**Theory:-**

Sure, let's break down the concept of Demonstrating Planning Network-based Firewalls:

**1. Network-based Firewalls:**

- Think of a firewall like a security guard for your computer or network.

- It's a barrier that checks and controls the incoming and outgoing data to make sure it's safe.

**2.** **Demonstrating Planning:**

- "Demonstrating" here means showing or proving something.

- So, we want to show or prove how we plan to use a firewall.

**3. Network-based Firewalls in Simple Terms:**

- These are special types of security guards that protect your computer or network from bad things on the internet.

- They decide what information can come in and go out, just like a gatekeeper.

**4. Putting it Together:**

- "Demonstrating Planning Network-based Firewalls" means showing how we plan to use these internet security guards to protect our computer or network.

So, in the simplest terms, it's like explaining the strategy or plan for using special guards (firewalls) to keep your computer or network safe from harmful things on the internet.

Planning network-based firewalls involves designing a security strategy that includes the placement, configuration, and rules for firewalls within a network.

**Practical 4: Planning Network-based Firewalls**

1. Click on End devices🡪 Drag on Server-PT server0.

2. Click on End devices🡪Drag 3 PC-PT machine.

3. Click on Network Devices🡪 Wireless Devices🡪 Drag on WRT300N Wireless Router0.

4. Connect Server0 to wireless Router0

: - Go to connection 🡪Choose copper straight- through wire.

Connect Server0 Fast Ethernet0 → Wireless Router0 Ethernet1

wait until connection converted to green (1 min)

5. Click on Server0🡪 Desktop →Click on IP Configuration →Click on DHCP

(then IP address of server0 will automatically be generated)

IP address: 192.168.0.100

6. Then add label above the Server 🡪192.168.0.100

7. Click on PC-PT PC0🡪 it is wired🡪 so switch off power button then remove the wired component with wireless component. And power on the machine.

8. Do Same thing for PC-PT PC1, PC-PT PC2.

9. Click on prompt PC-PT PC1🡪 Desktop🡪 Command Prompt🡪

And ping the server:

ping 192.168.0.100 ← (Insert this command in the command prompt.)

wait for replay.

10. Click on PC-PT PC1🡪 Desktop → Web Browser

🡪URL 192.168.0.100 →Click on Enter.

And you get web interface So Ip protocol also on.

11. Click on Server0🡪 Desktop🡪 Click on IPV4

Firewall in that: -

Services on (click on)

Action: Deny

Protocol: ICMP

Remote IP: 0.0.0.0

Remote wild card Mask: 255.255.255.255

then click on 🡪Add

12. Action: Allow

Protocol: IP

Remote IP: 0.0.0.0

Remote Wildcard Mask: 255. 255. 255. 255

Click on 🡪Add

So, I'm able to access the website.

13. Click on PC-PT PC1🡪 Desktop🡪 Command prompt & again enters same command: -

C:\> ping 192.168.0.100

We will be waiting for replay & the request is timeout. So, wait to 4 iterations.

You can see ping statistics for 192.168.0.100: packet: sent = 4, Received = 0, Lost =4 (100% loss).

in previous command we had 0% loss because 4 packets are received successfully.

14. Check IP protocol is on or not

PC-PT PC1🡪 Desktop🡪 web Browser

URL: 192.168.0.100🡪 Enter

we kept it on so it is accessible.

So, PC-PT PC1 I’m able to access server but I'm not able to ping because of the firewall

15. Same think you can check it out from PC-PT PC0 → Desktop 🡪command prompt →

ping 192.168.0.100 →Enter.

It has blocked.

Request timed out & let complete 4 iteration.

Check for web browser (PC0) → PC0→ Desktop 🡪web browser

URL: 192.168.0.100 🡪Enter

IP protocol is on.

16. Similarly do above (repeat) process that is step 15 for PC-PT PC2.

Ping is not accessible because ICMP is denied.