FortiClient

- Enable Debug Logging
- VPN Client Installation
- SSL-VPN on custom Interface

Enable Debug Logging

1. Open FortiClient
2. Click the “Cog” Icon in the top right corner

3. Click on the “Lock” Icon in the top right corner

4. Set “Log Level” to “Fehlersuche” / “Debug”

VPN Client Installation

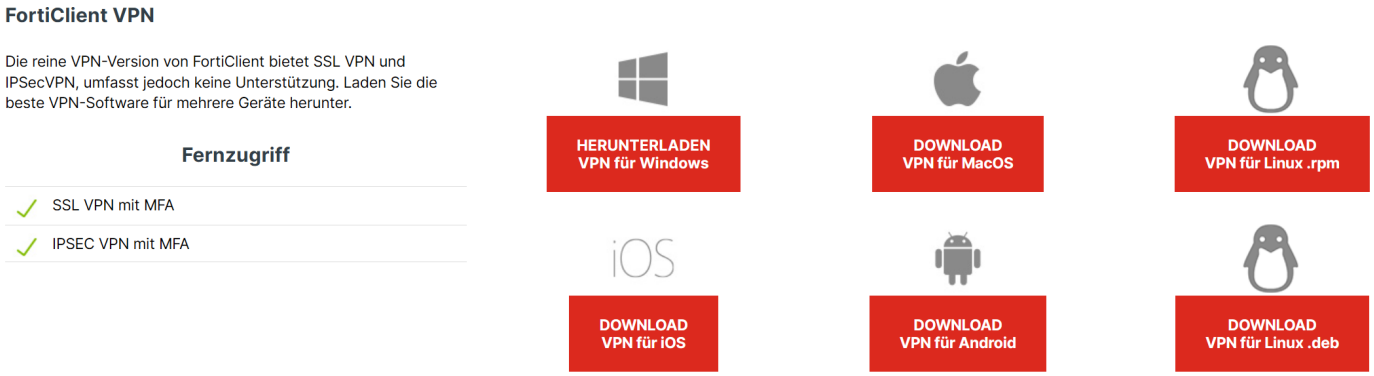
Requirements

- VPN Configuration File
- Username
- Password

Install FortiClient

Download latest FortiClient Release from https://www.fortinet.com/de/support/product-downloads

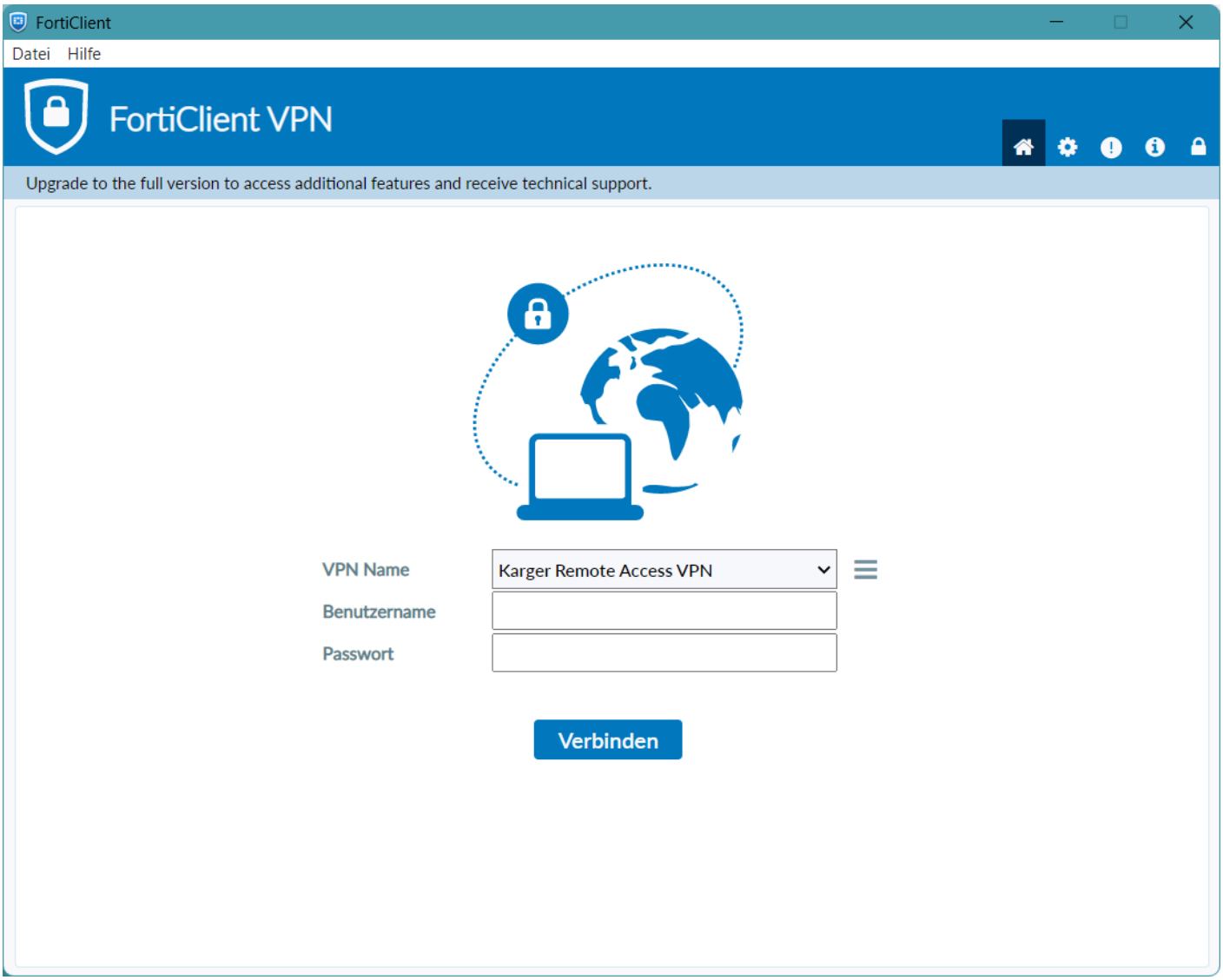
> Only Download the "VPN-only Version" !



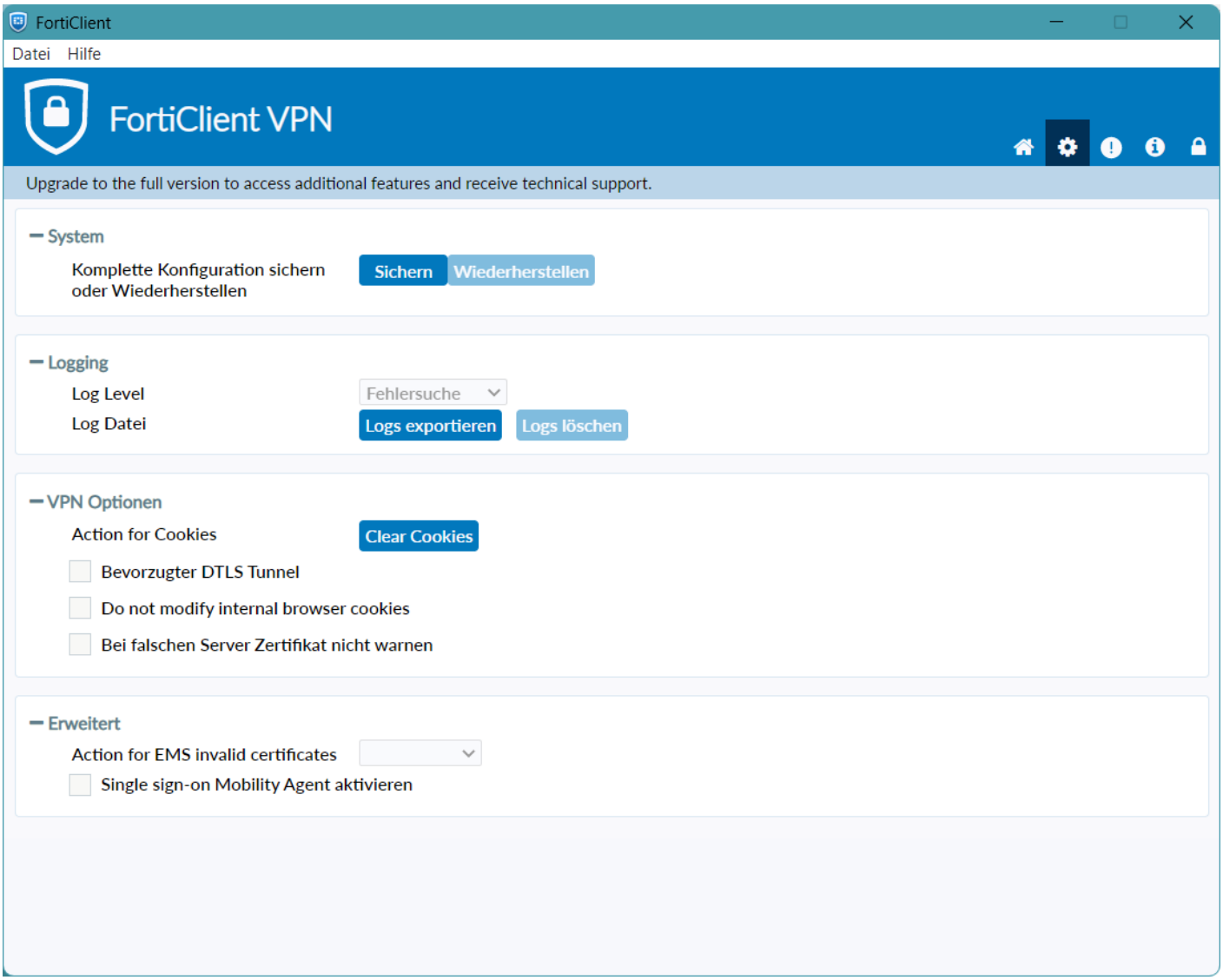
Run and complete the Setup after downloading

Importing VPN Configuration

Launch “FortiClient” after installing

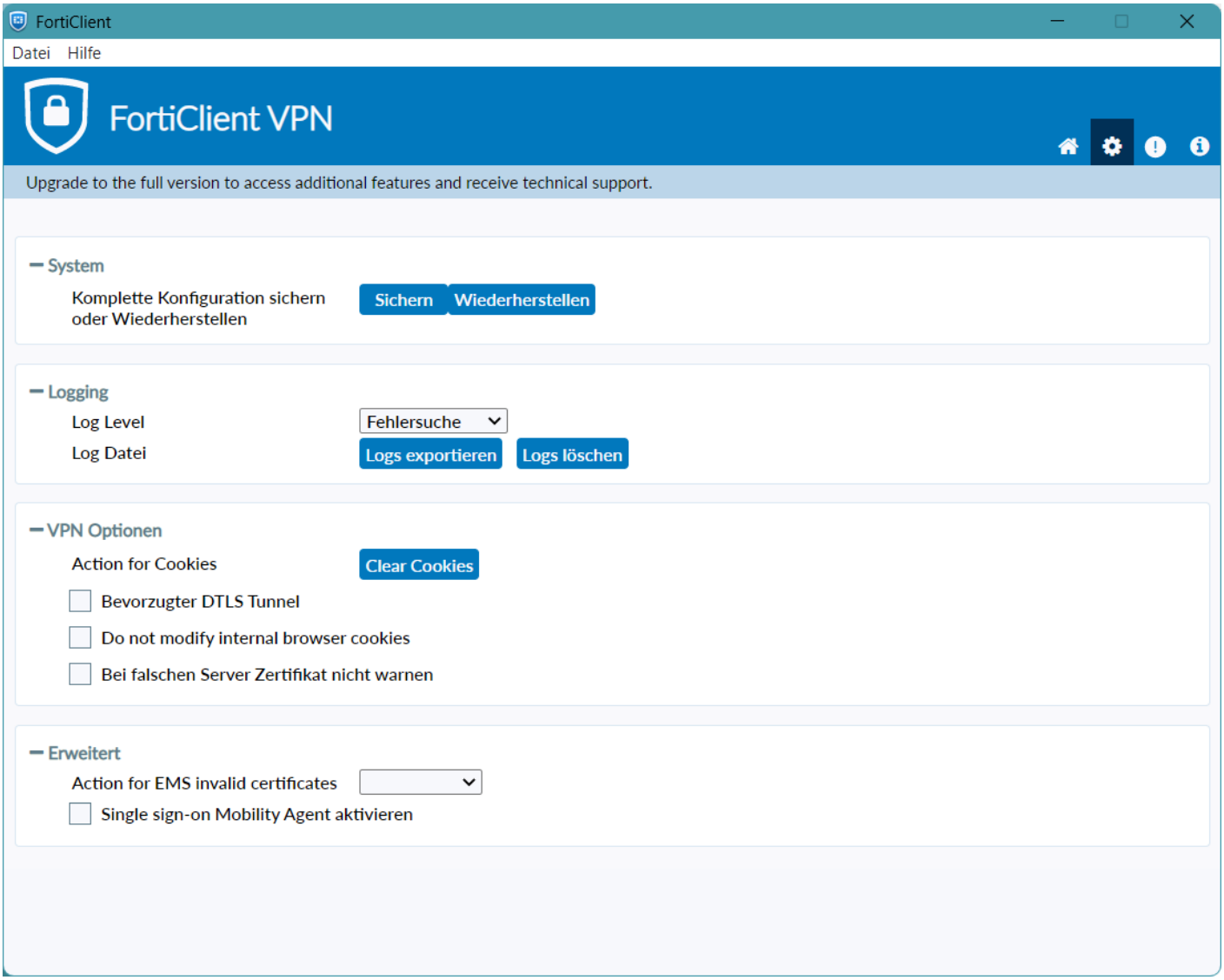


Click on the “Cog” Icon in the top right corner

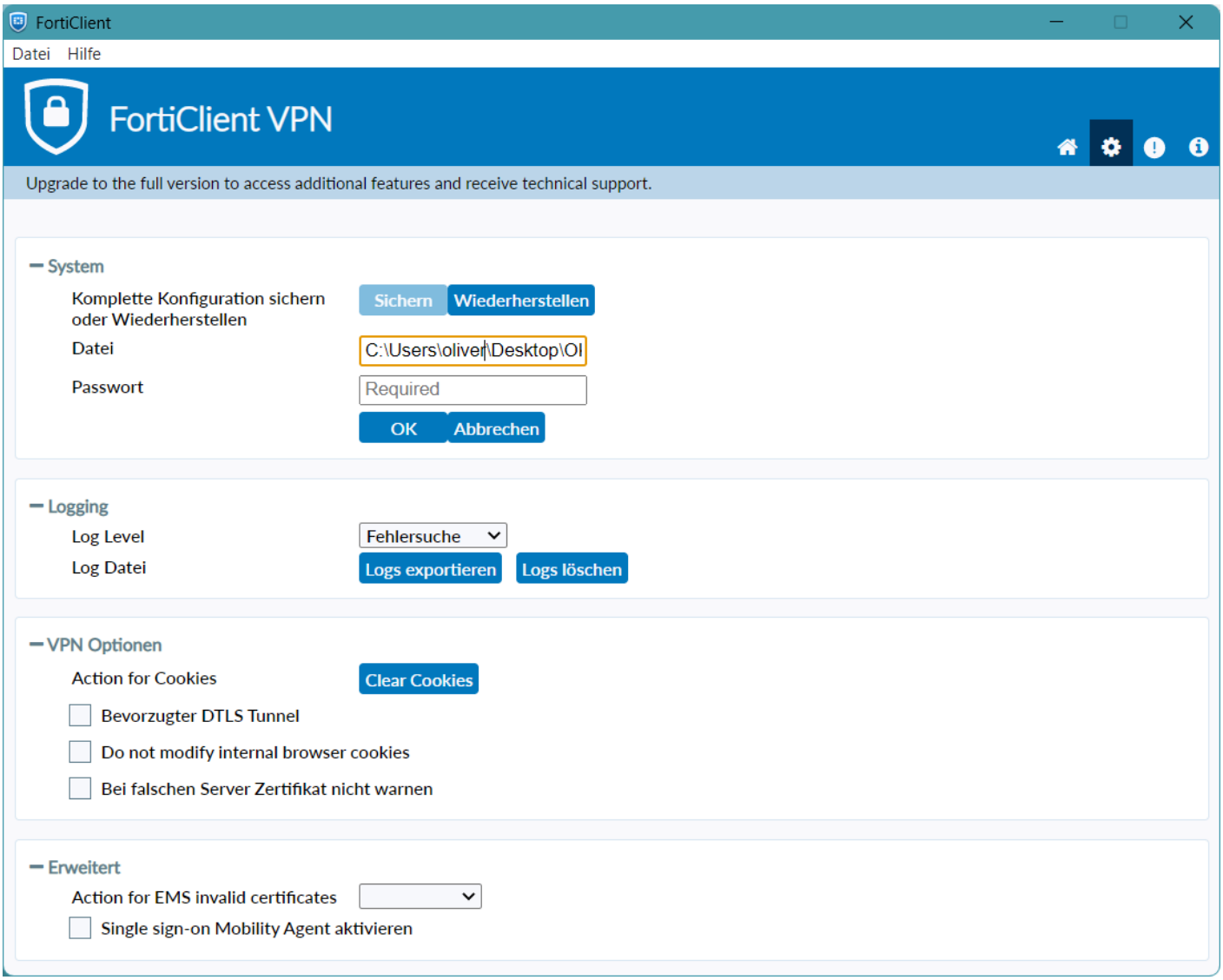


Click on the “Lock” icon in the top left corner to unlock the System Configuration Import ("Wiederherstellen" Button the the Screenshot)

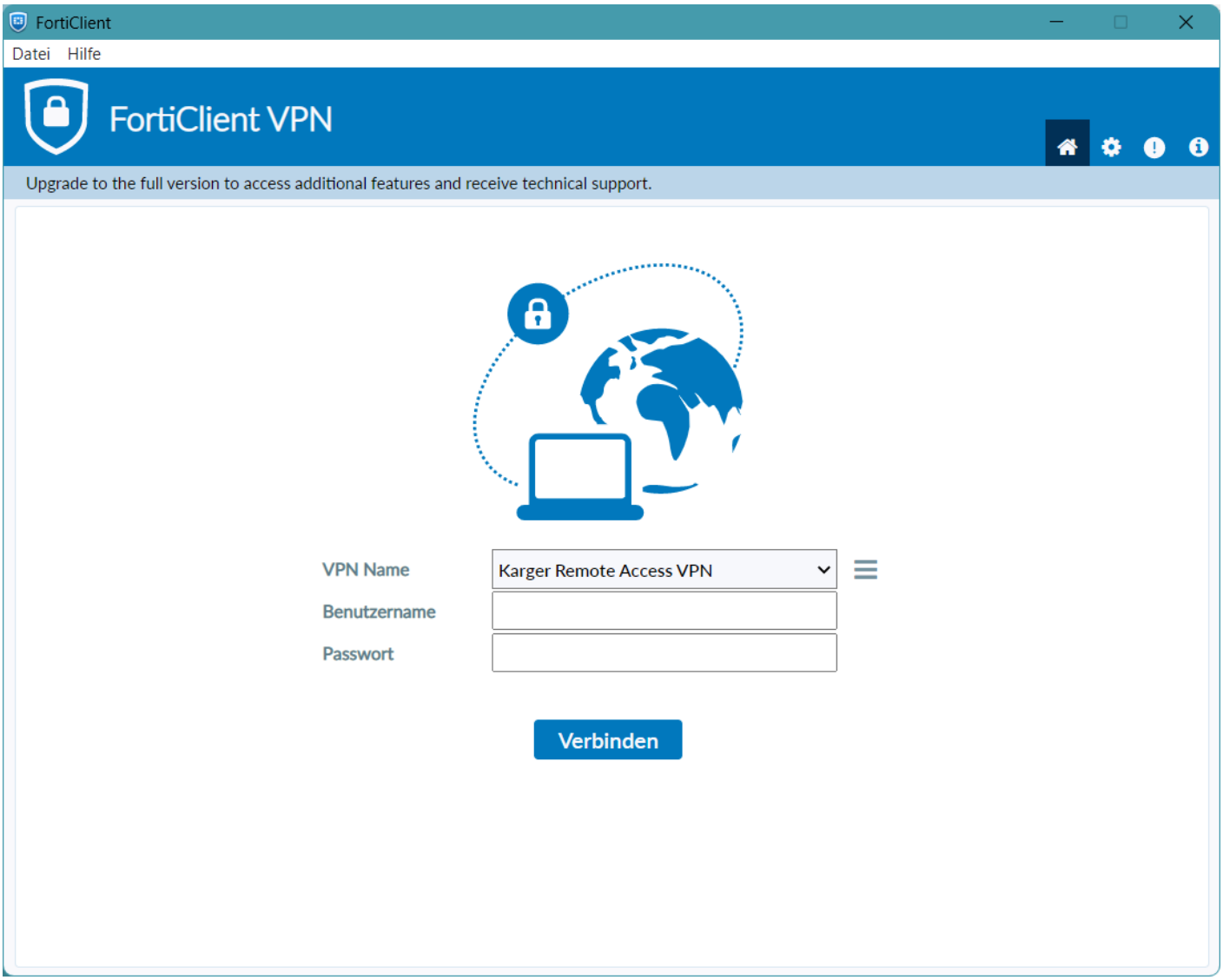
Click “Wiederherstellen and select your Configuration File”



5. (Optional) If your Configuration File is encrypted, enter your Password provided to you by your Administrator



Click on the “Home” Icon in the top left, enter your Username and Password to connect

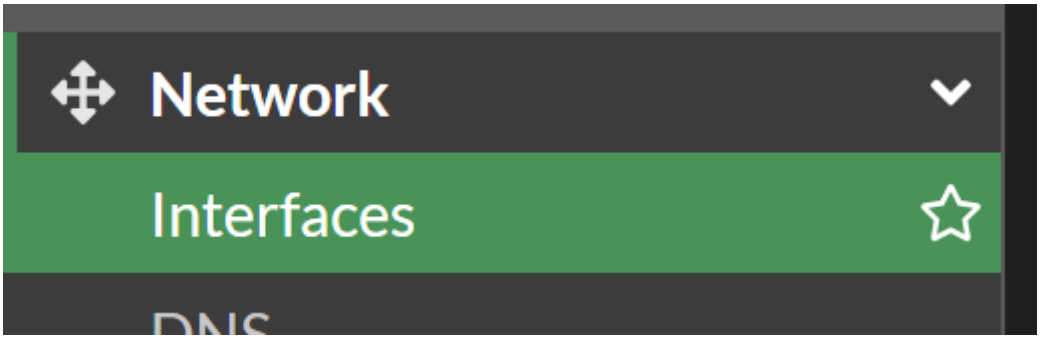

FortiClient
Datei
Hilfe
FortiClient VPN
Upgrade to the full version to access additional features and receive technical support.
VPN Name
Karger Remote Access VPN
Benutzername
Passwort
Verbinden

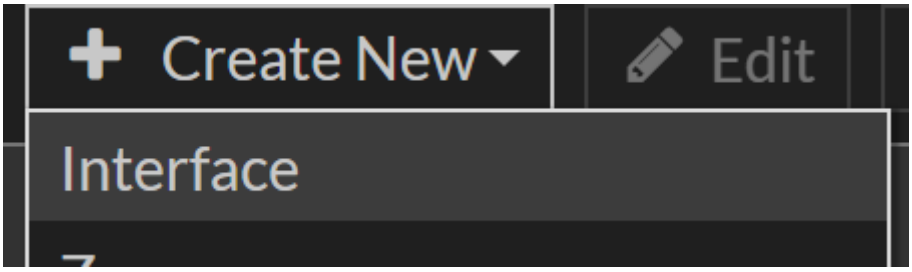
SSL-VPN on custom Interface

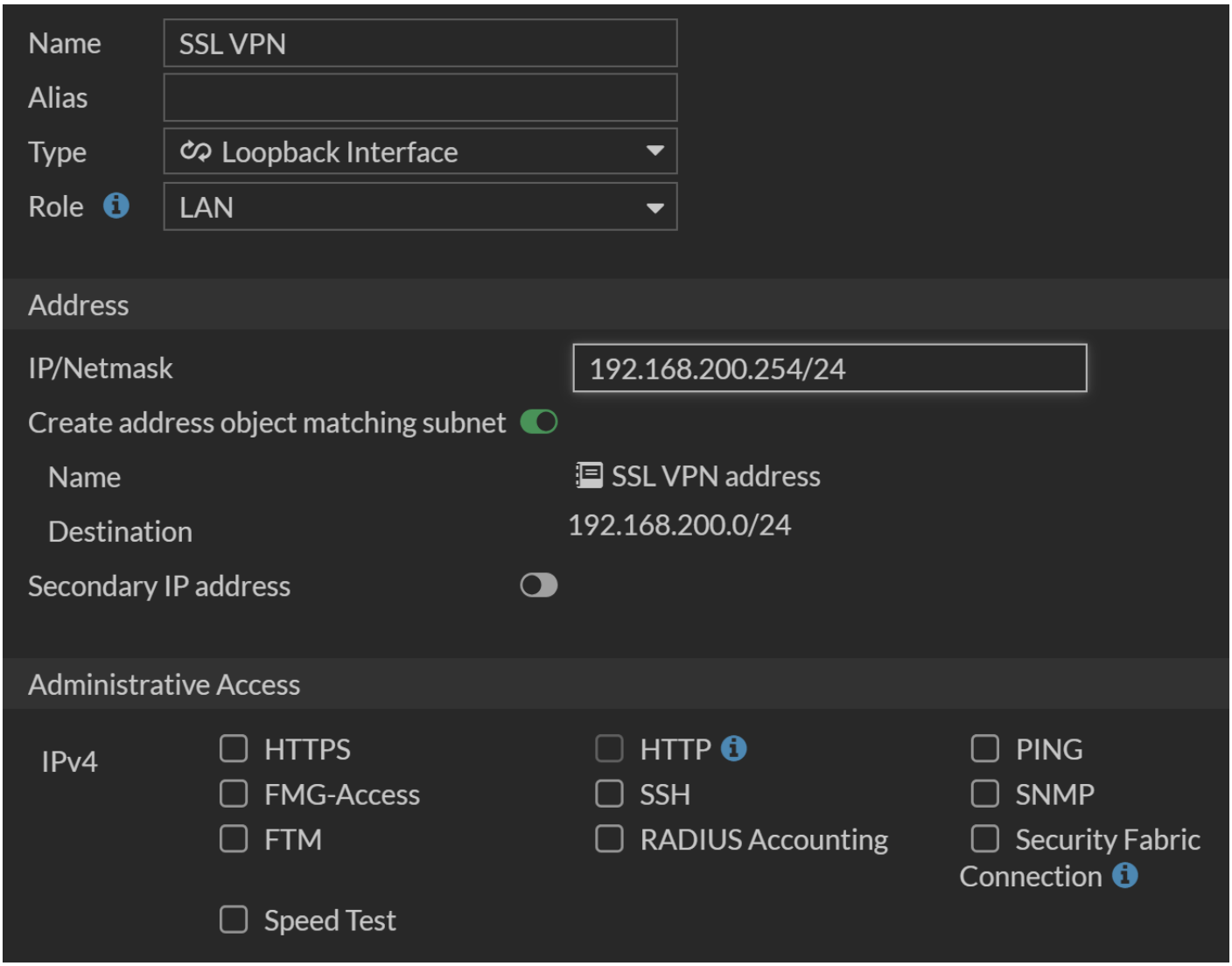
This explains how to setup the SSL-VPN on a FortiGate (E-Series) on a Custom Interface for better Controls.

This is done because per default, SSL-VPN Listens on the WAN Interface directly, therefor can not be controlled by any Policy.

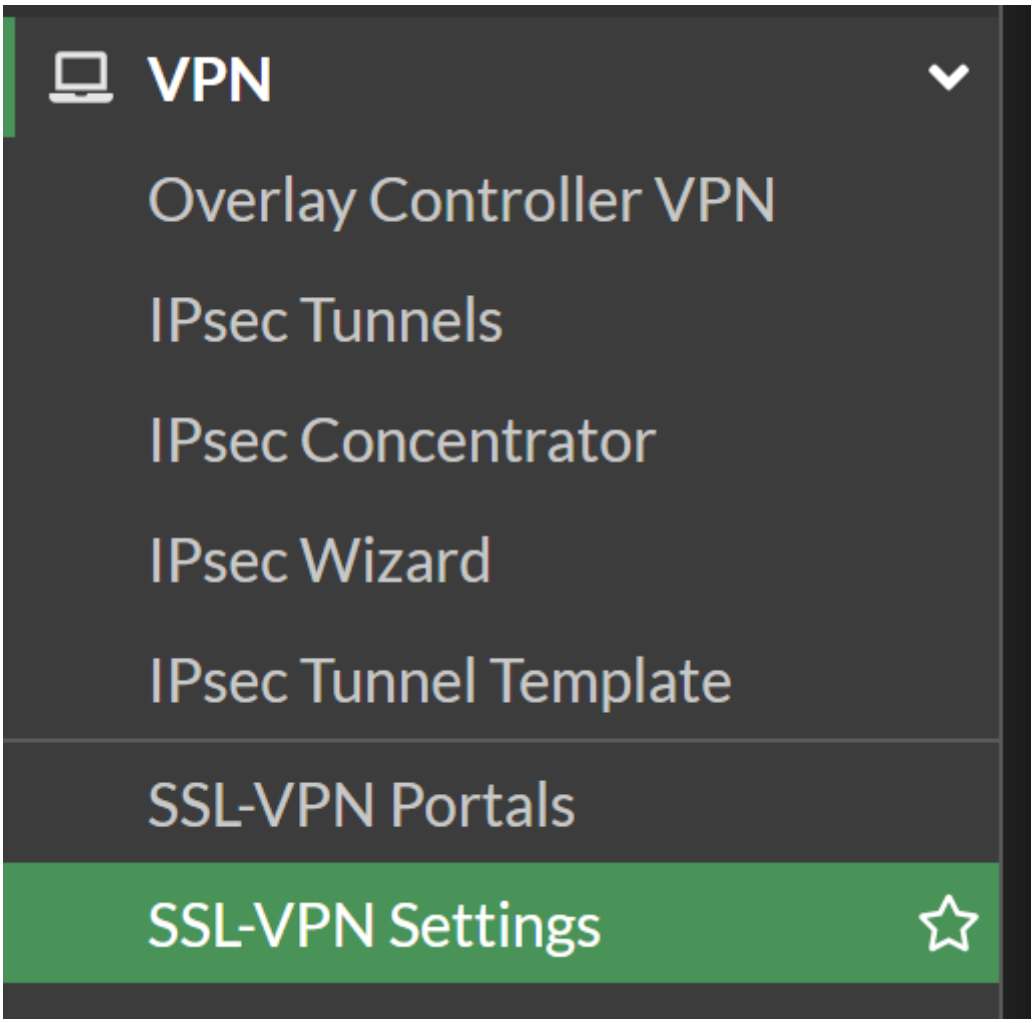
Create Loopback Interface

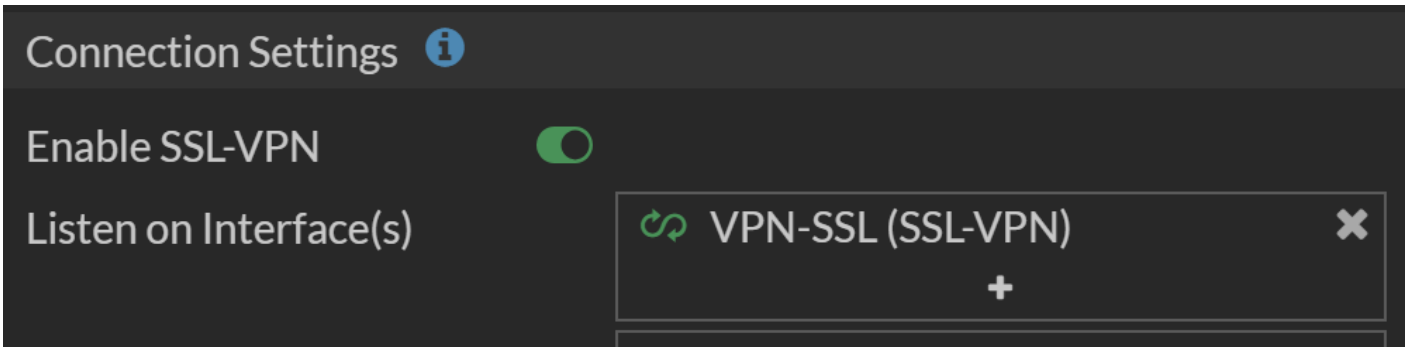






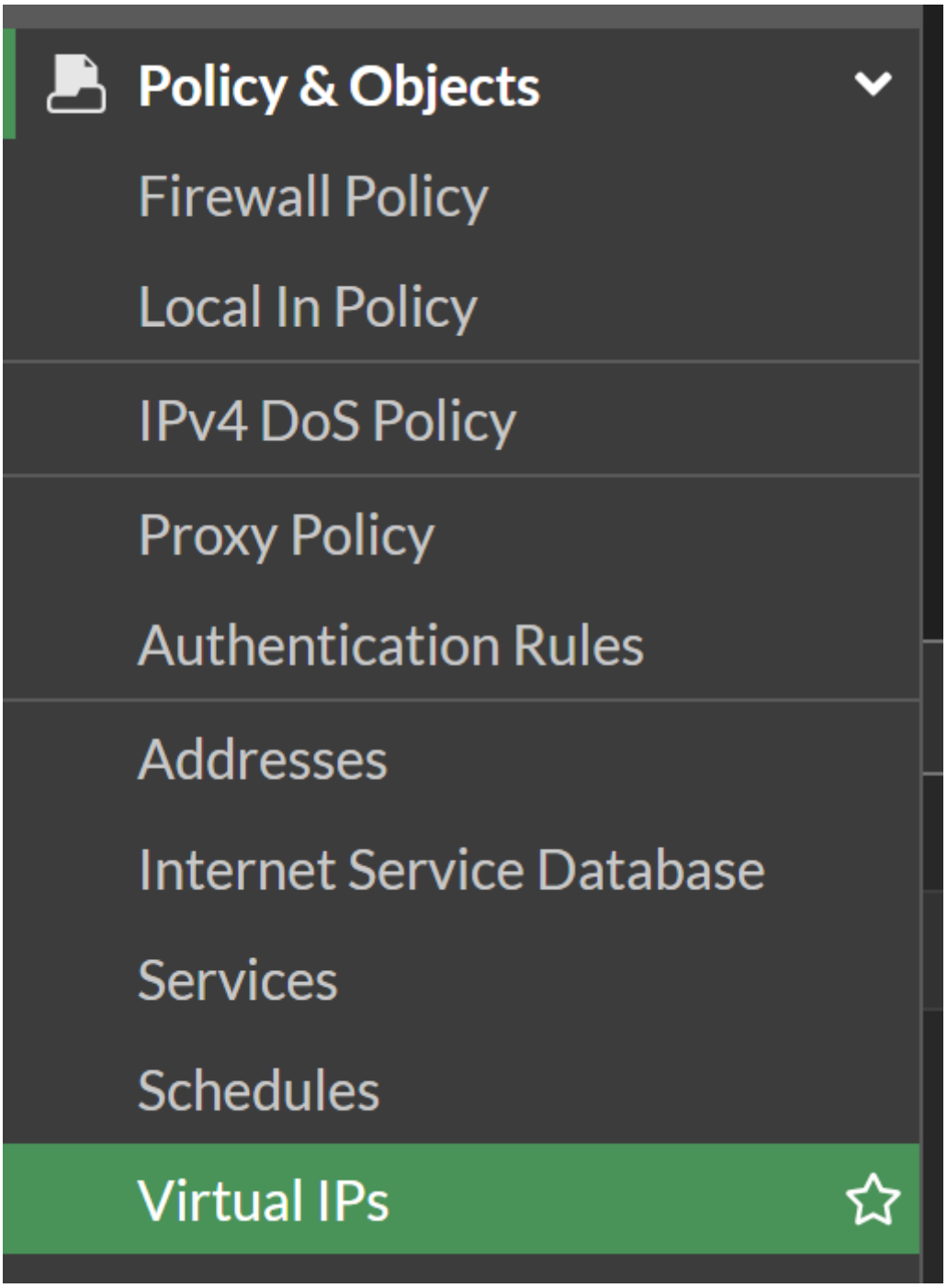
Bind SSL-VPN to new Loopback Interface

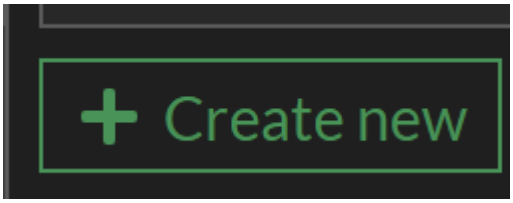


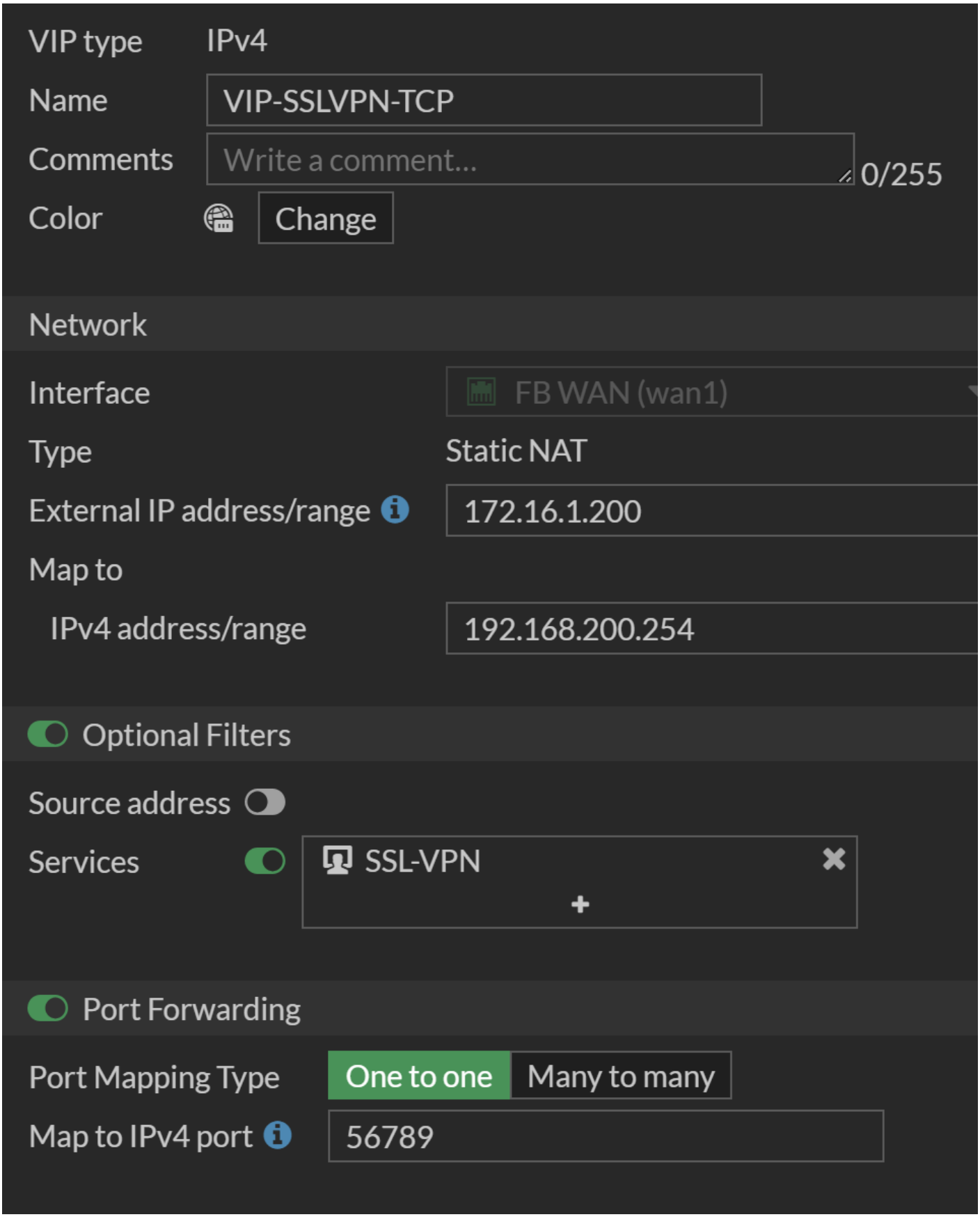


Redirect SSL-VPN Traffic

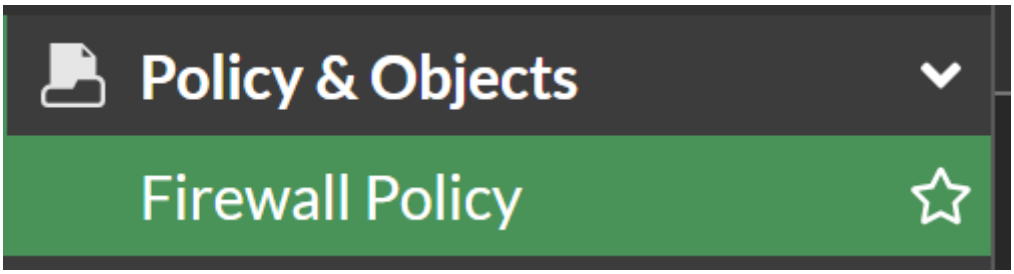
We now need to make sure the SSL-VPN Traffic actually reaches the new SSL-VPN Interface. We will use a Virtual IP with Port Forwarding for that.

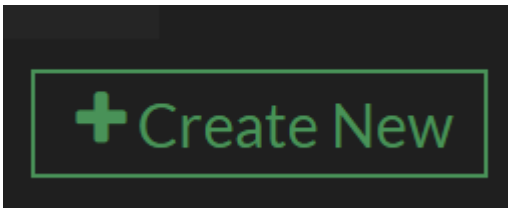

Policy & Objects
Firewall Policy
Local In Policy
IPv4 DoS Policy
Proxy Policy
Authentication Rules
Addresses
Internet Service Database
Services
Schedules
Virtual IPs

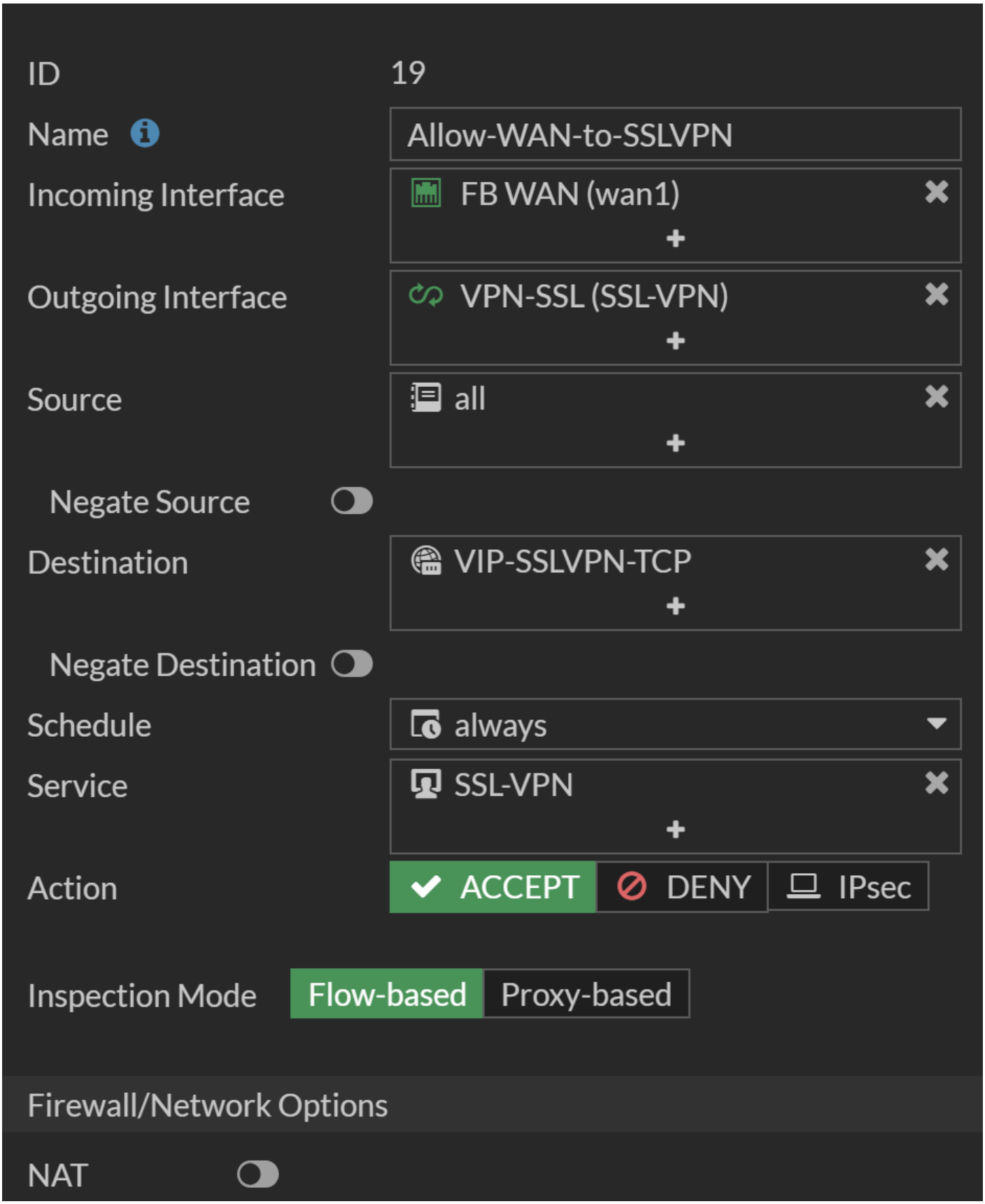

Create new



Allow Traffic to new Interface


Policy & Objects
Firewall Policy


Create New


ID
19
Name
Allow-WAN-to-SSLVPN
Incoming Interface
FB WAN (wan1)
Outgoing Interface
VPN-SSL (SSL-VPN)
Source
all
Negate Source
Destination
VIP-SSLVPN-TCP
Negate Destination
Schedule
always
Service
SSL-VPN
Action
ACCEPT
DENY
IPsec
Inspection Mode
Flow-based
Proxy-based
Firewall/Network Options
NAT