

Task 10: Firewall Configuration & Testing

Tools Used

- Linux: UFW (Uncomplicated Firewall)
- Windows: Windows Defender Firewall

Step 1: Open Firewall Configuration Tool

Linux:

Command:

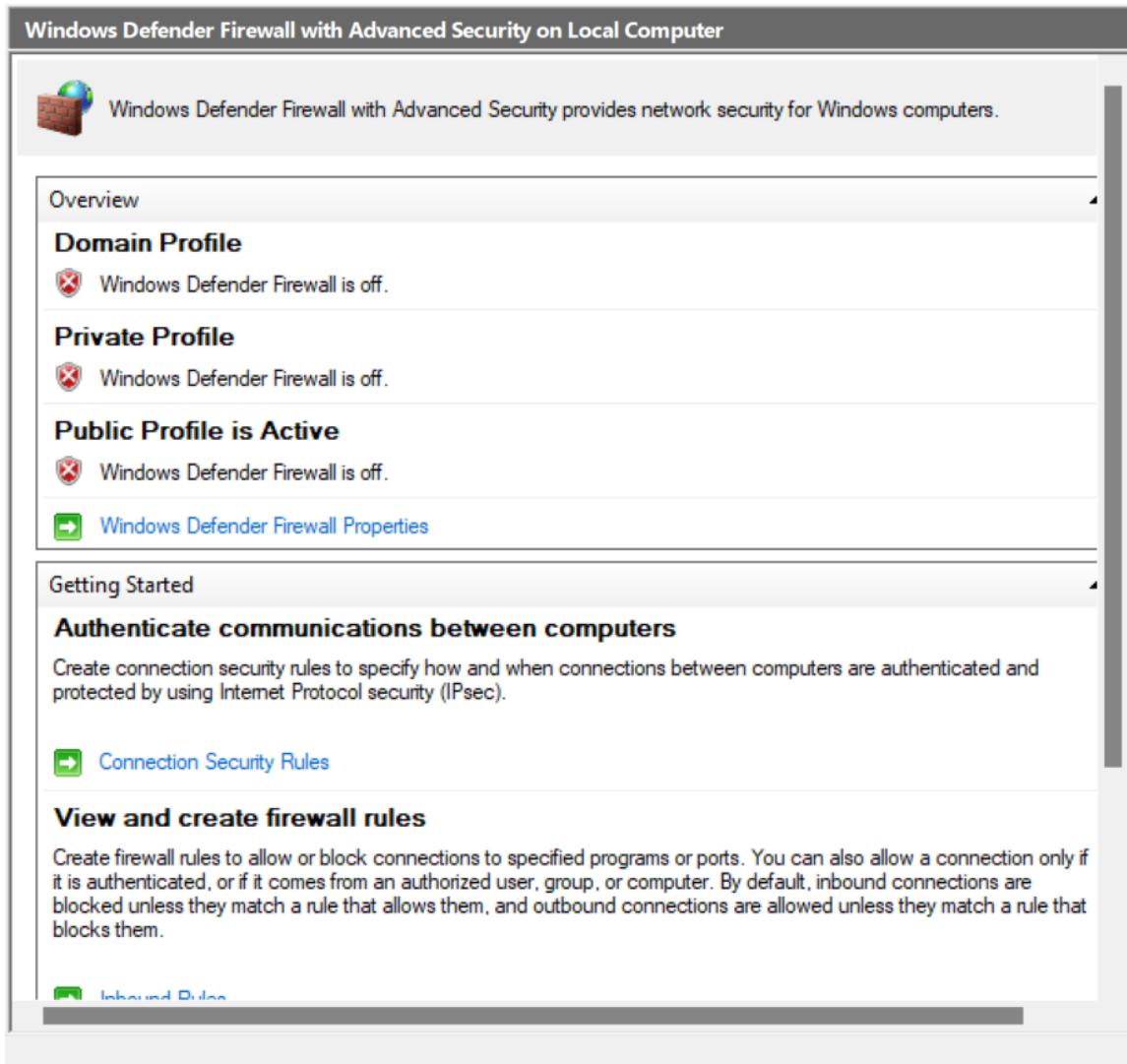
```
sudo ufw status verbose
```

```
[root@kali]# sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         --         --
22/tcp                      ALLOW IN   Anywhere
22/tcp (v6)                  ALLOW IN   Anywhere (v6)
```

Windows:

Open Windows Defender Firewall with Advanced Security.



Step 2: List Current Firewall Rules

Linux:

`sudo ufw status numbered`

```
(root㉿kali)-[~/home/kali]
# sudo ufw status numbered
Status: active

To                         Action      From
--                         --          --
[ 1] 22/tcp                 ALLOW IN   Anywhere
[ 2] 22/tcp (v6)            ALLOW IN   Anywhere (v6)
```

Windows:

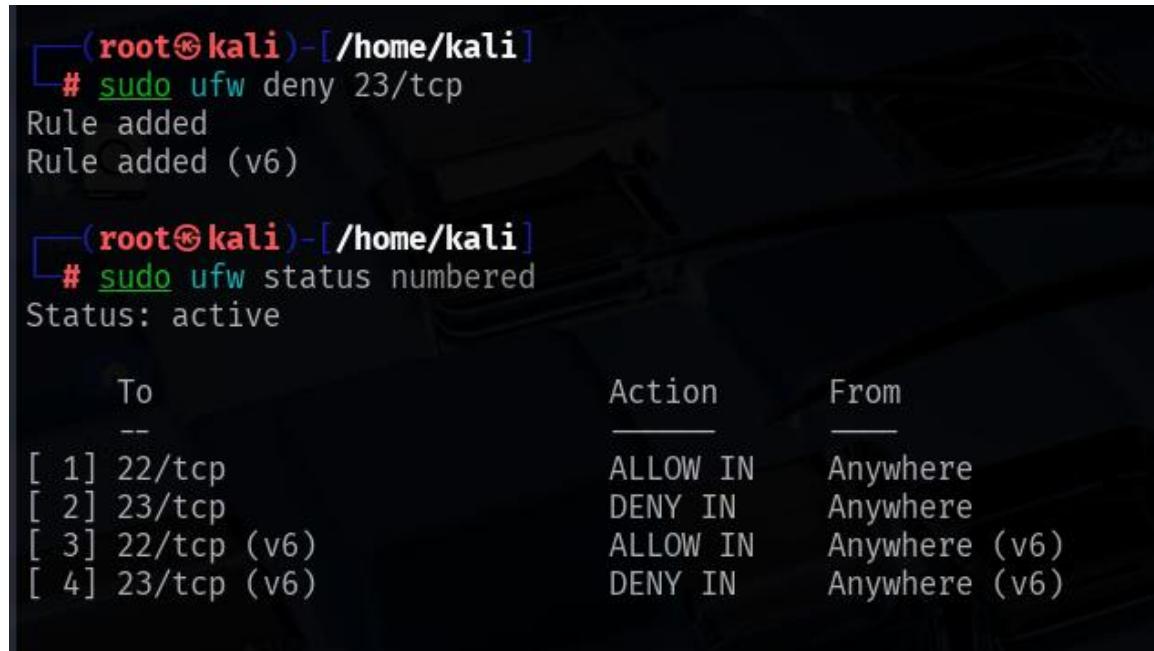
View Inbound Rules list.

| Inbound Rules | | | | |
|--|-------------------------------|----------|---------|--------|
| Name | Group | Profile | Enabled | Action |
| ✓ AnyDesk | | Public | Yes | Allow |
| ✓ AnyDesk | | Private | Yes | Allow |
| ✓ AnyDesk | | Private | Yes | Allow |
| ✓ AnyDesk | | Domain | Yes | Allow |
| ✓ AnyDesk | | Public | Yes | Allow |
| ✓ AnyDesk | | Domain | Yes | Allow |
| ✓ Firefox (C:\Program Files\Mozilla Firefox) | | Private | Yes | Allow |
| 🚫 Google Chrome | | Public | Yes | Block |
| 🚫 Google Chrome | | Public | Yes | Block |
| 🚫 Microsoft Teams | | Public | Yes | Block |
| 🚫 Microsoft Teams | | Public | Yes | Block |
| ✓ 腾讯手游助手下载器组件 | | Public | Yes | Allow |
| ✓ 腾讯手游助手下载器组件 | | Domain | Yes | Allow |
| ✓ 腾讯手游助手下载器组件 | | Private | Yes | Allow |
| ✓ 腾讯手游助手下载器组件 | | Domain | Yes | Allow |
| ✓ 腾讯手游助手下载器组件 | | Private | Yes | Allow |
| ✓ 腾讯手游助手下载器组件 | | Public | Yes | Allow |
| ✓ @{MicrosoftWindows.LKG.DesktopSpotlig...} | @{MicrosoftWindows.LKG.De... | Domai... | Yes | Allow |
| ✓ Microsoft Teams | {78E1CD88-49E3-476E-B926-...} | All | Yes | Allow |
| ✓ Microsoft Teams | {78E1CD88-49E3-476E-B926-...} | All | Yes | Allow |
| ✓ Microsoft Teams (personal) | {78E1CD88-49E3-476E-B926-...} | All | Yes | Allow |
| ✓ Microsoft Teams (personal) | {78E1CD88-49E3-476E-B926-...} | All | Yes | Allow |
| ✓ AllJoyn Router (TCP-In) | AllJoyn Router | Domai... | Yes | Allow |
| ✓ AllJoyn Router (UDP-In) | AllJoyn Router | Domai... | Yes | Allow |
| ✓ Amazon Alexa | Amazon Alexa | Domai... | Yes | Allow |
| ✓ App Installer | App Installer | Domai... | Yes | Allow |

Step 3: Add Rule to Block Port 23 (Telnet)

Linux:

```
sudo ufw deny 23/tcp  
sudo ufw status numbered
```

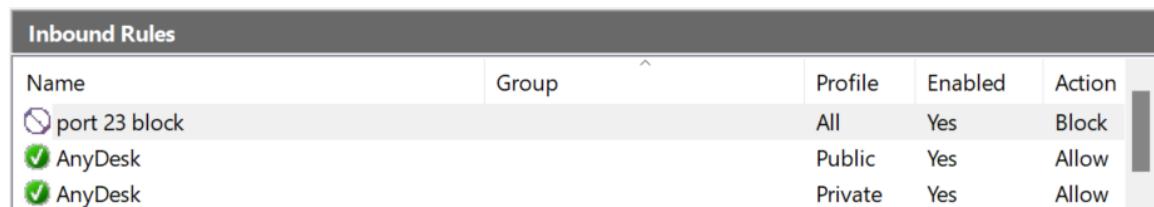


A terminal window titled '(root㉿kali)-[~/home/kali]' showing the configuration of the Uncomplicated Firewall (UFW). The user runs 'sudo ufw deny 23/tcp' which adds a rule to deny port 23 TCP traffic. Then, 'sudo ufw status numbered' is run to show the current rules. The output shows four numbered rules: rule 1 allows port 22 TCP from anywhere, rule 2 denies port 23 TCP from anywhere, rule 3 allows port 22 TCP (v6) from anywhere, and rule 4 denies port 23 TCP (v6) from anywhere. The status is listed as 'active'.

```
# sudo ufw deny 23/tcp  
Rule added  
Rule added (v6)  
  
# sudo ufw status numbered  
Status: active  
  
 To           Action    From  
 --          --  
 [ 1] 22/tcp      ALLOW IN  Anywhere  
 [ 2] 23/tcp      DENY IN   Anywhere  
 [ 3] 22/tcp (v6) ALLOW IN  Anywhere (v6)  
 [ 4] 23/tcp (v6) DENY IN   Anywhere (v6)
```

Windows:

Inbound Rules → New Rule → Port → TCP → Port 23 → Block.



A screenshot of the Windows Firewall's Inbound Rules table. It lists three rules: one named 'port 23 block' which is enabled and set to 'Block' action, and two rules for 'AnyDesk' which are enabled and set to 'Allow' action. The columns are Name, Group, Profile, Enabled, and Action.

| Name | Group | Profile | Enabled | Action |
|---------------|-------|---------|---------|--------|
| port 23 block | | All | Yes | Block |
| AnyDesk | | Public | Yes | Allow |
| AnyDesk | | Private | Yes | Allow |

Step 4: Test the Block Rule

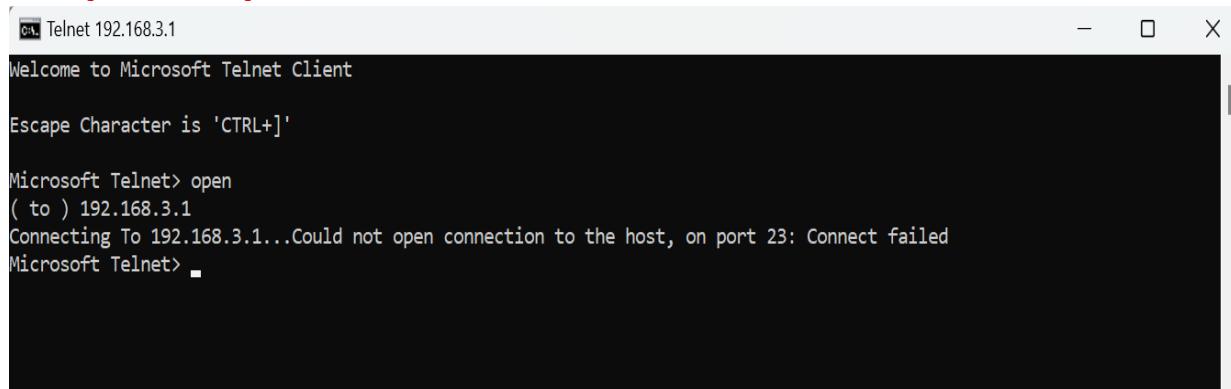
Linux:

```
telnet localhost 23
```

```
(root㉿kali)-[~/home/kali]
# telnet localhost 23
Trying ::1...
Connection failed: Connection refused
Trying 127.0.0.1...
telnet: Unable to connect to remote host: Connection refused
```

Windows:

Attempt Telnet on port 23.



Step 5: Add Rule to Allow SSH (Port 22)

Linux:

```
sudo ufw allow 22/tcp
sudo ufw status numbered
```

```

└─(root㉿kali)-[~/home/kali]
└─# sudo ufw allow 22/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)

└─(root㉿kali)-[~/home/kali]
└─# sudo ufw status numbered
Status: active

          To           Action    From
          --           —        —
[ 1] 22/tcp      ALLOW IN  Anywhere
[ 2] 23/tcp      DENY IN   Anywhere
[ 3] 22/tcp (v6) ALLOW IN  Anywhere (v6)
[ 4] 23/tcp (v6) DENY IN   Anywhere (v6)

```

Windows:

Inbound Rules → New Rule → Port → TCP → Port 22 → Allow.

| Inbound Rules | | | | |
|-----------------|-------|---------|---------|--------|
| Name | Group | Profile | Enabled | Action |
| ✓ port 22 allow | | All | Yes | Allow |
| ✗ port 23 block | | All | Yes | Block |
| ✓ AnyDesk | | Public | Yes | Allow |
| ✓ AnyDesk | | Private | Yes | Allow |
| ✓ AnyDesk | | Private | Yes | Allow |
| ✓ AnyDesk | | Domain | Yes | Allow |

Step 6: Remove Test Block Rule

Linux:

`sudo ufw delete <rule-number>`

sudo ufw status numbered

```
[root@kali]# sudo ufw delete allow 22/tcp
Rule deleted
Rule deleted (v6)
```

```
[root@kali]# sudo ufw status numbered
Status: active
```

| To | Action | From |
|------------------|---------|---------------|
| -- | | |
| [1] 23/tcp | DENY IN | Anywhere |
| [2] 23/tcp (v6) | DENY IN | Anywhere (v6) |

Windows:

Right-click “Block Telnet 23” → Delete.

| Inbound Rules | | | | |
|--|-------|---------|---------|--------|
| Name | Group | Profile | Enabled | Action |
| ✓ AnyDesk | | Public | Yes | Allow |
| ✓ AnyDesk | | Private | Yes | Allow |
| ✓ AnyDesk | | Private | Yes | Allow |
| ✓ AnyDesk | | Domain | Yes | Allow |
| ✓ AnyDesk | | Domain | Yes | Allow |
| ✓ AnyDesk | | Public | Yes | Allow |
| ✓ Firefox (C:\Program Files\Mozilla Firefox) | | Private | Yes | Allow |
| ✗ Google Chrome | | Public | Yes | Block |
| ✗ Google Chrome | | Public | Yes | Block |
| ✗ Microsoft Teams | | Public | Yes | Block |
| ✗ Microsoft Teams | | Public | Yes | Block |
| ✓ port 22 allow | All | Yes | Allow | |

Commands / GUI Steps

Linux (UFW):

```
sudo apt install ufw
sudo ufw status verbose
sudo ufw deny 23/tcp
sudo ufw allow 22/tcp
sudo ufw delete "allow 22/tcp"
```

Windows Firewall:

- Open Windows Defender Firewall with Advanced Security
- Create inbound rule for blocking port 23
- Create inbound rule for allowing port 22
- Delete the test block rule

Summary – How Firewall Filters Traffic

A firewall inspects incoming and outgoing network packets and decides whether to allow or block traffic based on configured rules.

- Example: SSH (22) is allowed for remote management.
- Example: Telnet (23) is blocked because it is insecure.

This ensures only authorized traffic reaches the system, reducing the attack surface and improving security.