|  |  |  |
| --- | --- | --- |
| Name: Adarsh Kumar | SRN No: PES2UG20CS016 | Assignment No: Optional |
| Section: B | Date: 8/11/2022 |

|  |  |
| --- | --- |
| Task 1: | VM Setup |
| Screenshots  of basics setups. | Both the VMs need to have the “NAT Network” Adapter enabled on them:  VPN Server (IP: 10.0.2.6) machine network configuration    VPN Client (IP: 10.0.2.15) machine network configuration    We have configured both VM at NAT network settings. |
| Task 2: | Set up Firewall |
| Screenshot | I have identified ‘www.wikipedia.org' as a website to be blocked on the client machine.  The client machine is inside the firewall.  The website is able to be pinged from the client machine initially:    Therefore, we can see that Wikipedia.org has a fixed IP address: 103.102.166.224  Now, we will set up a firewall to block this website from being accessed    Now we can see that [www.wikipedia.org](http://www.wikipedia.org) is blocked. The rule is added into our firewall table.    Now it can be observed that we are not able to ping to [www.wikipedia.org](http://www.wikipedia.org) website.  It is because we blocked the request message which was going outside to (103.102.166.224) from client machine. |
| Task 3: | Bypassing Firewall using VP |
| Step 1: | Run VPN Server:  Initially only two interfaces were present. There is no mention of tun0 interface, so it is inactive.  VPN server code run on the server to establish the tunnel.    Now we are assigning an IP address to the tun0 interface and activate it. IP Address assigned: 192.168.53.1/25  Upon checking ifconfig -a: we have an established tunnel    Here we can see that Tun0 interface got the IP address of 192.168.53.1  Now the VPN Server needs to forward packets to other destinations, so it needs to function as a gateway. We need to enable the IP forwarding for a computer to behave like a gateway. |
| Step 2: | Run VPN Client:    On the client machine we are checking that we got only 2 interface there is no tun0 interface now.    VPN client code run on the client to establish the tunnel.    Now we are assigning an IP address to the tun0 interface and activate it. IP Address assigned: 192.168.53.1/25 Upon checking ifconfig -a: we have an established tunnel:    We can see that tun0 interface got IP address of 192.168.53.5 |
| Step 3: | Set Up Routing on Client and Server VMs:  We can now see that the tunnel is established because of the messages displayed like  ‘Connected with client: Hello’  Server    Client    We need to set up routing paths on both client and server machines to direct the intended traffic through the tunnel. This is done on the client machine as follows:    This ensures that all the packets from the IP address 103.102.166.0/24 (Wikipedia’s IP) will be routed to tun0 interface. |
| Step 4: | Set Up NAT on Server VM:  We make NAT to believe that the MAC address of 192.168.53.5 is the VPN server’s MAC address. The following commands can enable the NAT on the Server VM |
| Task 4: | Demonstration    Client machine can now access W through the tunnel established. We can try ping command. Therefore, the task has been completed successfully |
| Screenshot | We can observe that the ICMP request packet from tunnel interface (192.168.53.5) is created to IP (157.240.228.35), the tunnel writes the packet to the UDP socket which sends the packet to server machine. (10.0.2.5). The ping reply is received back on tun0 interface. Hence, ping works bypassing firewall through the created tunnel. |