

Firewalls für Windows

Firewalls für Windows gibt es sowohl als integrierte Funktion von Windows als auch von Drittanbietern. Hier sind einige Empfehlungen und Informationen:

Integrierte Windows-Firewall

Die Windows-Firewall ist bereits im Betriebssystem integriert und bietet grundlegenden Schutz. Sie kann über die Systemsteuerung oder die Einstellungen verwaltet werden:

- **Aufrufen:**
 1. Gehe zu *Einstellungen > Netzwerk und Internet > Firewall und Netzwerkschutz*.
 2. Alternativ in der Systemsteuerung: *System und Sicherheit > Windows Defender Firewall*.
- **Features:**
 1. Blockieren von unerwünschtem eingehenden und ausgehenden Datenverkehr.
 2. Konfigurierbare Regeln für Programme, Ports und Protokolle.
 3. Aktiv auf Deutsch verfügbar.

Drittanbieter-Firewalls

Diese bieten oft erweiterte Funktionen wie erweiterte Netzwerkanalyse, Benachrichtigungen oder ein einfacher zu bedienendes Interface.

Beliebte Firewalls in deutscher Sprache:

1. **Comodo Firewall**
 - Kostenlos erhältlich, aber auch in kostenpflichtigen Versionen mit mehr Features.
 - Bietet erweiterte Überwachungsfunktionen und automatische Programmkontrolle.
2. **ZoneAlarm Free Firewall**
 - Kostenlos und benutzerfreundlich.
 - Ermöglicht detaillierte Kontrolle des Datenverkehrs.
3. **Bitdefender Total Security**
 - Enthält eine integrierte Firewall (kostenpflichtige Suite).
 - Hervorragend für Benutzer, die einen Rundumschutz suchen.
4. **ESET Internet Security**
 - Sehr bekannt im deutschsprachigen Raum.
 - Kombination aus Firewall, Virenschutz und Anti-Spam.
5. **Kaspersky Internet Security**
 - Enthält eine zuverlässige Firewall.
 - Einfache Benutzeroberfläche und hoher Schutz.

Kriterien für die Wahl einer Firewall:

- **Sprache:** Fast alle größeren Anbieter bieten deutsche Sprachunterstützung.

- **Benutzerfreundlichkeit:** Für Anfänger sind Programme mit einem Assistenten oder einfacher Konfiguration ideal.
- **Zusatzfunktionen:** Erweiterte Netzwerkanalysen oder Warnsysteme können hilfreich sein.
- **Kosten:** Einige kostenlose Lösungen bieten bereits guten Schutz, kostenpflichtige bieten oft mehr Anpassungsoptionen.

Freeware-Firewalls für Windows

Hier sind einige der besten **Freeware-Firewalls** für Windows, die kostenlos verfügbar und in der Regel auch in deutscher Sprache nutzbar sind:

1. Windows Defender Firewall (*Integriert in Windows*)

- **Vorteile:**
 - Kostenlos und bereits vorinstalliert.
 - Solider Basisschutz für eingehenden und ausgehenden Datenverkehr.
 - Regelbasierte Konfiguration (Programme, Ports).
- **Geeignet für:**
Nutzer, die keinen zusätzlichen Installationsaufwand möchten.

2. Comodo Free Firewall

- **Features:**
 - Benutzerfreundliche Oberfläche.
 - Bietet Warnungen zu unsicheren Verbindungen.
 - Virtuelle Umgebung für Programme, um potenziell schädliche Software zu isolieren.
- **Vorteile:**
 - Sehr anpassbar, ideal für erfahrenere Nutzer.
 - Unterstützt die deutsche Sprache.
- **Download:** <https://www.comodo.com>

3. ZoneAlarm Free Firewall

- **Features:**
 - Automatische Programmanalyse und Zugriffssteuerung.
 - Schutz vor eingehenden und ausgehenden Bedrohungen.
 - Integrierter WLAN-Schutz.
- **Vorteile:**
 - Einfach zu konfigurieren.
 - Geeignet für Einsteiger.
- **Download:** <https://www.zonealarm.com>

4. GlassWire Free Firewall

- **Features:**
 - Echtzeit-Netzwerküberwachung mit grafischer Darstellung.

- Warnmeldungen bei verdächtigem Netzwerkverkehr.
- Schutz vor unbefugtem Zugriff.
- **Vorteile:**
 - Intuitive Benutzeroberfläche.
 - Netzwerkaktivitäten auf einen Blick sichtbar.
- **Download:** <https://www.glasswire.com>

5. TinyWall

- **Features:**
 - Ergänzt die integrierte Windows-Firewall.
 - Blockiert schädliche Verbindungen ohne lästige Pop-ups.
 - Ermöglicht gezielte Freigaben für Programme.
- **Vorteile:**
 - Sehr ressourcenschonend und minimalistisch.
 - Keine Werbung oder Upselling.
- **Download:** <https://tinywall.pados.hu>

6. Privatefirewall

- **Features:**
 - Schutz vor Bedrohungen wie Keyloggern und Spyware.
 - Überwachung von Programmen und Prozessen in Echtzeit.
- **Vorteile:**
 - Benutzerfreundlich.
 - Kostenlos, aber weniger bekannt.
- **Download:** <https://www.privacyware.com/privatefirewall.html>

Empfehlung: Welche Firewall ist die richtige?

- **Für Einsteiger:** ZoneAlarm oder Windows Defender Firewall.
- **Für fortgeschrittene Nutzer:** Comodo oder GlassWire.
- **Für minimalistische Ansprüche:** TinyWall.

Firewalls für Linux

In der Linux-Welt werden häufig Tools wie **UFW**, **firewalld**, **iptables** oder **nftables** verwendet.

Alternativen zu "TinyFirewall" für Linux

Falls Sie nach einer einfachen und leichten Firewall-Lösung für Linux suchen, sind hier einige empfehlenswerte Alternativen:

1. UFW (Uncomplicated Firewall)

- **Beschreibung:** Ein unkompliziertes Kommandozeilen-Tool zur Verwaltung von **iptables**-Regeln.

- **Warum verwenden?**
 - Einfache Befehle und Syntax.
 - Besonders für Einsteiger und schnelle Setups geeignet.

- **Installation:**

```
sudo apt install ufw
```

- **Grundbefehle:**

- Firewall aktivieren:

```
sudo ufw enable
```

- Einen Port freigeben (z. B. SSH auf Port 22):

```
sudo ufw allow 22
```

2. Firewalld

- **Beschreibung:** Ein dynamischer Firewall-Daemon, der Netzwerkverkehr in Echtzeit verwaltet.
- **Warum verwenden?**
 - Bietet mehr Flexibilität für Zonen und Profile.
 - Besonders gut für Red Hat-basierte Systeme geeignet.

- **Installation:**

```
sudo apt install firewalld    # Für Debian-basierte Distributionen
sudo dnf install firewalld    # Für Fedora/CentOS
```

- **Grundbefehle:**

- Starten und aktivieren:

```
sudo systemctl start firewalld
sudo systemctl enable firewalld
```

- Einen Dienst freigeben:

```
sudo firewall-cmd --permanent --add-service=ssh
sudo firewall-cmd --reload
```

3. Direkte Verwendung von iptables oder nftables

- **Beschreibung:** Die Kern-Tools für Firewalls in Linux, die eine feingranulare Kontrolle ermöglichen.
- **Warum verwenden?**
 - Ideal für fortgeschrittene Benutzer.
 - Vollständig anpassbar.
- **Installation** (meist vorinstalliert):

```
sudo apt install iptables nftables
```

4. GFW (Graphisches UFW)

- **Beschreibung:** Eine grafische Benutzeroberfläche für UFW, die es noch einfacher macht.
- **Installation:**

```
sudo apt install gufw
```

- **Warum verwenden?**
 - Perfekt für Desktop-Benutzer.
 - Eine einfache Point-and-Click-Oberfläche.

guFW (Uncomplicated Firewall), UFW konfigurieren.

UFW ist besonders für Linux-Benutzer geeignet, da es eine benutzerfreundliche Oberfläche für die Verwaltung der iptables-Firewall bietet.

Was ist UFW?

UFW (Uncomplicated Firewall) ist ein einfaches Tool, das die Konfiguration einer Firewall unter Linux vereinfacht. Es ist ideal für Anfänger und für grundlegende Firewall-Einstellungen.

UFW installieren

Die meisten modernen Linux-Distributionen wie Ubuntu haben UFW bereits vorinstalliert. Falls nicht, kannst du es wie folgt installieren:

```
sudo apt update  
sudo apt install ufw
```

UFW aktivieren und deaktivieren

- **Aktivieren der Firewall:**

```
sudo ufw enable
```

Achtung: Stelle sicher, dass die erforderlichen Regeln (z. B. SSH) hinzugefügt wurden, bevor du UFW aktivierst.

- **Deaktivieren der Firewall:**

```
sudo ufw disable
```

- **Status der Firewall anzeigen:**

```
sudo ufw status
```

Nutze `sudo ufw status verbose`, um zusätzliche Informationen zu erhalten.

Grundlegende Befehle

1. Ports erlauben

- Einen bestimmten Port freigeben (z. B. HTTP auf Port 80):

```
sudo ufw allow 80
```

- Dienste nach Namen erlauben (z. B. SSH):
`sudo ufw allow ssh`
- Einen Port nur für ein bestimmtes Protokoll freigeben (z. B. TCP auf Port 443):
`sudo ufw allow 443/tcp`

2. Ports blockieren

- Einen Port explizit blockieren (z. B. FTP auf Port 21):
`sudo ufw deny 21`

3. Regeln entfernen

- Eine spezifische Regel löschen (z. B. Freigabe von Port 80):
`sudo ufw delete allow 80`

4. Bestimmte IP-Adressen zulassen oder blockieren

- IP-Adresse zulassen:
`sudo ufw allow from 192.168.1.100`
- IP-Adresse blockieren:
`sudo ufw deny from 192.168.1.100`
- Zugriff auf einen Port nur für eine IP-Adresse erlauben:
`sudo ufw allow from 192.168.1.100 to any port 22`

5. Alle Verbindungen blockieren und nur spezifische freigeben

- Standardmäßig alle eingehenden Verbindungen blockieren:
`sudo ufw default deny incoming`
- Standardmäßig alle ausgehenden Verbindungen zulassen:
`sudo ufw default allow outgoing`

Regeln überprüfen

- Aktuelle UFW-Regeln anzeigen:
`sudo ufw status numbered`
- Eine Regel mit einer Nummer löschen:
`sudo ufw delete <Nummer>`

Logging aktivieren

- UFW-Logs aktivieren:
`sudo ufw logging on`
- UFW-Logs deaktivieren:
`sudo ufw logging off`

Beispielkonfiguration

1. Standardrichtlinien setzen:

```
sudo ufw default deny incoming  
sudo ufw default allow outgoing
```

2. SSH-Port (z. B. 22) zulassen:

```
sudo ufw allow ssh
```

3. HTTP und HTTPS zulassen:

```
sudo ufw allow 80  
sudo ufw allow 443
```

4. Firewall aktivieren:

```
sudo ufw enable
```

5. Status prüfen:

```
sudo ufw status verbose
```

Zusätzliche Tipps

- UFW ist besonders nützlich für Server, um nur notwendige Dienste offen zu halten.
- Nutze spezifische Regeln, um Sicherheit zu maximieren (z. B. IP-Whitelist).
- Wenn du viele Regeln verwalten musst, können Tools wie `ufw-frontends` oder `GUFW` (grafische Oberfläche) hilfreich sein.

GUFW Zugriff Blockieren

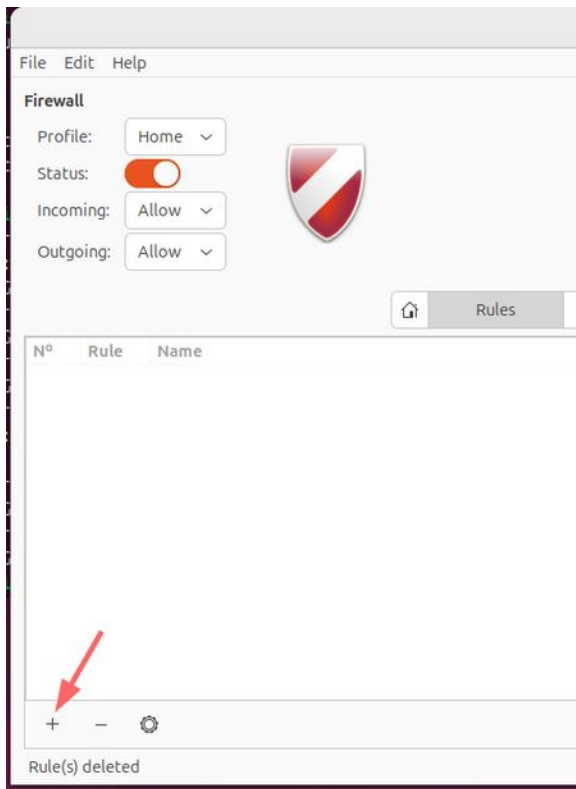
SSH Zugriff von einer spezifischen IP Adresse blockieren mit **Gufw** (Firewall Configuration Tool):

1. Öffnen Sie Gufw (Firewall-Konfigurationswerkzeug)

- Starten Sie **Gufw** aus Ihrem Anwendungsmenü (es heißt möglicherweise „Firewall-Konfiguration“).
- Geben Sie Ihr Passwort ein, um Änderungen vorzunehmen.

2. Eine Verweigern-Regel für die spezifische IP-Adresse hinzufügen

1. Klicken Sie im Gufw-Fenster auf den Reiter **„Regeln“**.
2. Klicken Sie auf das **„+“ (Regel hinzufügen)** Symbol, um eine neue Regel zu erstellen.
3. Im Dialogfenster **„Regel hinzufügen“**:
 - Wählen Sie **„Richtung“**: **„Eingehend“** (Incoming).
 - Wählen Sie **„Richtlinie“**: **„Verweigern“** (Deny).
 - Gehen Sie auf den Reiter **„Erweitert“**:
 - Im Feld **Von IP** geben Sie die spezifische IP-Adresse ein, die Sie blockieren möchten (z.B. 192 . 168 . 1 . 104 oder eine externe IP).
 - Im Abschnitt **An** wählen Sie **Port** und geben Sie **22** ein (der Standardport für SSH).
4. Klicken Sie auf **Hinzufügen**, um die Regel zu speichern.



Update a Firewall Rule

Name: sshf

Policy: Deny

Direction: In

Interface: All Interfaces

Log: Do not Log

Protocol: Both

From: 192.168.1.104

To: IP

Port: 22

The rule will be moved to the end of the list

Cancel Apply

Add a Firewall Rule

Preconfigured Simple Advanced

Policy: Deny

Direction: In

Category: All

Subcategory: All

Application: SSH

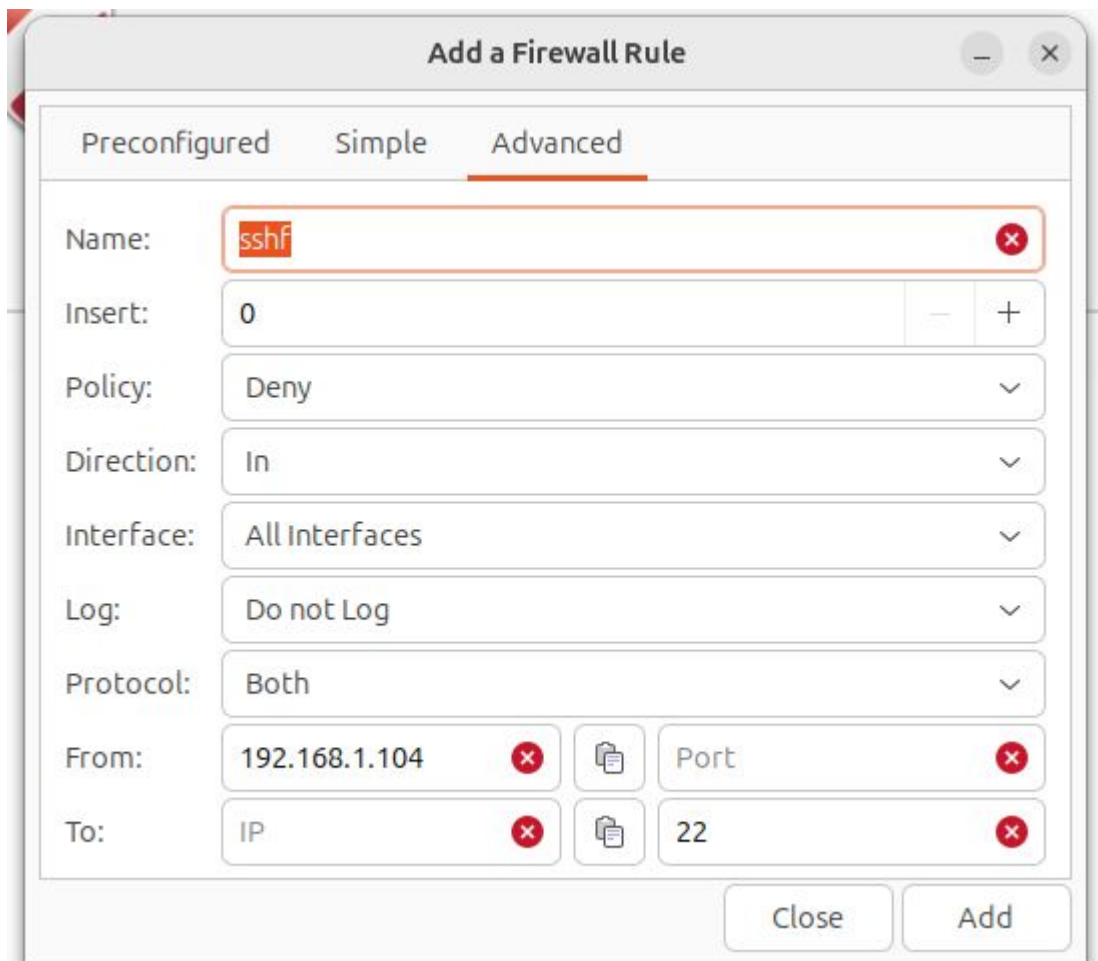
ssh

It may be a security risk to use a default allow policy

Close Add

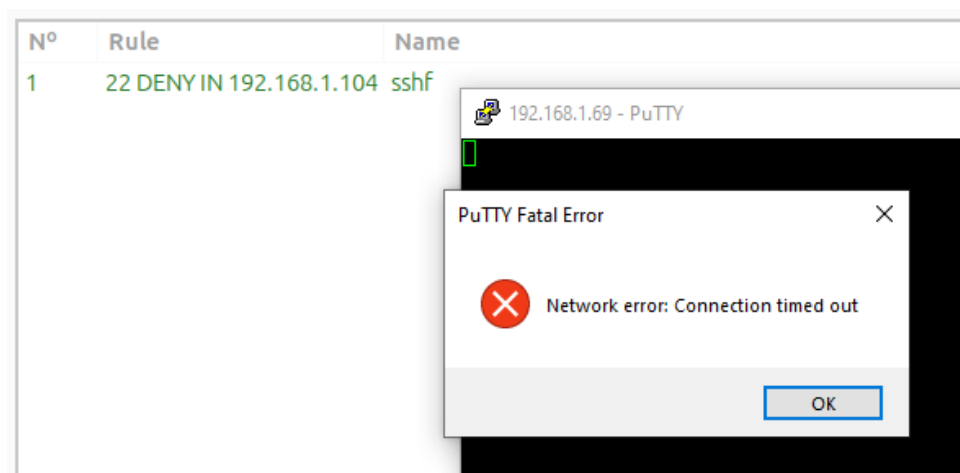
3. Überprüfen, ob die Regel angewendet wurde

- Stellen Sie sicher, dass die neue „**Verweigern**“-Regel in der Liste erscheint.
- Die Regel sollte SSH-Verbindungen (Port 22) von der eingegebenen IP-Adresse blockieren.



4. Testen der Regel

- Versuchen Sie, von der blockierten IP-Adresse aus per SSH auf den Computer zuzugreifen. Die Verbindung sollte verweigert werden.



Anmerkungen:

- **Alle IP-Adressen blockieren:** Um SSH komplett zu sperren, erstellen Sie eine allgemeine **Verweigern**-Regel für **Port 22**.
- Falls SSH auf einem anderen Port läuft (nicht Port 22), ersetzen Sie die Portnummer entsprechend.

Diese Schritte erstellen eine Blockregel in **Gufw**, die im Hintergrund **ufw** (Uncomplicated Firewall) aktualisiert.