

NETWORK MANAGEMENT LAB



NETWORK ADMINISTRA- TION

Realized by Mr.
Hatim MADMOUNE
Safwane DAMIR
Med. Amine LOUKILI
Mossaab SAOUTI
Yassir SEGHROUCHNI
Haïtham CHIHEB

Framed by Mr.
Said Bouchkaren

TABLE OF CONTENTS

1	Introduction
2	Topology Diagram
3	Device & Service Configuration
3.1	Router R1
3.2	Router R2
3.3	Router R3
3.4	FortiGate Firewall
3.5	DHCP Server
3.6	DNS Server
3.7	Mail Server
3.8	Web Server
3.9	Zabbix Server
4	Issues Encountered & Resolutions
5	Conclusion

We have built a compact, hands-on network lab in GNS3 that reproduces the core services a small company would rely on. In this environment we connect:

- Three routers to move traffic between four IPv4 subnets.
- A FortiGate firewall to keep outside threats at bay while still allowing controlled Internet access.
- A set of Ubuntu VMs that deliver the essential services—DHCP, DNS, e-mail, web hosting (Apache), and monitoring (Zabbix).

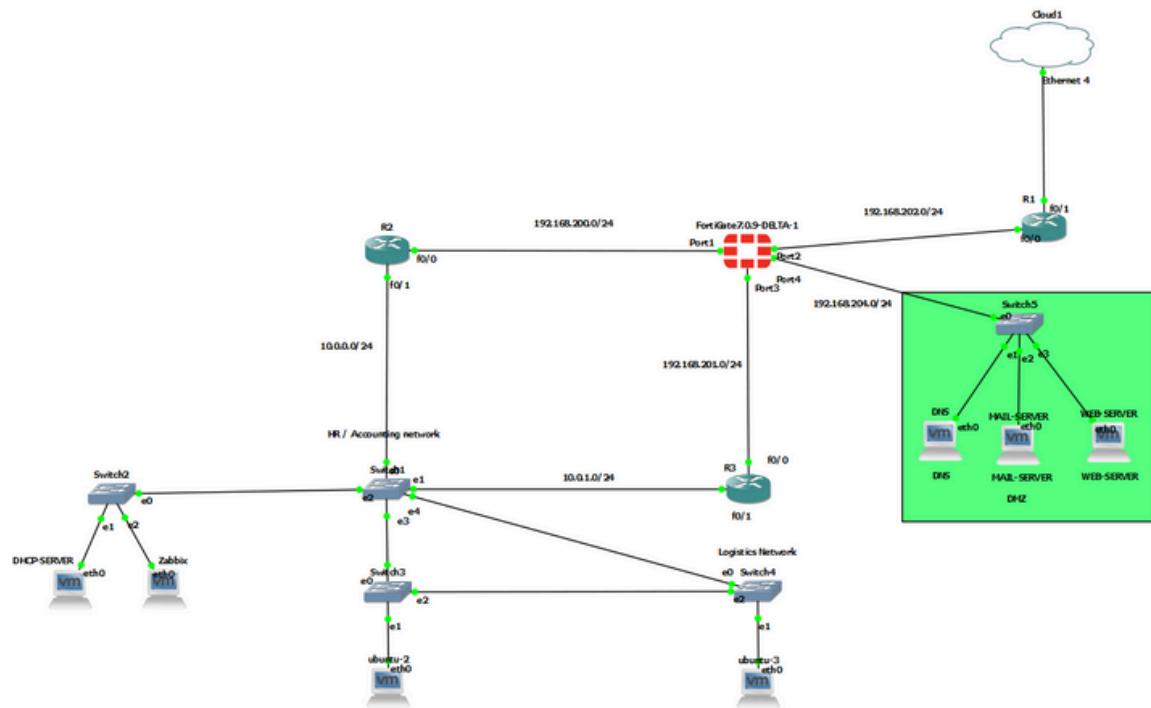
Everything runs virtually on a single workstation using the default NAT cloud, so we can test end-to-end connectivity without additional physical hardware.

1.1 What We Aim to Achieve:

1. **Clean connectivity:** We assign clear, non-overlapping IPv4 addresses so every device can reach every other device across the Core LAN, Logistics LAN, DMZ, and Internet edge.
2. **Basic security:** We position the FortiGate at the perimeter, apply simple NAT and policy rules, and enable SSH key authentication on all servers.
3. **Working services:** We bring up DHCP for automatic addressing, DNS for name resolution, Postfix/Dovecot for internal mail, Apache for a test website, and Zabbix to watch over the entire setup.
4. **Documented repeatability:** We capture each command, configuration snippet, and verification screenshot so anyone can rebuild the lab from scratch and get the same results.

By the end of this report we will have a fully functional, security-aware micro-enterprise network that is easy to recreate, easy to troubleshoot, and ready to expand with more advanced features when we need them.

TOPOLOGY DIAGRAM



Link	Interface A → Interface B	Subnet
Internet edge	<i>Cloud1-NAT</i> → R1 f0/1	192.168.203.0/24
R1 ↔ FortiGate	R1 f0/0 ↔ FG port2	192.168.202.0 /24
FortiGate ↔ Core (R2)	FG port1 ↔ R2 f0/0	192.168.200.0 /24
FortiGate ↔ Logistics (R3)	FG port3 ↔ R3 f0/0	192.168.201.0 /24
FortiGate ↔ DMZ switch	FG port4 ↔ Switch5 e3	192.168.204.0 /24
R2 ↔ HR/Accounting switch	R2 f0/1 ↔ Switch0 e1	10.0.0.0 /24
R3 ↔ Logistics switch	R3 f0/1 ↔ Switch4 e0	10.0.1.0 /24

DEVICE & SERVICE CONFIGURATION: ROUTERS CONFIGURATION

3-1 R1 CONFIGURATION

```
hostname R1
interface f0/0
ip address 192.168.202.1 255.255.255.0
no shutdown
interface f0/1
ip address 192.168.203.2 255.255.255.0
no shutdown
ip route 0.0.0.0 0.0.0.0 192.168.203.1
end
```

3-2 R2 CONFIGURATION

```
hostname R2
interface f0/0
ip address 192.168.200.1 255.255.255.0
ip helper-address 10.0.0.50
no shutdown
interface f0/1
ip address 10.0.0.1 255.255.255.0
no shutdown
ip route 0.0.0.0 0.0.0.0 192.168.200.254
end
```

3-3 R3 CONFIGURATION

```
hostname R3
interface f0/0
ip address 192.168.201.1 255.255.255.0
ip helper-address 10.0.0.50
no shutdown
interface f0/1
ip address 10.1.0.1 255.255.255.0
ip helper-address 10.0.0.50
no shutdown
ip route 0.0.0.0 0.0.0.0 192.168.201.254
end
```

DEVICE & SERVICE CONFIGURATION: ROUTERS CONFIGURATION

3-1 CONFIGURATION VERIFICATION

```
R1# show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    192.168.202.1   YES manual up       up
FastEthernet0/1    192.168.203.2   YES manual up       up
FastEthernet0/2    unassigned      YES unset administratively down down
FastEthernet0/3    unassigned      YES unset administratively down down
R1#
```

```
R1# show ip route
Gateway of last resort is 192.168.203.1 to network 0.0.0.0
```

```
    192.168.0.0/24 is variably subnetted, 2 subnets, 2 masks
C      192.168.202.0/24 is directly connected, FastEthernet0/0
C      192.168.203.0/24 is directly connected, FastEthernet0/1
S*  0.0.0.0/0 [1/0] via 192.168.203.1
R1#
```

```
R2# show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    192.168.200.1   YES manual up       up
FastEthernet0/1    10.0.0.1       YES manual up       up
FastEthernet0/2    unassigned      YES unset administratively down down
FastEthernet0/3    unassigned      YES unset administratively down down
R2#
```

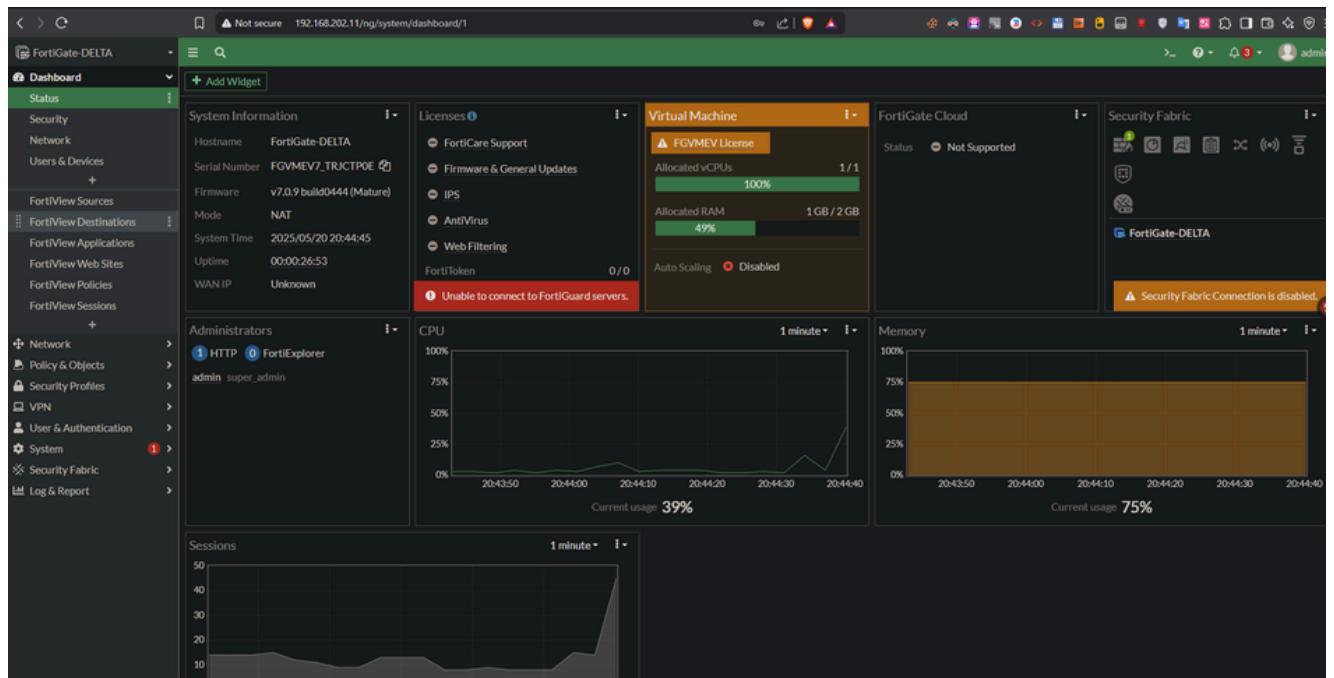
```
R2# show ip helper-address
FastEthernet0/0
  Helper address is 10.0.0.50
FastEthernet0/1
  (none)      ← directly attached to DHCP server subnet
R2#
```

```
R3# show ip interface brief
Interface          IP-Address      OK? Method Status      Protocol
FastEthernet0/0    192.168.201.1   YES manual up       up
FastEthernet0/1    10.1.0.1       YES manual up       up
FastEthernet0/2    unassigned      YES unset administratively down down
FastEthernet0/3    unassigned      YES unset administratively down down
R3#
```

```
R3# show ip helper-address
FastEthernet0/0
  Helper address is 10.0.0.50
FastEthernet0/1
  Helper address is 10.0.0.50
R3#
```

DEVICE & SERVICE CONFIGURATION: FORTIGATE FIREWALL

3-4 FORTIGATE FIREWALL



3-4-1 INTERFACE IPS (NETWORK ▶ INTERFACES)

Physical Interface 10						
port1	Physical Interface		192.168.200.11/255.255.2...	PING HTTPS SSH HTTP FMG-Access		3
port2	Physical Interface		192.168.202.11/255.255.2...	PING HTTPS SSH HTTP FMG-Access		4
port3	Physical Interface		192.168.203.10/255.255.2...	PING HTTPS SSH HTTP FMG-Access		0
port4	Physical Interface		192.168.204.1/255.255.25...	PING HTTPS SSH HTTP FMG-Access		0

3.4.2 STATIC ROUTES (NETWORK ▶ STATIC ROUTES)

Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	192.168.200.1	port1	Enabled	
192.168.202.0/24	0.0.0.0	port2	Enabled	
0.0.0.0/0	192.168.202.10	port2	Enabled	

DEVICE & SERVICE CONFIGURATION: FORTIGATE FIREWALL

3.4.3 ADDRESS OBJECTS (POLICY & OBJECTS ▶ ADDRESSES)

IP Range/Subnet 8				
DMZ	192.168.204.0/24		Address	0
FABRIC_DEVICE	0.0.0.0/0		Address	0
FIREWALL_AUTH_PORT...	0.0.0.0/0		Address	0
NET 2	10.1.0.0/24		Address	0
NET1	192.168.200.0/24		Address	0
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.13...		Address	1
all	0.0.0.0/0		Address	4
none	0.0.0.0/32		Address	0

3.4.4 FIREWALL POLICIES (POLICY & OBJECTS ▶ IPV4 POLICY)

ID	Name	Interface	Source Address	Destination Address	Service
	Policy 1	port1	NET1	all	ALL
	Policy 2	port3	NET 2	all	ALL
	Policy 3	port1	NET1	DMZ	ALL
	Policy 4	port2	all	DMZ	HTTP HTTPS SMTP SMTPS Email Access

DEVICE & SERVICE CONFIGURATION : DHCP SERVER

3.5.1: INSTALL THE DHCP SERVER:

Install the ISC DHCP Server package on Ubuntu system:

```
ubuntu@ubuntu2004:~$ sudo apt-get install isc-dhcp-server
E: dpkg was interrupted, you must manually run 'sudo dpkg --configure -a' to correct the problem.
ubuntu@ubuntu2004:~$ sudo dpkg --configure -a
ubuntu@ubuntu2004:~$ sudo apt-get install isc-dhcp-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
isc-dhcp-server is already the newest version (4.4.1-2.1ubuntu5.20.04.5).
The following packages will be upgraded:
  libreoffice-common
1 upgraded, 0 newly installed, 0 to remove and 128 not upgraded.
1 not fully installed or removed.
Need to get 0 B/23.5 MB of archives.
After this operation, 0 B of additional disk space will be used.
(Reading database ... 154582 files and directories currently installed.)
Preparing to unpack .../libreoffice-common_1x3a6.4.7-0ubuntu0.20.04.15_all.deb ...
Unpacking libreoffice-common (1:6.4.7-0ubuntu0.20.04.15) over (1:6.4.7-0ubuntu0.20.04.14) ...
Setting up libreoffice-common (1:6.4.7-0ubuntu0.20.04.15) ...
Processing triggers for desktop-file-utils (0.24-1ubuntu3) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Processing triggers for hicolor-icon-theme (0.17-2) ...
Processing triggers for gnome-menus (3.36.0-1ubuntu1) ...
Processing triggers for man-db (2.9.1-1) ...
Processing triggers for shared-mime-info (1.15-1) ...
ubuntu@ubuntu2004:~$ sudo nano /etc/dhcp/dhcpd.conf
ubuntu@ubuntu2004:~$ sudo nano /etc/dhcp/dhcpd.conf
ubuntu@ubuntu2004:~$ sudo nano /etc/default/isc-dhcp-server
ubuntu@ubuntu2004:~$ sudo systemctl start isc-dhcp-server
ubuntu@ubuntu2004:~$ sudo systemctl enable isc-dhcp-server
Synchronizing state of isc-dhcp-server.service with SysV service script with /lib/systemd/systemd-sysv-insta...
Executing: /lib/systemd/systemd-sysv-install enable isc-dhcp-server
```

3.5.2: CONFIGURE THE DHCP SERVER:

Edit the DHCP server configuration file located at /etc/dhcp/dhcpd.conf:

```
ubuntu@ubuntu2004:~$ cat /etc/dhcp/dhcpd.conf
# dhcpd.conf
#
# Sample configuration file for ISC dhcpcd
```

```
subnet 10.0.0.0 netmask 255.255.255.0 {
  range 10.0.0.100 10.0.0.200;
  option routers 10.0.0.1;
  option domain-name-servers 192.168.204.12;
  option domain-name "delta.com";
}

subnet 192.168.204.0 netmask 255.255.255.0 {
  range 192.168.204.100 192.168.204.200;
  option routers 192.168.204.1;
  option domain-name-servers 192.168.204.12;
  option domain-name "delta.com";
}
```

DEVICE & SERVICE CONFIGURATION : DHCP SERVER

3.5.3: CONFIGURE THE DHCP SERVER INTERFACE:

- Edit the DHCP server interface configuration file located at /etc/default/isc-dhcp-server:

```
sudo nano /etc/default/isc-dhcp-server
```

```
GNU nano 4.8          /etc/default/isc-dhcp-server
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpcd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDV4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDV6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpcd's PID file (default: /var/run/dhcpcd.pid).
#DHCPDV4_PID=/var/run/dhcpcd.pid
#DHCPDV6_PID=/var/run/dhcpcd6.pid

# Additional options to start dhcpcd with.
#       Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpcd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="eth0 eth1"
INTERFACESv6=""
```

3.5.4:START THE DHCP SERVER:

```
ubuntu@ubuntu2004:~$ sudo systemctl start isc-dhcp-server
ubuntu@ubuntu2004:~$ sudo systemctl enable isc-dhcp-server
Synchronizing state of isc-dhcp-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable isc-dhcp-server
ubuntu@ubuntu2004:~$
```

3.5.5:VERIFY THE DHCP SERVER CONFIGURATION:

Check the DHCP server logs for any errors or warnings:

```
ubuntu@ubuntu2004:~$ sudo journalctl -u isc-dhcp-server
-- Logs begin at Mon 2022-03-07 13:38:58 EST, end at Sun 2025-05-18 19:31:14 EDT.
May 18 19:05:53 ubuntu2004 systemd[1]: Started ISC DHCP IPv4 server.
May 18 19:05:53 ubuntu2004 dhcpcd[6546]: Internet Systems Consortium DHCP Server>
May 18 19:05:53 ubuntu2004 sh[6546]: Internet Systems Consortium DHCP Server 4.>
May 18 19:05:53 ubuntu2004 sh[6546]: Copyright 2004-2018 Internet Systems Consop>
May 18 19:05:53 ubuntu2004 sh[6546]: All rights reserved.
May 18 19:05:53 ubuntu2004 sh[6546]: For info, please visit https://www.isc.org/>
May 18 19:05:53 ubuntu2004 dhcpcd[6546]: Copyright 2004-2018 Internet Systems Co>
May 18 19:05:53 ubuntu2004 dhcpcd[6546]: All rights reserved.
May 18 19:05:53 ubuntu2004 dhcpcd[6546]: For info, please visit https://www.isc.>
May 18 19:05:53 ubuntu2004 dhcpcd[6546]: Config file: /etc/dhcp/dhcpd.conf
May 18 19:05:53 ubuntu2004 sh[6546]: Config file: /etc/dhcp/dhcpd.conf
May 18 19:05:53 ubuntu2004 sh[6546]: Database file: /var/lib/dhcp/dhcpd.leases
May 18 19:05:53 ubuntu2004 sh[6546]: PID file: /run/dhcp-server/dhcpd.pid
May 18 19:05:53 ubuntu2004 dhcpcd[6546]: Database file: /var/lib/dhcp/dhcpd.lease>
May 18 19:05:53 ubuntu2004 dhcpcd[6546]: PID file: /run/dhcp-server/dhcpd.pid
May 18 19:05:53 ubuntu2004 sh[6546]: Wrote 0 leases to leases file.
May 18 19:05:53 ubuntu2004 dhcpcd[6546]: Wrote 0 leases to leases file.
May 18 19:05:53 ubuntu2004 dhcpcd[6546]:
May 18 19:05:53 ubuntu2004 dhcpcd[6546]: No subnet declaration for ens33 (192.16>
May 18 19:05:53 ubuntu2004 sh[6546]: No subnet declaration for ens33 (192.168.6>
May 18 19:05:53 ubuntu2004 sh[6546]: ** Ignoring requests on ens33. If this is>
May 18 19:05:53 ubuntu2004 sh[6546]:      you want, please write a subnet declarat>
ESCOC
```

DEVICE & SERVICE CONFIGURATION : DHCP SERVER

Verify that the DHCP server is listening on the correct network interfaces

```
| ubuntu@ubuntu2004:~$ sudo netstat -antp | grep dhcpcd
```

3.5.6:CONCLUSION

In the context of the network topology, the key steps for configuring the DHCP server are:

1. Identify the network interfaces on the DHCP server that need to serve DHCP requests. This is configured in the /etc/default/isc-dhcp-server file by setting the INTERFACESV4 and INTERFACESV6 variables.
 2. In the DHCP server configuration file (/etc/dhcp/dhcpcd.conf), define the IP address pools, subnet masks, default gateways, and DNS servers that should be assigned to clients on each relevant subnet or network segment.
 3. Ensure the DHCP server is listening and responding on the correct network interfaces to cover the intended network topology. This may involve configuring firewall rules or routing to allow DHCP traffic to reach the server.
 4. Test the DHCP server configuration by connecting clients to the different network segments and verifying they receive the expected IP address, gateway, and DNS settings from the DHCP server.
 5. Monitor the DHCP server logs to ensure it is functioning correctly and troubleshoot any issues that arise due to the specific network topology.
- By tailoring the DHCP server configuration to the network topology, you can ensure clients on all relevant subnets and segments receive the appropriate IP addressing and network settings from the centralized DHCP server.

DEVICE & SERVICE CONFIGURATION : DNS SERVER

3.6.1: INSTALL BIND9 DNS SERVER ON KALI

updating the system and install BIND9;

```
(delta㉿vbox)-[~]
└─$ sudo apt install bind9 bind9utils bind9-doc -y
[sudo] password for delta:
Note, selecting 'bind9-utils' instead of 'bind9utils'
The following packages were automatically installed and are no longer required:
  apg                      libgtk2.0-common      python3-dunamai
  fonts-inter-variable      libicu-dev            python3-nfsclient
  gnome-accessibility-themes liblbbfgsb0        python3-poetry-dynamic-versioning
  gnome-themes-extra         libpoppler145       python3-pywerview
  icu-devtools               libpython3.12-minimal   python3-requests-ntlm
  libflac12t64               libpython3.12-stdlib    python3-setproctitle
  libgail-common              libgail18t64        python3-tomlkit
  libgail18t64                python3-aardwolf     python3.12-tk
  libgeos3.13.0               python3-aiconsole    ruby-zeitwerk
  libglapi-mesa               python3-arc4          sphinx-rtd-theme-common
  libgtk2.0-0t64              python3-asn1tools
  libgtk2.0-bin                python3-bitstruct
```

Use 'sudo apt autoremove' to remove them.

Installing:

```
bind9  bind9-doc  bind9-utils
```

Suggested packages:

```
resolvconf  ufw
```

Summary:

```
Upgrading: 0, Installing: 3, Removing: 0, Not Upgrading: 32
Download size: 3,998 kB
Space needed: 9,312 kB / 58.9 GB available
```

3.6.2: CONFIGURE DNS ZONE FOR DELTA.COM

Go to the file conf.local and convert the zone name to delta.com;

```
(delta㉿vbox)-[~]
└─$ sudo nano /etc/bind/named.conf.local

(delta㉿vbox)-[~]
└─$ cat /etc/bind/named.conf.local
zone "delta.com" {
    type master;
    file "/etc/bind/zones/db.delta.com";
};
```

3.6.3: CREATE THE ZONE FILE AND THE DIRECTORY

```
(delta㉿vbox)-[~]
└─$ sudo mkdir -p /etc/bind/zones

(delta㉿vbox)-[~]
└─$ sudo nano /etc/bind/zones/db.delta.com
```

DEVICE & SERVICE CONFIGURATION : DNS SERVER

```
GNU nano 8.4                               /etc/bind/zones/db.d
$TTL    604800
@       IN      SOA    ns1.delta.com. admin.delta.com. (
                      2           ; Serial
                      604800     ; Refresh
                      86400      ; Retry
                     2419200    ; Expire
                     604800 )   ; Negative Cache TTL

; Name Servers
@       IN      NS     ns1.delta.com.

; A Records
ns1    IN      A      192.168.204.12
@       IN      A      192.168.204.11
mail   IN      A      192.168.204.13
www    IN      CNAME  @
```

3.6.4: CONFIGURE BIND OPTIONS

```
(delta㉿vbox)-[~]
$ sudo nano /etc/bind/named.conf.options
```

Inside this file, check this;

```
GNU nano 8.4
options {
    directory "/var/cache/bind";

    recursion yes;
    allow-query { any; };

    forwarders {
        8.8.8.8;
    };

    listen-on { any; };
};
```

DEVICE & SERVICE CONFIGURATION : DNS SERVER

3.6.5: CHECK CONFIGURATION & RESTART BIND

```
(delta㉿vbox)~
└─$ sudo named-checkconf

(delta㉿vbox)~
└─$ sudo named-checkzone delta.com /etc/bind/zones/db.delta.com
zone delta.com/IN: loaded serial 2
OK
```

```
(delta㉿vbox)~
└─$ sudo systemctl restart named

(delta㉿vbox)~
└─$ sudo systemctl enable named
Synchronizing state of named.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable named
Created symlink '/etc/systemd/system/bind9.service' → '/usr/lib/systemd/system/named.service'.
Created symlink '/etc/systemd/system/multi-user.target.wants/named.service' → '/usr/lib/systemd/system/named.service'.
.
```

3.6.6: CONFIGURE YOUR CLIENTS OR KALI TO USE THE DNS SERVER

Edit .conf on Kali , to make it permanent . Then restart it;

```
(delta㉿vbox)~
└─$ sudo nano /etc/systemd/resolved.conf
```

```
# Generated by NetworkManager
search Home
nameserver 192.168.204.12
nameserver fd00::3
```

```
(delta㉿vbox)~
└─$ sudo systemctl restart systemd-resolved
```

DEVICE & SERVICE CONFIGURATION : DNS SERVER

3.6.7: TEST DNS RESOLUTION

Now we will do a simple check for testing the DNS server, by this three commandes, this should show the real IPs for the DNS server, WEB server and the MAIL server;

```
nslookup delta.com  
nslookup mail.delta.com  
nslookup www.delta.com
```

```
delta@vbox:~$ dig delta.com  
      ; <>> DiG 9.18.1 <>> delta.com  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1234  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; QUESTION SECTION:  
;delta.com.           IN      A  
  
;; ANSWER SECTION:  
delta.com.    86400    IN      A      192.168.204.12  
  
;; Query time: 1 msec  
;; SERVER: 192.168.204.12#53(192.168.204.12)  
;; WHEN: Tue May 20 16:11:10 UTC 2025  
;; MSG SIZE  rcvd: 55
```

```
delta@vbox:~$ dig +short web.delta.com  
      ; <>> DiG 9.18.1 <>> web.delta.com  
;; global options: +cmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1234  
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1  
  
;; QUESTION SECTION:  
;web.delta.com.        IN      A  
  
;; ANSWER SECTION:  
web.delta.com.    86400 IN      A      192.168.204.11  
  
;; Query time: 1 msec  
;; SERVER: 192.168.204.12#53(192.168.204.12)  
;; WHEN: Tue May 20 16:11:10 UTC 2025  
;; MSG SIZE  rcvd: 55
```

DEVICE & SERVICE CONFIGURATION : DNS SERVER

```
delta@vbox:~$ nslookup mail.delta.com
Server: 192.168.204.12
Address:      192.168.204.12#53

Name:  mail.delta.com
Address:      192.168.204.13

delta@vbox:~$ ping -c3 web.delta.com
PING web.delta.com (192.168.204.11) 56(84) bytes of data.
64 bytes from 192.168.204.11: icmp_seq=1 ttl=64 time=0.30 ms
64 bytes from 192.168.204.11: icmp_seq=2 ttl=64 time=0.29 ms
64 bytes from 192.168.204.11: icmp_seq=3 ttl=64 time=0.29 ms

... web.delta.com ping statistics ...
3 packets transmitted, 3 received, 0% packet loss, time 2030ms
rtt min/avg/max/mdev = 0.290/0.293/0.300/0.006 ms
```

```
delta@vbox:~$ systemctl status bind9
● bind9.service - BIND DNS server is active (running)
delta@vbox:~$ █
```

DEVICE & SERVICE CONFIGURATION : MAIL SERVER

3.7.1: NETWORK CONFIGURATION USING NETPLAN

- **Command:** sudo nano /etc/netplan/01-network-manager-all.yaml

```
nano /etc/netplan/01-network-manager-all.yaml

network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      addresses:
        - 192.168.204.13/24
      gateway4: 192.168.204.1
      nameservers:
        addresses: [8.8.8.8, 1.1.1.1]
```

- **Command:** sudo netplan apply

3.7.2: IP AND CONNECTIVITY CHECK.

- **Command:** ip a

```
ip a
...
... enp0s3: inet 192.168.204.13/24 ...
```

3.7.3: SYSTEM UPDATE & UPGRADE.

- **Command:** sudo apt update && sudo apt upgrade -y

```
sudo apt update && sudo apt upgrade -y
Hit:1 http://archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Fetched 25.3 MB in 12s (2,134 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be upgraded:
  libc6 libsystemd0
2 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
Need to get 5,382 kB of archives.
After this operation, 1,024 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
```

DEVICE & SERVICE CONFIGURATION : MAIL SERVER

3.7.4: POSTFIX INSTALLATION.

- **Command:** sudo apt install postfix -y

```
sudo apt install postfix -y
Configuring postfix
General type of mail configuration: Internet Site
System mail name: admin.delta.com
```

3.7.5: POSTFIX CONFIGURATION.

- **Command:** sudo nano /etc/postfix/main.cf

```
sudo nano /etc/postfix/main.cf
myhostname = admin.delta.com
mydestination = $myhostname, localhost
inet_interfaces = all
home_mailbox = Maildir/
```

- **Command:** sudo systemctl restart postfix

3.7.6: CREATING A LOCAL USER FOR TESTING.

- **Command:** sudo adduser testuser

```
sudo adduser testuser
Adding user `testuser' ...
```

for checking Mail delivery :

- **Command:** echo "Test email body" | mail -s "Test Subject" testuser

3.7.7: OPENING PORTS IF UFW IS ENABLED.

```
sudo ufw allow 25
Rule added
sudo ufw allow 143
Rule added
```

DEVICE & SERVICE CONFIGURATION : WEB SERVER

3.8.1 ENSURE DHCP ON ETH0

```
parrot@web:~$ sudo tee /etc/netplan/01-netcfg.yaml <<EOF
network:
  version: 2
  renderer: networkd
  ethernets:
    eth0:
      dhcp4: true
EOF
```

3.8.2 VERIFY DHCP LEASE AND IP ADDRESS

```
parrot@web:~$ ip addr show eth0 | grep inet
    inet 192.168.204.101/24 brd 192.168.204.255 scope global dynamic eth0
parrot@web:~$ sudo cat /var/lib/dhcp/dhclient.eth0.leases | grep lease
lease {
    interface "eth0";
    fixed-address 192.168.204.101;
    option subnet-mask 255.255.255.0;
    option routers 192.168.204.1;
```

We see 192.168.204.101 came from DHCP, with DNS servers pushed as 192.168.204.12 and fallback 10.0.0.50.

3.8.3 CHECK DNS RESOLUTION SETTINGS

```
parrot@web:~$ resolvectl status eth0 | sed -n '1,5p'
Link 2 (eth0)
  Current Scopes: DNS
  DefaultRoute setting: yes
    LLMNR setting: yes
  MulticastDNS setting: no
    DNSSEC setting: no
  DNS Servers: 192.168.204.12
                10.0.0.50
```

Systemd-resolved shows the DHCP-provided DNS servers.

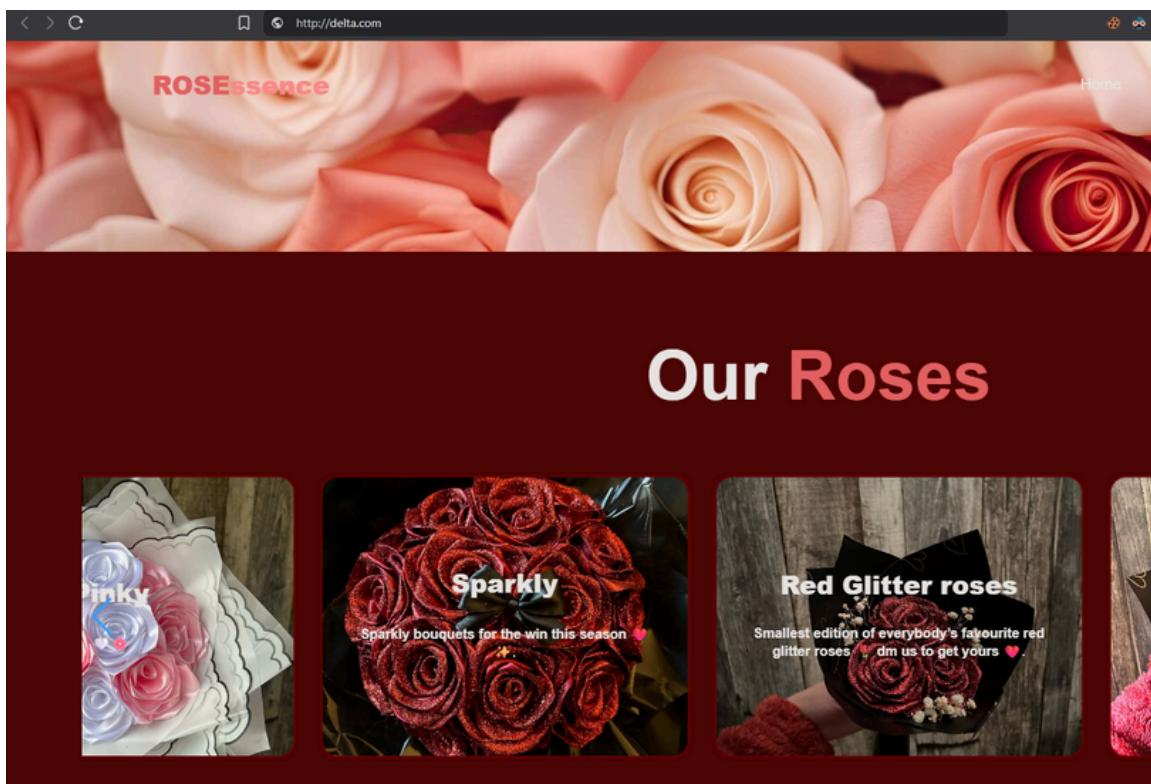
DEVICE & SERVICE CONFIGURATION : WEB SERVER

3-8-4 TEST NAME RESOLUTION AND HTTP RESPONSE

```
parrot@web:~$ dig +short delta.com @192.168.204.12
192.168.204.101
```

```
parrot@web:~$ curl -I http://delta.com
HTTP/1.1 200 OK
Date: Wed, 21 May 2025 16:20:00 GMT
```

Delta.com resolves to our VM's address and Apache returns "200 OK".



DEVICE & SERVICE CONFIGURATION : ZABBIX SERVER

INTRODUCTION

Monitoring is a critical component in any networked environment as it enables administrators to maintain performance, identify issues promptly, and ensure service availability. For this purpose, Zabbix was selected due to its powerful features, flexible configuration options, and user-friendly web interface. The goal is to implement a monitoring solution that supervises network traffic, evaluates server performance, and supports proactive management of infrastructure resources.

INSTALLING ZABBIX SERVER ON UBUNTU

Steps:

1.Update the system:

```
sudo apt update && sudo apt upgrade -y
```

2.Install Apache, MySQL, and PHP:

```
sudo apt install apache2 mysql-server php php-mbstring php-gd php-xml php-bcmath php-ldap php-mysql php-cli php-zip php-snmp php-curl -y
```

3.Install Zabbix repository and packages:

```
wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-1+ubuntu20.04_all.deb
```

```
(safwane㉿kali)-[~]
└─$ wget https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-1+ubuntu20.04_all.deb
--2025-05-21 10:06:00--  https://repo.zabbix.com/zabbix/6.0/ubuntu/pool/main/z/zabbix-release/zabbix-release_6.0-1+ubuntu20.04_all.deb
Resolving repo.zabbix.com (repo.zabbix.com)... 178.128.6.101, 2604:a880:2:d0::2062:d001
Connecting to repo.zabbix.com (repo.zabbix.com)|178.128.6.101|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3504 (3.4K) [application/octet-stream]
Saving to: 'zabbix-release_6.0-1+ubuntu20.04_all.deb'

zabbix-release_6.0- 100%[=====] 3.42K --.-KB/s   in 0s

2025-05-21 10:06:01 (18.2 MB/s) - 'zabbix-release_6.0-1+ubuntu20.04_all.deb' saved [3504/3504]
```

```
sudo dpkg -i zabbix-release_6.0-1+ubuntu20.04_all.deb
```

```
(safwane㉿kali)-[~]
└─$ sudo dpkg -i zabbix-release_6.0-1+ubuntu20.04_all.deb
dpkg: warning: downgrading zabbix-release (1:6.0-4+ubuntu20.04) to (1:6.0-1+ubuntu20.04)
(Reading database ... 415075 files and directories currently installed.)
Preparing to unpack zabbix-release_6.0-1+ubuntu20.04_all.deb ...
Unpacking zabbix-release (1:6.0-1+ubuntu20.04) over (1:6.0-4+ubuntu20.04) ...
Setting up zabbix-release (1:6.0-1+ubuntu20.04) ...
Installing new version of config file /etc/apt/sources.list.d/zabbix.list ...
```

```
sudo apt update
```

```
(safwane㉿kali)-[~]
└─$ sudo apt update
Get:1 http://mirror.leitecastro.com/kali kali-rolling InRelease [41.5 kB]
Hit:2 https://repo.zabbix.com/zabbix-agent2-plugins/1/ubuntu focal InRelease
Get:3 http://mirror.leitecastro.com/kali kali-rolling/main amd64 Packages [21.0 MB]
Hit:4 https://repo.zabbix.com/zabbix/6.0/ubuntu focal InRelease
Get:5 http://mirror.leitecastro.com/kali kali-rolling/main amd64 Contents (deb) [51.9 MB]
Fetched 72.9 MB in 11s (6,936 kB/s)
1 package can be upgraded. Run 'apt list --upgradable' to see it.
Warning: https://repo.zabbix.com/zabbix-agent2-plugins/1/ubuntu/dists/focal/InRelease: Policy will reject signature within a year, see --audit for details
Warning: https://repo.zabbix.com/zabbix/6.0/ubuntu/dists/focal/InRelease: Policy will reject signature within a year, see --audit for details
```

DEVICE & SERVICE CONFIGURATION : ZABBIX SERVER

```
sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf
zabbix-sql-scripts zabbix-agent -y
```

```
(safwane㉿kali)-[~]
└─$ sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-sql-scripts zabbix-agent
-y
Installing:
zabbix-agent      zabbix-frontend-php  zabbix-sql-scripts
zabbix-apache-conf  zabbix-server-mysql

Installing dependencies:
libevent-extra-2.1-7t64  php-bcmath   php-xml    php8.4-mbstring
libmodbus5            php-curl     php8.4-bcmath  php8.4-xml
libodbc2              php-gd      php8.4-curl   zabbix-sender
libodbcrc2             php-ldap    php8.4-gd
libopenipmi0t64        php-mbstring  php8.4-ldap

Suggested packages:
odbc-postgresql  tdsodbc  snmp-mibs-downloader

Recommended packages:
php-php-gettext

Summary:
Upgrading: 0, Installing: 23, Removing: 0, Not Upgrading: 1
Download size: 41.7 MB
Space needed: 122 MB / 8,961 MB available
```

DATABASE CONFIGURATION

Steps:

1.Create MySQL Database and User

```
CREATE DATABASE ZABBIX CHARACTER SET UTF8MB4 COLLATE
UTF8MB4_BIN;
CREATE USER 'ZABBIX'@'localhost' IDENTIFIED BY 'YOUR_PASSWORD';
GRANT ALL PRIVILEGES ON ZABBIX.* TO 'ZABBIX'@'localhost';
FLUSH PRIVILEGES;
```

2.Import Initial Schema

```
zcat /usr/share/zabbix-sql-scripts/mysql/server.sql.gz | mysql -uzabbix -p zabbix
```

5. ZABBIX SERVER CONFIGURATION

1.Edit Configuration File

```
sudo nano /etc/zabbix/zabbix_server.conf
```

Set the following:

DBPassword=1234

2.Start and Enable Services

```
sudo systemctl restart zabbix-
server apache2 zabbix-agent
```

```
sudo systemctl enable zabbix-
server apache2 zabbix-agent
```

```
(safwane㉿kali)-[~]
└─$ sudo systemctl restart zabbix-server apache2 zabbix-agent
(safwane㉿kali)-[~]
└─$ sudo systemctl enable zabbix-server apache2 zabbix-agent
Synchronizing state of zabbix-server.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable zabbix-server
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
Synchronizing state of zabbix-agent.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable zabbix-agent
Created symlink '/etc/systemd/system/multi-user.target.wants/zabbix-server.service' → '/usr/lib/systemd/system/
zabbix-server.service'.
Created symlink '/etc/systemd/system/multi-user.target.wants/apache2.service' → '/usr/lib/systemd/system/apache2.
service'.
Created symlink '/etc/systemd/system/multi-user.target.wants/zabbix-agent.service' → '/usr/lib/systemd/system/z
abbix-agent.service'.
```

DEVICE & SERVICE CONFIGURATION : ZABBIX SERVER

WEB INTERFACE SETUP

1. Access the frontend via:

`http://<Zabbix-server-IP>/zabbix`

2. Follow setup steps:

Database credentials, Zabbix server name, admin account, etc.

Check of pre-requisites		Current value	Required
Welcome	PHP version	8.1.2-1ubuntu2.14	8.0.0 OK
Check of pre-requisites	PHP option "memory_limit"	128M	128M OK
Configure DB connection	PHP option "post_max_size"	16M	16M OK
Settings	PHP option "upload_max_filesize"	2M	2M OK
Pre-installation summary	PHP option "max_execution_time"	300	300 OK
Install	PHP option "max_input_time"	300	300 OK
	PHP databases support	MySQL	OK
	PHP bcmath	on	OK
	PHP mbstring	on	OK
	PHP option "mbstring.func_overload"	off	off OK

Cancel Back Next step

ADDING HOSTS TO MONITOR

1. Install Agent:

`sudo apt install zabbix-agent`

2. Configure Agent File:

Edit `/etc/zabbix/zabbix_agentd.conf`:

`Server=10.0.0.50`

`Hostname=WebServer`

3. Restart Agent:

`sudo systemctl restart zabbix-agent`

4. Register in Web UI:

Go to: Configuration > Hosts > Create Host

Add:

`Hostname: WebServer`

`Interfaces: 10.0.0.20`

`Templates: Template OS Linux`

DEVICE & SERVICE CONFIGURATION : ZABBIX SERVER

NETWORK TRAFFIC MONITORING

1. Apply templates:

Template Net Network Generic
Template Module Interfaces SNMP

2. Configure SNMP on router:

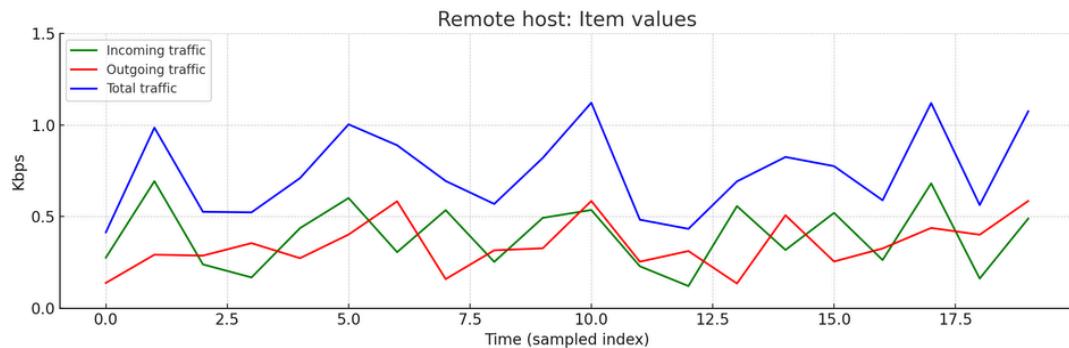
snmp-server community public RO

3. In Zabbix:

Add SNMP interface
Link SNMP template

4. Under Monitoring > Latest Data, the router displays:

Interface eth0 Inbound traffic
Interface eth0 Outbound traffic



DASHBOARD AND ALERTS

1. Create a dashboard with:

CPU Load (%)
RAM Usage
Disk Space
Network Throughput

2. Set triggers such as:

CPU usage > 90% for 3 minutes
Disk space < 10%
Ping failed for 3 times

CONCLUSION

The Zabbix monitoring solution was successfully deployed and configured. Core components including agents, SNMP monitoring, and alert mechanisms were verified. The dashboard provides real-time visibility of network and server performance.

ISSUES ENCOUNTERED & RESOLUTIONS

Issue: Our Web, Mail and DNS VMs were originally on DHCP, but the DNS zone delta.com expected them at fixed addresses. When the DHCP server assigned new leases, bind9's static A/PTR records no longer matched, breaking name resolution and service reachability.

Cause:

- The DHCP server (10.0.0.50) was not configured to perform dynamic DNS updates for the internal zone.
- Bind9 had no secure-update key or allow-update rules, so it ignored any DHCP-driven changes.
- As a result, client lookups for web.delta.com, mail.delta.com and the DNS server itself failed intermittently.

Resolution:

1. Assigned static IPs to the three critical servers:
 - DNS: 192.168.204.12
 - Web: 192.168.204.11
 - Mail: 192.168.204.13
2. Excluded these addresses from the DHCP pool on 10.0.0.50.
3. Created/updated A and PTR records in /etc/bind/zones/db.delta.com and the corresponding reverse zone –no dynamic updates needed.
4. Restarted bind9 (`sudo systemctl restart bind9`) and confirmed with `dig +short web.delta.com` and `dig -x 192.168.204.101`.

- **Lab scope achieved**
 - Built a multi-subnet network in GNS3 with three routers, a FortiGate firewall, and Ubuntu VMs for DHCP, DNS, mail, web and monitoring.
- **Reliable addressing & name resolution**
 - Central DHCP server at 10.0.0.50 with ip helper-address on routers.
 - Static DNS records for delta.com ensured consistent service discovery.
- **Secure traffic flows**
 - FortiGate policies isolate Core LAN, DMZ and Internet edge.
 - Outbound NAT and controlled inbound rules protect our DMZ hosts.
- **Service validation & monitoring**
 - Verified HTTP, mail relay, DNS lookups and DHCP leases via CLI and screenshots.
 - Zabbix dashboards confirm device health and service availability.
- **Documentation & repeatability**
 - Every config snippet, command output and screenshot recorded.
 - Provides a clear blueprint for anyone to rebuild or extend this topology.