

Windows Netzwerk

- Powersehll Privates Netzwerk definieren
- Bei Guest Accounts auf dem SMB Server aktiv , keine Verbindung
- portforwarding unter Windows 10/11 und auch Server
- FritzBox WireGuard: NetBIOS-Option & SMB / SAMBA

Powersehll Privates Netzwerk definieren

Beschreibung:

Es gibt leider Situationen da wird das Netzwerk falsch erkannt. Anstatt Privat ist es Öffentlich.
Das können wir mit einem Powershell Befehl ändern.

Los gehts:

Powersehll als Admin starten

Als erstes die Netzwerk Nummer herausfinden

```
C:\> Get-NetConnectionProfile
```

Ausgabe:

```
Copyright (C) Microsoft Corporation. Alle Rechte vorbehalten.  
Lernen Sie das neue plattformübergreifende PowerShell kennen - https://aka.ms/pscore6  
PS C:\Windows\system32> Get-NetConnectionProfile  
  
Name : Netzwerk 3  
InterfaceAlias : Ethernet 3  
InterfaceIndex : 13  
NetworkCategory : Public  
DomainAuthenticationKind : None  
IPv4Connectivity : Internet  
IPv6Connectivity : NoTraffic  
  
PS C:\Windows\system32> █
```

```
Name : Netzwerk 2  
InterfaceAlias : Ethernet  
InterfaceIndex : 15  
NetworkCategory : Private
```

DomainAuthenticationKind : None

IPv4Connectivity : Internet

IPv6Connectivity : NoTraffic

Nun die Netzwekid <index number> einstecken die man haben möchte

```
Set-NetConnectionProfile -InterfaceIndex <index number> -NetworkCategory Private
```

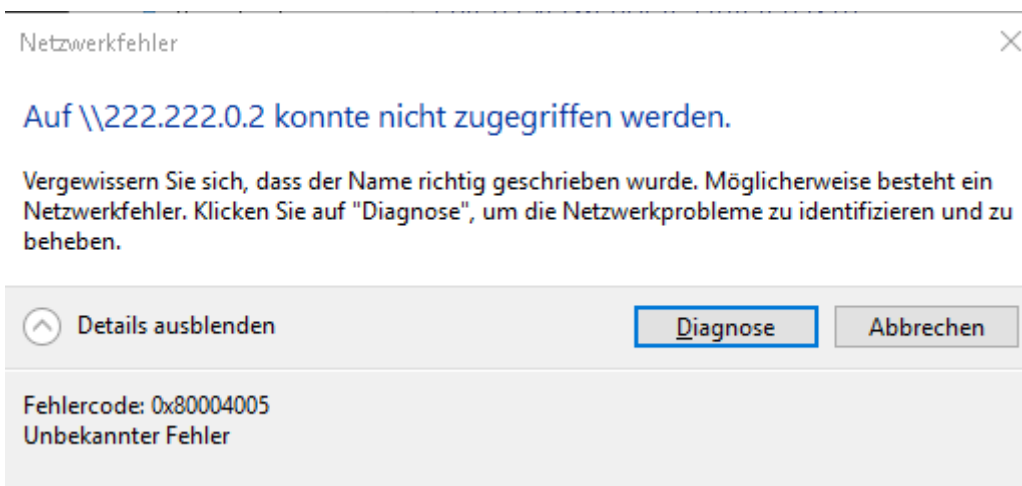
Beispiel

```
Set-NetConnectionProfile -InterfaceIndex 15 -NetworkCategory Private
```

Bei Guest Accounts auf dem SMB Server aktiv , keine Verbindung

Beschreibung:

Wenn man per Explorer auf eine SMB Freigabe zugreifen möchte, wo Guest verbinden erlaubt sind oder zumindest auf Bad User eingestellt sind, bekommt diese total aussagekräftige Fehlermeldung.



Versucht man allerdings per net use eine Verbindung herzustellen

```
net use h: \\meinserver\freiagbe
```

Bekommt diese Meldung.

Sie können nicht auf diesen freigegebenen Ordner zugreifen, weil der Zugriff nicht authentifizierter Gäste durch die Sicherheitsrichtlinien Ihrer Organisation blockiert werden. Diese Richtlinien helfen, Ihren PC vor unsicheren oder bösartigen Geräten im Netzwerk zu schützen.

Nun wissen wir aber, es hat was mit dem Gast Konto zu tun.

Würde man dem net use Befehl übrigens noch den Username übergeben, klapp die Anmeldung auch.

```
net use h: \\meinserver\freiagbe /username:jens
```

Aber wir wollen ja auch das es im explorer funktioniert.

Samba conf anpassen.

```
nano /etc/samba/smb.conf
```

Hier dirin nach folgenden abschnitten suchen:

Diese auf never stellen, könnte noch auf bad user gestellt sein.

```
map to guest = never
```

```
usershare allow guests = yes
```

```
auskommentieren
```

```
#usershare allow guests = yes
```

In allen Freigaben guest ok=no

Beispiel bei einer Freigabe:

```
[groups]
```

```
comment= Groups Freigabe
```

```
path= /daten/groups
```

```
read only=no
```

```
browseable=yes
```

```
guest ok=no
```

Danach den smbd Dienst neustarten

```
systemctl restart smbd
```

Nun funktioniert auch wieder das aufrufen und anzeigen des Benutzereingabedialoges

Netzwerkanmeldeinformationen eingeben

Geben Sie Ihre Anmeldeinformationen ein, um eine Verbindung mit folgendem Netzwerk herzustellen: 222.222.0.2

Domäne: GBL-TAIFUN

Anmeldedaten speichern

Der Benutzername bzw. das Kennwort ist falsch.

portforwarding unter Windows 10/11 und auch Server

Beschreibung:

Es gibt Situationen da möchte man gerne einen Port vom Windows PC umleiten zu einem anderen hin.

Zum Beispiel weil nur der Windows PC den Tunnel ins Firmennetzwerk hat, man aber trotzdem gerne mit dem Heimischen Scanner auf den Server scannen möchte.

In unserem Szenario wollen wir mit SFTP auf den Server scannen.

Durchführung

Portforwarding einrichten:

```
netsh interface portproxy add v4tov4 listenaddress=0.0.0.0 listenport=<localport> connectaddress=<ip-des-zielservers> connectport=<zielport>
```

Unser SSH Beispiel

```
netsh interface portproxy add v4tov4 listenaddress=0.0.0.0 listenport=22 connectaddress=172.0.2.21 connectport=22
```

In der Firewall Freischalten

```
New-NetFirewallRule -DisplayName "<Beschreibung der Rule" -Direction Inbound -Protocol <Protokoll, TCP,UDP> -LocalPort <localport> -Action Allow
```

```
New-NetFirewallRule -DisplayName "SFTP Portforwarding" -Direction Inbound -Protocol TCP -LocalPort 22 -Action Allow
```

Ausgabe:

```
New-NetFirewallRule -DisplayName "SFTP Portforwarding" -Direction Inbound -Protocol TCP -LocalPort 22 -Action Allow
```

Name : {67966c98-5e49-47f5-a907-fcaaea4630a6}
DisplayName : SFTP Portforwarding
Description :
DisplayGroup :
Group :
Enabled : True
Profile : Any
Platform : {}
Direction : Inbound
Action : Allow
EdgeTraversalPolicy : Block
LooseSourceMapping : False
LocalOnlyMapping : False
Owner :
PrimaryStatus : OK
Status : Die Regel wurde erfolgreich vom Speicher aus analysiert. (65536)
EnforcementStatus : NotApplicable
PolicyStoreSource : PersistentStore
PolicyStoreSourceType : Local
RemoteDynamicKeywordAddresses : {}
PolicyAppId :
PackageFamilyName :

Portforwarding wieder entfernen

FritzBox WireGuard: NetBIOS-Option & SMB / SAMBA

Beschreibung:

Fehler 80004005 bedeutet entweder Benutzername Kennwort sind falsch, bzw. im Credentialmanager beschädigt.

Dann in der Systemsteuerung Anmeldeinformationen diese löschen neu anmelden oder, es ist eine Fritzbox als Wireguard Client konfiguriert zum Zugriff auf den Zielservers.

Netzwerkfehler ×

Auf \\192.168.2.11 konnte nicht zugegriffen werden.

Vergewissern Sie sich, dass der Name richtig geschrieben wurde. Möglicherweise besteht ein Netzwerkfehler. Klicken Sie auf "Diagnose", um die Netzwerkprobleme zu identifizieren und zu beheben.

Details ausblenden Diagnose Abbrechen

Fehlercode: 0x80004005
Unbekannter Fehler

Warum Windows-Dateifreigaben über WireGuard-VPN ohne die NetBIOS-Option nicht funktionieren — auch bei direkter IP-Adresse

- [Das Problem](#)
- [Hintergrund](#)
- [Protokolle & Ports](#)
- [Was passiert](#)
- [Warum auch direkte IP?](#)
- [FritzBox intern](#)
- [Fix](#)
- [Quellen](#)

Inhaltsverzeichnis

1. Das Problem in der Praxis
2. Hintergrund: SMB vs. NetBIOS
3. Protokolle & Ports im Überblick
4. Was passiert beim Verbindungsaufbau?
5. Warum scheitert es auch bei direkter IP-Eingabe?
6. FritzBox-interne Mechanik
7. Fix & Empfehlungen
8. Quellen

☐☐ Das Problem in der Praxis

Wer über eine FritzBox, die als WireGuard-Client konfiguriert ist, auf Windows-Dateifreigaben (SMB/CIFS) im Remote-Netz zugreift, erlebt oft folgenden Fehler:

```
\\192.168.2.11\Freigabe Fehlercode: 0x80004005 "Zugriff verweigert" / "Auf Netzwerkressource kann nicht zugegr
```

Das Verwirrende: Port-Checks auf TCP 445 schlagen durch, die Authentifizierung klappt in separaten Test-Tools — aber Windows Explorer und `net use` scheitern zuverlässig.



Die Lösung In der FritzBox-Oberfläche unter dem WireGuard-Peer den Haken bei "**NetBIOS über diese Verbindung zulassen**" setzen. Danach funktioniert der Zugriff sofort — ohne Neustart.

Aber *warum* ist das nötig? Und warum hilft es sogar, wenn man gar keinen Hostnamen, sondern direkt die IP-Adresse eingibt?

☐☐ Hintergrund: SMB vs. NetBIOS

SMB (Server Message Block) ist das Windows-Protokoll für Dateifreigaben. Es existiert in zwei grundlegend verschiedenen Betriebsmodi:

☐ Modernes SMB (Direct Hosting)

- TCP Port **445**
- SMB 2.x und 3.x
- Ab Windows Vista / Server 2008
- Kein NetBIOS benötigt
- Direkte TCP-Verbindung
- Sicherer, effizienter

⚠ Legacy SMB über NetBIOS

- TCP Port **139**
- SMB 1.0 / CIFS
- Ältere Systeme, NAS-Geräte
- Benötigt NBNS (Port 137)
- Namensauflösung über Broadcast
- Sicherheitsrisiken bekannt



Das zentrale Problem Windows versucht beim Verbindungsaufbau *immer beide Wege gleichzeitig*. Auch wenn der Server modernes SMB auf Port 445 spricht, sendet Windows parallel NetBIOS-Queries (Broadcasts auf UDP 137/138). Diese Broadcasts werden von WireGuard-Tunneln und den Firewalls dahinter standardmäßig **gefiltert**.

📁 Protokolle & Ports im Überblick

Port	Protokoll	Dienst	Ohne NetBIOS-Option	Zweck
445/TCP	TCP	Direct SMB	DURCH	Modernes SMB, direkte Verbindung
137/UDP	UDP	NBNS (Name Service)	BLOCKIERT	NetBIOS-Namensauflösung via Broadcast
138/UDP	UDP	NetBIOS Datagram	BLOCKIERT	Verbindungslose Broadcasts, Netzwerk-Discovery
139/TCP	TCP	NetBIOS Session	BLOCKIERT	Legacy SMB über NetBIOS (ältere Systeme)

NetBIOS wurde ursprünglich für kleine Netzwerke der 1980er Jahre entwickelt und basiert konzeptionell auf **Broadcasts**. Broadcasts können per Design **nicht durch IP-Router geleitet werden**. WireGuard als Layer-3-Protokoll routet nur Unicast-Pakete — Broadcasts bleiben am

Tunnel-Ende stecken.

☐ Was passiert beim Verbindungsaufbau?

☐ Ohne "NetBIOS aktivieren"

Schritt 1

Windows-Client gibt `\\192.168.2.11\Freigabe` ein

↓

Schritt 2

Windows startet parallel: TCP-Verbindung auf Port 445 *und* NetBIOS-Query auf UDP 137

↓

Schritt 3

UDP 137-Broadcast → WireGuard-Tunnel → FritzBox-Firewall filtert → **kein NBNS-Response**

↓

Schritt 4

Windows wartet auf NBNS-Timeout, versucht LLMNR als Fallback — auch geblockt

↓

Schritt 5

Verbindungsaufbau schlägt fehl: **0x80004005 — Zugriff verweigert**

☐ Mit "NetBIOS aktivieren"

Schritt 1

Windows-Client gibt `\\192.168.2.11\Freigabe` ein

↓

Schritt 2

Windows startet parallel: TCP Port 445 *und* NBNS-Query (UDP 137)

↓

Schritt 3

FritzBox lässt UDP 137/138 und TCP 139 durch (`dont_filter_netbios = yes`)

↓

Schritt 4

NBNS-Response kommt zurück — Windows nimmt das schnellste

↓

Schritt 5

SMB-Session wird aufgebaut — Freigabe erreichbar ✓

☐ Warum scheitert es auch bei direkter IP-Eingabe?

Die häufigste Verwunderung: "Ich gebe doch `\\192.168.2.11\Freigabe` ein — keine Hostnamen! Warum brauche ich NetBIOS?"

Das liegt am Windows-SMB-Stack. Auch bei direkter IP-Eingabe sendet Windows intern zunächst eine **NBNS-Reverse-Query** — eine Art "Wer bist du?" an die Ziel-IP. Das dient der Sessionvorbereitung und Capability-Discovery, nicht nur der Namensauflösung.

Konkret: Windows sendet einen **NetBIOS Node Status Request** (UDP 137) direkt an die Ziel-IP um den NetBIOS-Namen des Ziels herauszufinden und die SMB-Session korrekt zu initialisieren. Das ist Legacy-Verhalten das auch in modernen Windows-Versionen mit SMB 2/3 beibehalten wird.

Windows Explorer / net use

- · Nutzt den Windows LanmanWorkstation-Dienst
- · Vollständiger SMB-Stack inkl. NetBIOS-Init
- · Sendet NBNS Node Status Request
- · Scheitert wenn UDP 137 geblockt ist

Eigene SMB-Test-Tools

- · Nutzen oft eigene SMB-Bibliotheken
- · Direkte TCP-445-Verbindung
- · Überspringen die NetBIOS-Phase
- · Funktionieren auch ohne NetBIOS-Freigabe



Erklärt den scheinbaren Widerspruch Deshalb meldet ein eigenes Test-Tool "Authentifizierung OK, Freigaben erreichbar" — während Windows Explorer gleichzeitig `0x80004005` wirft. Das Tool umgeht den Windows-Stack und damit die NetBIOS-Phase vollständig.

⚙️ FritzBox-interne Mechanik

Hinter der UI-Option steckt ein interner FritzBox-Konfigurationsparameter:

NetBIOS deaktiviert (Standard nach Stromausfall/Reset): dont_filter_netbios = no # → FritzBox-Firewall filtert UD

Es handelt sich dabei **nicht** um ein echtes Application-Level Gateway (ALG) — die FritzBox modifiziert den SMB-Traffic nicht. Sie öffnet lediglich Firewall-Regeln für die betreffenden NetBIOS-Ports auf dem WireGuard-Interface.



Wichtig: Nur für Site-to-Site AVM bietet diese Option offiziell nur für *Netzwerk-zu-Netzwerk*-WireGuard-Verbindungen an, nicht für reine Client-VPN-Profile.

Warum nach Stromausfall weg?

Ein Stromausfall kann dazu führen, dass die FritzBox ihre WireGuard-Konfiguration aus einem älteren Checkpoint restauriert, oder dass einzelne Konfigurationsparameter auf Defaults zurückfallen. Der Default für `dont_filter_netbios` ist in manchen Firmware-Versionen `no`.



Historisch In FritzOS 8.20 wurde der Default auf `no` geändert, was bei vielen Nutzern SMB-Probleme über WireGuard auslöste.

Fix & Empfehlungen

Sofort-Fix (FritzBox-Oberfläche)

FritzBox UI → Internet → Freigaben → VPN (WireGuard) → WireGuard-Peer auswählen (Bearbeiten) → Haken bei "Ne



Kein Neustart nötig — wirkt sofort.

Dauerhaft absichern

Nach dem Fix die aktuelle Konfiguration als Backup exportieren: *System* → *Sicherung*. Dann überlebt die Einstellung den nächsten Stromausfall.

Alternative: NetBIOS clientseitig abschalten

Langfristig sauberer: NetBIOS auf den Clients vollständig deaktivieren und nur Direct-SMB auf TCP 445 zulassen — setzt voraus, dass alle Server SMB 2+ sprechen.

```
# PowerShell (als Admin): $adapters = Get-WmiObject Win32_NetworkAdapterConfiguration -Filter "IPEnabled=Tru
```



Achtung: Wenn noch ein altes NAS oder Gerät mit SMB1/CIFS im Netz ist (ältere Synology, QNAP, Windows XP), kann NetBIOS deaktivieren den Zugriff darauf brechen.

Quellen

- [AVM: WireGuard-VPN zwischen zwei FRITZ!Box-Netzwerken einrichten](#)
- [IP-Phone-Forum: WireGuard-VPN Zugriff SMB nicht erfolgreich](#)
- [Administrator.de: Kein SMB Zugriff über Fritzbox Wireguard](#)
- [Microsoft Learn: Direct hosting of SMB over TCP/IP](#)
- [4sysops: SMB port numbers explained](#)