Networks and Systems Security - Winter 2019

Sambuddho Chakravarty

April 10, 2019

Lab Assignment 6 (total points: 60)

Due date: April 14. Time: 23:59 Hrs.

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

1.1 LibreSwan IPSec/IKE (points: 20)

1.1.1 Basic IPSec/IKE setup

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).

One 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

1.1.2 Traffic Selection

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.

1.2 IPSec/L2TP(points: 20)

The second part of the exercise involves only three VMs. Here we do not use the VM1 and VM2 communicates to VM4 via the IPSec gateway VM3. The VM, VM2 communicates to VM4 through a transport mode connection (unlike the previous tunnel mode) (see figure 2 Create users corresponding to the IPSec tunnels and associate fake passwords to them which would be used for performing CHAP authentication for allowing (or preventing) the VM2 from

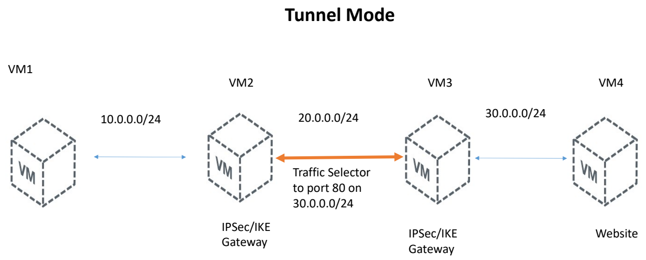

Figure 1: IPSec/IKE tunnel which allows access to port 80 on the webserver VM

connecting to the VM4, via VM3. For this you need to use L2TP which does the user authentication, instead if IKEv1/IKEv2,

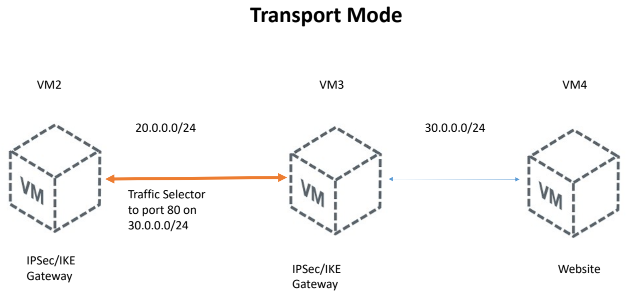

Figure 2: IPSec/IKE tunnel which allows access to port 80 on the webserver VM

You need to submit the screen shots showing the commands you typed, their semantics, and traffic captured between the VMs (IPSec encrypted/encapsulated) and the corresponding traffic originating and terminating at the end points.