Networks and Systems Security 2 - Winter 2022

Sambuddho Chakravarty

April 5, 2022

Exercise 5 (total points: 30)

Due date: April 19, 2022. Time: 23:59 Hrs.

IPSec/IKE and IPSec/L2TP VPNs (total points: 40)

LibreSwan IPSec/IKE

Basic IPSec/IKE setup (points: 20)

The objective of this assignment is to familiarize you with using LibreSwan IPSec/IKEv2 protocol. For this you need to create a set-up involving four VMs, as shown in figure 1. The VMs 2 and 3 are supposed to VPN Gateways. By default the VM1 and VM4 are should not know about one another and should not be able to ping one another. The VM2 and VM3 are however enabled to forward IP traffic (/proc/sys/net/ipv4/ip_forward ==> 1).

You need to install LibreSwan on VM2 and VM3. Configure LibreSwan on both the VM2 and VM3. They should be configured to establish mutual authenticated connection through X.509 public key certificates (self signed).

Once established, the tunnel should allow the VM1 to ping VM4 WITHOUT changing the underlying routing table entries. Capture the traffic between VM2 and VM3 showing the IKE tunnel setup and the encrypted ICMP echo (ping) messages being transported as ESP packets

Traffic Selection (points: 10)

Set up a webserver on VM4 with a few files. Configure traffic selector on VPN gateway VMs VM2 and VM3 such that the IPSec/IKE tunnel allows only traffic to the webserver on the host VM4.

What to submit/Grading rubric:

1. Description of the commands that were ran for configuring the IPSec/IKE tunnel for both tunnel and transport modes, including details of the commands used to setup the tunnel [10 points].

2. Screenshot showing that `ping` and `wget` from client to server via the IPSec tunnel, along with that of Wireshark showing the traffic between the client

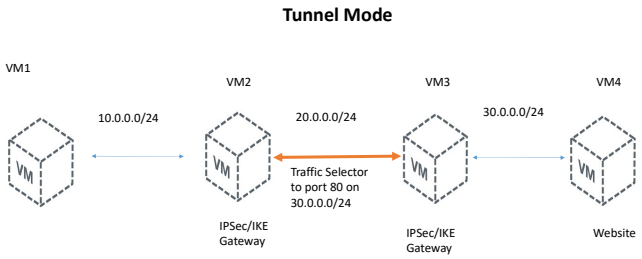

Figure 1: IPSec/IKE tunnel which allows access to port 80 on the webserver VM

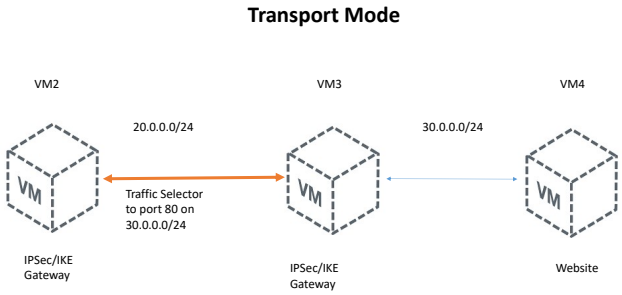

Figure 2: IPSec/IKE tunnel which allows access to port 80 on the webserver VM

and server and their respective VPN gateways and between gateways. The traffic must show the ESP packets being transported between gateways while regular TCP/IP packets going to the end hosts [20 points].