, messages are exchanged to established the security association.



User messages, using ESP protocol



A.2 MACsec

1. Concept

MACsec (Media Access Control security) provides security of data between Ethernet-connected devices.

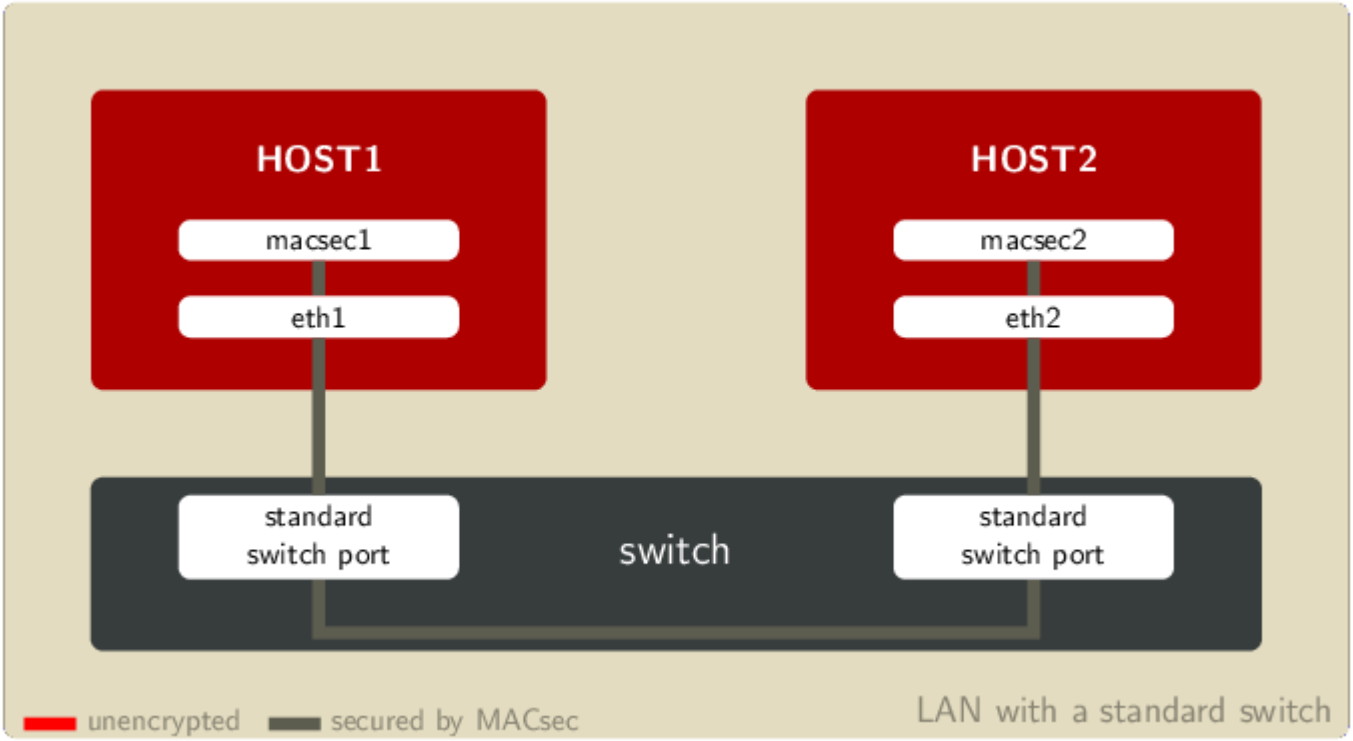
MACsec	IPsec
Work over layer 2 network	Work over layer 3 network
Work across WAN	Work on switches or end-nodes on LAN

1.1 Component

- Secure channel: used to send traffic to others. Each channel has a Secure channel identifier (SCI). The receive secure channel must have a SCI corresponding to the SCI of the transmit secure channel of the peer.
- Secure association: hold encryption key and packet number. On the transmit side, this packet number is put in the MACsec header and used in the encryption process. On the receive side, the packet number from the MACsec header can be checked against the packet number locally stored in the corresponding secure association to perform replay protection.

2. Demo

Create MACsec devices on 2 machines (host 1 and host 2)



MACsec example. Source: [MACsec: a different solution to encrypt network traffic | Red Hat Developer]

2.1 Setup macsec

host1

```
host1# ip link show eth0
7: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP mode
DEFAULT group default qlen 1000
    link/ether 42:f8:ad:3a:e6:08 brd ff:ff:ff:ff:ff:ff link-netnsid 0
host1# ip link add link eth0 macsec0 type macsec encrypt on
host1# ip link show macsec0
8: macsec0@eth0: <BROADCAST,MULTICAST> mtu 1468 qdisc noop state DOWN mode DEFAULT
group default qlen 1000
    link/ether 42:f8:ad:3a:e6:08 brd ff:ff:ff:ff:ff:ff
host1# ip macsec show
8: macsec0: protect on validate strict sc off sa off encrypt on send_sci on
end_station off scb off replay off
    cipher suite: GCM-AES-128, using ICV length 16
    TXSC: 42f8ad3ae6080001 on SA 0
```

host2

```
host2# ip link show eth0
```

```
7: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP mode
DEFAULT group default qlen 1000
    link/ether 32:53:41:bd:7c:27 brd ff:ff:ff:ff:ff:ff link-netnsid 0
host2# ip link add link eth0 macsec0 type macsec encrypt on
host2# ip link show macsec0
8: macsec0@eth0: <BROADCAST,MULTICAST> mtu 1468 qdisc noop state DOWN mode DEFAULT
group default qlen 1000
    link/ether 32:53:41:bd:7c:27 brd ff:ff:ff:ff:ff:ff
host2# ip macsec show
8: macsec0: protect on validate strict sc off sa off encrypt on send_sci on
end_station off scb off replay off
    cipher suite: GCM-AES-128, using ICV length 16
    TXSC: 325341bd7c270001 on SA 0
```

2.2 Add receive address

host1

```
host1# ip macsec add macsec0 rx port 1 address 32:53:41:bd:7c:27
host1# ip macsec show
8: macsec0: protect on validate strict sc off sa off encrypt on send_sci on
end_station off scb off replay off
    cipher suite: GCM-AES-128, using ICV length 16
    TXSC: 42f8ad3ae6080001 on SA 0
    RXSC: 325341bd7c270001, state on
```

host2

```
host2# ip macsec add macsec0 rx port 1 address 42:f8:ad:3a:e6:08
host2# ip macsec show
8: macsec0: protect on validate strict sc off sa off encrypt on send_sci on
end_station off scb off replay off
    cipher suite: GCM-AES-128, using ICV length 16
    TXSC: 325341bd7c270001 on SA 0
    RXSC: 42f8ad3ae6080001, state on
```

2.3 Configure transmit keys

host1

```
host1# ip macsec add macsec0 tx sa 0 pn 1 on key 00
12121212121212121212121212121212
host1# ip macsec show
8: macsec0: protect on validate strict sc off sa off encrypt on send_sci on
end_station off scb off replay off
    cipher suite: GCM-AES-128, using ICV length 16
    TXSC: 42f8ad3ae6080001 on SA 0
        0: PN 1, state on, key 00000000000000000000000000000000
    RXSC: 325341bd7c270001, state on
```

host2

```
host2# ip macsec add macsec0 tx sa 0 pn 1 on key 01
13131313131313131313131313131313
host2# ip macsec show
8: macsec0: protect on validate strict sc off sa off encrypt on send_sci on
end_station off scb off replay off
```

```
    cipher suite: GCM-AES-128, using ICV length 16
    TXSC: 325341bd7c270001 on SA 0
        0: PN 1, state on, key 01000000000000000000000000000000
    RXSC: 42f8ad3ae6080001, state on
```

2.4 Configure receive keys

host1

```
host1# ip macsec add macsec0 rx port 1 address 32:53:41:bd:7c:27 sa 0 pn 1 on key
01 13131313131313131313131313131313
host1# ip macsec show
8: macsec0: protect on validate strict sc off sa off encrypt on send_sci on
end_station off scb off replay off
    cipher suite: GCM-AES-128, using ICV length 16
    TXSC: 42f8ad3ae6080001 on SA 0
        0: PN 1, state on, key 00000000000000000000000000000000
    RXSC: 325341bd7c270001, state on
        0: PN 1, state on, key 01000000000000000000000000000000
```

host2

```
host2# ip macsec add macsec0 rx port 1 address 42:f8:ad:3a:e6:08 sa 0 pn 1 on key
00 12121212121212121212121212121212
host2# ip macsec show
8: macsec0: protect on validate strict sc off sa off encrypt on send_sci on
end_station off scb off replay off
    cipher suite: GCM-AES-128, using ICV length 16
    TXSC: 325341bd7c270001 on SA 0
        0: PN 1, state on, key 01000000000000000000000000000000
    RXSC: 42f8ad3ae6080001, state on
        0: PN 1, state on, key 00000000000000000000000000000000
```

2.5 Enable MACsec links

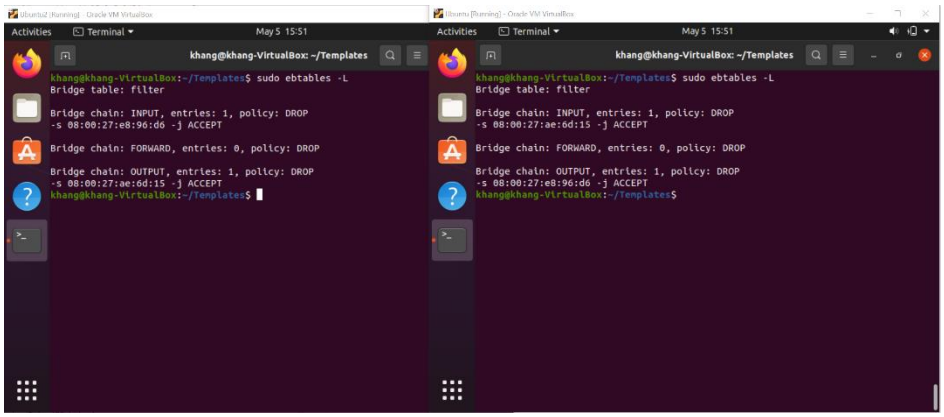
host1

```
host1# ip link set macsec0 up
host1# ip addr add 10.1.0.1/24 dev macsec0
```

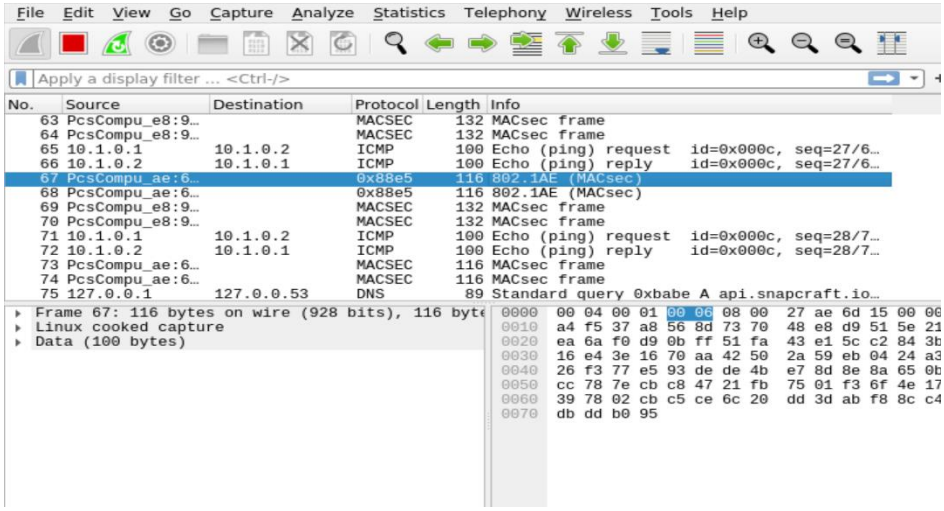
host2

```
host2# ip link set macsec0 up
host2# ip addr add 10.1.0.2/24 dev macsec0
```

2.6 Add ebtables rules



2.7 Capture packets by wireshark



B. Questions, exercises

C. References

No.	Info	Link / file / name of ebook
1	IPsec definition	What is IPsec? | How IPsec VPNs work | Cloudflare
2	IPsec definition	IPsec - Wikipedia

3	Demo IPsec	Who To Setup a Site To Site IPSEC | Zulqarnain Hayat - YouTube
4	MACsec definition	Enhancing Network Security with MACsec (IEEE 802.1AE) | Military Aerospace
5	MACsec definition-demo	MACsec: a different solution to encrypt network traffic | Red Hat Developer