Firewall Task – Interview Q&A; and Practical Steps

Interview Questions and Answers

1. What is a firewall?

A firewall is a security system designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks.

2. Difference between stateful and stateless firewall?

Stateless firewalls filter packets based only on predefined rules, treating each packet independently. Stateful firewalls track the state of connections and make decisions based on the context of the traffic.

3. What are inbound and outbound rules?

Inbound rules control incoming traffic to your device. Outbound rules control outgoing traffic from your device.

4. How does UFW simplify firewall management?

UFW (Uncomplicated Firewall) is a user-friendly interface to manage iptables on Linux. It simplifies firewall rule management with easy-to-remember commands.

5. Why block port 23 (Telnet)?

Port 23 is used by Telnet, which transmits data in plaintext, making it insecure. Blocking it prevents unauthorized remote access.

6. What are common firewall mistakes?

Common mistakes include allowing unnecessary ports, not updating rules, or misconfiguring rules that block important traffic.

7. How does a firewall improve network security?

A firewall filters out malicious or unwanted traffic, prevents unauthorized access, and enforces security policies to protect systems.

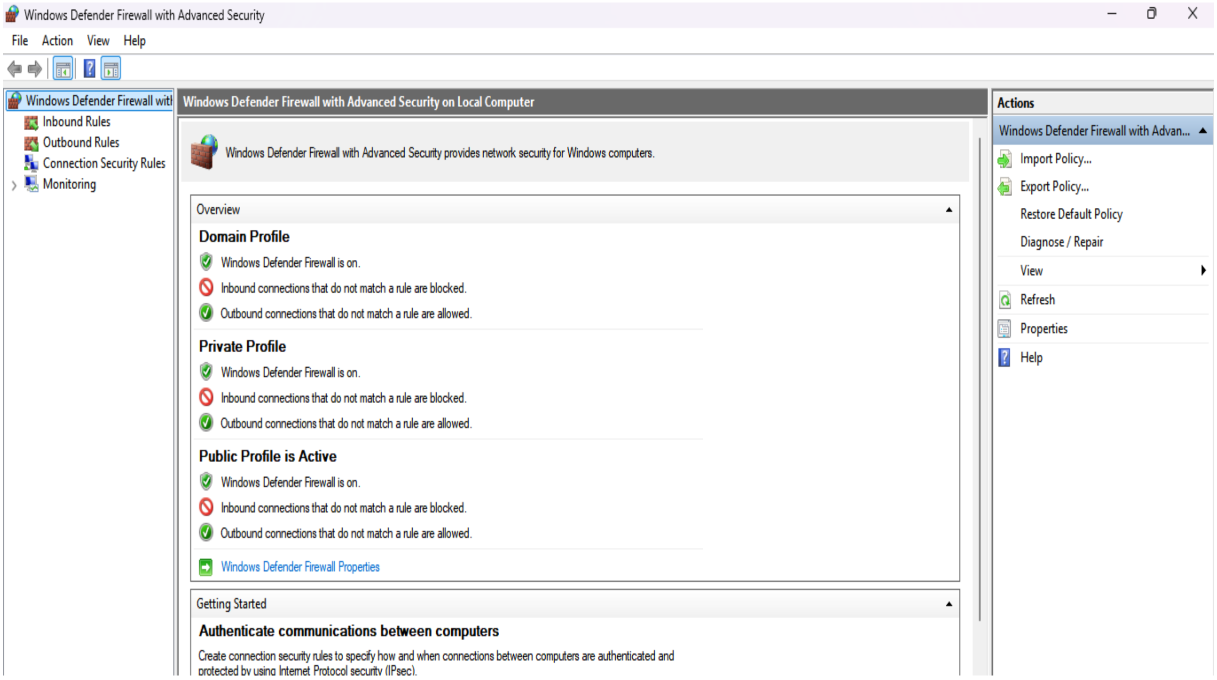
8. What is NAT in firewalls?

NAT (Network Address Translation) allows private IP addresses to communicate with the internet using a shared public IP. It enhances security by hiding internal IP addresses.

Step-by-Step Explanation with Screenshots

Step 1: Open Windows Firewall

We accessed the Windows Defender Firewall with Advanced Security to manage firewall rules. This tool allows detailed configuration of inbound/outbound network rules.



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

✓ Windows Defender Firewall is on.
⊘ Inbound connections that do not match a rule are blocked.
✓ Outbound connections that do not match a rule are allowed.

Private Profile

✓ Windows Defender Firewall is on.
⊘ Inbound connections that do not match a rule are blocked.
✓ Outbound connections that do not match a rule are allowed.

Public Profile is Active

✓ Windows Defender Firewall is on.
⊘ Inbound connections that do not match a rule are blocked.
✓ Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

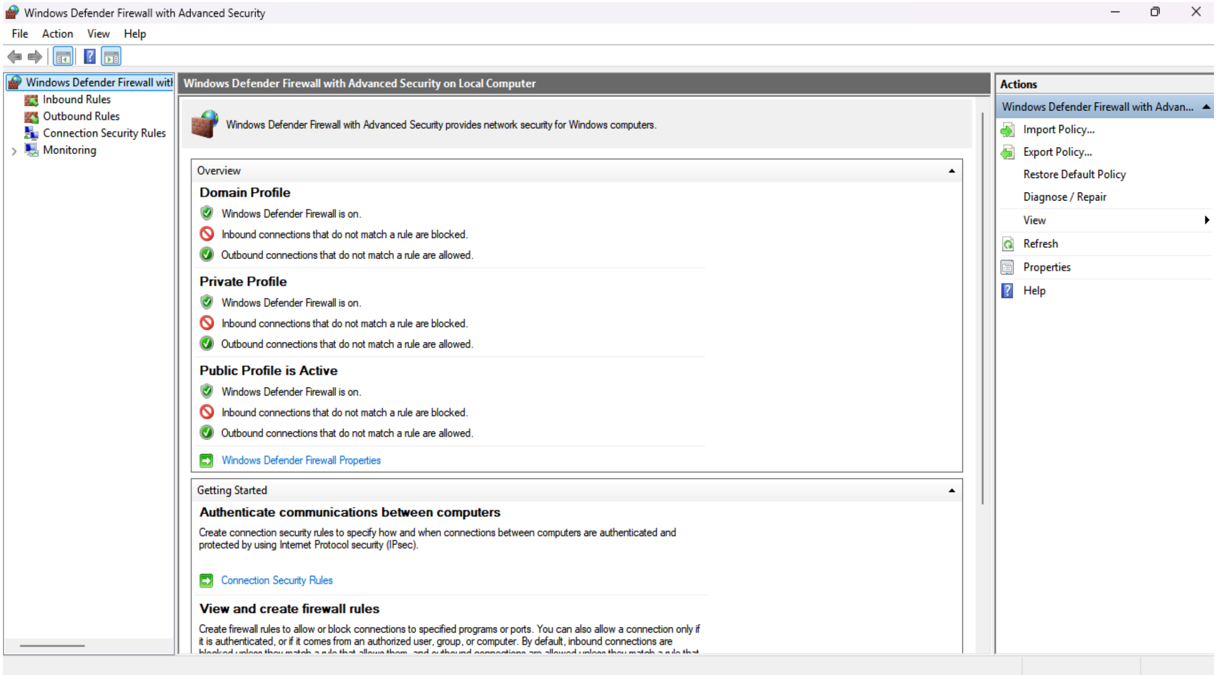
Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Step 2: Block Port 23

Created a new inbound rule to block TCP traffic on port 23 (Telnet). This improves system security by disabling an insecure protocol.



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

✓ Windows Defender Firewall is on.
⊘ Inbound connections that do not match a rule are blocked.
✓ Outbound connections that do not match a rule are allowed.

Private Profile

✓ Windows Defender Firewall is on.
⊘ Inbound connections that do not match a rule are blocked.
✓ Outbound connections that do not match a rule are allowed.

Public Profile is Active

✓ Windows Defender Firewall is on.
⊘ Inbound connections that do not match a rule are blocked.
✓ Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

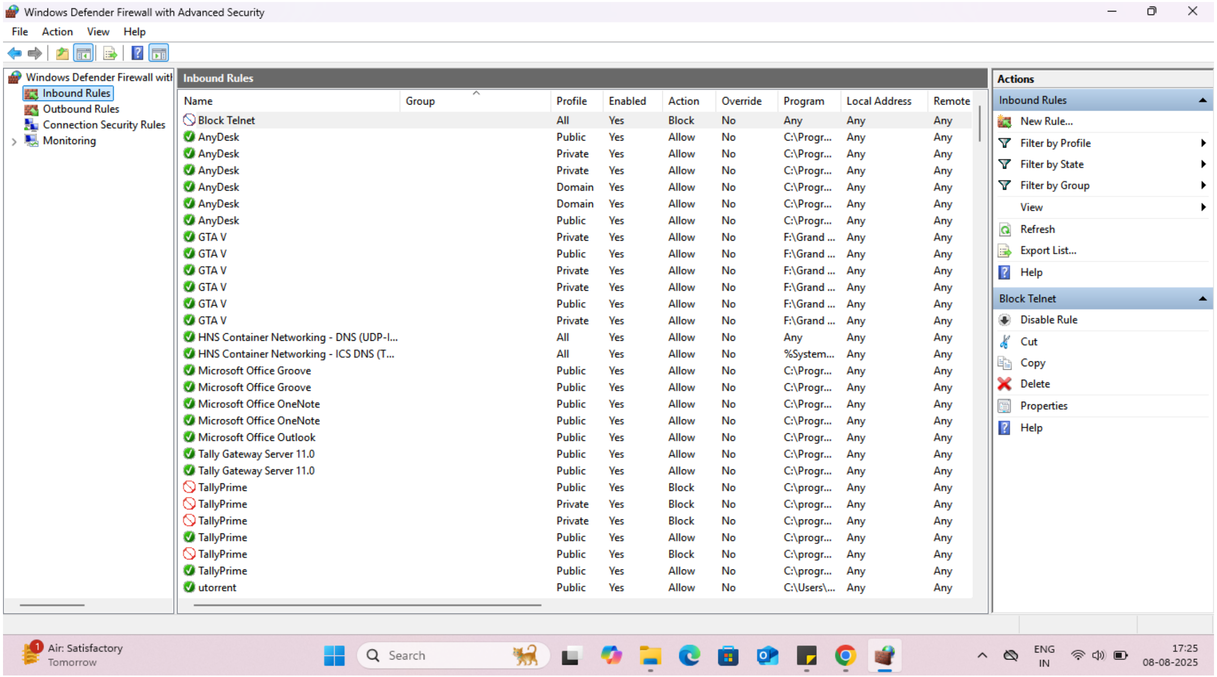
Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that

Step 3: Verify the Rule

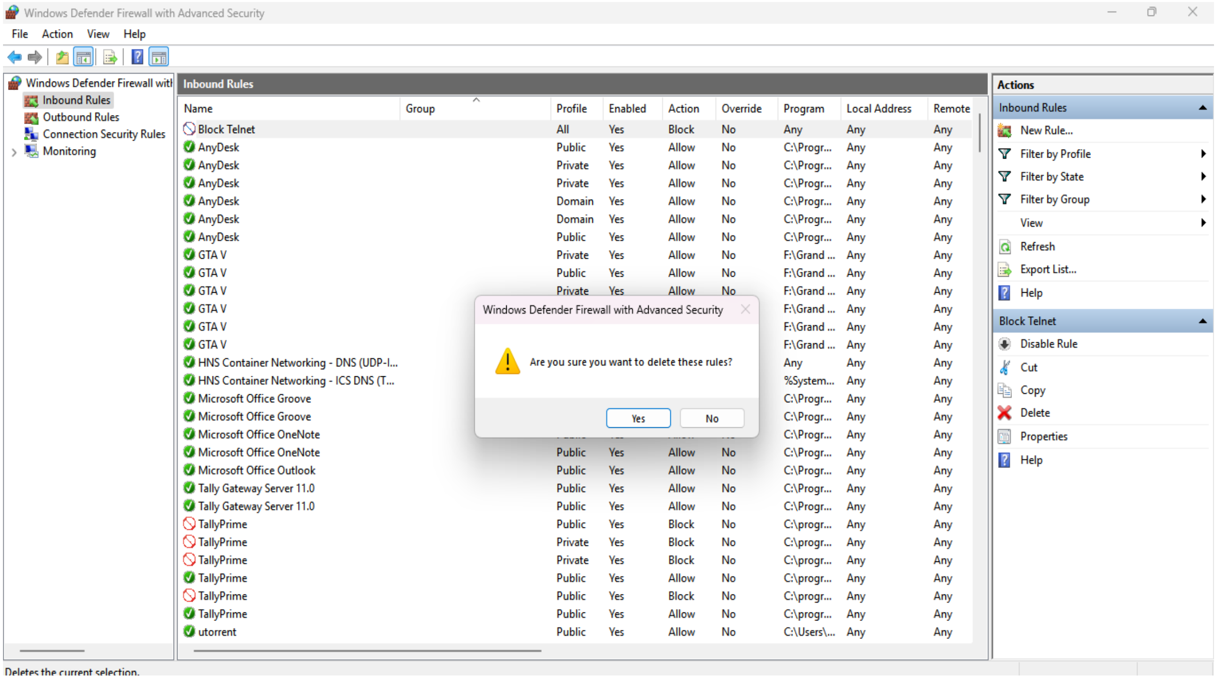
Confirmed that the 'Block Telnet' rule appeared in the list of inbound rules, meaning the firewall is now actively blocking traffic on port 23.



Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote
Block Telnet		All	Yes	Block	No	Any	Any	Any
AnyDesk		Public	Yes	Allow	No	C:\Progr...	Any	Any
AnyDesk		Private	Yes	Allow	No	C:\Progr...	Any	Any
AnyDesk		Private	Yes	Allow	No	C:\Progr...	Any	Any
AnyDesk		Domain	Yes	Allow	No	C:\Progr...	Any	Any
AnyDesk		Domain	Yes	Allow	No	C:\Progr...	Any	Any
AnyDesk		Public	Yes	Allow	No	C:\Progr...	Any	Any
GTA V		Private	Yes	Allow	No	F:\Grand ...	Any	Any
GTA V		Public	Yes	Allow	No	F:\Grand ...	Any	Any
GTA V		Private	Yes	Allow	No	F:\Grand ...	Any	Any
GTA V		Private	Yes	Allow	No	F:\Grand ...	Any	Any
GTA V		Public	Yes	Allow	No	F:\Grand ...	Any	Any
GTA V		Private	Yes	Allow	No	F:\Grand ...	Any	Any
HNS Container Networking - DNS (UDP-I...		All	Yes	Allow	No	Any	Any	Any
HNS Container Networking - ICS DNS (T...		All	Yes	Allow	No	%System...	Any	Any
Microsoft Office Groove		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Office Groove		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Office OneNote		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Office OneNote		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Office Outlook		Public	Yes	Allow	No	C:\Progr...	Any	Any
Tally Gateway Server 11.0		Public	Yes	Allow	No	C:\Progr...	Any	Any
Tally Gateway Server 11.0		Public	Yes	Allow	No	C:\Progr...	Any	Any
TallyPrime		Public	Yes	Block	No	C:\progr...	Any	Any
TallyPrime		Private	Yes	Block	No	C:\progr...	Any	Any
TallyPrime		Private	Yes	Block	No	C:\progr...	Any	Any
TallyPrime		Public	Yes	Allow	No	C:\progr...	Any	Any
TallyPrime		Public	Yes	Block	No	C:\progr...	Any	Any
TallyPrime		Public	Yes	Allow	No	C:\progr...	Any	Any
utorrent		Public	Yes	Allow	No	C:\Users\...	Any	Any

Step 4: Delete the Rule

To restore the system to its previous state, we deleted the test rule. This is best practice after completing firewall configuration testing.



Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote
Block Telnet		All	Yes	Block	No	Any	Any	Any
AnyDesk		Public	Yes	Allow	No	C:\Progr...	Any	Any
AnyDesk		Private	Yes	Allow	No	C:\Progr...	Any	Any
AnyDesk		Private	Yes	Allow	No	C:\Progr...	Any	Any
AnyDesk		Domain	Yes	Allow	No	C:\Progr...	Any	Any
AnyDesk		Domain	Yes	Allow	No	C:\Progr...	Any	Any
AnyDesk		Public	Yes	Allow	No	C:\Progr...	Any	Any
GTA V		Private	Yes	Allow	No	F:\Grand ...	Any	Any
GTA V		Public	Yes	Allow	No	F:\Grand ...	Any	Any
GTA V		Private	Yes	Allow	No	F:\Grand ...	Any	Any
GTA V						F:\Grand ...	Any	Any
GTA V						F:\Grand ...	Any	Any
GTA V						F:\Grand ...	Any	Any
HNS Container Networking - DNS (UDP-I...						Any	Any	Any
HNS Container Networking - ICS DNS (T...						%System...	Any	Any
Microsoft Office Groove						C:\Progr...	Any	Any
Microsoft Office Groove						C:\Progr...	Any	Any
Microsoft Office OneNote						C:\Progr...	Any	Any
Microsoft Office OneNote		Public	Yes	Allow	No	C:\Progr...	Any	Any
Microsoft Office Outlook		Public	Yes	Allow	No	C:\Progr...	Any	Any
Tally Gateway Server 11.0		Public	Yes	Allow	No	C:\Progr...	Any	Any
Tally Gateway Server 11.0		Public	Yes	Allow	No	C:\Progr...	Any	Any
TallyPrime		Public	Yes	Block	No	C:\progr...	Any	Any
TallyPrime		Private	Yes	Block	No	C:\progr...	Any	Any
TallyPrime		Private	Yes	Block	No	C:\progr...	Any	Any
TallyPrime		Public	Yes	Allow	No	C:\progr...	Any	Any
TallyPrime		Public	Yes	Block	No	C:\progr...	Any	Any
TallyPrime		Public	Yes	Allow	No	C:\progr...	Any	Any
utorrent		Public	Yes	Allow	No	C:\Users\...	Any	Any

Windows Defender Firewall with Advanced Security

Are you sure you want to delete these rules?

Yes No

Deletes the current selection.