

DHCP Relay Setup with FortiGate + Windows Server

Submitted by: Rahul K G
www.linkedin.com/in/rahul-k-gopi-a703ba16a

◆ DHCP Relay Agent – Use Case in Enterprise Networks

What it is:

A DHCP Relay Agent is used when DHCP clients and the DHCP server are on different networks or VLANs.

👉 Normally, DHCP works with broadcasts (UDP 67/68), but broadcasts do not cross routers or firewalls.

👉 The relay agent solves this by:

- Listening for client broadcast requests
- Forwarding them as unicast packets to the DHCP server
- Relaying the server's reply back to the correct client

💡 Real-Time Use Case

- In large **enterprise networks** or **branch office setups**, DHCP servers are centralized in the datacenter.
- Instead of deploying a separate DHCP server for every subnet/VLAN, **routers**, **firewalls (FortiGate, Cisco, etc.)**, or **Windows servers** act as relay agents.
- This ensures all devices get IPs seamlessly from the central pool.

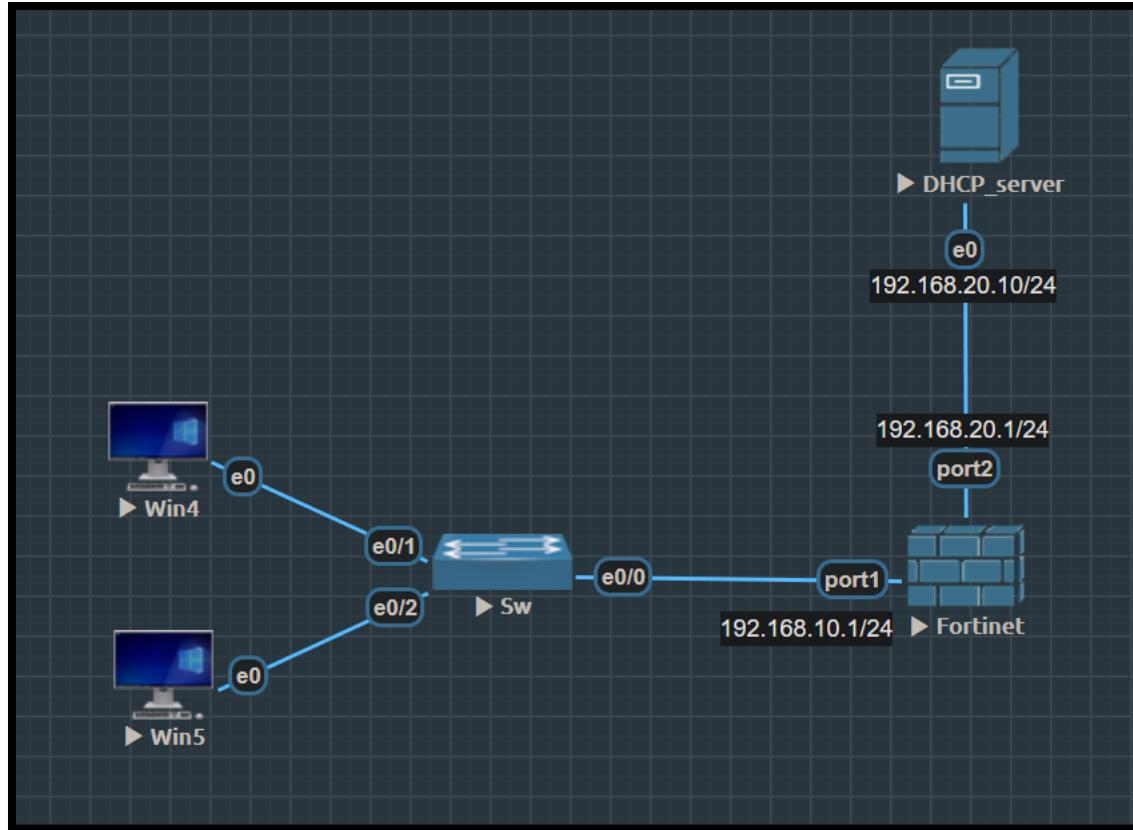
🔑 Key Benefits

- **Centralized IP management** → Easier to monitor and control
- **Cost-effective** → No need for multiple DHCP servers
- **Scalable** → Works smoothly across many VLANs and remote sites

Flow Example:

Client → Firewall/Router (Relay) → DHCP Server → Firewall/Router → Client

Network Overview



Our network is designed with two zones:

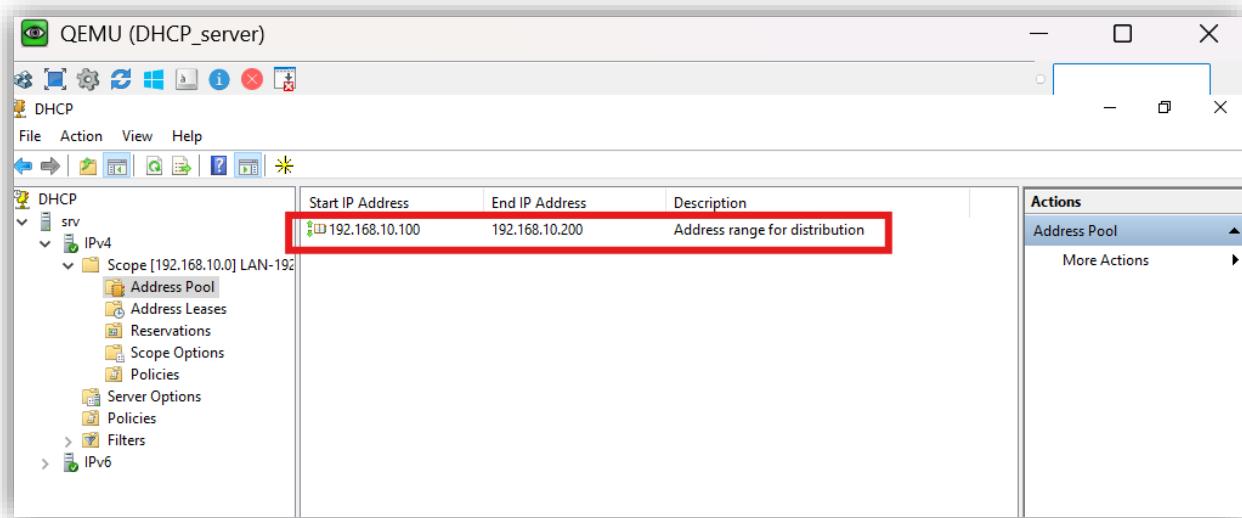
- 1** LAN Zone – where end-user devices are connected (192.168.10.x/24)
- 2** DHCP Zone – where the centralized DHCP server is installed (192.168.20.x/24)

According to our topology, the firewall is configured to act as a DHCP Relay Agent, ensuring that DHCP requests from the LAN zone are forwarded to the DHCP server in the DHCP zone.

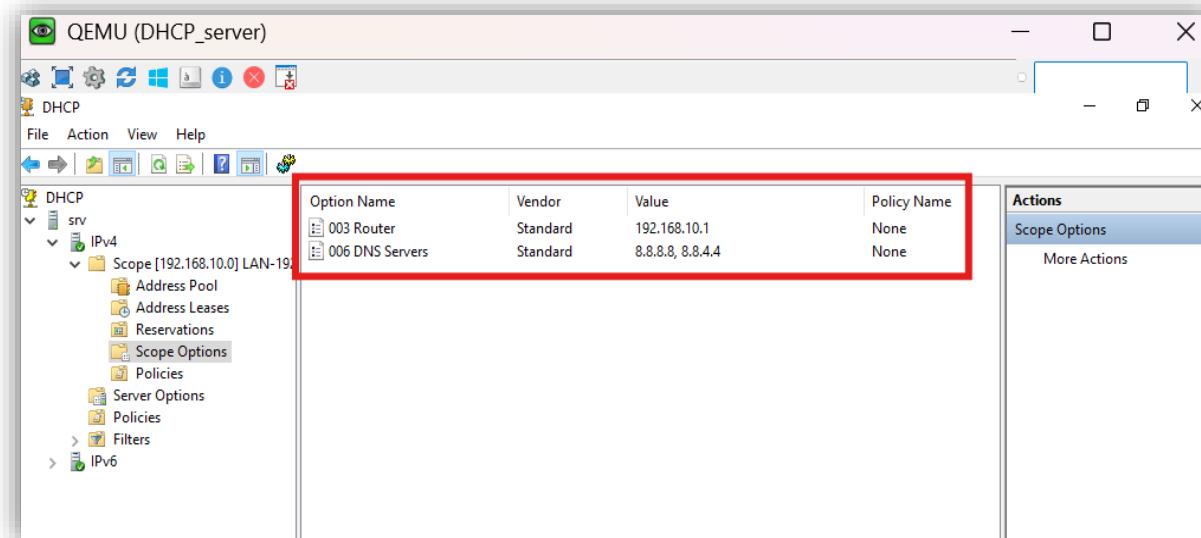
Steps to Configure DHCP with Relay

1. Install and Configure DHCP Server (Windows Server)

- Installed the DHCP Server role on Windows Server.
- Configured a DHCP scope:
 - IP Range: 192.168.10.100 – 192.168.10.200

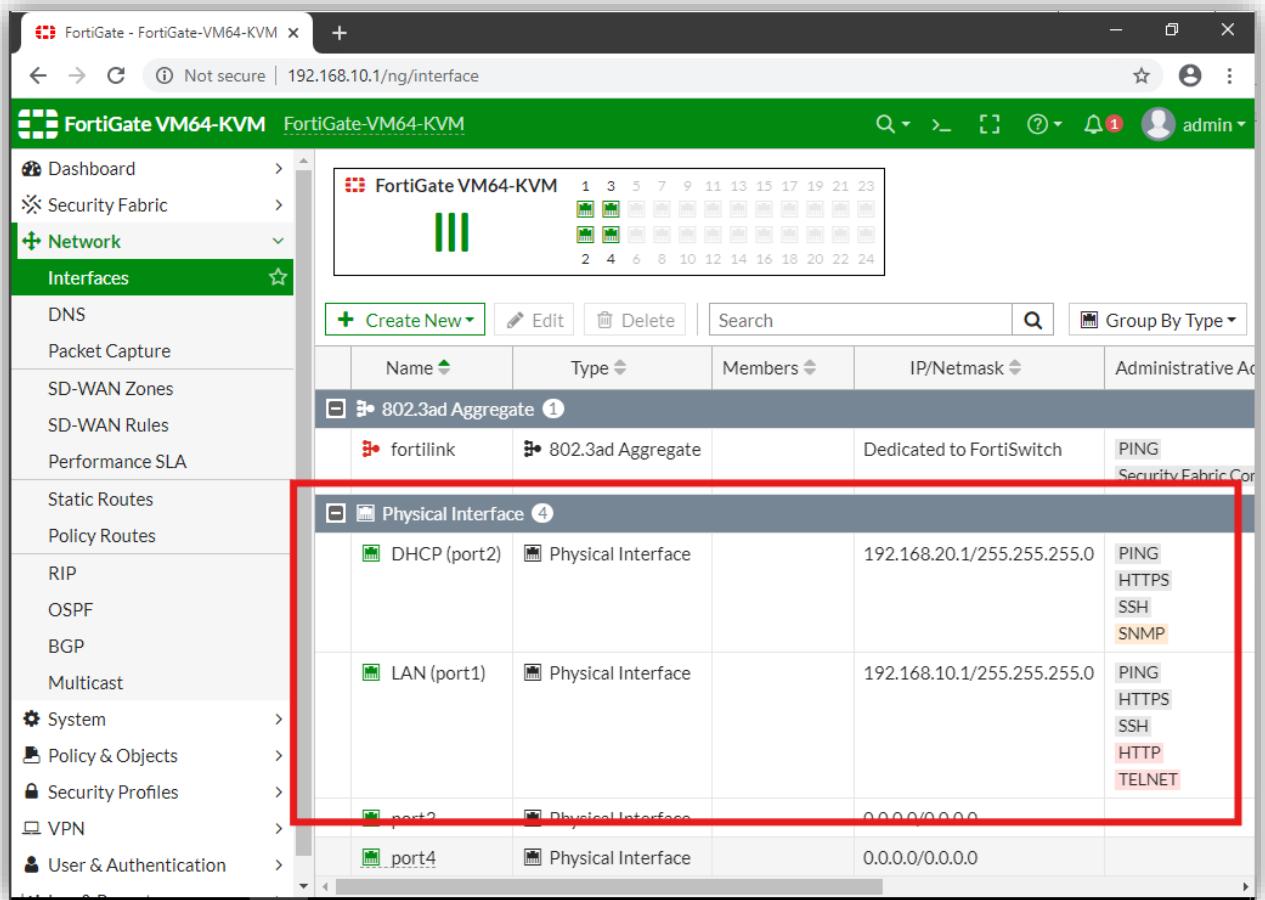


- Gateway: 192.168.10.1
- DNS Servers: 8.8.8.8, 8.8.4.4



2. Configure Firewall for DHCP Relay

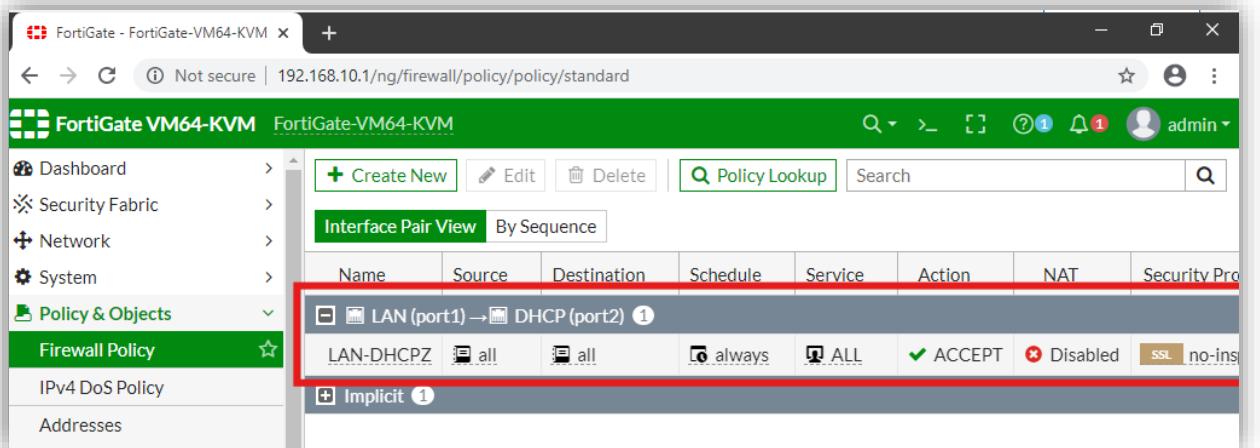
- Set up firewall interfaces: LAN and DHCP Zone.



The screenshot shows the FortiGate VM64-KVM interface configuration. The left sidebar navigation includes: Dashboard, Security Fabric, Network (selected), Interfaces (selected), DNS, Packet Capture, SD-WAN Zones, SD-WAN Rules, Performance SLA, Static Routes, Policy Routes, RIP, OSPF, BGP, Multicast, System, Policy & Objects, Security Profiles, VPN, User & Authentication. The main content area shows a summary of 24 ports, followed by a table of Physical Interfaces:

Name	Type	Members	IP/Netmask	Administrative
fortilink	802.3ad Aggregate			Dedicated to FortiSwitch
DHCP (port2)	Physical Interface		192.168.20.1/255.255.255.0	PING HTTPS SSH SNMP
LAN (port1)	Physical Interface		192.168.10.1/255.255.255.0	PING HTTPS SSH HTTP TELNET
port2	Physical Interface		0.0.0.0/0.0.0.0	
port4	Physical Interface		0.0.0.0/0.0.0.0	

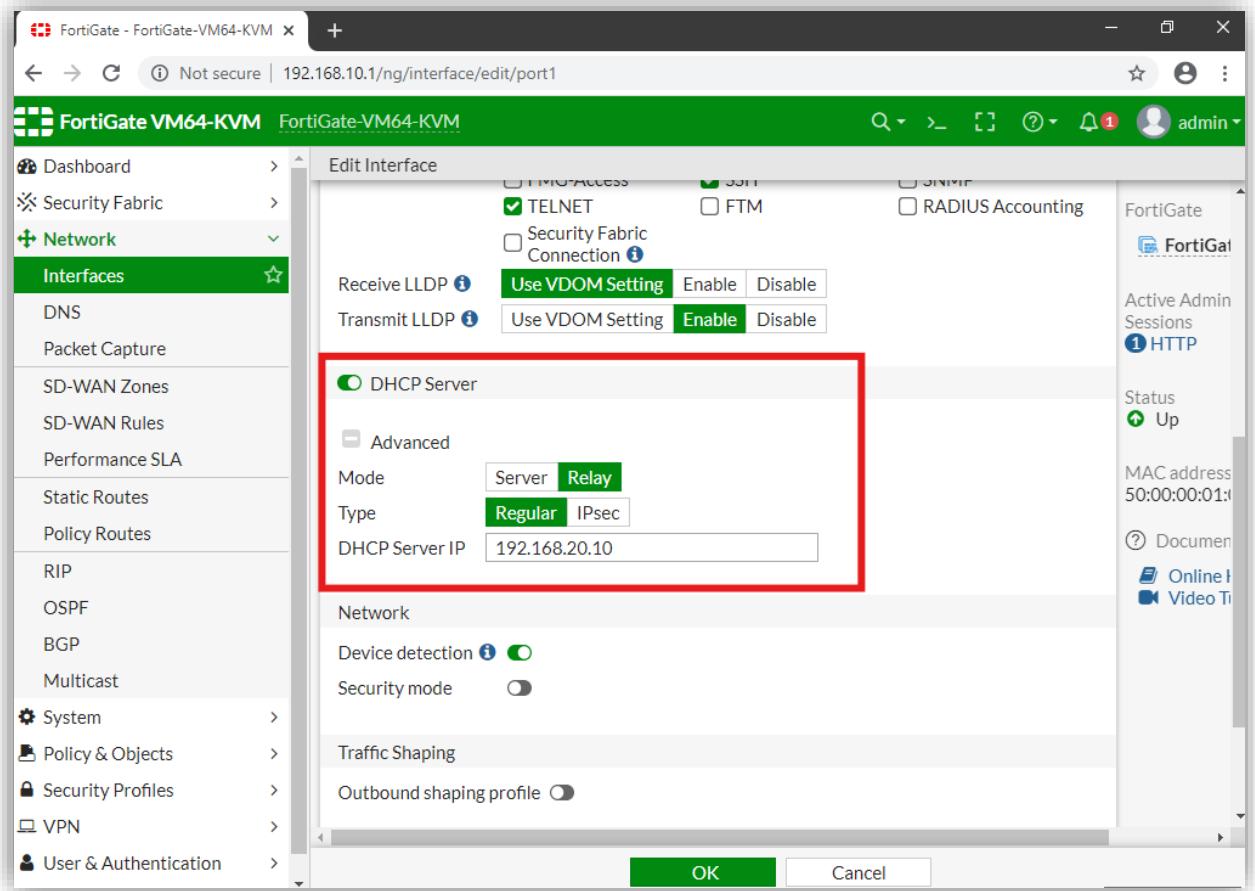
- Created a policy from LAN → DHCP Zone.



The screenshot shows the FortiGate VM64-KVM firewall policy configuration. The left sidebar navigation includes: Dashboard, Security Fabric, Network, System, Policy & Objects (selected), Firewall Policy (selected), IPv4 DoS Policy, Addresses. The main content area shows a table of Firewall Policies:

Name	Source	Destination	Schedule	Service	Action	NAT	Security
LAN-DHCPZ	all	all	always	ALL	ACCEPT	Disabled	SSL no-ins
Implicit							

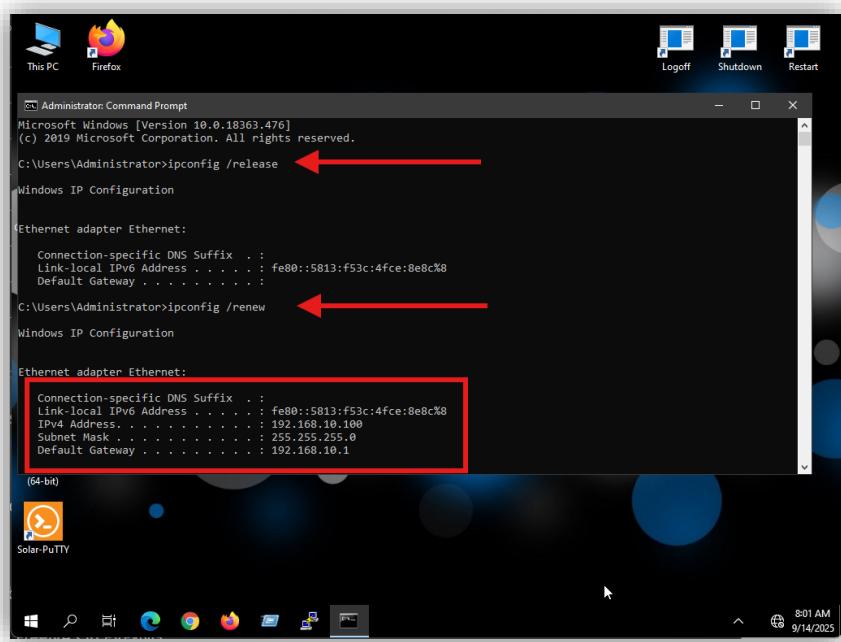
- On the LAN-side interface, enabled DHCP Relay instead of DHCP Server.



- Added the DHCP Server IP address as the relay target.

3. Verify DHCP Functionality

- On a LAN client PC:
 - Run ipconfig /release and ipconfig /renew to request a new IP.



```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.18363.476]
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ipconfig /release
Windows IP Configuration

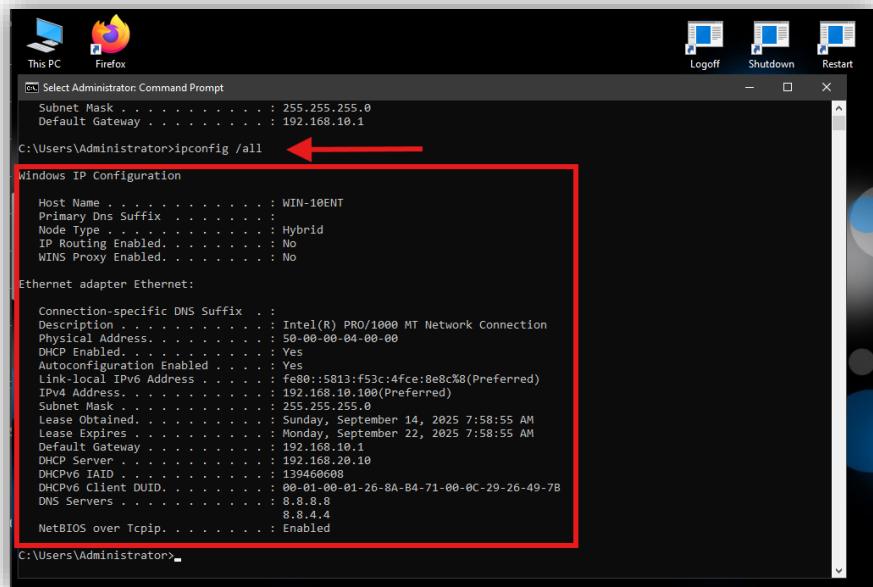
Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . . . . . : fe80::5813:f53c:4fce:8e8c%8
  Link-local IPv6 Address . . . . . : fe80::5813:f53c:4fce:8e8c%8
  Default Gateway . . . . . : 192.168.10.1

C:\Users\Administrator>ipconfig /renew
Windows IP Configuration

Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . . . . . : fe80::5813:f53c:4fce:8e8c%8
  IPv4 Address . . . . . : 192.168.10.100
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.10.1

```

- Used ipconfig /all to confirm the client received:
 - IP address from 192.168.10.100–200 range
 - Correct Gateway (192.168.10.1)
 - DNS servers (8.8.8.8, 8.8.4.4)



```

Administrator: Command Prompt
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.10.1

C:\Users\Administrator>ipconfig /all
Windows IP Configuration

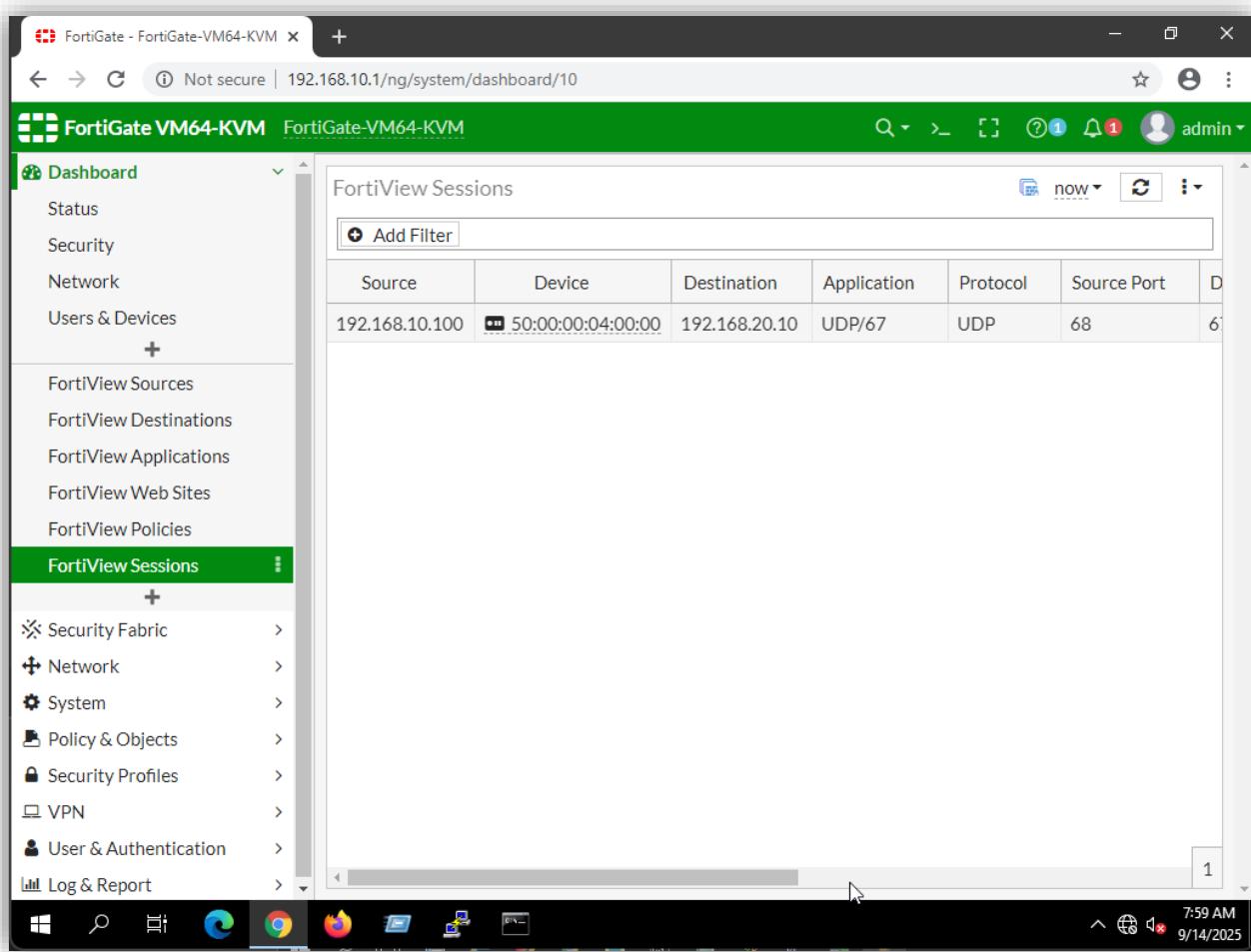
Host Name . . . . . : WIN-10ENT
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled . . . . . : No
WINS Proxy Enabled . . . . . : No

Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . . . . . : Intel(R) PRO/1000 MT Network Connection
  Description . . . . . : Intel(R) PRO/1000 MT Network Connection
  Physical Address . . . . . : 50-00-00-04-00-00
  DHCP Enabled . . . . . : Yes
  Auto-configuration Enabled . . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::5813:f53c:4fce:8e8c%8(Preferred)
  IPv4 Address . . . . . : 192.168.10.100(Preferred)
  Subnet Mask . . . . . : 255.255.255.0
  Lease Obtained . . . . . : Sunday, September 14, 2025 7:58:55 AM
  Lease Expires . . . . . : Monday, September 22, 2025 7:58:55 AM
  Default Gateway . . . . . : 192.168.10.1
  DHCP Server . . . . . : 192.168.20.10
  DHCPv6 IAID . . . . . : 139460608
  DHCPv6 Client DUID . . . . . : 00-01-00-01-26-8A-B4-71-00-0C-29-26-49-7B
  DNS Servers . . . . . : 8.8.8.8
                                         8.8.4.4
  NetBIOS over Tcpip . . . . . : Enabled

```

4. DHCP Relay Traffic Verification in Firewall

While monitoring the network using **FortiView**, we observed DHCP traffic passing through the firewall configured as a relay agent:



The screenshot shows the FortiView interface on a Windows desktop. The title bar reads "FortiGate - FortiGate-VM64-KVM". The address bar shows "Not secure | 192.168.10.1/ng/system/dashboard/10". The top navigation bar includes a search icon, a refresh icon, a help icon, a bell icon with a red notification, and a user icon for "admin". The left sidebar has a "Dashboard" section with "Status", "Security", "Network", and "Users & Devices" options, and a "FortiView Sessions" section with "FortiView Sources", "Destinations", "Applications", "Web Sites", and "Policies". The main content area is titled "FortiView Sessions" and shows a table with one row of data. The table columns are "Source", "Device", "Destination", "Application", "Protocol", and "Source Port". The data row is: "192.168.10.100", "50:00:00:04:00:00", "192.168.20.10", "UDP/67", "UDP", "68". A timestamp "now" and a refresh icon are at the top of the table. The bottom of the screen shows the Windows taskbar with icons for File Explorer, Start, Task View, Edge, Chrome, and File Explorer, and a system tray with a network icon, a battery icon, and the date and time "7:59 AM 9/14/2025".

Source	Device	Destination	Application	Protocol	Source Port
192.168.10.100	50:00:00:04:00:00	192.168.20.10	UDP/67	UDP	68

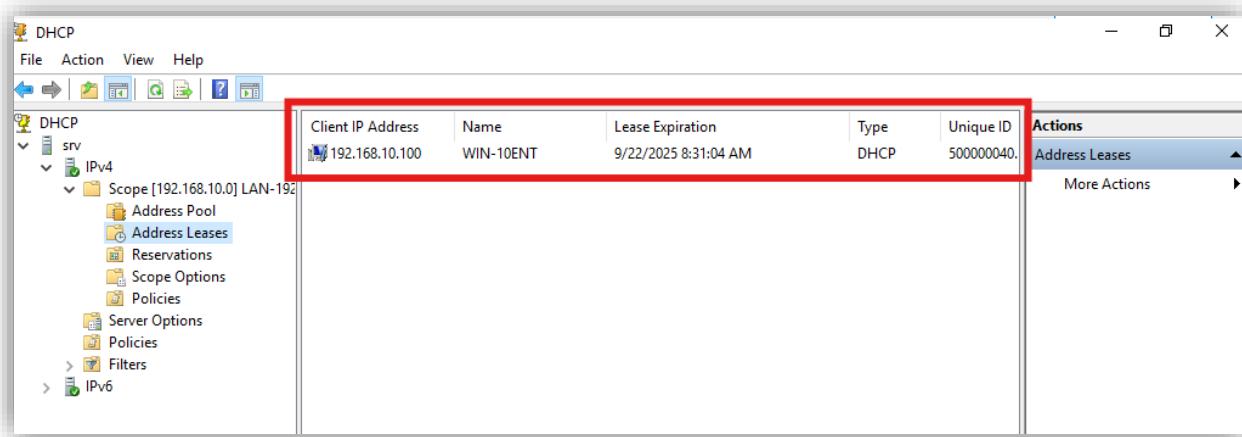
This confirms that the **client's DHCP request** from the LAN zone is successfully forwarded by the **firewall acting as a DHCP Relay Agent** to the DHCP server in the DHCP zone.

5. DHCP Leased Address Verification on Server

While checking the DHCP server leases, we verified that the assigned IP addresses for client PCs are correctly listed.

- This confirms that the DHCP server is successfully issuing IPs to clients through the firewall relay.

- Ensures that clients in the LAN zone receive valid IP configuration for network connectivity.



The screenshot shows the Microsoft DHCP Management console. The left pane displays a tree structure of DHCP configurations, including a 'Scope [192.168.10.0] LAN-192' node under 'IPv4'. The right pane is a table of client leases:

Client IP Address	Name	Lease Expiration	Type	Unique ID	Actions
192.168.10.100	WIN-10ENT	9/22/2025 8:31:04 AM	DHCP	500000040	Address Leases

◆ Conclusion

In this lab, we successfully demonstrated the use of a **firewall as a DHCP Relay Agent** to forward client requests from the LAN zone to a centralized DHCP server in a different network zone.

Key takeaways:

- DHCP Relay allows **centralized IP management** across multiple subnets without deploying DHCP servers on every network.
- FortiView verification confirmed that **client requests are correctly reaching the DHCP server** and responses are returned properly.
- Checking the DHCP server leases verified that **clients received valid IP addresses**, ensuring network connectivity.

This exercise highlights the importance of **relay agents in enterprise networks** for efficient, secure, and centralized DHCP management.

Thanks for your time!

Keep learning, and keep growing!....