

# Anleitung zur Herstellung einer IPSec/Ikev2 Site-to-Site Verbindung mit der OPNSense Option iVm einer Digitalisierungsbox Premium, die eine statische öffentliche IP Adresse hat

RA Thomas Schmidt – RA-MICRO Vertriebs GmbH – Stand 13.07.2020 – Alle Angaben ohne Gewähr

---

## 1. Teil: Rechenzentrum:

The screenshot shows the OPNSense web interface for configuring VPN tunnels. The browser address bar indicates the URL is `172.25.0.1/vpn_ipsec.php`. The sidebar on the left contains a navigation menu with the following items: Lobby, Berichterstattung, System, Schnittstellen, Firewall, VPN, IPsec, Tunnelnesteinstellungen, Mobile Clients, Pre-Shared Schlüssel, RSA Key Pairs, Erweiterte Einstellungen, Statusübersicht, Lease Status, Datenbank Sicherheitszuordnung, Datenbank Sicherheitsregelwerk, and Protokolldatei. The 'VPN' and 'IPsec' items are highlighted with red arrows. The main content area is titled 'VPN: IPsec: Tunnelnesteinstellungen' and features a table with the following columns: Typ, Ferner Gateway, Modus, Phase 1 Vorschlag, Authentifizierung, and Beschreibung. The table contains one entry with the following values: Typ: Lokales Subnetz, Ferner Gateway: Fernes Subnetz, Modus: Phase 2 Proposal. Below the table, there is a checkbox for 'IPsec aktivieren' and a 'Speichern' button. A red arrow points to the '+' button in the table's action column.

Typ	Ferner Gateway	Modus	Phase 1 Vorschlag	Authentifizierung	Beschreibung
Lokales Subnetz	Fernes Subnetz	Phase 2 Proposal			

- Lobby
- Berichterstattung
- System
- Schnittstellen
- Firewall
- VPN
  - IPsec 🔒
  - Tunneleinstellungen**
  - Mobile Clients
  - Pre-Shared Schlüssel
  - RSA Key Pairs
  - Erweiterte Einstellungen
  - Statusübersicht
  - Lease Status
  - Datenbank Sicherheitszuordnung
  - Datenbank Sicherheitsregelwerk
  - Protokolldatei
  - OpenVPN 🔒
- Dienste
- Energie
- Hilfe

## VPN: IPsec: Tunneleinstellungen

### Allgemeine Information

Deaktiviert	<input type="checkbox"/> Deaktiviere diesen Phase 1 Eintrag
Anschlussart	standard
Schlüsselaustauschversion	V2
Internet Protokoll	IPv4
Schnittstelle	WAN
Ferner Gateway	xxx.xx.xx.xx (die öffentliche IP der Digitalisierungsbox)
Dynamic gateway	<input type="checkbox"/> Allow any remote gateway to connect
Beschreibung	

### Phase 1 Vorschlag (Authentifizierung)

Authentifizierungsmethode	Mutual PSK
Meine Kennung	Meine IP-Adresse
Peer-Identifizierer	Peer IP-Adresse
Pre-Shared Schlüssel	ihreigenenSchlüsseleintragen

### Phase 1 Vorschlag (Algorithmen)

Verschlüsselungsalgorithmus	AES 256
Hashalgorithmus	SHA256
DH Schlüsselgruppe	14 (2048 bits)
Lebenszeit	28800

### Erweiterte Optionen

Lebenszeit	28800
<b>Erweiterte Optionen</b>	
Install policy	<input checked="" type="checkbox"/>
ReKey deaktivieren	<input type="checkbox"/>
Reauth deaktivieren	<input type="checkbox"/>
Tunnelisolation	<input type="checkbox"/>
NAT Traversal	Aktivieren
MOBIKE deaktivieren	<input type="checkbox"/>
Dead Peer Detection	<input type="checkbox"/>
Inactivity timeout	
Margintime	
Rekeyfuzz	

Speichern

Tunneleinstellungen | IPsec | VPN | x +

Nicht sicher | 172.25.0.1/vpn\_ipsec.php

root@OPNsense.localdomain

### VPN: IPsec: Tunneleinstellungen

Die IPsec-Tunnel Konfiguration wurde geändert.  
Sie müssen die Änderungen übernehmen, damit diese in Kraft treten. [Änderungen übernehmen](#)

	Typ	Ferner Gateway	Modus	Phase 1 Vorschlag	Authentifizierung	Beschreibung	
		<i>Lokales Subnetz</i>	<i>Fernes Subnetz</i>	<i>Phase 2 Proposal</i>			
<input type="checkbox"/>	IPV4 IKEv2	WAN 0.0.0.0		AES (256 Bits) + SHA512 + DH-Gruppe 14	Mutual PSK	Kanzlei_ohne_feste_offentliche_IP-Adresse	  
							 
<input type="checkbox"/>	IPsec aktivieren						

[Speichern](#)



- Lobby
- Berichterstattung
- System
- Schnittstellen
- Firewall
- VPN
  - IPsec
  - Tunneleinstellungen
  - Mobile Clients
  - Pre-Shared Schlüssel
  - RSA Key Pairs
  - Erweiterte Einstellungen
  - Statusübersicht
  - Lease Status
  - Datenbank Sicherheitszuordnung
  - Datenbank Sicherheitsregelwerk
  - Protokolldatei
  - OpenVPN
- Dienste
- Energie
- Hilfe

## VPN: IPsec: Tunneleinstellungen

### Allgemeine Information

Deaktiviert

Modus: Tunnel IPv4

Beschreibung: eigene Beschreibung

### Lokales Netzwerk

Typ: LAN Subnetz

Adresse: / 32

### Entferntes Netzwerk

Typ: Netzwerk

Adresse: 192.168.0.0 (Netzbereich der Kanzlei) / 24

### Phase-2-Vorschlag (SA / Schlüsselaustausch)

Protokoll: ESP

Verschlüsselungsalgorithmen:
 

- AES
  - 256 Bits
  - aes128gcm16
  - aes192gcm16
  - aes256gcm16
  - Blowfish
  - automatisch
  - 3DES
  - CAST128
  - DES
  - NULL (keine Verschlüsselung)

Hashalgorithmen: SHA256

PFS Schlüsselgruppe: 14 (2048 bits)

Lebenszeit: 28800 Sekunden

### Erweiterte Optionen

Automatisch Host pingen

Manuelle SPD-Einträge

Speichern

Tunneleinstellungen | IPsec | VPN | x +

Nicht sicher | 172.25.0.1/vpn\_ipsec.php

root@OPNsense.localdomain

VPN: IPsec: Tunneleinstellungen

Die IPsec-Tunnel Konfiguration wurde geändert.  
Sie müssen die Änderungen übernehmen, damit diese in Kraft treten.

**Änderungen übernehmen**

Typ	Ferner Gateway	Modus	Phase 1 Vorschlag	Authentifizierung	Beschreibung
Lokales Subnetz		Fernes Subnetz		Phase 2 Proposal	
<input type="checkbox"/>	IPV4 IKEV2	WAN 0.0.0.0	AES (256 Bits) + SHA512 + DH-Gruppe 14	Mutual PSK	Kanzlei_ohne_feste_öffentliche_IP-Adresse
<input type="checkbox"/>	ESP IPV4 tunnel	LAN	192.168.2.0/24	AES (256 Bits) + SHA512 + 14 (2048 bits)	Angaben_zu_den_zu_verbindenen_Netzwerken

IPsec aktivieren

**Speichern**

Tunneleinstellungen | IPsec | VPN | x +

Nicht sicher | 172.25.0.1/vpn\_ipsec.php

root@OPNsense.localdomain

VPN: IPsec: Tunneleinstellungen

Die Änderungen wurden erfolgreich angewandt.

Typ	Ferner Gateway	Modus	Phase 1 Vorschlag	Authentifizierung	Beschreibung
Lokales Subnetz		Fernes Subnetz		Phase 2 Proposal	
<input type="checkbox"/>	IPV4 IKEV2	WAN 0.0.0.0	AES (256 Bits) + SHA512 + DH-Gruppe 14	Mutual PSK	Kanzlei_ohne_feste_öffentliche_IP-Adresse
<input type="checkbox"/>	ESP IPV4 tunnel	LAN	192.168.2.0/24	AES (256 Bits) + SHA512 + 14 (2048 bits)	Angaben_zu_den_zu_verbindenen_Netzwerken

IPsec aktivieren

**Speichern**

Tunneleinstellungen | IPsec | VPN | x +

Nicht sicher | 172.25.0.1/vpn\_ipsec.php

OPNsense root@OPNsense.localdomain

Lobby  
Berichterstattung  
System  
Schnittstellen  
Firewall  
VPN  
IPsec  
Tunneleinstellungen  
Mobile Clients  
Pre-Shared Schlüssel  
RSA Key Pairs  
Erweiterte Einstellungen  
Statusübersicht  
Lease Status  
Datenbank Sicherheitszuordnung  
Datenbank Sicherheitsregelwerk  
Protokolldatei  
OpenVPN  
Dienste  
Energie  
Hilfe

### VPN: IPsec: Tunneleinstellungen

Die Änderungen wurden erfolgreich angewandt.

Typ	Ferner Gateway	Modus	Phase 1 Vorschlag	Authentifizierung	Beschreibung
Lokales Subnetz Fernes Subnetz Phase 2 Proposal					
<input type="checkbox"/> IPv4 IKEv2	WAN 0.0.0.0		AES (256 Bits) + SHA512 + DH-Gruppe 14	Mutual PSK	Kanzlei_ohne_feste_öffentliche_IP-Adresse
<input type="checkbox"/> ESP IPv4 tunnel	LAN	192.168.2.0/24	AES (256 Bits) + SHA512 + 14 (2048 bits)		Angaben_zu_den_zu_verbindenen_Netzwerken

IPsec aktivieren

**Speichern**

IPsec | Regeln | Firewall | OPNsense x Neuer Tab x +

Nicht sicher | 172.25.0.1/firewall\_rules.php?if=enc0

OPNsense root@OPNsense.localdomain

Lobby  
Berichterstattung  
System  
Schnittstellen  
Firewall  
Aliase  
Regeln  
Fließend  
IPsec  
LAN  
WAN  
NAT  
Shaper  
Gruppen  
Virtuelle IPs  
Einstellungen  
Protokolldateien  
Diagnose  
VPN  
Dienste

### Firewall: Regeln: IPsec

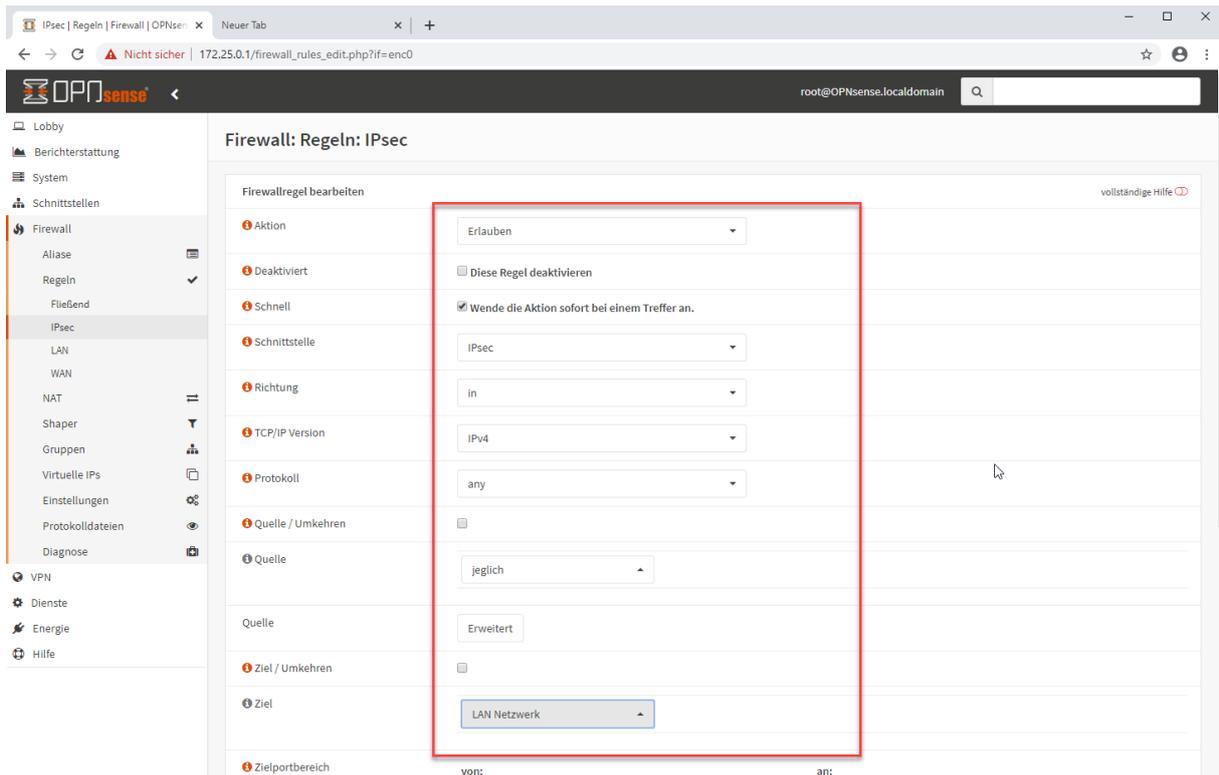
Nothing selected Inspect **Hinzufügen**

Die Änderungen wurden erfolgreich angewandt.

No IPsec rules are currently defined. All incoming connections on this interface will be blocked until you add a pass rule. Exceptions for automatically generated rules may apply.

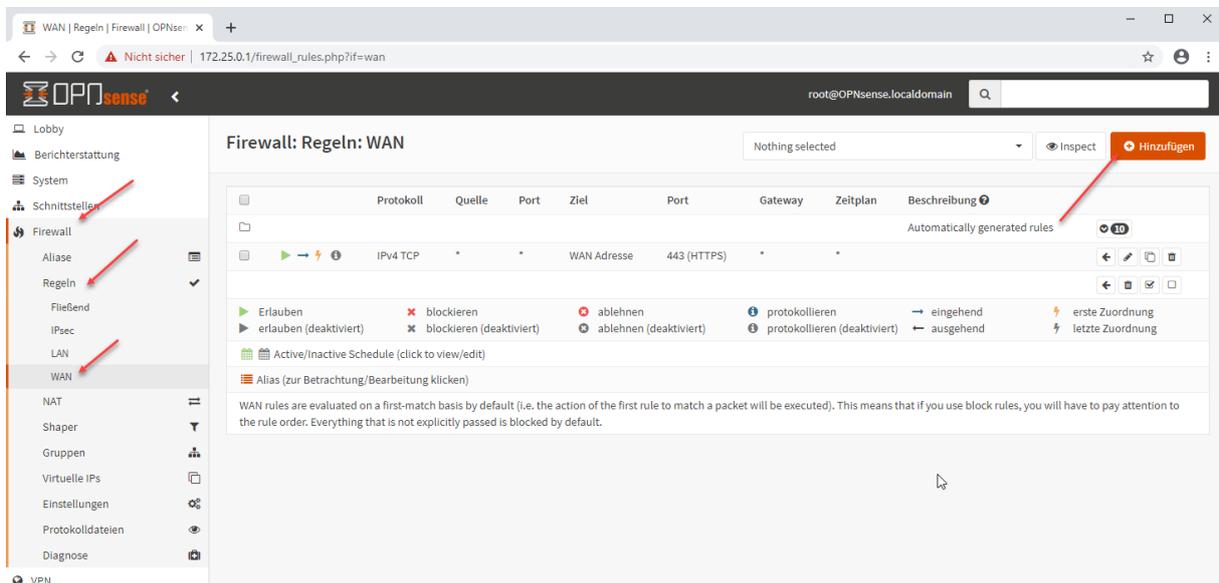
Protokoll	Quelle	Port	Ziel	Port	Gateway	Zeitplan	Beschreibung
Automatically generated rules							
<input type="checkbox"/>							
<input checked="" type="checkbox"/>	erlauben (deaktiviert)	blockieren (deaktiviert)	ablehnen (deaktiviert)	ablehnen (deaktiviert)	protokollieren (deaktiviert)	protokollieren (deaktiviert)	→ eingehend ← ausgehend ⚡ erste Zuordnung ⚡ letzte Zuordnung
<input checked="" type="checkbox"/>	Active/Inactive Schedule (click to view/edit)						
<input checked="" type="checkbox"/>	Alias (zur Betrachtung/Bearbeitung klicken)						

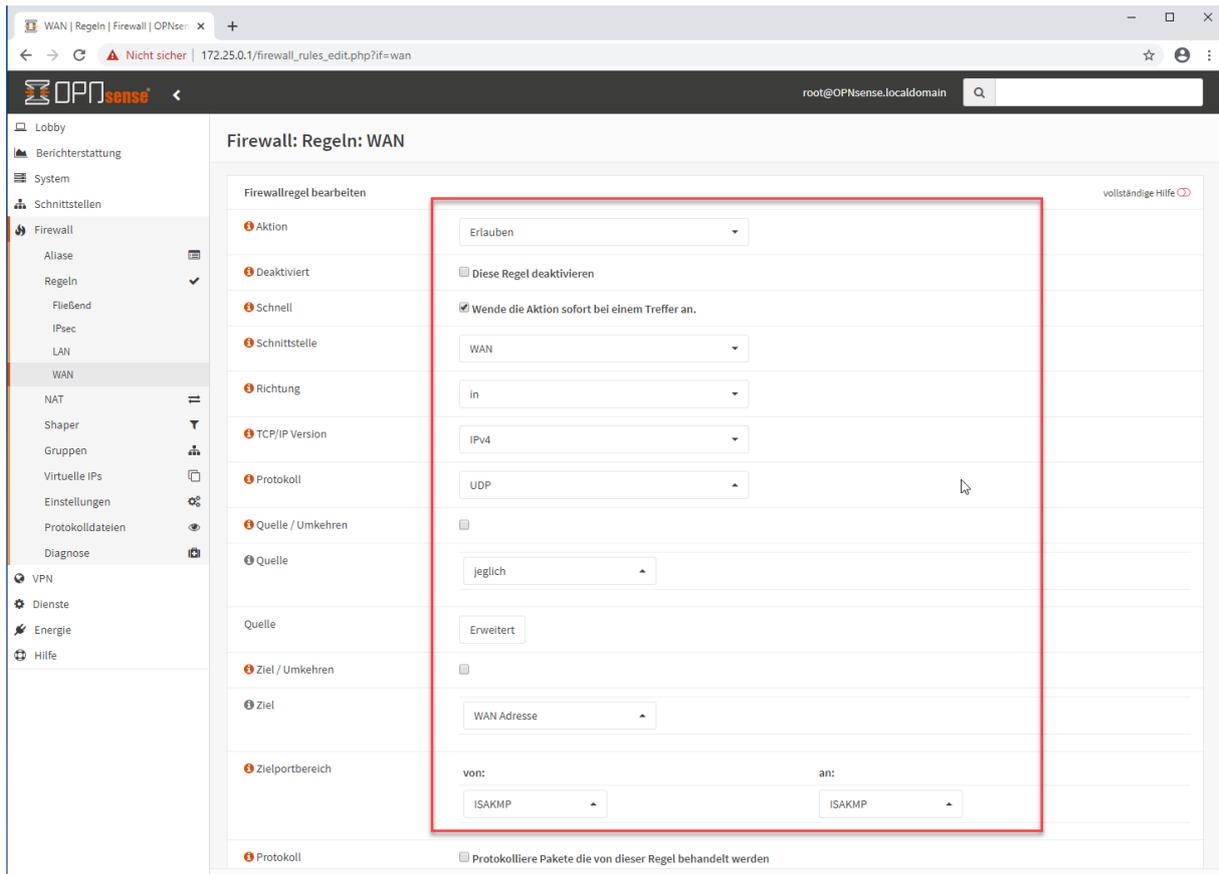
IPsec rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.



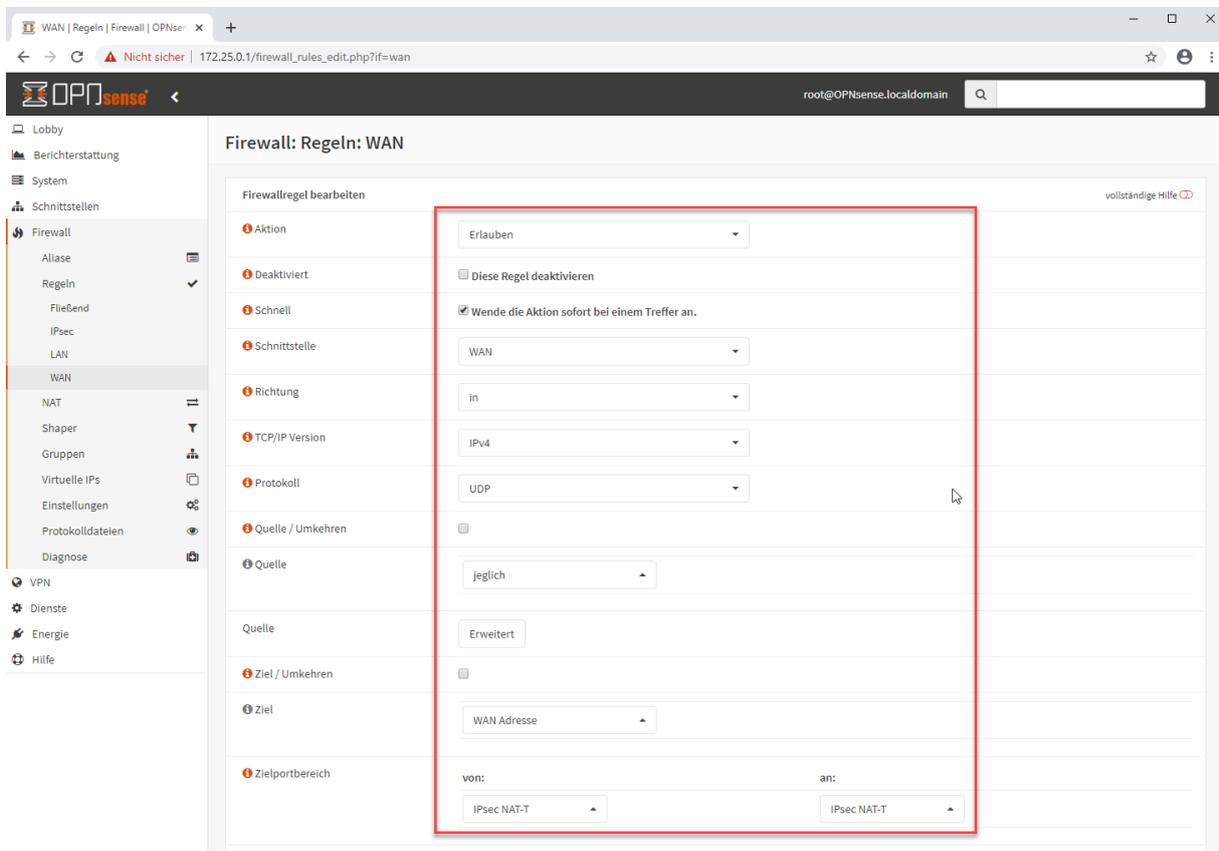
→ auf *Speichern* klicken

Falls die Kanzlei keine feste öffentliche IP-Adresse hat, muss die OPNsense im Rechenzentrum alle IP-Anfragen auf den Ports 500, 4500 und ESP akzeptieren:





→ Speichern und wieder auf Hinzufügen klicken



→ Speichern und wieder auf Hinzufügen klicken

WAN | Regeln | Firewall | OPNsense

172.25.0.1/firewall\_rules\_edit.php?fif=wan

root@OPNsense.localdomain

### Firewall: Regeln: WAN

Firewallregel bearbeiten vollständige Hilfe

**Aktion**: Erlauben

**Deaktiviert**:  Diese Regel deaktivieren

**Schnell**:  Wende die Aktion sofort bei einem Treffer an.

**Schnittstelle**: WAN

**Richtung**: in

**TCP/IP Version**: IPv4

**Protokoll**: ESP

**Quelle / Umkehren**:

**Quelle**: jeglich

**Quelle**: Erweitert

**Ziel / Umkehren**:

**Ziel**: WAN Adresse

**Zielportbereich**: von: jeglich an: jeglich

→Speichern

WAN | Regeln | Firewall | OPNsense

172.25.0.1/firewall\_rules.php?fif=wan

root@OPNsense.localdomain

### Firewall: Regeln: WAN

Nothing selected Inspect Hinzufügen

Die Firewall Regel Konfiguration wurde geändert.  
Sie müssen die Änderungen bestätigen damit sie wirksam werden. Änderungen übernehmen

	Protokoll	Quelle	Port	Ziel	Port	Gateway	Zeitplan	Beschreibung
Automatically generated rules <span>10</span>								
<input type="checkbox"/>	IPv4 TCP	*	*	WAN Adresse	443 (HTTPS)	*	*	
<input type="checkbox"/>	IPv4 UDP	*	*	WAN Adresse	500 (ISAKMP)	*	*	
<input type="checkbox"/>	IPv4 UDP	*	*	WAN Adresse	4500 (IPsec NAT-T)	*	*	
<input type="checkbox"/>	IPv4 ESP	*	*	WAN Adresse	*	*	*	

▶ Erlauben ✘ blockieren 🚫 ablehnen 🔍 protokollieren ➡ eingehend ⚡ erste Zuordnung  
▶ erlauben (deaktiviert) ✘ blockieren (deaktiviert) 🚫 ablehnen (deaktiviert) 🔍 protokollieren (deaktiviert) ⬅ ausgehend ⚡ letzte Zuordnung

Active/Inactive Schedule (click to view/edit)

Alias (zur Betrachtung/Bearbeitung klicken)

WAN rules are evaluated on a first-match basis by default (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you will have to pay attention to the rule order. Everything that is not explicitly passed is blocked by default.

## Teil 2: Kanzlei

### Willkommen bei Ihrer Digitalisierungsbox Premium

**Internetzugang**

Verbindungsinformation	Aktiv
IPv4 Adresse	[REDACTED]
IPv6 Adresse	[REDACTED]
Downstream	99916 kbit/s
Upstream	36467 kbit/s

**WLAN-Netzwerke**      **Rufnummern**

1 Netzwerk      3 Rufnummern, alle registriert

**KONFIGURATION STARTEN**

Firmware-Version 11.01.03.101 from 2020/03/02 00:00:00

### Willkommen bei Ihrer Digitalisierungsbox Premium



Melden Sie sich mit Ihrem Benutzernamen und Ihrem Kennwort an. Der Standard-Benutzername lautet 'admin'.

**Anmelden**

Benutzername  
admin

Kennwort  
\*\*\*\*\*

**Anmelden**

Home   Telefonie   WLAN   **Internet & Netzwerk**   Sprache   Konfiguration speichern   Ausloggen

## Internet & Netzwerk

**Internetverbindung**  
Download Speed: 99.91 MBit/s  
Upload Speed: 36.46 MBit/s  
Verbindungsinformation [REDACTED]

**Lokales Netzwerk einrichten**

Hier nehmen Sie einige grundlegende Einstellungen für Ihr lokales Netzwerk vor.

**Internet einrichten**

Hier richten Sie Ihren Internetzugang ein.

**VPN einrichten**

Über ein VPN können Sie eine verschlüsselte Verbindung zwischen zwei Netzwerken aufbauen oder einem PC Zugang zu Ihrem lokalen Netz ermöglichen.

**Portweiterleitungen einrichten**

Die Firewall schützt Ihr lokales Netzwerk vor unerwünschtem Datenverkehr und vor Angriffen aus dem Internet.

**Mehr anzeigen**

Home Telefonie WLAN **Internet & Netzwerk** Zugriffsregeln

UOS

Multicast

Allgemein IGMP Weiterleiten

WAN

Internet + Einwählen ATM Real Time Jitter Control

VPN

IPSec Digitalisierungsbox Secure Client

INTERNET & NETZWERK > VPN > IPSEC > IPSEC-PEERS

IPSEC-PEERS PHASE-1-PROFILE PHASE-2-PROFILE XAUTH-PROFILE IP POOLS OPTIONEN

## IKEv1 (Internet Key Exchange, Version 1)

Prio	Beschreibung	Peer-Adresse	Peer-ID	Phase-1-Profil	Phase-2-Profil	Status	Aktion
1	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	↑ ↓ T <sub>1</sub>	[Icon] [Icon] [Icon]
3	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	↑ ↓ T <sub>1</sub>	[Icon] [Icon] [Icon]
4	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	↑ ↓ T <sub>1</sub>	[Icon] [Icon] [Icon]
5	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	↑ ↓ T <sub>1</sub>	[Icon] [Icon] [Icon]
6	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	↑ ↓ T <sub>1</sub>	[Icon] [Icon] [Icon]

IPSec-Statische-Peers

NEU

Home Telefonie WLAN **Internet & Netzwerk**

Standard	Beschreibung	Proposals	Authentifizierung	Modus	Diff-Gruppe	Lebensdauer	Aktion
<input type="radio"/>	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Icon] [Icon]
<input checked="" type="radio"/>	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Icon] [Icon]
<input type="radio"/>	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Icon] [Icon]
<input type="radio"/>	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Icon] [Icon]
<input type="radio"/>	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Icon] [Icon]
<input type="radio"/>	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Icon] [Icon]

NEUES IKEV1-PROFIL ERSTELLEN

## IKEv2 (Internet Key Exchange, Version 2)

Standard	Beschreibung	Proposals	Lebensdauer	Aktion
<input checked="" type="radio"/>	[Redacted]	[Redacted]	[Redacted]	[Icon] [Icon]
<input type="radio"/>	[Redacted]	[Redacted]	[Redacted]	[Icon] [Icon]

NEUES IKEV2-PROFIL ERSTELLEN

OK ABBRECHEN

Home Telefonie WLAN **Internet & Netzwerk**

INTERNET & NETZWERK > VPN > IPSEC > PHASE-1-PROFILE > BEARBEITEN

IPSEC-PEERS PHASE-1-PROFILE PHASE-2-PROFILE XAUTH-PROFILE IP POOLS OPTIONEN

## Phase-1-Parameter (IKEv2)

**Beschreibung**  
IKE-2

**Proposals**

Verschlüsselung	Authentifizierung	DH-Gruppe	Aktiviert
AES	SHA2 256	14(2048 Bit)	<input checked="" type="checkbox"/>
AES	SHA1	2(1024 Bit)	<input type="checkbox"/>
AES	SHA1	2(1024 Bit)	<input type="checkbox"/>
AES	SHA1	2(1024 Bit)	<input type="checkbox"/>

**Lebensdauer**  
28800 Sekunden / Schlüssel erneut erstellen nach 80 % Lebensdauer

OK ABBRECHEN

Home Telefonie WLAN **Internet & Netzwerk**

INTERNET & NETZWERK > VPN > IPSEC > PHASE-2-PROFILE

IPSEC-PEERS PHASE-1-PROFILE PHASE-2-PROFILE XAUTH-PROFILE IP POOLS OPTIONEN

## IPSec-Phase-2-Profil

Standard	Beschreibung	Proposals	PFS-Gruppe	Lebensdauer	
<input checked="" type="radio"/>					
<input type="radio"/>					
<input type="radio"/>					
<input type="radio"/>					
<input type="radio"/>					
<input type="radio"/>					
<input type="radio"/>					

NEU OK ABBRECHEN

Home Telefonie WLAN **Internet & Netzwerk**

INTERNET & NETZWERK > VPN > IPSEC > PHASE-2-PROFILE > BEARBEITEN

IPSEC-PEERS PHASE-1-PROFILE PHASE-2-PROFILE XAUTH-PROFILE IP POOLS OPTIONEN

## Phase-2-Parameter (IPSEC)

**Beschreibung**  
IPSec-8

**Proposals**

Verschlüsselung	Authentifizierung	Aktiviert
AES	SHA2-256	<input checked="" type="checkbox"/>
AES	SHA1	<input type="checkbox"/>
AES	SHA1	<input type="checkbox"/>

**PFS-Gruppe verwenden**  
 Aktiviert  
14(2048 Bit)

**Lebensdauer**  
28800 Sekunden 0 kBytes Schlüssel erneut erstellen nach 80 % Lebensdauer

OK ABBRECHEN

INTERNET & NETZWERK > VPN > IPSEC > IPSEC-PEERS

IPSEC-PEERS PHASE-1-PROFILE PHASE-2-PROFILE XAUTH-PROFILE IP POOLS OPTIONEN

## IKEv1 (Internet Key Exchange, Version 1)

Prio	Beschreibung	Peer-Adresse	Peer-ID	Phase-1-Profil	Phase-2-Profil	Status	Aktion
1	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	↑ ↓ t <sub>1</sub>	[edit] [delete] [search]
3	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	↑ ↓ t <sub>1</sub>	[edit] [delete] [search]
4	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	↑ ↓ t <sub>1</sub>	[edit] [delete] [search]
5	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	↑ ↓ t <sub>1</sub>	[edit] [delete] [search]
6	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	↑ ↓ t <sub>1</sub>	[edit] [delete] [search]

IPSec-Statistische-Peers

NEU

INTERNET & NETZWERK > VPN > IPSEC > IPSEC-PEERS > BEARBEITEN

IPSEC-PEERS PHASE-1-PROFILE PHASE-2-PROFILE XAUTH-PROFILE IP POOLS OPTIONEN

## Peer-Parameter

Administrativer Status  
 Aktiv  
 Inaktiv

Beschreibung  
OPNSense\_vCloud

Peer-Adresse  
IP-Version: Nur IPv4  
IP-Adresse gemäß vCloud Info im RZ

Peer-ID  
IPv4-Adresse  
IP-Adresse gemäß vCloud Info im RZ

Lokaler ID-Typ  
IPv4-Adresse

IP-Version des Tunnelnetzwerks  
IPv4

IKE (Internet Key Exchange)  
IKEv2

Lokale ID  
öffentliche IP-Adresse Ihrer Kanzlei

Authentifizierungsmethode  
Preshared Keys

Preshared Key  
\*\*\*\*\*

OK ABBRECHEN

Home Telefonie WLAN Internet & Netzwerk

## IPv4-Schnittstellenrouten

Sicherheitsrichtlinie  
 Nicht vertrauenswürdig  
 Vertrauenswürdig

Standardroute  
 Deaktiviert

IPv4-Adressvergabe  
Client im IKE-Konfigurationsmodus

Konfigurationsmodus  
 Pull  
 Push

Routeneinträge

Entfernte IP-Adresse	Netzmaske	Metrik
172.25.0.0	255.255.255.0	1

HINZUFÜGEN  
mehr anzeigen  
Weniger anzeigen

Erweiterte IPSec-Optionen

hier die erstellten Profile für Phase-1 und Phase-2 auswählen

Phase-1-Profil  
IKE-1

Phase-2-Profil  
IPSec-7

Startmodus  
 Auf Anforderung  
 Immer aktiv

OK ABBRECHEN

