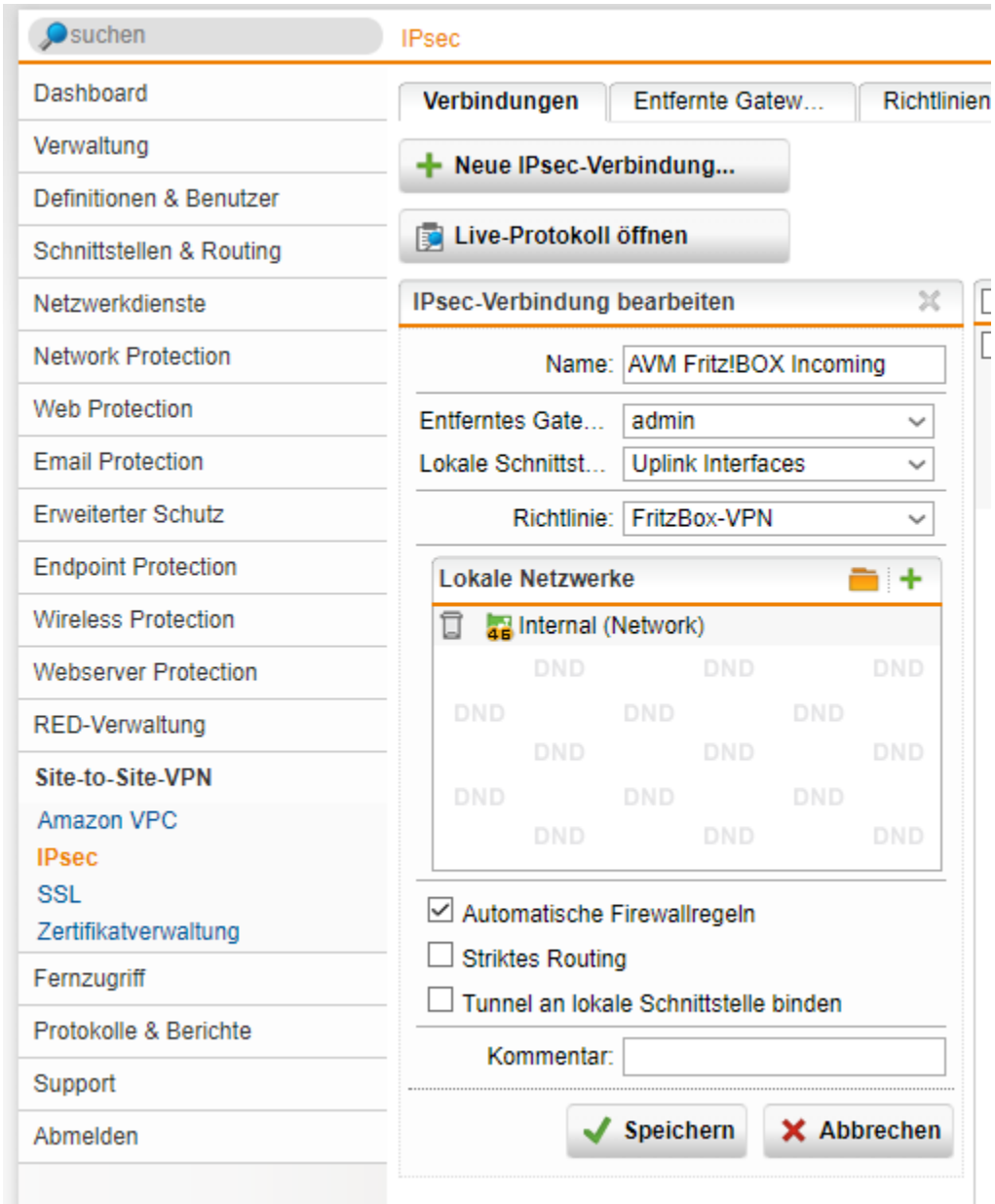
# VPN zwischen FritzBox und Sophos UTM - Update: 12.05.2022

Update

12.05.2022 - Verschlüsselung von Diffie-Hellman 14 auf 15 angehoben + Neuen Screenshots
11.05.2022 - Verschlüsselung von Diffie-Hellman 2 auf 14 angehoben + Neuen Screenshots

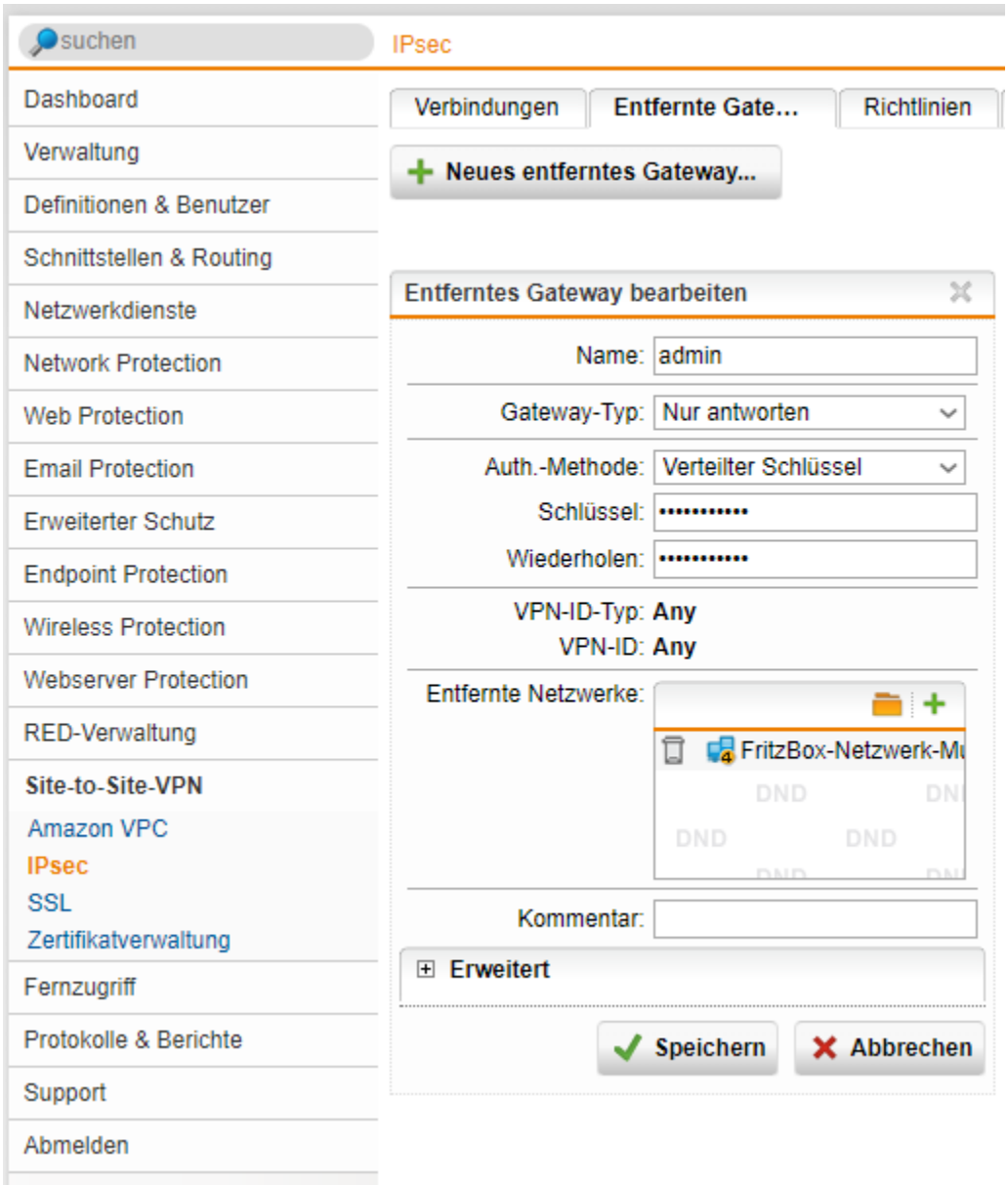
**UTM 9 -> Site-to-Site-VPN -> IPsec -> Verbindungen:**
Name: AVM Fritz!BOX Incoming
Entferntes Gateway: AVM Fritz!BOX GW
Lokale Schnittstelle: Uplink Interface (WAN)
Richtlinie: AVM Fritz!BOX policy
Lokale Netzwerke: Internal (Network)

Automatische Firewallregeln: ja
Striktes Routing : nein
Tunnel an lokale Schnittstelle binden: nein



**UTM 9 -> Site-to-Site-VPN -> IPsec -> entfernte Gateways:**
Name: AVM Fritz!BOX GW
Gateway-Typ: nur antworten
Auth.-Methode: Verteilter Schlüssel
Schlüssel: Gehe!mn!5
Wiederholen: Gehe!mn!5

Entfernte Netzwerke:
Name: AVM Fritz!BOX Netzwerk
Typ: Netzwerk
IPv4-Adresse: 192.168.178.0
Netzmaske: /24 255.255.255.0
Kommentar: AVM Standard 192.168.178.0/24

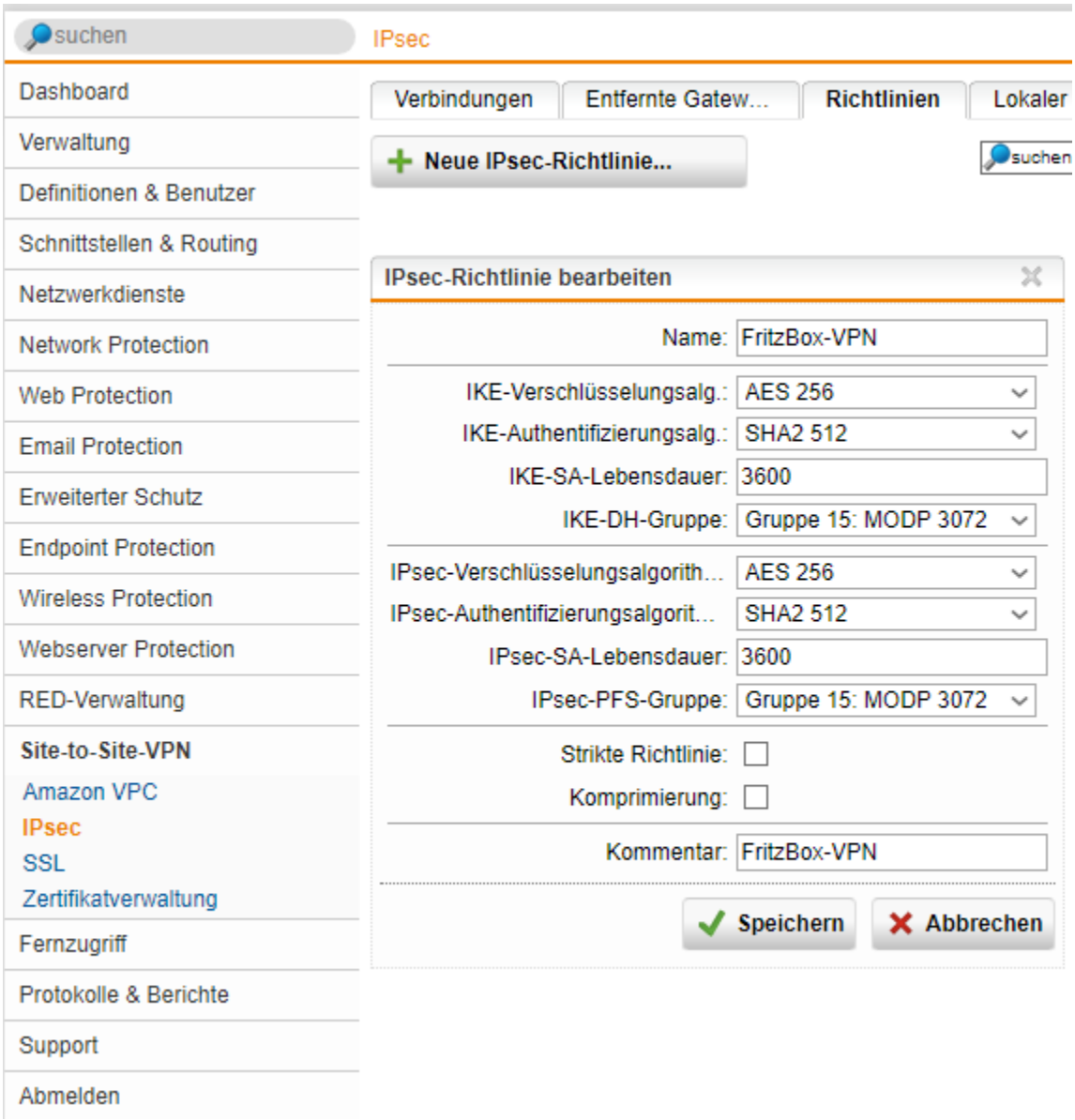



**UTM 9 -> Site-to-Site-VPN -> IPsec -> Richtlinie:**
Name: AVM Fritz!BOX policy

| IKE Verschl. | IKE Auth | IKE Lifetime | IKE Gruppe |
|---|---|---|---|
| AES 256 | SHA2 512 | 3600 | Group15: MODP 3072 |

| IPSec Verschl. | IPSec Auth | IPSec Lifetime | IPSec Gruppe |
|---|---|---|---|
| AES 256 | SHA2 512 | 3600 | Group15: MODP 3072 |

Strikte Richtlinie: NEIN
Komprimierung: NEIN




**Voraussetzungen / Einschränkungen durch die FirtzBox - Quelle: https://avm.de/service/vpn/tipps-tricks/fritzbox-mit-einem-firmen-vpn-verbinden/**

**Voraussetzungen / Einschränkungen**

- Die FRITZ!Box unterstützt VPN-Verbindungen nach dem IPSec-Standard mit ESP, IKEv1 und Pre-Shared Keys. Authentication Header (AH) und Perfect Forward Security (PFS) werden nicht unterstützt.
- Unterstützte IPSec-Algorithmen für IKE-Phase 1:
  - Verschlüsselungsverfahren: AES mit 256, 192, 128 Bit, Triple-DES mit 168 Bit oder DES mit 56 Bit
  - Hash-Algorithmus: SHA2-512, SHA1 oder MD5-96
  - Die FRITZ!Box nutzt beim Schlüsselaustausch über Diffie-Hellman initial 1024 Bit (DH-Gruppe 2). Sie akzeptiert danach aber auch 768, 1536, 2048 und 3072 Bit (DH-Gruppe 1, 5, 14 und 15).
- Unterstützte IPSec-Algorithmen für IKE-Phase 2:
  - Verschlüsselungsverfahren: AES mit 256, 192, 128 Bit, Triple-DES mit 168 Bit oder DES mit 56 Bit
  - Hash-Algorithmus: SHA2-512, SHA1 oder MD5-96
  - Die Diffie-Hellman-Gruppe wird durch IKE-Phase 1 bestimmt
  - Kompression: keine

Diese Anleitung bezieht sich auf FRITZ!OS 7.28 oder neuer. Unter einem älteren FRITZ!OS kann die Einrichtung abweichen oder die Funktion nicht zur Verfügung stehen. Die FRITZ!OS-Version finden Sie in der Benutzeroberfläche auf der Seite "Übersicht".

## Vorbereitung auf der AVM Seite:

Windows-Programm: Fernzugriff einrichten von AVM holen und starten, VPN Templatedatei erstellen und dann anpassen:
Angepasst müssen Folgende werte:
Zeile 5, Zeile 7, Zeile 14, Zeile 16, Zeile 19, Zeile 24, Zeile 31-32, Zeile 37-38 und Zeile 42
Zeile 5: Name der VPN Verbindung der in der FirtzBox angezeigt wird.
Zeile 7: keepalive_ip = <IP Adresse der UTM>;
Zeile 14: remotehostname = "<FQDN der Sophos UTM>";
Zeile 16: fqdn = "<FQDN der FritzBox>";
Zeile 19: fqdn = "<FQDN der Sophos UTM>";
Zeile 24: key = "<Gemeinsamer Schluessel>";
Zeile 31-32: IP Netz inkl. Subnet der FirtzBox
Zeile 37-38: IP Netz inkl. Subnet der Sopohs UTM
Zeile 42: accesslist = "permit ip any <IP Netz der UTM> <Subnet, Beispiel: 255.255.255.0>";

**VPN Config FritzBox**

```
vpncfg {
        connections {
                enabled = yes;
                conn_type = conntype_lan;
                name = "VPN zu SG EMSdetten";
                always_renew = yes;
                keepalive_ip = <IP Adresse der UTM>;
                reject_not_encrypted = no;
                dont_filter_netbios = yes;
                localip = 0.0.0.0;
                local_virtualip = 0.0.0.0;
                remoteip = 0.0.0.0;
                remote_virtualip = 0.0.0.0;
                remotehostname = "<FQDN der Sophos UTM>";
        localid {
                fqdn = "<FQDN der FritzBox>";
        }
        remoteid {
                fqdn = "<FQDN der Sophos UTM>";
        }
                mode = phase1_mode_idp;
                phase1ss = "dh15/aes/sha";
                keytype = connkeytype_pre_shared;
                key = "<Gemeinsamer Schluessel>";
                cert_do_server_auth = no;
                use_nat_t = yes;
                use_xauth = no;
                use_cfgmode = no;
                phase2localid {
                        ipnet {
                                ipaddr = <IP Netz der FritzBox>;
                                mask = 255.255.255.0;
                        }
                }
                phase2remoteid {
                        ipnet {
                                ipaddr = <IP Netz der UTM>;
                                mask = 255.255.255.0;
                        }
                }
                phase2ss = "esp-aes256-3des-sha/ah-no/comp-lzs-no/pfs";
                accesslist = "permit ip any <IP Netz der UTM> 255.255.255.0";
                }
                ike_forward_rules = "udp 0.0.0.0:500 0.0.0.0:500",
                "udp 0.0.0.0:4500 0.0.0.0:4500";
}
// EOF
```

Konfiguration anpassen (orange Parameter anzupassen) und dann in der Box als neues VPN einspielen.