

VPN zwischen FritzBox und Sophos UTM

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

The screenshot shows the Sophos UTM web interface. On the left is a navigation menu with categories like 'Dashboard', 'Verwaltung', 'Definitionen & Benutzer', 'Schnittstellen & Routing', 'Netzwerkdienste', 'Network Protection', 'Web Protection', 'Email Protection', 'Erweiterter Schutz', 'Endpoint Protection', 'Wireless Protection', 'Webserver Protection', 'RED-Verwaltung', 'Site-to-Site-VPN', 'Amazon VPC', 'IPsec', 'SSL', 'Zertifikatverwaltung', 'Fernzugriff', 'Protokolle & Berichte', 'Support', and 'Abmelden'. The main content area is titled 'IPsec' and has tabs for 'Verbindungen', 'Entfernte Gatew...', and 'Richtlinien'. A '+ Neue IPsec-Verbindung...' button is visible. Below it is a 'Live-Protokoll öffnen' button. A modal window titled 'IPsec-Verbindung bearbeiten' is open, showing the configuration for the 'AVM Fritz!BOX Incoming' connection. The configuration includes: 'Entferntes Gate...' set to 'admin', 'Lokale Schnittst...' set to 'Uplink Interfaces', and 'Richtlinie' set to 'FritzBox-VPN'. Under 'Lokale Netzwerke', there is a table with one entry: 'Internal (Network)'. The table has columns for 'DND' and 'DND' (repeated three times). Below the table are three checkboxes: 'Automatische Firewallregeln' (checked), 'Striktes Routing' (unchecked), and 'Tunnel an lokale Schnittstelle binden' (unchecked). There is also a 'Kommentar:' field and two buttons: 'Speichern' (with a green checkmark) and 'Abbrechen' (with a red X).

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

suchen IPsec

Dashboard Verbindungen Entfernte Gate... Richtlinien

Verwaltung + Neues entferntes Gateway...

Definitionen & Benutzer

Schnittstellen & Routing

Netzwerkdienste

Network Protection

Web Protection

Email Protection

Erweiterter Schutz

Endpoint Protection

Wireless Protection

Webserver Protection

RED-Verwaltung

Site-to-Site-VPN

Amazon VPC

IPsec

SSL

Zertifikatverwaltung

Fernzugriff

Protokolle & Berichte

Support

Abmelden

Entferntes Gateway bearbeiten

Name: admin

Gateway-Typ: Nur antworten

Auth.-Methode: Verteilter Schlüssel

Schlüssel:

Wiederholen:

VPN-ID-Typ: Any

VPN-ID: Any

Entfernte Netzwerke:

FritzBox-Netzwerk-M	DND	DN
	DND	DND

Kommentar:

Erweitert

Speichern Abbrechen

UTM 9 -> Site-to-Site-VPN -> IPsec -> Richtlinie:

Name: **AVM Fritz!BOX policy**

IKE: AES 256 - SHA1 - 3600 - Group2: MODP 1024

IPsec: AES 256 - SHA1 - 3600 - Group2: MODP 1024

suchen IPsec

Dashboard Verbindungen Entfernte Gatew... Richtlinien Lokaler

Verwaltung + Neue IPsec-Richtlinie...

Definitionen & Benutzer

Schnittstellen & Routing

Netzwerkdienste

Network Protection

Web Protection

Email Protection

Erweiterter Schutz

Endpoint Protection

Wireless Protection

Webserver Protection

RED-Verwaltung

Site-to-Site-VPN

Amazon VPC

IPsec

SSL

Zertifikatverwaltung

Fernzugriff

Protokolle & Berichte

Support

Abmelden

IPsec-Richtlinie bearbeiten

Name: FritzBox-VPN

IKE-Verschlüsselungsalg.: AES 256

IKE-Authentifizierungsalg.: SHA1

IKE-SA-Lebensdauer: 3600

IKE-DH-Gruppe: Gruppe 2: MODP 1024

IPsec-Verschlüsselungsalgorith... AES 256

IPsec-Authentifizierungsalgorit... SHA1

IPsec-SA-Lebensdauer: 3600

IPsec-PFS-Gruppe: Gruppe 2: MODP 1024

Strikte Richtlinie:

Komprimierung:

Kommentar: FritzBox-VPN

Speichern Abbrechen

Vorbereitung auf der AVM Seite:

Windows-Programm: Fernzugriff einrichten von AVM holen und starten, VPN Templatedatei erstellen und dann anpassen:

VPN Config FritzBox

```
vpncfg {  
  
connections {  
  
enabled = yes;  
conn_type = conntype_lan;  
name = "VPN zu Sophos UTM";  
always_renew = yes;  
keepalive_ip = <Gateway der UTM Firewall>;  
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 UTM Firewall";  
localid {  
  
fqdn = "FQDN der FritzBox";  
  
}  
remoteid {  
  
fqdn = "FQDN Der UTM Firewall";  
  
}  
mode = phase1_mode_idp;  
phase1ss = "all/all/all";  
keytype = connkeytype_pre_shared;  
key = "<GEHEIMES Passwort>";  
cert_do_server_auth = no;  
use_nat_t = yes;  
use_xauth = no;  
use_cfgmode = no;  
phase2localid {  
  
ipnet {  
  
ipaddr = <IP der FirtzBox. Default: 192.168.178.0>;  
mask = 255.255.255.0;  
  
}  
  
}  
phase2remoteid {  
  
ipnet {  
  
ipaddr = <IP Kreis der UTM. Example: 192.168.110.0>;  
mask = 255.255.255.0;  
  
}  
  
}  
phase2ss = "esp-aes256-3des-sha/ah-no/comp-lzs-no/pfs";  
accesslist = "permit ip any <IP Kreis der UTM. Example: 192.168.110.0> 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.