

Anleitung zur Herstellung einer IPSec/Ikev2 Site-to-Site Verbindung mit der OPNSense Option und einem Lancom-Router z.B. 1781EF+

RA Thomas Schmidt – RA-MICRO Vertriebs GmbH – Stand 03.02.2021 – Alle Angaben ohne Gewähr

1. Teil: Rechenzentrum:

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

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 Deaktiviere diesen Phase 1 Eintrag

Anschlussart

Schlüsselaustauschversion

Internet Protokoll

Schnittstelle

Ferner Gateway

Dynamic gateway Allow any remote gateway to connect

Beschreibung

Phase 1 Vorschlag (Authentifizierung)

Authentifizierungsmethode

Meine Kennung

Peer-Identifizierer

Pre-Shared Schlüssel

Phase 1 Vorschlag (Algorithmen)

Verschlüsselungsalgorithmus

Hashalgorithmus

DH Schlüsselgruppe

Lebenszeit

Erweiterte Optionen

Install policy

ReKey deaktivieren

Reauth deaktivieren

Tunnelisolation

NAT Traversal

MOBIKE deaktivieren

Dead Peer Detection

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
Lokales Subnetz		Fernes Subnetz		Phase 2 Proposal	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<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

IPsec aktivieren

Speichern

Tunneleinstellungen | IPsec | VPN | x +

Nicht sicher | 172.25.0.1/vpn_ipsec_phase2.php?ikeid=1

root@OPNsense.localdomain

VPN: IPsec: Tunneleinstellungen

Allgemeine Information vollständige Hilfe

Deaktiviert

Modus: Tunnel IPv4

Beschreibung: Angaben_zu_den_zu_verbindenden_Netzwerken

Lokales Netzwerk

Typ: LAN Subnetz

Adresse: / 32

Entferntes Netzwerk

Typ: Netzwerk

Adresse: 192.168.2.0 / 24

Phase-2-Vorschlag (SA / Schlüsselaustausch)

Protokoll: ESP

Verschlüsselungsalgorithmen: AES, 256 Bits, aes128gcm16, aes192gcm16, aes256gcm16, Blowfish, automatisch

OPNsense (c) 2014-2020 Deciso B.V.

Hier wird das lokale Netzwerk in der Kanzlei beschrieben. Z.B. die IP-Adresse des Routers nehmen und statt der letzten Ziffer eine "0" eintragen.

Tunneleinstellungen | IPsec | VPN | x +

172.25.0.1/vpn_ipsec_phase2.php?ikeid=1

root@OPNsense.localdomain

VPN > IPsec > Tunneleinstellungen

Typ: Netzwerk

Adresse: 192.168.2.0 / 24

Phase-2-Vorschlag (SA / Schlüsselaustausch)

Protokoll: ESP

Verschlüsselungsalgorithmen:

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

Hashalgorithmen: SHA512

PFS Schlüsselgruppe: 14 (2048 bits)

Lebenszeit: 3600 Sekunden

Erweiterte Optionen:

- Automatisch Host pingen
- Manuelle SPD-Einträge

Speichern

OPNsense (c) 2014-2020 Deciso B.V.

Tunneleinstellungen | IPsec | VPN | x +

172.25.0.1/vpn_ipsec.php

root@OPNsense.localdomain

VPN > IPsec > Tunneleinstellungen

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_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
<i>Lokales Subnetz Fernes Subnetz 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_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
<i>Lokales Subnetz Fernes Subnetz 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_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

Die Änderungen wurden erfolgreich angewandt.

Nothing selected Inspect Hinzufügen

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							
Erlauben	blockieren		ablehnen				protokollieren
erlauben (deaktiviert)	blockieren (deaktiviert)		ablehnen (deaktiviert)				protokollieren (deaktiviert)
Active/inactive Schedule (click to view/edit)							
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.

Firewallregel bearbeiten vollständige Hilfe

- Aktion: Erlauben
- Deaktiviert: Diese Regel deaktivieren
- Schnell: Wende die Aktion sofort bei einem Treffer an.
- Schnittstelle: IPsec
- Richtung: in
- TCP/IP Version: IPv4
- Protokoll: any
- Quelle / Umkehren:
- Quelle: jeglich
- Quelle: Erweitert
- Ziel / Umkehren:
- Ziel: LAN Netzwerk
- Zielportbereich: von: an:

→ 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:

WAN | Regeln | Firewall | OPNsense

172.25.0.1/firewall_rules.php?fif=wan

root@OPNsense.localdomain

Firewall: Regeln: WAN

Nothing selected [Inspect] **Hinzufügen**

Protokoll	Quelle	Port	Ziel	Port	Gateway	Zeitplan	Beschreibung
Automatically generated rules							
IPv4 TCP	*	*	WAN Adresse	443 (HTTPS)	*	*	
Erlauben (deaktiviert)	blockieren (deaktiviert)	ablehnen (deaktiviert)	protokollieren (deaktiviert)	→ 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.

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**: UDP
- Quelle / Umkehren**:
- Quelle**: jeglich
- Quelle**: Erweitert
- Ziel / Umkehren**:
- Ziel**: WAN Adresse
- Zielportbereich**: von: ISAKMP an: ISAKMP
- Protokoll**: Protokolliere Pakete die von dieser Regel behandelt werden

→ Speichern und wieder auf Hinzufügen klicken

WAN | Regeln | Firewall | OPNsense

172.25.0.1/firewall_rules_edit.php?if=wan

root@OPNsense.localdomain

Firewall: Regeln: WAN

Firewallregel bearbeiten vollständige Hilfe

Aktion	Erlauben
Deaktiviert	<input type="checkbox"/> Diese Regel deaktivieren
Schnell	<input checked="" type="checkbox"/> Wende die Aktion sofort bei einem Treffer an.
Schnittstelle	WAN
Richtung	in
TCP/IP Version	IPv4
Protokoll	UDP
Quelle / Umkehren	<input type="checkbox"/>
Quelle	jeglich
Quelle	Erweitert
Ziel / Umkehren	<input type="checkbox"/>
Ziel	WAN Adresse
Zielportbereich	von: IPsec NAT-T an: IPsec NAT-T

→ Speichern und wieder auf Hinzufügen klicken

WAN | Regeln | Firewall | OPNsense

172.25.0.1/firewall_rules_edit.php?if=wan

root@OPNsense.localdomain

Firewall: Regeln: WAN

Firewallregel bearbeiten vollständige Hilfe

Aktion	Erlauben
Deaktiviert	<input type="checkbox"/> Diese Regel deaktivieren
Schnell	<input checked="" type="checkbox"/> Wende die Aktion sofort bei einem Treffer an.
Schnittstelle	WAN
Richtung	in
TCP/IP Version	IPv4
Protokoll	ESP
Quelle / Umkehren	<input type="checkbox"/>
Quelle	jeglich
Quelle	Erweitert
Ziel / Umkehren	<input type="checkbox"/>
Ziel	WAN Adresse
Zielportbereich	von: jeglich an: jeglich

→ Speichern

WAN | Regeln | Firewall | OPNsense x +

Nicht sicher | 172.25.0.1/firewall_rules.php?f=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. Anderungen übernehmen

	Protokoll	Quelle	Port	Ziel	Port	Gateway	Zeitplan	Beschreibung	
	Automatically generated rules 10								
<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 mit Lancom-Router z.B. 1781EF+

Die VPN LAN-zu-LAN Verbindung kann entweder manuell oder mit Hilfe des Assistenten erstellen werden. Wichtig ist, dass im Ergebnis die nachfolgend angezeigten Einstellungen entsprechend gesetzt sind.

The screenshot displays the Lancom Systems web interface. On the left is a navigation menu with the following items: Dashboard, Setup-Wizards, Systeminformation, Konfiguration (highlighted with a red arrow), Management, IoT, Schnittstellen, Datum/Zeit, Meldungen/Monitoring, Kommunikation, IPv4, IPv6, IP-Router, Routing Protokolle, Multicast, Firewall, QoS, VPN (with sub-items: Allgemein, IKE/IPSec, IKEv2/IPSec, myVPN, Zertifikate, NetBIOS, Public-Spot, RADIUS, Sonstige Dienste), and Extras. The main content area is titled "VPN: Allgemein" and contains several sections:


- Virtual Private Network:** A list of settings with checkboxes. "Aktiviert" is checked and highlighted with a red box and a red arrow labeled "1.". Other settings include "Vereinfachte Einwahl mit Zertifikaten aktiviert", "Gegenstelle die Auswahl des entfernten Netzwerks erlauben", "NAT-Traversal aktiviert" (highlighted with a red box and a red arrow labeled "2."), "IPSec-over-HTTPS annehmen", and "Flexibler Identitätsvergleich aktiviert".
- Entfernte Gateways:** A section with explanatory text and links for "Weitere entfernte Gateways", "Gateway-Gruppen", and "Gateway-Zuordnungen".
- Netzwerk-Regeln:** A section with sub-sections for "IPv4-Netzwerk-Regeln" (containing links for "IPv4-Regelliste" and "IPv4-Regeln", with a red arrow labeled "2." pointing to "IPv4-Regeln") and "IPv6-Netzwerk-Regeln" (containing links for "IPv6-Regelliste" and "IPv6-Regeln").




IPv4-Regeln - Hinzufügen

Name	OPNS	(max. 31 Zeichen) (notwendig)
Lokale Netzwerke	192.168.7.0/24	▼
Entfernte Netzwerke	172.25.0.0/24	▼

 Dashboard

 Setup-Wizards

 Systeminformation

 **Konfiguration**

Management

IoT

Schnittstellen

Datum/Zeit

Meldungen/Monitoring

Kommunikation

IPv4

IPv6

IP-Router

Routing Protokolle

Multicast

Firewall/QoS

VPN

 Allgemein

 IKE/IPSec

IKEv2/IPSec

 myVPN


Zertifikate

NetBIOS

Public-Spot

RADIUS

Sonstige Dienste

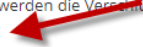
 Extras

- Dashboard
- Setup-Wizards
- Systeminformation
- Konfiguration**
 - Management
 - IoT
 - Schnittstellen
 - Datum/Zeit
 - Meldungen/Monitoring
 - Kommunikation
 - IPv4
 - IPv6
 - IP-Router
 - Routing Protokolle
 - Multicast
 - Firewall/QoS
 - VPN
 - Allgemein
 - IKE/IPSec
 - IKEv2/IPSec**
 - myVPN
 - Zertifikate
 - NetBIOS
 - Public-Spot
 - RADIUS
 - Sonstige Dienste
- Extras

VPN: IKEv2/IPSec

VPN-Verbindungen
Konfigurieren Sie in dieser Tabelle IKEv2 VPN-Verbindungen. Die Netzbeziehungen werden in der VPN-Regeltabelle (VPN/Allgemein) definiert.
[Verbindungs-Liste](#)
[Verbindungs-Parameter](#)

Authentifizierung
Definieren Sie in diesen Tabellen Identitäten für die VPN-Verbindungen, sowie die damit verbundenen Profile für Digital-Signatures.
[Authentifizierung](#)
[Digital-Signature-Profile](#)

Verschlüsselung
In dieser Tabelle werden die Verschlüsselungsparameter definiert.
[Verschlüsselung](#) 

Adressen für Einwahlzugänge (CFG-Mode-Server)
Definieren Sie hier die Parameter die einwählenden Clients per CFG-Mode zugewiesen werden.
[IPv4-Adressen](#)
[IPv6-Adressen](#)
[Split-DNS-Domänen](#)
[Split-DNS-Profile](#)

Erweiterte Einstellungen

Authentifizierung
Weitere entfernte Identitäten
[Identitäten-Liste](#)
[Identitäten](#)
[EAP-Profile](#)
 Preshared Key-Regeln erzwingen

Gültigkeitsdauer
Diese Tabelle definiert die IKEv2-Rekeying-Parameter.
[Gültigkeitsdauer](#)

IKEv2-Routing
Definieren Sie hier die Präfixe, die über dynamisches Routing per IKEv2 propagiert werden.
[IPv4-Routing](#)
[IPv6-Routing](#)

HSVPN

- VPN
 - Allgemein
 - IKE/IPSec
 - IKEv2/IPSec**
 - myVPN
 - Zertifikate
 - NetBIOS
 - Public-Spot
 - RADIUS
 - Sonstige Dienste
- Extras

[Vorherige Seite](#)
[Hinzufügen](#)

VPN: IKEv2/IPSec

Verschlüsselung - Hinzufügen

Name (max. 16 Zeichen) (notwendig)

Erlaubte DH-Gruppen

- DH32 (Curve448)
- DH31 (Curve25519)
- DH30 (ECP-512BP)
- DH29 (ECP-384BP)
- DH28 (ECP-256BP)
- DH21 (ECP-521)
- DH20 (ECP-384)
- DH19 (ECP-256)
- DH16 (MODP-4096)
- DH15 (MODP-3072)
- DH14 (MODP-2048)
- DH5 (MODP-1536)
- DH2 (MODP-1024)

PFS

IKE-SA Verschlüsselungsliste

- AES-CBC-256
- AES-CBC-192
- AES-CBC-128
- 3DES
- AES-GCM-256
- AES-GCM-192
- AES-GCM-128
- CHACHA20-POLY1305

Hash-Liste

- SHA-512
- SHA-384
- SHA-256
- SHA1
- MD5

Child-SA Verschlüsselungsliste

- AES-CBC-256
- AES-CBC-192
- AES-CBC-128
- 3DES
- AES-GCM-256
- AES-GCM-192
- AES-GCM-128
- CHACHA20-POLY1305

Hash-Liste


- SHA-512
- SHA-384
- SHA-256
- SHA1
- MD5

Setzen
Zurücksetzen
Vorherige Seite

- Dashboard
- Setup-Wizards
- Systeminformation
- Konfiguration**
 - Management
 - IoT
 - Schnittstellen
 - Datum/Zeit
 - Meldungen/Monitoring
 - Kommunikation
 - IPv4
 - IPv6
 - IP-Router
 - Routing Protokolle
 - Multicast
 - Firewall/QoS
 - VPN
 - Allgemein
 - IKE/IPSec
 - IKEv2/IPSec**
 - myVPN
 - Zertifikate
 - NetBIOS
 - Public-Spot
 - RADIUS
 - Sonstige Dienste
- Extras

VPN: IKEv2/IPSec

VPN-Verbindungen
Konfigurieren Sie in dieser Tabelle IKEv2 VPN-Verbindungen. Die Netzbeziehungen werden in der VPN-Regeltabelle (VPN/Allgemein) definiert.
[Verbindungs-Liste](#)
[Verbindungs-Parameter](#)

Authentifizierung
Definieren Sie in diesen Tabellen Identitäten für die VPN-Verbindungen, sowie die damit verbundenen Profile für Digital-Signatures.
[Authentifizierung](#) 
[Digital-Signature-Profile](#)

Verschlüsselung
In dieser Tabelle werden die Verschlüsselungsparameter definiert.
[Verschlüsselung](#)

Adressen für Einwahlzugänge (CFG-Mode-Server)
Definieren Sie hier die Parameter die einwählenden Clients per CFG-Mode zugewiesen werden.
[IPv4-Adressen](#)
[IPv6-Adressen](#)
[Split-DNS-Domänen](#)
[Split-DNS-Profile](#)

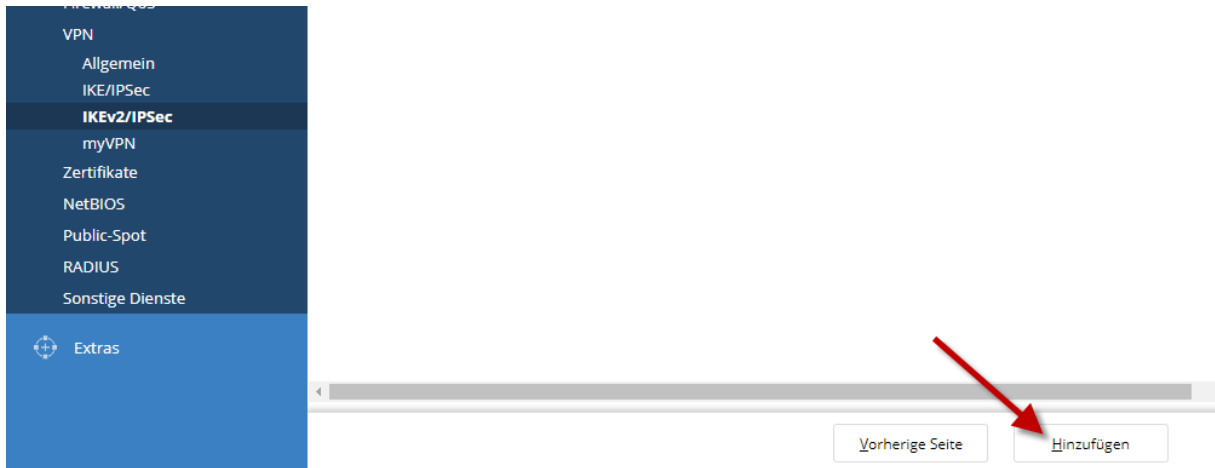
Erweiterte Einstellungen

Authentifizierung
Weitere entfernte Identitäten
[Identitäten-Liste](#)
[Identitäten](#)
[EAP-Profile](#)
 Preshared Key-Regeln erzwingen

Gültigkeitsdauer
Diese Tabelle definiert die IKEv2-Rekeying-Parameter.
[Gültigkeitsdauer](#)

IKEv2-Routing
Definieren Sie hier die Präfixe, die über dynamisches Routing per IKEv2 propagiert werden.
[IPv4-Routing](#)
[IPv6-Routing](#)

HSVPN

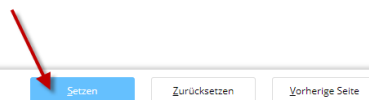


Bei **Lokales** und **Entferntes Passwort** das in der OPNSense im Rechenzentrum vergebene Kennwort unter „Pre-Shared Schlüssel“ eintragen.

VPN: IKEv2/IPSec

Authentifizierung

Name	OPNS
Lokale Authentifizierung	PSK
Lokales Dig. Signature-Prof.	andere Wahl...
Lokaler Identitätstyp	E-Mail-Adresse (FQUN)
Lokale Identität	bellebiger@my.Text.OPNS (max. 254 Zeichen)
Lokales Passwort	• (max. 64 Zeichen)
Passwort-Qualität (Wiederholen)	
Lokales Passwort	• (max. 64 Zeichen)
Entfernte Authentifizierung	PSK
Entf. Dig. Signature-Profil	andere Wahl...
EAP-Profil	andere Wahl...
Entfernter Identitätstyp	IPv4-Adresse
Entfernte Identität	die mitgeteilte öffentliche OPNSense IP eintragen (max. 254 Zeichen)
Entferntes Passwort	• (max. 64 Zeichen)
Passwort-Qualität (Wiederholen)	
Entferntes Passwort	• (max. 64 Zeichen)
Weitere entf. Identitäten	andere Wahl...
Lokales Zertifikat	andere Wahl...
Entfernter Zert.-ID-Check	Nein
OCSP-Überprüfung	Nein
CRL Check	Nein



Konfiguration

- Management
- IoT
- Schnittstellen
- Datum/Zeit
- Meldungen/Monitoring
- Kommunikation
- IPv4
- IPv6
- IP-Router
- Routing Protokolle
- Multicast
- Firewall/QoS
- VPN
 - Allgemein
 - IKE/IPSec
 - IKEv2/IPSec**
 - myVPN
 - Zertifikate
 - NetBIOS
 - Public-Spot
 - RADIUS
 - Sonstige Dienste
- Extras

VPN: IKEv2/IPSec

Adressen für Einwahlzugänge (CFG-Mode-Server)

Definieren Sie hier die Parameter die einwählenden Clients per CFG-Mode zugewiesen werden.

[IPv4-Adressen](#)
[IPv6-Adressen](#)
[Split-DNS-Domänen](#)
[Split-DNS-Profile](#)

Erweiterte Einstellungen

Authentifizierung

Weitere entfernte Identitäten

[Identitäten-Liste](#)
[Identitäten](#)
[EAP-Profile](#)

Preshared Key-Regeln erzwingen

Gültigkeitsdauer

Diese Tabelle definiert die IKEv2-Rekeying-Parameter.

[Gültigkeitsdauer](#)

IKEv2-Routing

Setzen

Konfiguration

- Management
- IoT
- Schnittstellen
- Datum/Zeit
- Meldungen/Monitoring

VPN: IKEv2/IPSec

Gültigkeitsdauer

Name	IKE SA	IKE SA	Child SA	Child SA
DEFAULT	28800	0	28800	2000000

Konfiguration

- Management
- IoT
- Schnittstellen
- Datum/Zeit
- Meldungen/Monitoring
- Kommunikation
- IPv4
- IPv6
- IP-Router
- Routing Protokolle
- Multicast
- Firewall/QoS
- VPN
 - Allgemein
 - IKE/IPSec
 - IKEv2/IPSec**
 - myVPN
 - Zertifikate
 - NetBIOS
 - Public-Spot
 - RADIUS
 - Sonstige Dienste
- Extras

VPN: IKEv2/IPSec

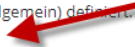
Gültigkeitsdauer

Name	DEFAULT		
IKE SA	<input type="text" value="28800"/>	Sekunden (mögliche Werte: 0 bis 2147483647)	
	<input type="text" value="0"/>	kBytes (mögliche Werte: 0 bis 2147483647)	
Child SA	<input type="text" value="3600"/>	Sekunden (mögliche Werte: 0 bis 2147483647)	
	<input type="text" value="2000000"/>	kBytes (mögliche Werte: 0 bis 2147483647)	

Setzen Zurücksetzen Vorherige Seite

- Dashboard
- Setup-Wizards
- Systeminformation
- Konfiguration**
 - Management
 - IoT
 - Schnittstellen
 - Datum/Zeit
 - Meldungen/Monitoring
 - Kommunikation
 - IPv4
 - IPv6
 - IP-Router
 - Routing Protokolle
 - Multicast
 - Firewall/QoS
 - VPN
 - Allgemein
 - IKE/IPSec
 - IKEv2/IPSec**
 - myVPN
 - Zertifikate
 - NetBIOS
 - Public-Spot
 - RADIUS
 - Sonstige Dienste
- Extras

VPN: IKEv2/IPSec

VPN-Verbindungen
Konfigurieren Sie in dieser Tabelle IKEv2 VPN-Verbindungen. Die Netzbeziehungen werden in der VPN-Regeltabelle (VPN/Allgemein) definiert.
[Verbindungs-Liste](#) 
[Verbindungs-Parameter](#)

Authentifizierung
Definieren Sie in diesen Tabellen Identitäten für die VPN-Verbindungen, sowie die damit verbundenen Profile für Digital-Signatures.
[Authentifizierung](#)
[Digital-Signature-Profile](#)

Verschlüsselung
In dieser Tabelle werden die Verschlüsselungsparameter definiert.
[Verschlüsselung](#)

Adressen für Einwahlzugänge (CFG-Mode-Server)
Definieren Sie hier die Parameter die einwählenden Clients per CFG-Mode zugewiesen werden.
[IPv4-Adressen](#)
[IPv6-Adressen](#)
[Split-DNS-Domänen](#)
[Split-DNS-Profile](#)

Erweiterte Einstellungen

Authentifizierung
Weitere entfernte Identitäten
[Identitäten-Liste](#)
[Identitäten](#)
[EAP-Profile](#)
 Preshared Key-Regeln erzwingen

Gültigkeitsdauer
Diese Tabelle definiert die IKEv2-Rekeying-Parameter.
[Gültigkeitsdauer](#)

IKEv2-Routing
Definieren Sie hier die Präfixe, die über dynamisches Routing per IKEv2 propagiert werden.
[IPv4-Routing](#)
[IPv6-Routing](#)

HSVPN

- VPN
 - Allgemein
 - IKE/IPSec
 - IKEv2/IPSec**
 - myVPN
 - Zertifikate
 - NetBIOS
 - Public-Spot
 - RADIUS
 - Sonstige Dienste
- Extras

Vorherige Seite

Hinzufügen

VPN: IKEv2/IPSec

Verbindungs-Liste - Hinzufügen

Name der Verbindung	OPNS	
<input checked="" type="checkbox"/> Eintrag aktiv		
Haltezeit	9999	Sekunden (mögliche Werte: 0 bis 9999)
Entferntes Gateway	die mitgeteilte öffentliche OPNSense IP Adresse eintragen (max. 64 Zeichen)	
Routing-Tag	0	(mögliche Werte: 0 bis 65535)
Verschlüsselung	OPNS	
Authentifizierung	OPNS	
Verbindungs-Parameter	DEFAULT	
Gültigkeitsdauer	DEFAULT	
VPN-Regelerzeugung		
Regelerzeugung	Manuell	
IPv4-Regeln	OPNS	
IPv6-Regeln	andere Wahl...	
IKE Config-Mode		
IKE-CFG	Aus	
IPv4-Adress-Pool	andere Wahl...	
IPv6-Adress-Pool	andere Wahl...	
Split-DNS-Profil	andere Wahl...	
Routing	andere Wahl...	
CFG-Client-Profil	andere Wahl...	
HSVPN		
RADIUS-Auth.-Server	andere Wahl...	
RADIUS-Acc.-Server	andere Wahl...	
IPv6-Profil	DEFAULT	
Kommentar	<input type="text" value=""/> (max. 63 Zeichen)	

Setzen

Zurücksetzen

Vorherige Seite

LANCOM Systems Suchen Logout

Dashboard
Setup-Wizards
Systeminformation
Konfiguration
Management
IoT
Schnittstellen
Datum/Zeit
Meldungen/Monitoring
Kommunikation
IPv4
IPv6
IP-Router
Allgemein
Routing
Maskierung
N:N-Mapping
VRRP
Routing Protokolle
Multicast
Firewall/QoS
VPN
Zertifikate
NetBIOS
Public-Spot
RADIUS
Sonstige Dienste
Extras

IP-Router: Routing

Routing-Tabelle

In dieser Tabelle geben Sie ein, über welche Gegenstellen bestimmte Netzwerke oder Stationen erreicht werden können.

[IPv4-Routing-Tabelle](#)
[IPv6-Routing-Tabelle](#)

Load-Balancing (Last-Verteilung)

Wenn Ihr Internet-Anbieter keine echte Kanal-Bündelung zur Verfügung stellt, ist es möglich mehrere Verbindungen mit Hilfe des Load-Balancing zusammenzufassen.

Load-Balancing aktiviert
[Load-Balancing](#)

Client-Binding kann Verbindungen, die bestimmten Protokoll/Port-Kombinationen entsprechen, pro Zieladresse eine feste WAN-Verbindung zuordnen. Wechselnde Quelladressen bei der Kommunikation über diese Verbindungen werden dadurch vermieden.

Binding-Minuten: (max. 3 Zeichen)
Balance-Sekunden: (max. 3 Zeichen)
[Client-Binding-Protokolle](#)

LANCOM Systems Suchen Logout

Dashboard
Setup-Wizards
Systeminformation
Konfiguration
Management
IoT
Schnittstellen
Datum/Zeit
Meldungen/Monitoring
Kommunikation
IPv4
IPv6
IP-Router
Allgemein
Routing
Maskierung
N:N-Mapping
VRRP
Routing Protokolle
Multicast
Firewall/QoS
VPN
Zertifikate
NetBIOS
Public-Spot
RADIUS
Sonstige Dienste
Extras

IP-Router: Routing

IPv4-Routing-Tabelle

IP-Adresse	Netzmaske	Tag	Schaltzustand	Router	RIP-Distanz	Mask.	Administrative Distanz	Kommentar
<input type="checkbox"/> 172.25.0.0	255.255.255.0	0	An, sticky für RIP	OPNS	0	Aus	0	
<input type="checkbox"/> 192.168.7.0	255.255.255.0	0	An, sticky für RIP	OPNS	0	Aus	0	
<input type="checkbox"/> 192.168.0.0	255.255.0.0	0	Aus	0.0.0.0	0	Aus	0	template: block private networks: 192.168.x.y
<input type="checkbox"/> 172.16.0.0	255.240.0.0	0	Aus	0.0.0.0	0	Aus	0	template: block private networks: 172.16-31.x.y
<input type="checkbox"/> 10.0.0.0	255.0.0.0	0	Aus	0.0.0.0	0	Aus	0	template: block private networks: 10.x.y.z
<input type="checkbox"/> 255.255.255.255	0.0.0.0	0	An, sticky für RIP	INTERNET	0	An	0	Diese Route wurde durch den Internet-Assistenten erzeugt

- Dashboard
- Setup-Wizards
- Systeminformationen
- Konfiguration**
- Management
- IoT
- Schnittstellen
- Datum/Zeit
- Meldungen/Monitoring
- Kommunikation
- IPV4
- IPV6
- IP-Router
 - Allgemein
 - Routing**
 - Maskierung
 - N:N-Mapping
 - VRRP
- Routing Protokolle
 - Multicast
 - Firewall/QoS
 - VPN
 - Zertifikate
 - NetBIOS
 - Public-Spot
 - RADIUS
 - Sonstige Dienste
- Extras

IP-Router: Routing

IPv4-Routing-Tabelle

IP-Adresse	<input type="text" value="172.25.0.0"/>
Netzmaske	<input type="text" value="255.255.255.0"/>
Routing-Tag	<input type="text" value="0"/>
Schaltzustand	<input checked="" type="radio"/> Route ist aktiviert und wird immer via RIP propagiert (sticky) <input type="radio"/> Route ist aktiviert und wird via RIP propagiert, wenn das Zielnetzwerk erreichbar ist (konditional) <input type="radio"/> Diese Route ist aus
Router	<input type="text" value="OPNS"/>
RIP-Distanz	<input type="text" value="0"/> (mögliche Werte: 0 bis 16)
IP-Maskierung	<input checked="" type="radio"/> IP-Maskierung abgeschaltet <input type="radio"/> IP-Netz und DMZ maskieren (Standard) <input type="radio"/> Nur Internet maskieren
Administrative Distanz	<input type="text" value="0"/>
Kommentar	<input type="text"/> (max. 64 Zeichen)