Digital Egypt Pioneers

Design and Implementation of a Secure and Highly Available Network Infrastructure Using FortiGate Firewalls with Trust, Untrust, and DMZ Zones

Submitted by: John Armia

Training: Digital Egypt Pioneers Initiative

Group: DEPI_1_CAI1_ISS8_S1e Fortinet Cybersecurity Engineer

Round: 1

Acknowledgment

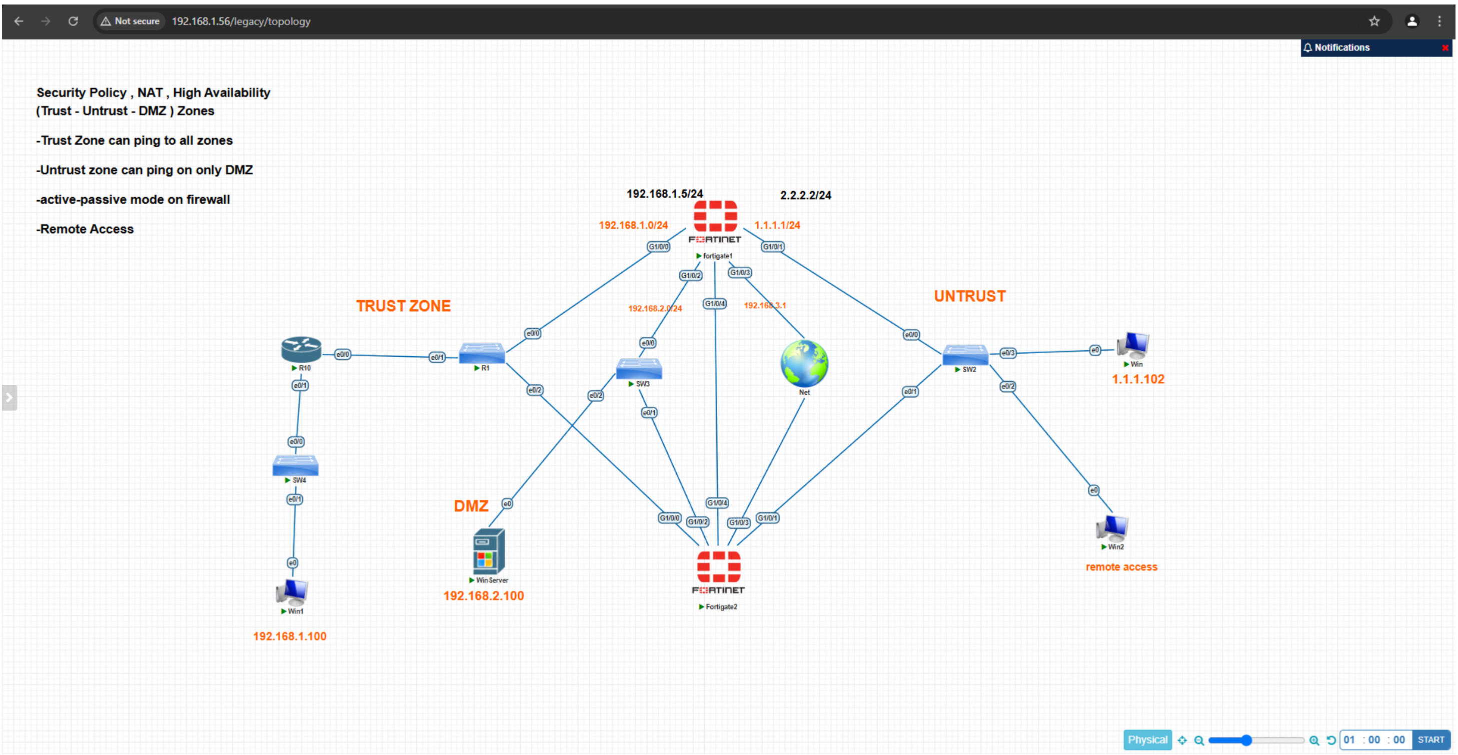
At first, Thanks to my **GOD** the most merciful the most gracious, for this moment has come and this work has been accomplished. Thanks to the **National Telecommunication Institute (NTI)** for preparing me to be a successful Engineer and lifting me up to achieve this training in an environment that's full of encouragement and motivation.

I would like to extend my heartfelt gratitude to the **Digital Egypt Pioneers Initiative** by the **Ministry of Communications and Information Technology (MCIT)** for providing me with the training and knowledge that made this project possible. The initiative’s exceptional programs and resources have equipped me with the technical expertise and practical skills required to design and implement this network infrastructure.

Your support and commitment to fostering technological advancement have been invaluable, and this project stands as a testament to the transformative impact of your initiative. Thank you for empowering me to achieve this milestone and contribute meaningfully to the field of IT and cybersecurity.

Table of Contents

Project Topology



Security Policy , NAT , High Availability
(Trust - Untrust - DMZ) Zones

-Trust Zone can ping to all zones

-Untrust zone can ping on only DMZ

-active-passive mode on firewall

-Remote Access

Objectives of the Project

The primary objective of this project is to design, configure, and secure a network infrastructure that adheres to best practices for security, availability, and performance. The network is built around two FortiGate firewalls in active-passive mode, ensuring high availability and robust security policies between three zones: **Trust**, **Untrust**, and **DMZ.** Below are the key objectives:

1. Security Policy

2. High Availability (HA)

3. Access Control

4. Secure Remote Access

5. Network Address Translation (NAT)

6. Scalability

7. Logging and Monitoring

8. Testing and Validation

Network Topology Overview

The network topology for this project involves two FortiGate firewalls configured in active-passive high availability (HA) mode and three distinct zones: **Trust**, **Untrust**, and **DMZ**. Below is an in-depth explanation of the topology:

1. Network Zones

The topology segregates traffic and enforces security policies using three logical zones:

- **Trust Zone**:
    - Represents the internal, secure network.
    - Contains trusted devices such as internal servers, routers, and switches.
    - Subnets:
        - 192.168.1.0/24 (internal devices, e.g., Win1).
        - 192.168.2.0/24 (additional internal network, e.g., R1, SW3).
    - Trust Zone has unrestricted access to all other zones (Untrust and DMZ).

- **DMZ Zone**:
    - Represents a semi-trusted zone, hosting services (e.g., web servers or public-facing resources) that are accessible from the internet.
    - Contains Windows Server with IP 192.168.2.100.
    - Accessible by both the Trust Zone and Untrust Zone, but isolated from internal networks.

- **Untrust Zone**:
    - Represents the external/public-facing network.
    - Contains internet-facing devices, such as:
        - Win with IP 1.1.1.102 (example of an external workstation).

        - Win2 (remote access device), which requires access to both Trust and DMZ zones.
    - Subnet: 1.1.1.0/24.

2. FortiGate Firewalls

The two FortiGate firewalls are deployed in **active-passive HA mode**:

- One firewall actively processes all traffic, while the other serves as a backup.
- Ensures high availability and minimal downtime in case of failure.

Firewall Interface Mapping:

- **G0/0**: Trust Zone (connected to internal networks 192.168.1.0/24 and 192.168.2.0/24).
- **G0/1**: Untrust Zone (connected to 1.1.1.0/24 and the internet).
- **G0/2**: DMZ Zone (connected to 192.168.2.100)

3. Security Policies

The topology enforces strict security rules between zones:

- **Trust Zone**:
    - Full access to Untrust and DMZ zones.
- **Untrust Zone**:
    - Limited access to DMZ Zone.
    - Specific access to Trust Zone only for remote access devices (Win2).
- **DMZ Zone**:
    - Isolated from the Untrust Zone except for allowed traffic.
    - Accessible from the Trust Zone for internal management.

4. High Availability (HA)

- The FortiGate firewalls operate in **active-passive mode**:
    - Ensures seamless failover during outages.
    - Monitors the active firewall’s health to automatically switch roles if needed.

5. Physical Topology

- Devices are interconnected with clear separation between zones:
  - **Switches**: Connect devices within the same zone.
  - **Routers**: Ensure inter-zone routing (as per the firewall’s rules).
  - **Internet**: Connects the Untrust Zone to external resources.

6. Traffic Flow Summary

- **Trust Zone**: Can access DMZ and Untrust Zone.
- **Untrust Zone**: Can access DMZ Zone and specific resources in Trust Zone (remote access).
- **DMZ Zone**: Hosts public-facing resources while maintaining isolation from critical internal systems.

Firewall Configuration Steps

Below is a step-by-step guide for configuring the FortiGate firewalls in your network. These steps cover interface setup, zone creation, NAT configuration, security policy definitions, remote access VPN, and high availability (HA) configuration. All commands are provided using FortiGate's CLI for precision and automation.

1. Initial Setup

- Connect to the FortiGate firewalls via console or SSH.

Set Hostname

```
config system global
```

```
   set hostname FortiGate1
end

config system global
   set hostname FortiGate2
end
```

Configure Basic Network Settings:

- Set management IP for each firewall (example IPs):

```
config system interface
   edit "mgmt."
      set ip 192.168.1.5/24
      set allowaccess ping http https ssh
   next
end
```

2. Configure Interfaces

Assign the interfaces to respective zones and configure IPs:

Trust Zone (Internal):

```
config system interface
   edit "port1"
```

```
        set mode static
        set ip 192.168.1.1/24
        set alias "Trust"
    next
end
```

Firewall Configuration Steps

Below is a step-by-step guide for configuring the FortiGate firewalls in your network. These steps cover interface setup, zone creation, NAT configuration, security policy definitions, remote access VPN, and high availability (HA) configuration. All commands are provided using FortiGate's CLI for precision and automation.

1. Initial Setup

- Connect to the FortiGate firewalls via console or SSH.

Set Hostname:

bash

Copy code

```
config system global
    set hostname FortiGate1
end

config system global
    set hostname FortiGate2
end
```

Configure Basic Network Settings:

- Set management IP for each firewall (example IPs):

```
config system interface
    edit "mgmt"
        set ip 192.168.1.5/24
        set allowaccess ping http https ssh
    next
end
```

2. Configure Interfaces

Assign the interfaces to respective zones and configure IPs:

Trust Zone (Internal):

```
config system interface
    edit "port1"
        set mode static
        set ip 192.168.1.1/24
        set alias "Trust"
    next
end
```

Untrust Zone (External):

```
config system interface
    edit "port2"
```

```
        set mode static
        set ip 1.1.1.1/24
        set alias "Untrust"
    next
end
```

DMZ Zone:

```
config system interface
    edit "port3"
        set mode static
        set ip 192.168.2.1/24
        set alias "DMZ"
    next
end
```

3. Create Zones

Organize interfaces into security zones:

```
config system zone
    edit "Trust"
        set interface "port1"
    next
    edit "Untrust"
```

```
        set interface "port2"
    next
    edit "DMZ"
        set interface "port3"
    next
end
```

4. Configure Static Routes

- Set default route for external internet access:

```
config router static
    edit 1
        set gateway 1.1.1.254
        set device "port2"
    next
end
```

5. Configure NAT (Network Address Translation)

Enable NAT for outbound traffic from Trust Zone to Untrust Zone:

```
config firewall ippool
    edit "NAT-Pool"
        set startip 1.1.1.100
        set endip 1.1.1.200
    next
```

```
end
config firewall policy
    edit 1
        set srcintf "Trust"
        set dstintf "Untrust"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
        set nat enable
        set ippool enable
        set poolname "NAT-Pool"
    next
end
```

6. Configure Security Policies

- Define inter-zone traffic rules based on requirements:

Trust Zone to All Zones:

```
config firewall policy
    edit 2
        set srcintf "Trust"
        set dstintf "DMZ"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
    next
    edit 3
        set srcintf "Trust"
        set dstintf "Untrust"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
    next
end
```

Untrust Zone to DMZ Zone:

```
config firewall policy
    edit 4
        set srcintf "Untrust"
        set dstintf "DMZ"
        set srcaddr "all"
        set dstaddr "all"
        set action accept
    next
end
```

Remote Access Device to Trust and DMZ Zones:

```
config firewall policy
    edit 5
        set srcintf "Untrust"
        set dstintf "Trust"
        set srcaddr "Remote-Device-IP"
        set dstaddr "all"
        set action accept
    next
    edit 6
        set srcintf "Untrust"
        set dstintf "DMZ"
        set srcaddr "Remote-Device-IP"
        set dstaddr "all"
        set action accept
    next
end
```

7. Configure High Availability (HA)

Enable HA in **active-passive** mode:

Primary (FortiGate1):

```
config system ha
```

```
    set mode a-p
    set group-name "FGT-HA"
    set password "HA-Password"
    set priority 200
    set hbdev "port4"
end
```

Secondary (FortiGate2):

```
config system ha
    set mode a-p
    set group-name "FGT-HA"
    set password "HA-Password"
    set priority 100
    set hbdev "port4"
end
```

8. Configure Remote Access VPN

- Allow remote access to Trust and DMZ zones.

Create VPN Settings:

```
config vpn ipsec phase1-interface
    edit "VPN-Remote"
        set interface "port2"
        set peertype any
        set proposal aes256-sha256
        set psksecret "your-vpn-key"
    next
end

config vpn ipsec phase2-interface
    edit "VPN-Remote-P2"
        set phase1name "VPN-Remote"
        set proposal aes256-sha256
    next
end
```

Allow VPN Traffic:

```
config firewall policy
    edit 7
        set srcintf "VPN-Remote"
        set dstintf "Trust"
        set action accept
    next
    edit 8
        set srcintf "VPN-Remote"
        set dstintf "DMZ"
        set action accept
```

Testing and Validation Steps

Once the configuration is complete, it is critical to test and validate the setup to ensure that all requirements are met, including zone access, NAT functionality, remote access, and high availability (HA). Here is a structured approach to testing and validation:

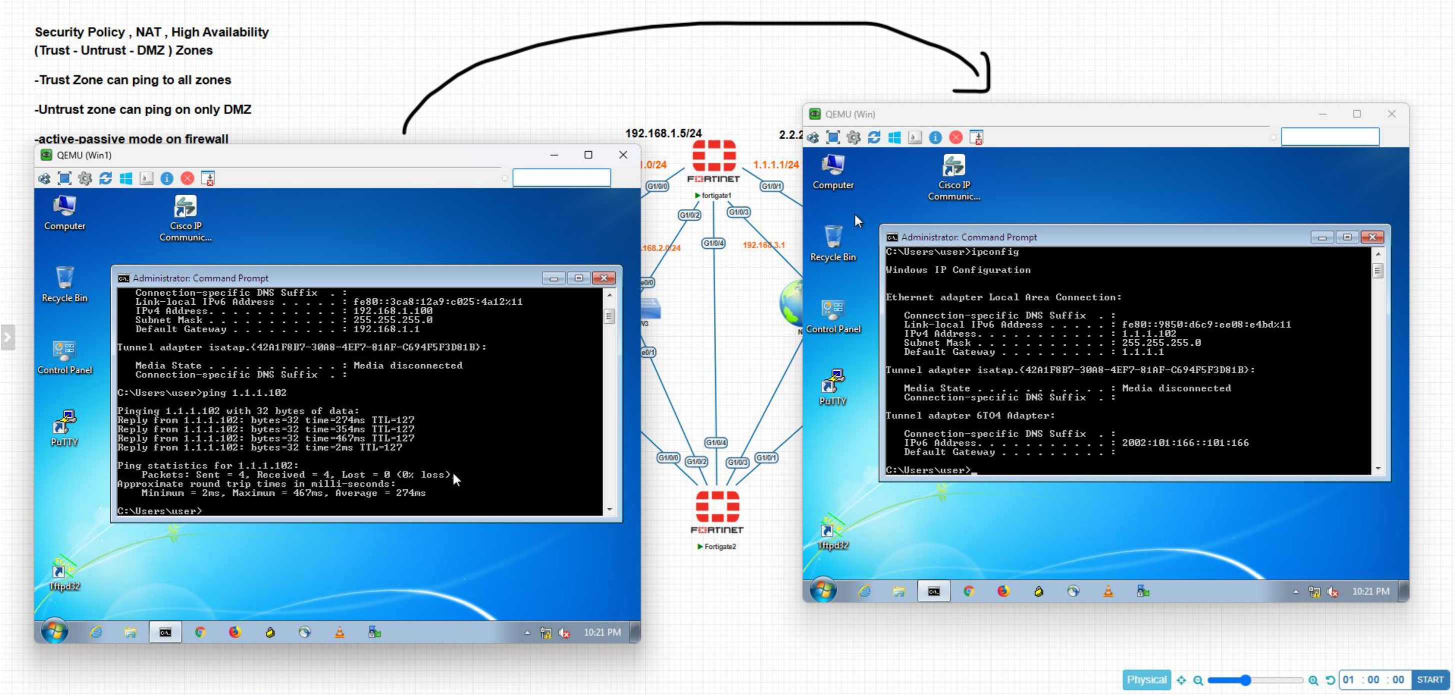
1. Connectivity Tests

- **Purpose**: Ensure that devices can communicate as per the security policies.
- **Tools**: Use ping, traceroute, and network monitoring tools.

Tests:

Trust Zone to Untrust Zone:

- From a device in the Trust Zone (192.168.1.100), ping in the Untrust device (1.1.1.102):



Security Policy , NAT , High Availability
(Trust - Untrust - DMZ) Zones

-Trust Zone can ping to all zones

-Untrust zone can ping on only DMZ

-active-passive mode on firewall

Administrator: Command Prompt

```
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3ca8:12a9:c025:4a12%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.{42A1F8B7-30A8-4EF7-81AF-C694F5F3D81B}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\user>ping 1.1.1.102

Pinging 1.1.1.102 with 32 bytes of data:
Reply from 1.1.1.102: bytes=32 time=274ms TTL=127
Reply from 1.1.1.102: bytes=32 time=354ms TTL=127
Reply from 1.1.1.102: bytes=32 time=467ms TTL=127
Reply from 1.1.1.102: bytes=32 time=2ms TTL=127

Ping statistics for 1.1.1.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 467ms, Average = 274ms

C:\Users\user>
```

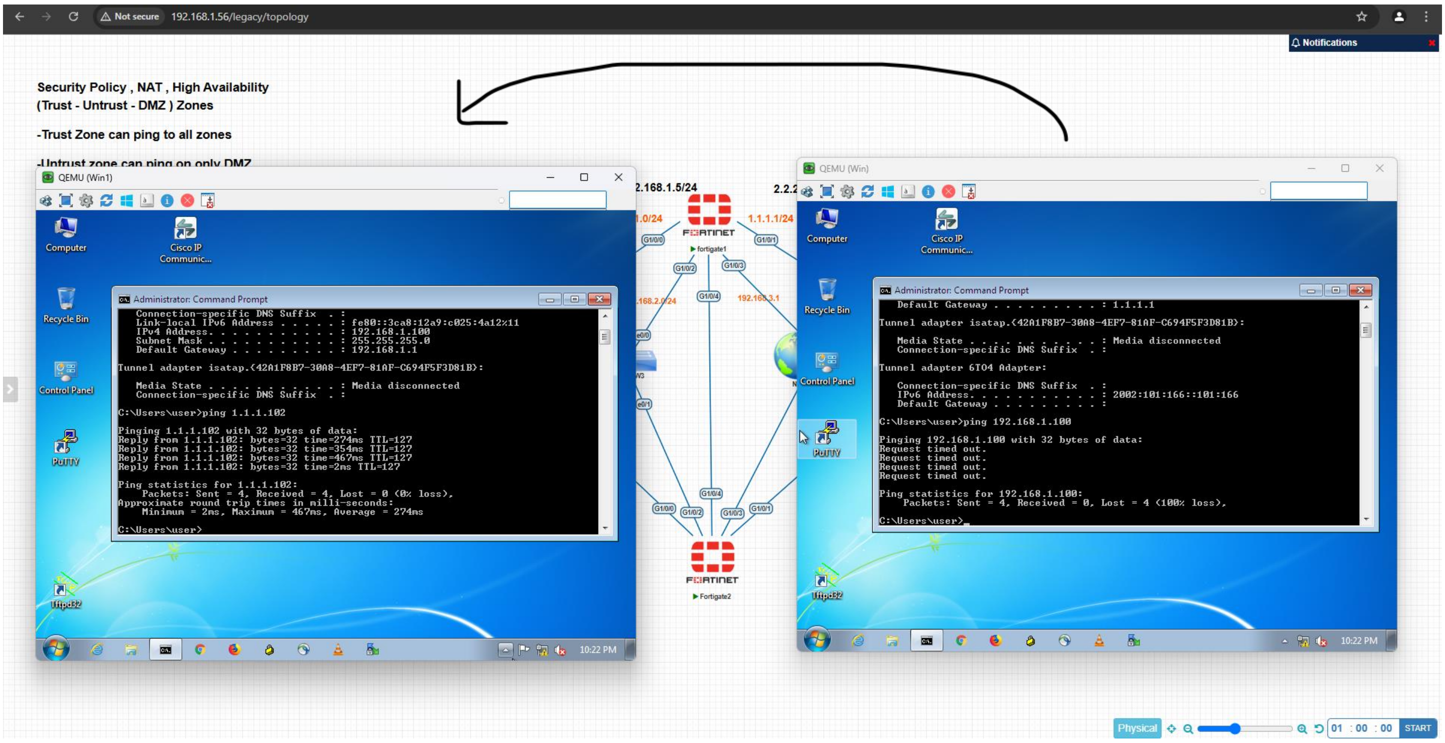
Administrator: Command Prompt

```
C:\Users\user>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9850:d6c9:ee08:e4bd%11
   IPv4 Address. . . . . . . . . . . : 1.1.1.102
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 1.1.1.1

Tunnel adapter isatap.{42A1F8B7-30A8-4EF7-81AF-C694F5F3D81B}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter 6TO4 Adapter:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2002:101:166::101:166
   Default Gateway . . . . . . . . . :

C:\Users\user>_
```

Reply from 1.1.1.102

Untrust Zone to Trust Zone:

- From a device in the Untrust Zone (1.1.1.102) to ping the trust device (192.168.1.100):



Security Policy , NAT , High Availability
(Trust - Untrust - DMZ) Zones

-Trust Zone can ping to all zones

-Untrust zone can ping on only DMZ

QEMU (Win1)

Administrator: Command Prompt

```
   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3ca8:12a9:c025:4a12%11
   IPv4 Address. . . . . . . . . . . : 192.168.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.1.1

Tunnel adapter isatap.{42A1F8B7-30A8-4EF7-81AF-C694F5F3D81B}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\user>ping 1.1.1.102

Pinging 1.1.1.102 with 32 bytes of data:
Reply from 1.1.1.102: bytes=32 time=274ms TTL=127
Reply from 1.1.1.102: bytes=32 time=354ms TTL=127
Reply from 1.1.1.102: bytes=32 time=467ms TTL=127
Reply from 1.1.1.102: bytes=32 time=2ms TTL=127

Ping statistics for 1.1.1.102:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 467ms, Average = 274ms

C:\Users\user>
```

QEMU (Win)

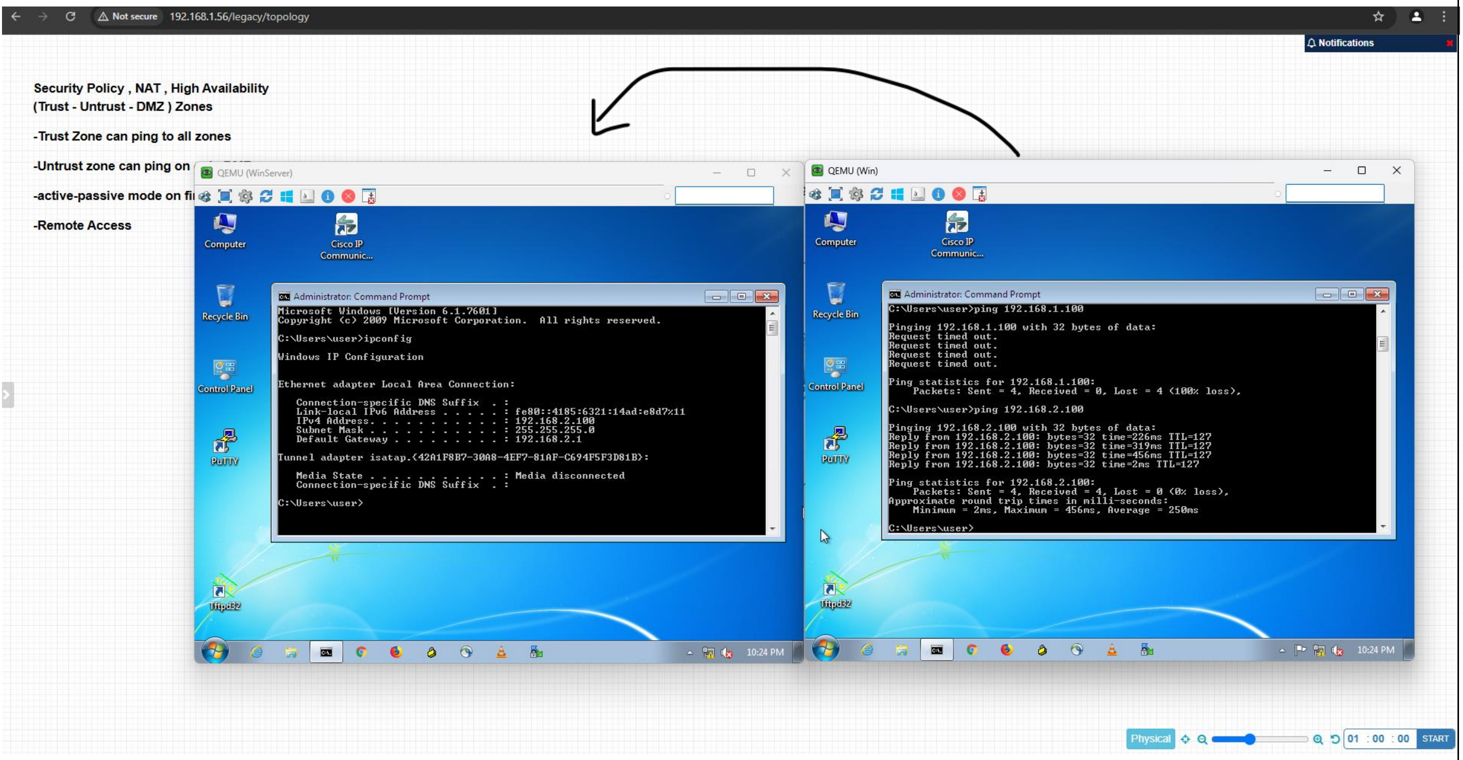
Administrator: Command Prompt

```
   Default Gateway . . . . . . . . . : 1.1.1.1

Tunnel adapter isatap.{42A1F8B7-30A8-4EF7-81AF-C694F5F3D81B}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter 6TO4 Adapter:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2002:101:166::101:166
   Default Gateway . . . . . . . . . :

C:\Users\user>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\user>_
```

Request timed out.

Untrust Zone to DMZ Zone:

- From a device in the Untrust Zone (1.1.1.102) to ping the DMZ Windows server (192.168.2.100):



Security Policy , NAT , High Availability
(Trust - Untrust - DMZ) Zones

-Trust Zone can ping to all zones

-Untrust zone can ping on

-active-passive mode on fi

-Remote Access

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\user>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4185:6321:14ad:e8d7%11
   IPv4 Address. . . . . . . . . . . : 192.168.2.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.2.1

Tunnel adapter isatap.{42A1F8B7-30A8-4EF7-81AF-C694F5F3D81B}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\user>
```

```
C:\Users\user>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\user>ping 192.168.2.100

Pinging 192.168.2.100 with 32 bytes of data:
Reply from 192.168.2.100: bytes=32 time=226ms TTL=127
Reply from 192.168.2.100: bytes=32 time=319ms TTL=127
Reply from 192.168.2.100: bytes=32 time=456ms TTL=127
Reply from 192.168.2.100: bytes=32 time=2ms TTL=127

Ping statistics for 192.168.2.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 456ms, Average = 250ms

C:\Users\user>
```

Reply from 192.168.2.100

2. Security Policy Validation

- **Purpose**: Verify that access between zones adheres to the defined security policies.
- **Tools**: Use network monitoring or firewall logs to validate traffic flow.

Tests:

1. **Allow Rules**:
   - Confirm that traffic from Trust Zone can access both DMZ and Untrust Zones.
   - Verify that Untrust Zone traffic can only access DMZ Zone and specific Trust Zone resources.
2. **Deny Rules**:
   - Attempt to access restricted zones (e.g., Untrust Zone to Trust Zone).
   - Ensure the traffic is blocked.

Expected Results:

- Traffic adheres to the allow/deny rules defined in the security policies.

3. NAT Functionality

- **Purpose**: Verify that NAT translates private IP addresses correctly for internet access.
- **Tools**: Check the source IP of outbound traffic using a packet capture tool.

Tests:

1. From a Trust Zone device, access an external website (e.g., using curl or a browser):

```
curl http://example.com
```

2. Perform packet captures on the Untrust Zone interface (e.g., port2) to verify the source IP is translated to the public NAT pool.

Expected Results:

- Outbound traffic from Trust Zone devices appears with the NATed IP from the NAT pool.

4. Remote Access VPN

- **Purpose**: Verify that the remote access VPN is configured and operational.

Tests:

1. From the remote access device (Win2), initiate a VPN connection using the configured IPsec VPN settings.
2. Once connected, ping resources in both the Trust and DMZ Zones:
   - Trust Zone: 192.168.1.100
   - DMZ Zone: 192.168.2.100
3. Verify VPN logs on the firewall:

bash

Copy code

```
execute log display | grep VPN
```

Expected Results:

- VPN connection is established successfully.
- Remote device can access the allowed resources in the Trust and DMZ Zones.

5. High Availability (HA)

- **Purpose**: Test failover functionality between the primary and secondary firewalls.
- **Tools**: FortiGate CLI and monitoring tools.

Tests:

1. Verify HA status on the primary firewall:

```
get system ha status
```

2. Manually trigger a failover by shutting down the primary firewall or disconnecting its heartbeat interface (port4).
3. Verify that the secondary firewall takes over as the primary:

```
get system ha status
```

4. Test connectivity by repeating basic ping tests during the failover.

.

Conclusion

This project successfully demonstrates the implementation of a secure, high-availability network infrastructure using two FortiGate firewalls operating in active-passive mode. By segmenting the network into **Trust**, **Untrust**, and **DMZ** zones, applying robust security policies, and enabling NAT, the network meets modern security and scalability requirements.

Key outcomes of this project include:

1. **Enhanced Security**:

   Proper segmentation and strict access controls ensure that sensitive resources in the Trust Zone are protected.

   Only authorized traffic is allowed between zones, minimizing the attack surface.

2. **High Availability (HA)**:

   The active-passive configuration of the firewalls ensures continuous network availability even during hardware or software failures.

3. **Secure Remote Access**:

   Remote users in the Untrust Zone can securely access resources in the Trust and DMZ Zones using IPsec VPN.

4. **Effective NAT Implementation**:

   Internal resources can communicate with external networks securely, while hiding private IP addresses from the public network.

5. **Scalability and Flexibility**:

   The configuration is designed to support future expansion, such as adding new zones or devices, without significant reconfiguration.