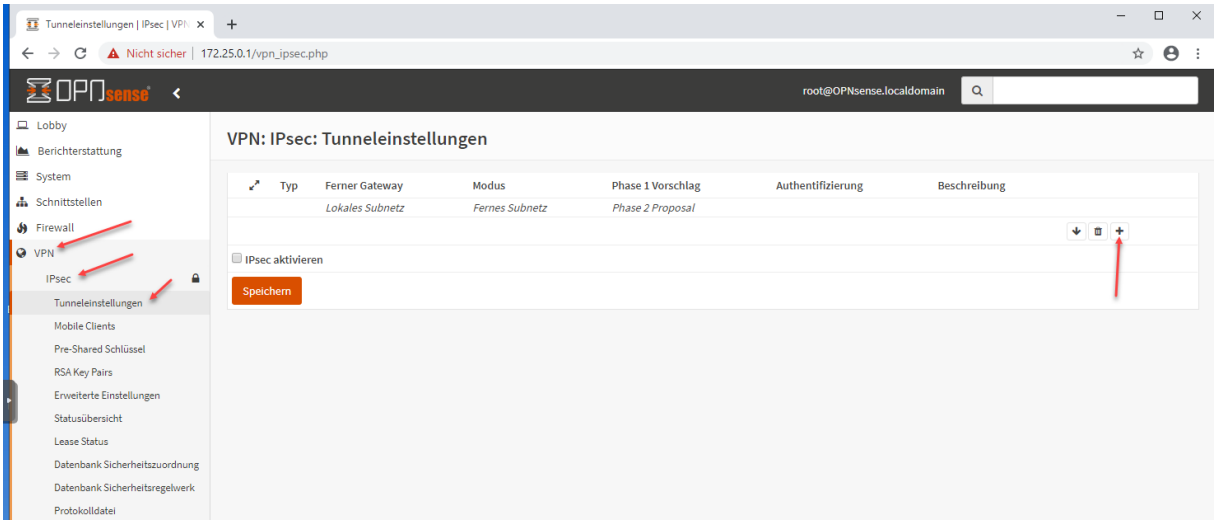
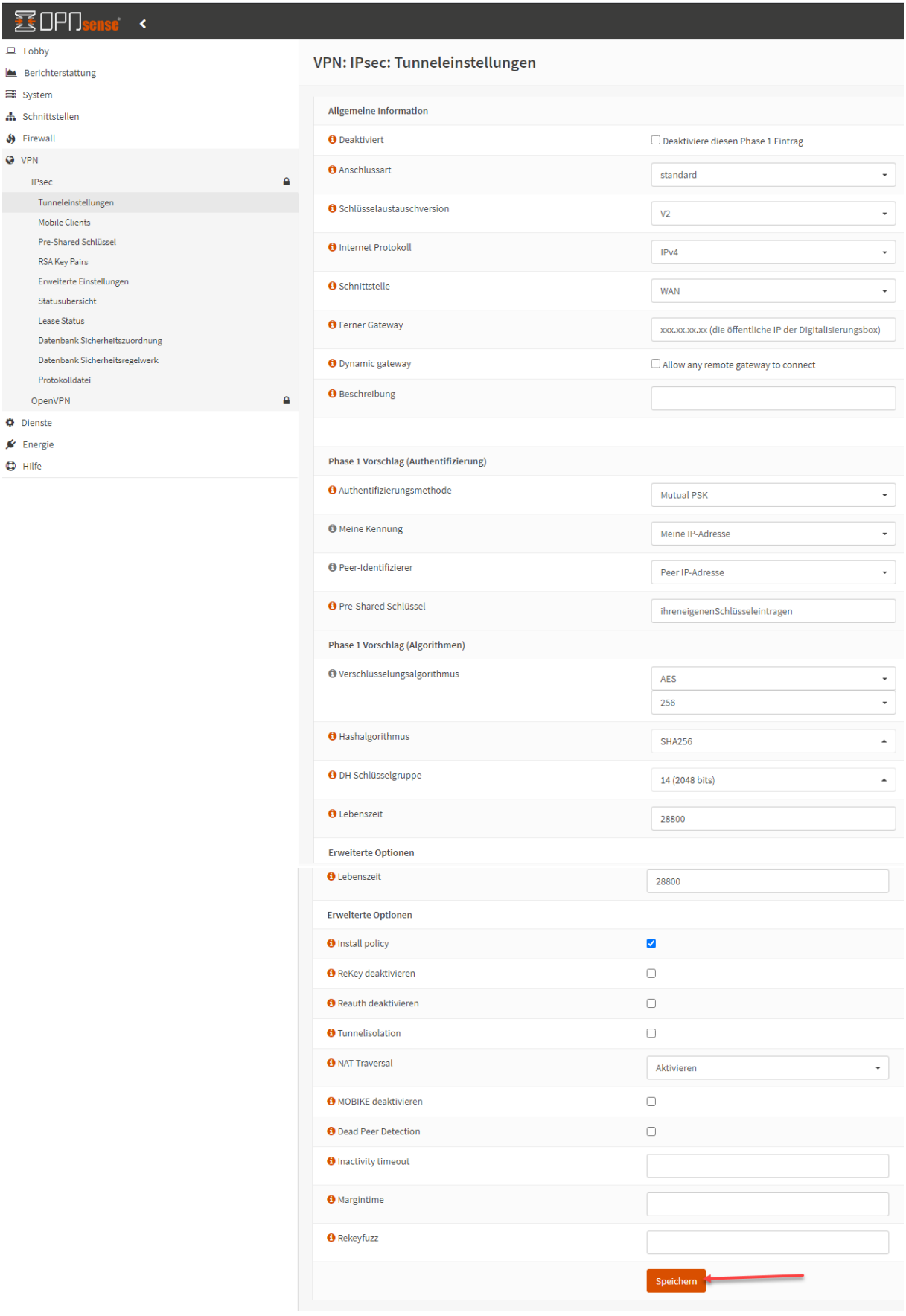
Anleitung zur Herstellung einer IPSec/IKev2 Site-to-Site Verbindung mit der OPNSense Option iVm einer Digitalisierungsbox Premium, die eine statische öffentliche IP Adresse hat

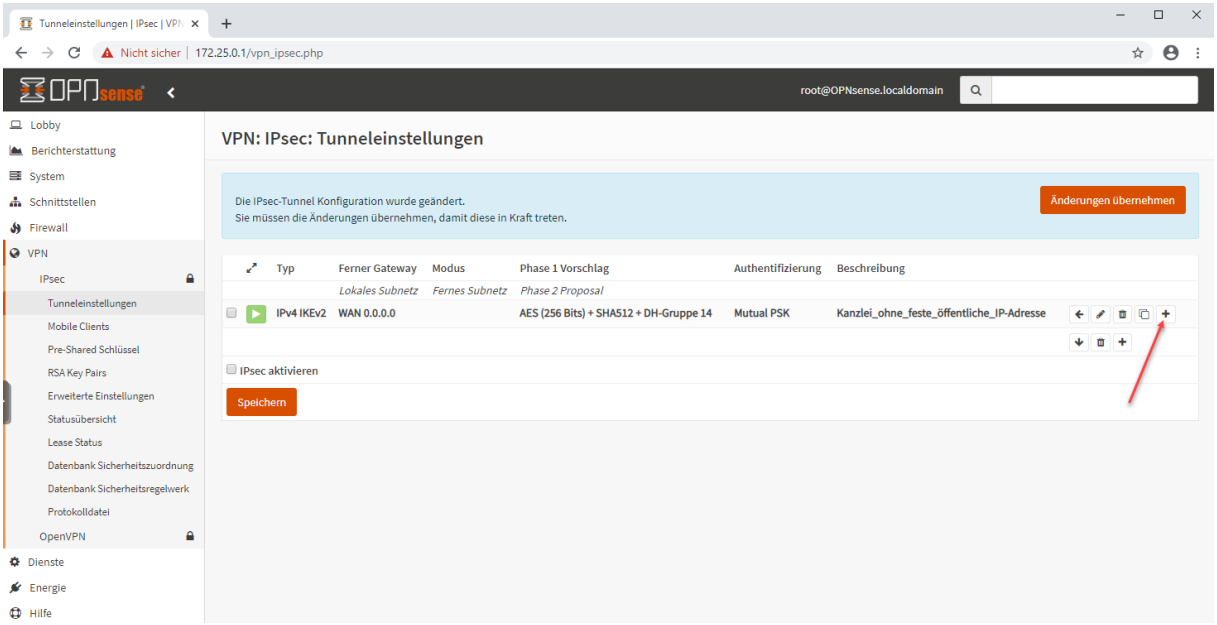
RA Thomas Schmidt – RA-MICRO Vertriebs GmbH – Stand 13.07.2020 – Alle Angaben ohne Gewähr

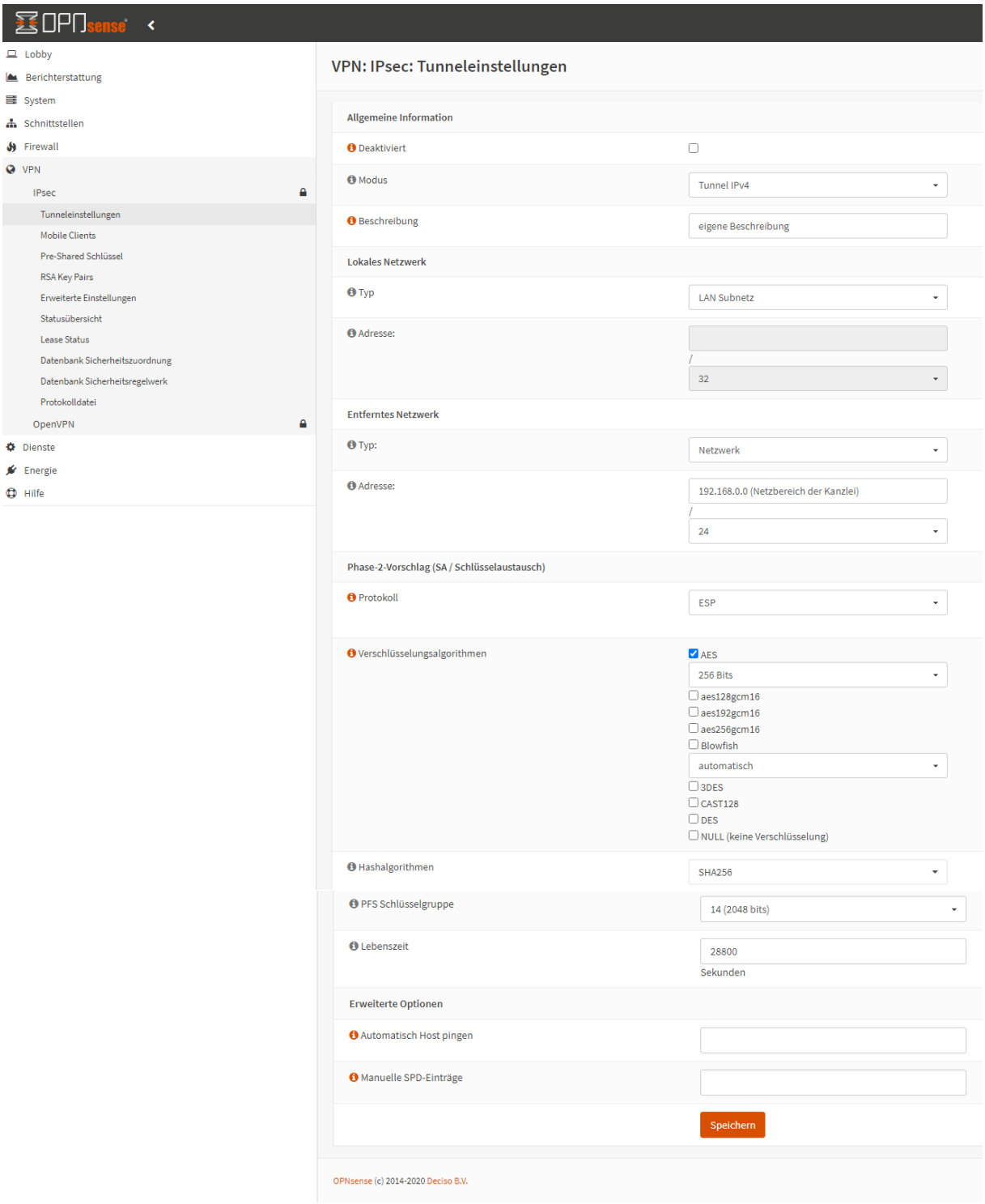
---

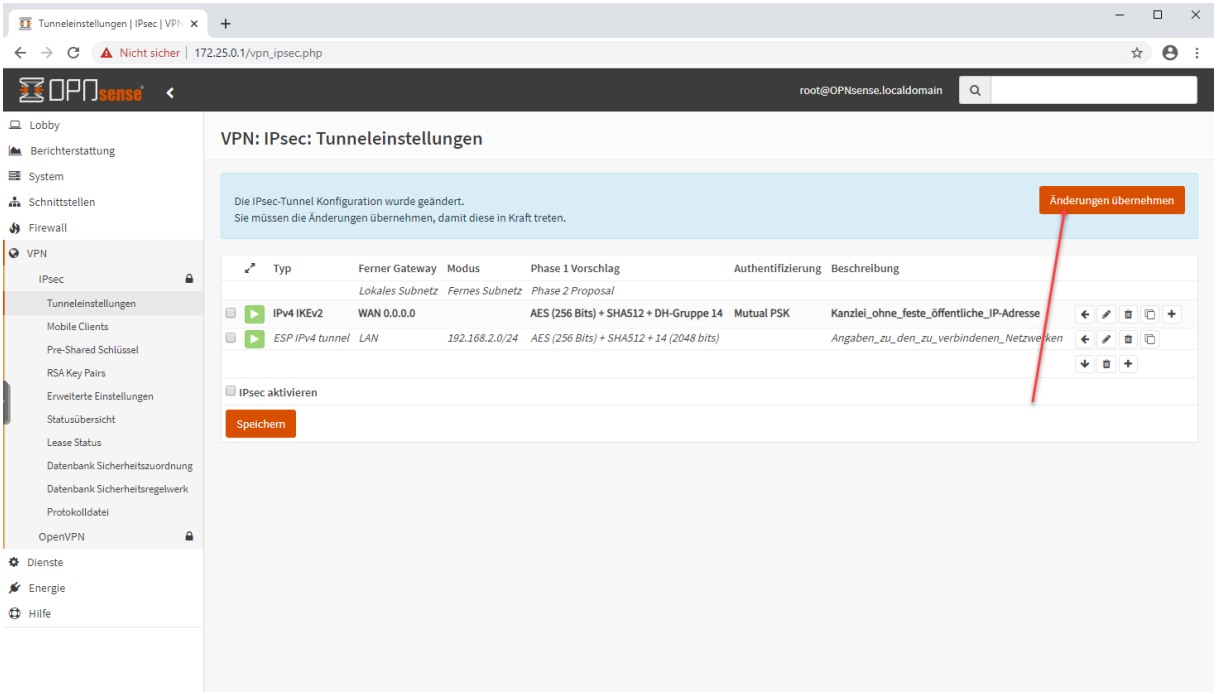
1. Teil: Rechenzentrum:

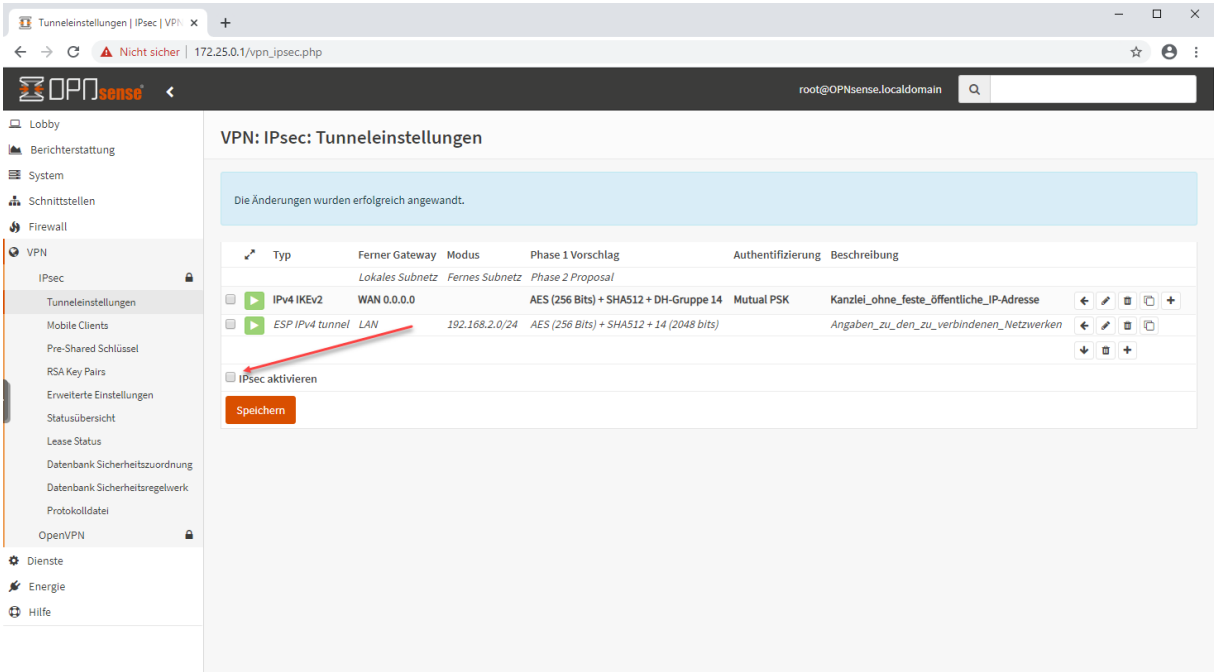


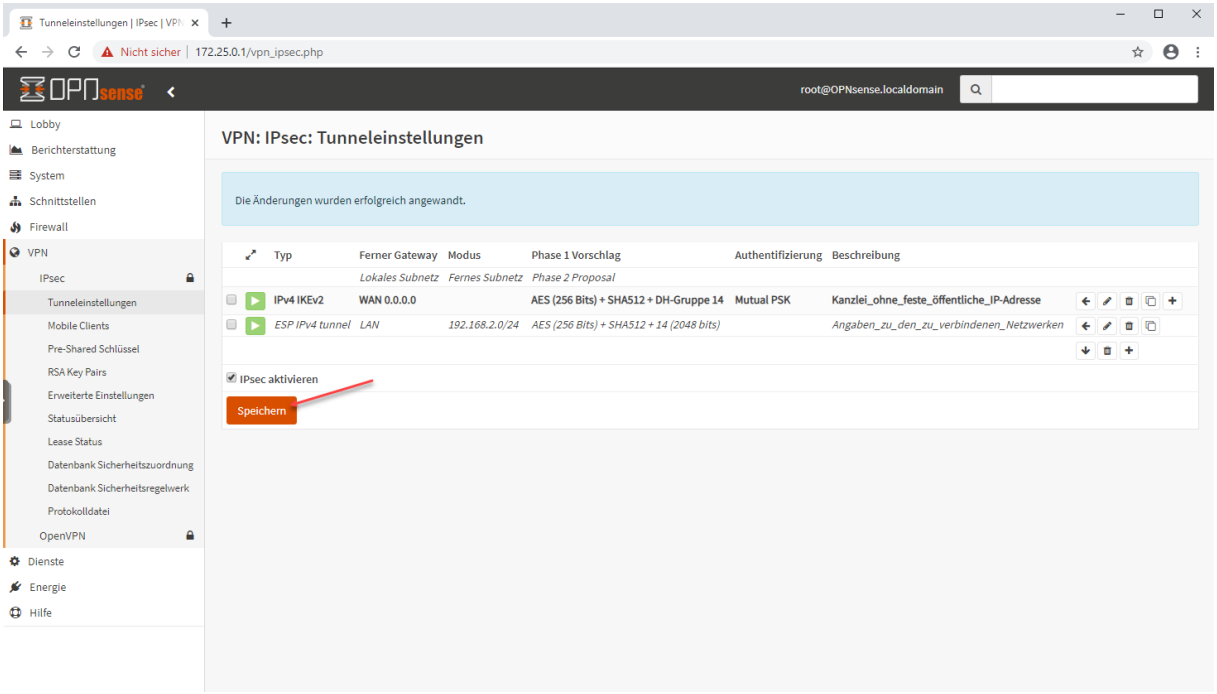

OPNsense
Lobby
Berichterstattung
System
Schnittstellen
Firewall
VPN
IPsec
Tunneleinstellungen
Mobile Clients
Pre-Shared Schlüssel
RSA Key Pairs
Erweiterte Einstellungen
Statusübersicht
Lease Status
Datenbank Sicherheitszuordnung
Datenbank Sicherheitsregelwerk
Protokolldatei
OpenVPN
Dienste
Energie
Hilfe
VPN: IPsec: Tunneleinstellungen
Allgemeine Information
Deaktiviert
Deaktiviere diesen Phase 1 Eintrag
Anschlussart
standard
Schlüsselaustauschversion
V2
Internet Protokoll
IPv4
Schnittstelle
WAN
Ferner Gateway
xxx.xx.xx.xx (die öffentliche IP der Digitalisierungsbox)
Dynamic gateway
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
ihreneigenenSchlüsseleintragen
Phase 1 Vorschlag (Algorithmen)
Verschlüsselungsalgorithmus
AES
256
Hashalgorithmus
SHA256
DH Schlüsselgruppe
14 (2048 bits)
Lebenszeit
28800
Erweiterte Optionen
Lebenszeit
28800
Erweiterte Optionen
Install policy
ReKey deaktivieren
Reauth deaktivieren
Tunnelisolation
NAT Traversal
Aktivieren
MOBIKE deaktivieren
Dead Peer Detection
Inactivity timeout
Margintime
Rekeyfuzz
Speichern

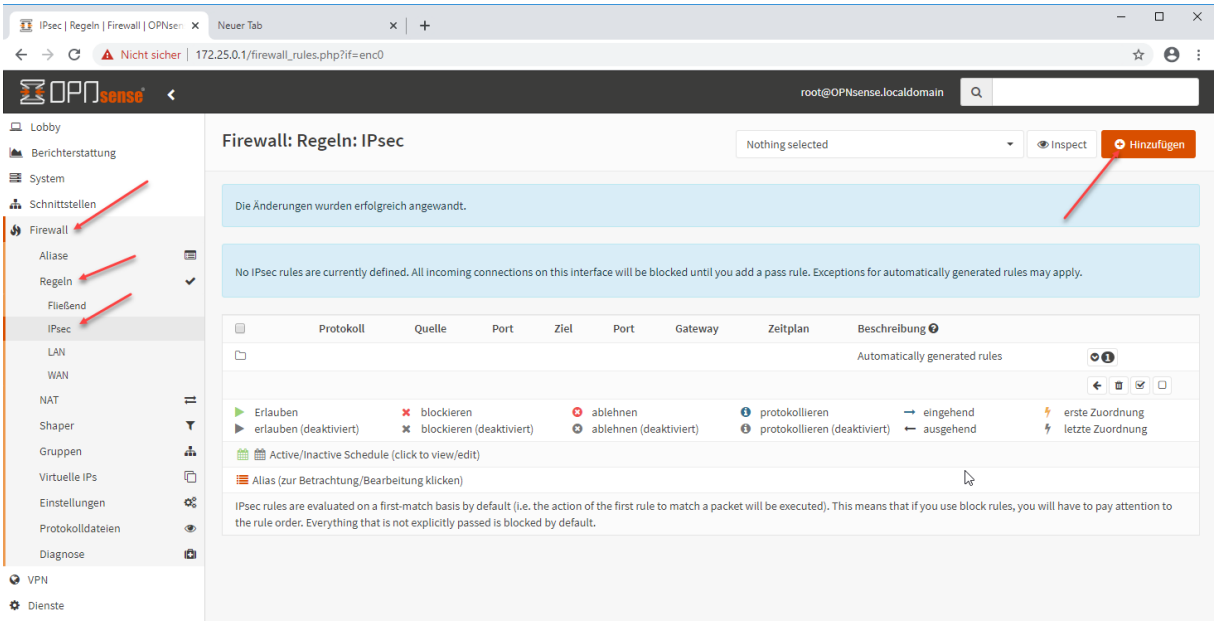

Tunneleinstellungen | IPsec | VPN
Nicht sicher | 172.25.0.1/vpn_ipsec.php
root@OPNsense.localdomain
Lobby
Berichterstattung
System
Schnittstellen
Firewall
VPN
IPsec
Tunneleinstellungen
Mobile Clients
Pre-Shared Schlüssel
RSA Key Pairs
Erweiterte Einstellungen
Statusübersicht
Lease Status
Datenbank Sicherheitszuordnung
Datenbank Sicherheitsregelwerk
Protokolldatei
OpenVPN
Dienste
Energie
Hilfe
VPN: IPsec: Tunneleinstellungen
Die 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
IPv4 IKEv2
WAN 0.0.0.0
AES (256 Bits) + SHA512 + DH-Gruppe 14
Mutual PSK
Kanzlei_ohne_feste_öffentliche_IP-Adresse
IPsec aktivieren
Speichern

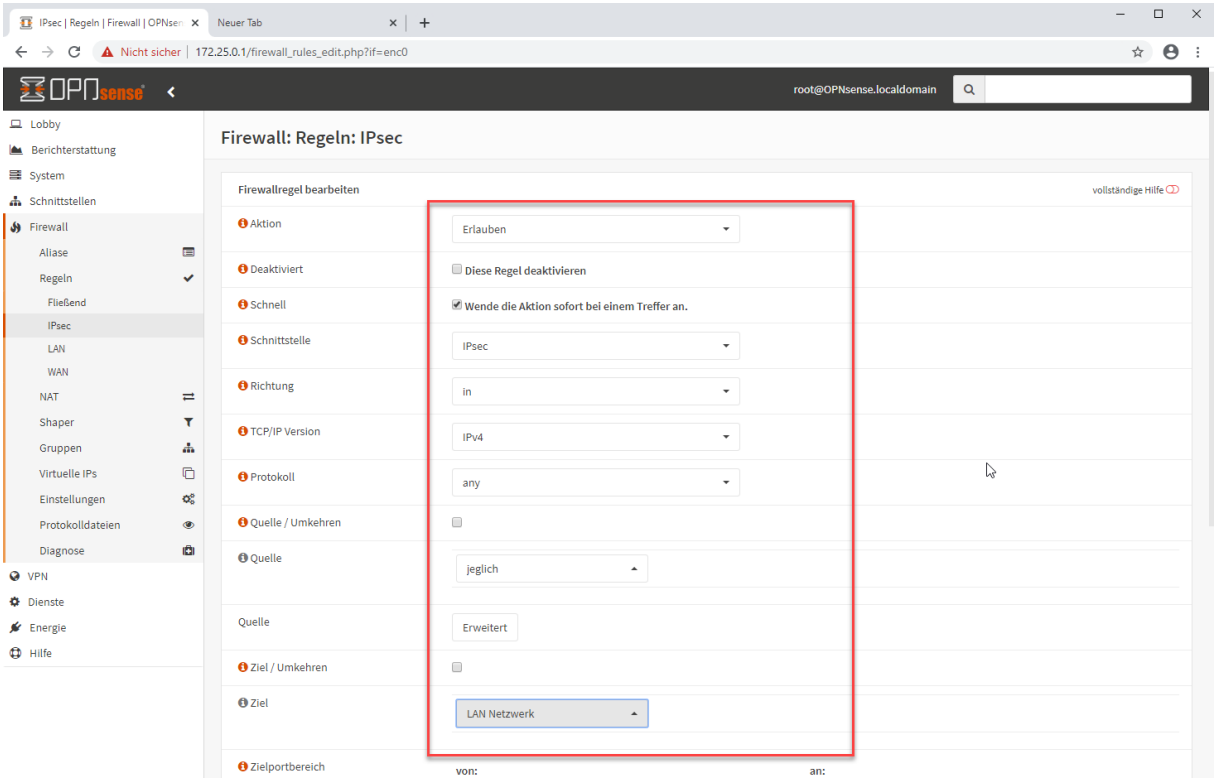

OPNsense
Lobby
Berichterstattung
System
Schnittstellen
Firewall
VPN
IPsec
Tunneleinstellungen
Mobile Clients
Pre-Shared Schlüssel
RSA Key Pairs
Erweiterte Einstellungen
Statusübersicht
Lease Status
Datenbank Sicherheitszuordnung
Datenbank Sicherheitsregelwerk
Protokolldatei
OpenVPN
Dienste
Energie
Hilfe
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
OPNsense (c) 2014-2020 Deciso B.V.


Tunneleinstellungen | IPsec | VPN
Nicht sicher | 172.25.0.1/vpn_ipsec.php
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 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
IPv4 IKEv2
WAN 0.0.0.0
AES (256 Bits) + SHA512 + DH-Gruppe 14
Mutual PSK
Kanzlei_ohne_feste_öffentliche_IP-Adresse
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
Nicht sicher | 172.25.0.1/vpn_ipsec.php
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
IPv4 IKEv2
WAN 0.0.0.0
AES (256 Bits) + SHA512 + DH-Gruppe 14
Mutual PSK
Kanzlei_ohne_feste_öffentliche_IP-Adresse
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

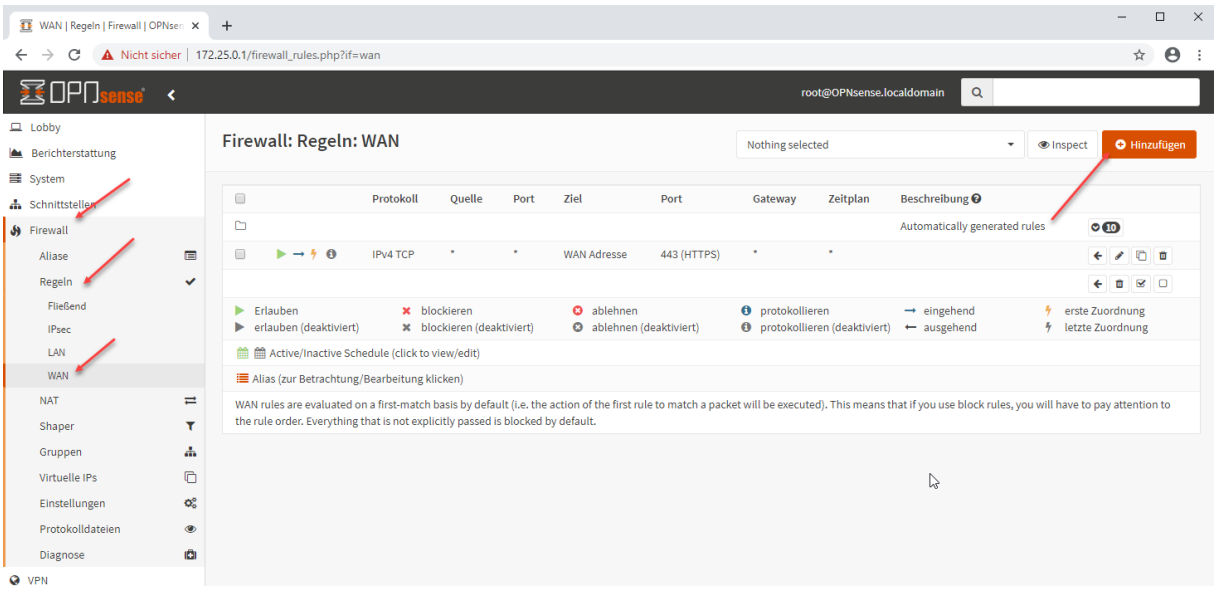

Tunneleinstellungen | IPsec | VPN
Nicht sicher | 172.25.0.1/vpn_ipsec.php
root@OPNsense.localdomain
Lobby
Berichterstattung
System
Schnittstellen
Firewall
VPN
IPsec
Tunneleinstellungen
Mobile Clients
Pre-Shared Schlüssel
RSA Key Pairs
Erweiterte Einstellungen
Statusübersicht
Lease Status
Datenbank Sicherheitszuordnung
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
IPv4 IKEv2
WAN 0.0.0.0
AES (256 Bits) + SHA512 + DH-Gruppe 14
Mutual PSK
Kanzlei_ohne_feste_öffentliche_IP-Adresse
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

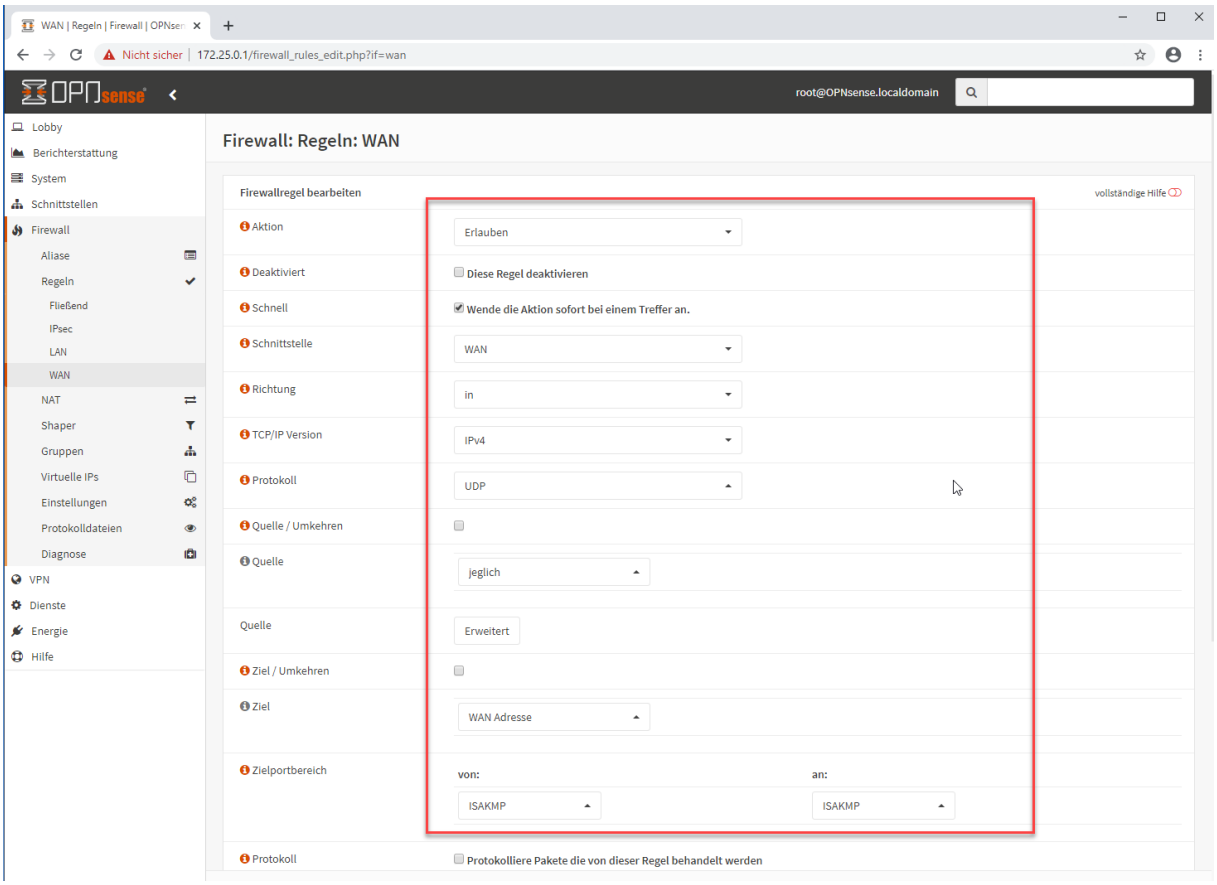

IPsec | Regeln | Firewall | OPNsen
Neuer Tab
Nicht sicher | 172.25.0.1/firewall_rules.php?if=enc0
root@OPNsense.localdomain
Lobby
Berichterstattung
System
Schnittstellen
Firewall
Aliase
Regeln
Fließend
IPsec
LAN
WAN
NAT
Shaper
Gruppen
Virtuelle IPs
Einstellungen
Protokolldateien
Diagnose
VPN
Dienste
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
Erlauben
erlauben (deaktiviert)
blockieren
blockieren (deaktiviert)
ablehnen
ablehnen (deaktiviert)
protokollieren
protokollieren (deaktiviert)
eingehend
ausgehend
erste Zuordnung
letzte Zuordnung
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.



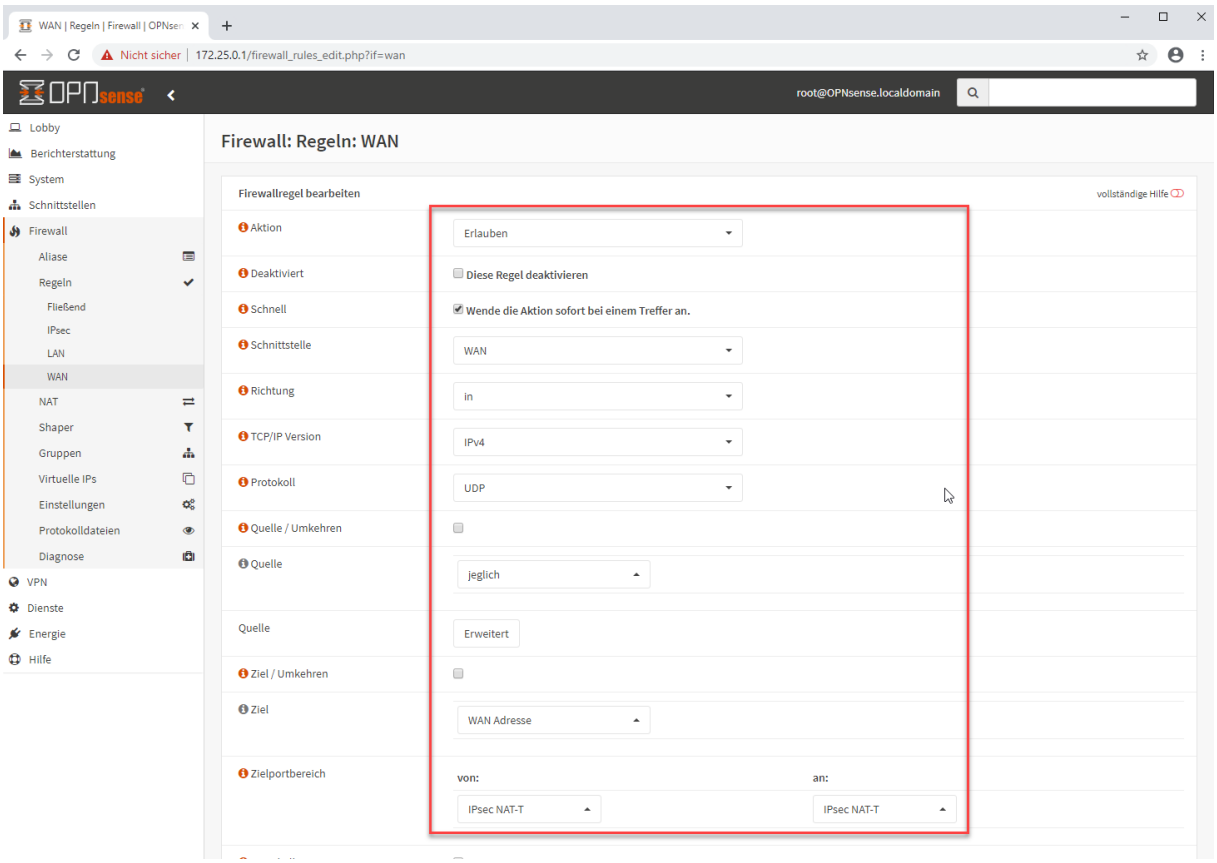
→ auf *Speichern* klicken

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:

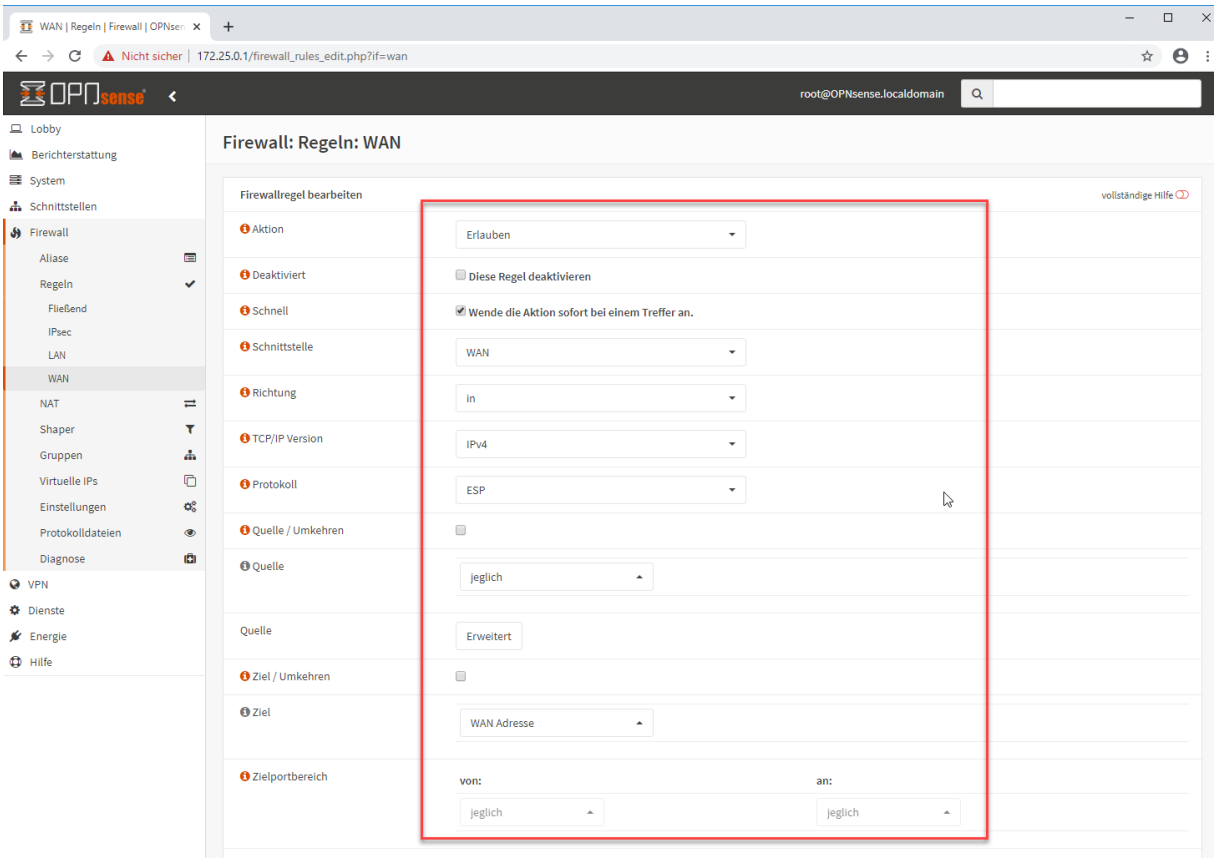




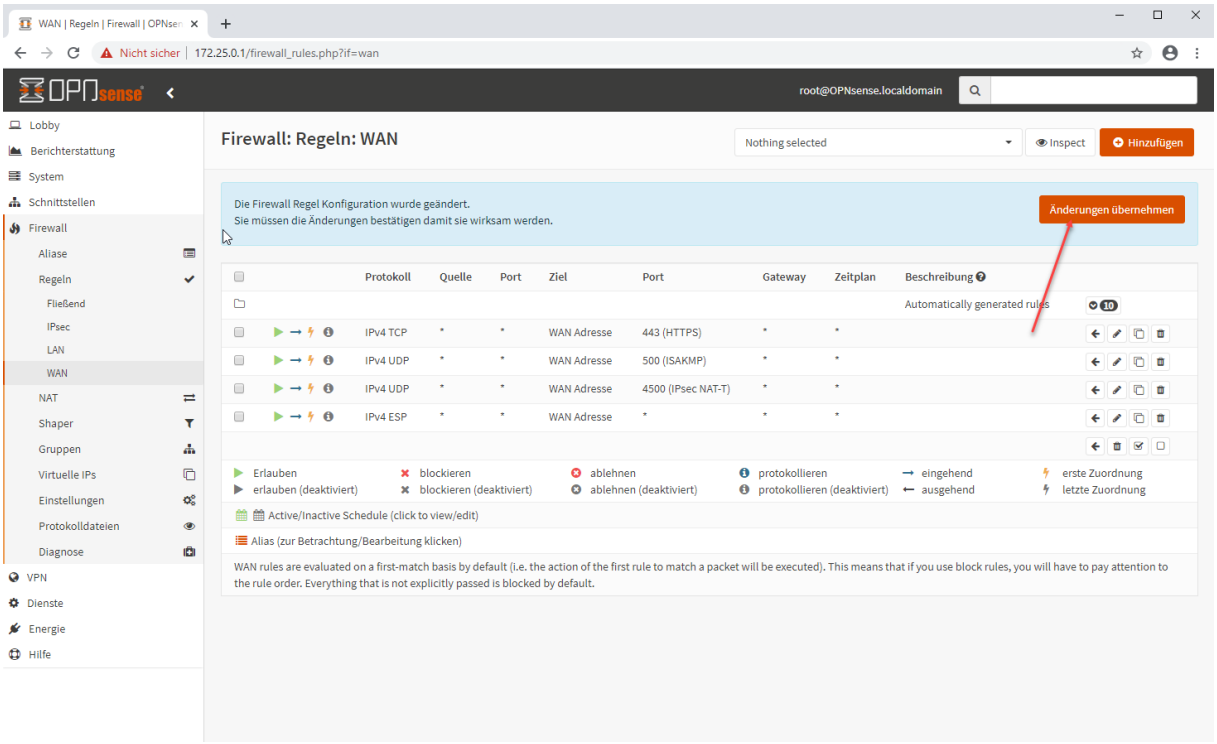
→ Speichern und wieder auf Hinzufügen klicken



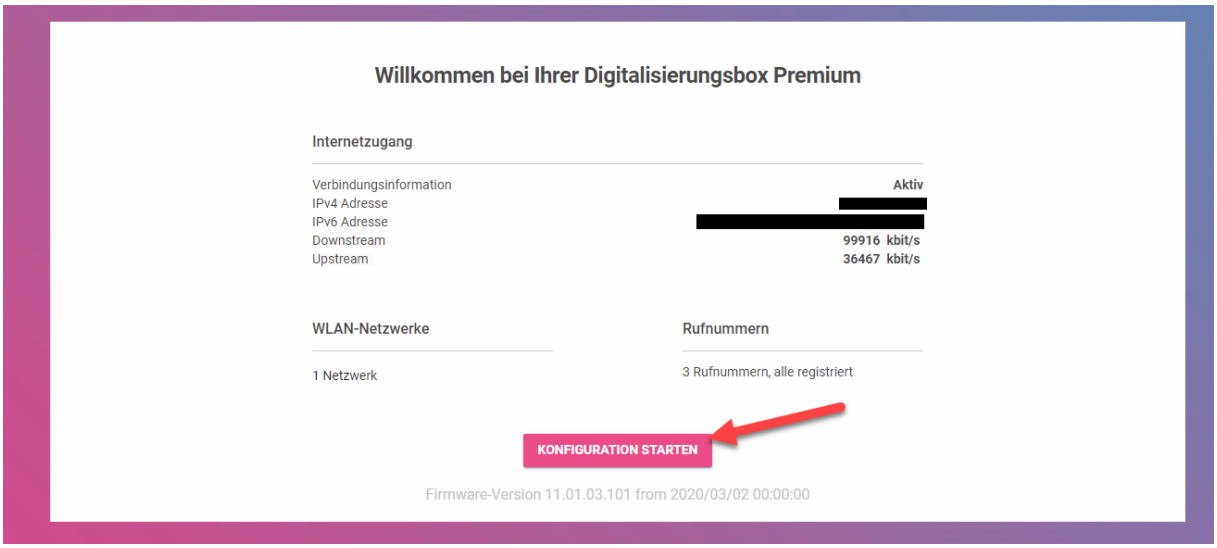
→ Speichern und wieder auf Hinzufügen klicken

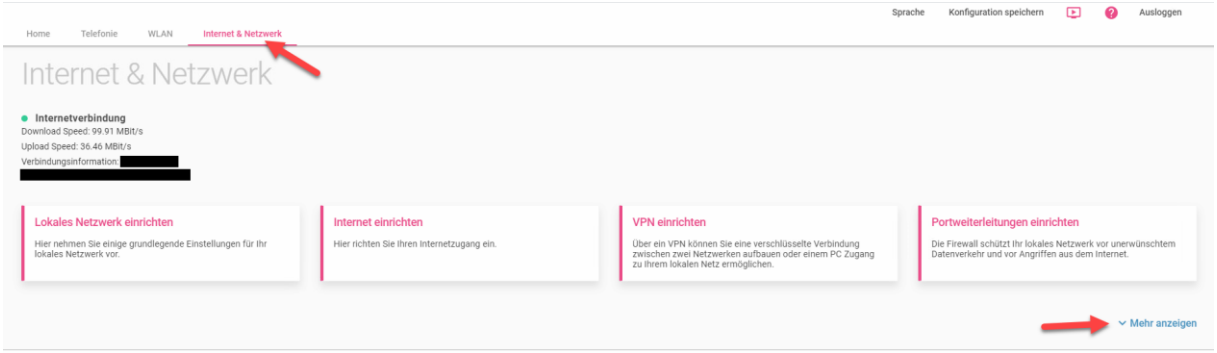

WAN | Regeln | Firewall | OPNsen
Nicht sicher | 172.25.0.1/firewall_rules_edit.php?if=wan
root@OPNsense.localdomain
Lobby
Berichterstattung
System
Schnittstellen
Firewall
Aliase
Regeln
Fließend
IPsec
LAN
WAN
NAT
Shaper
Gruppen
Virtuelle IPs
Einstellungen
Protokolldateien
Diagnose
VPN
Dienste
Energie
Hilfe
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:
an:
jeglich
jeglich

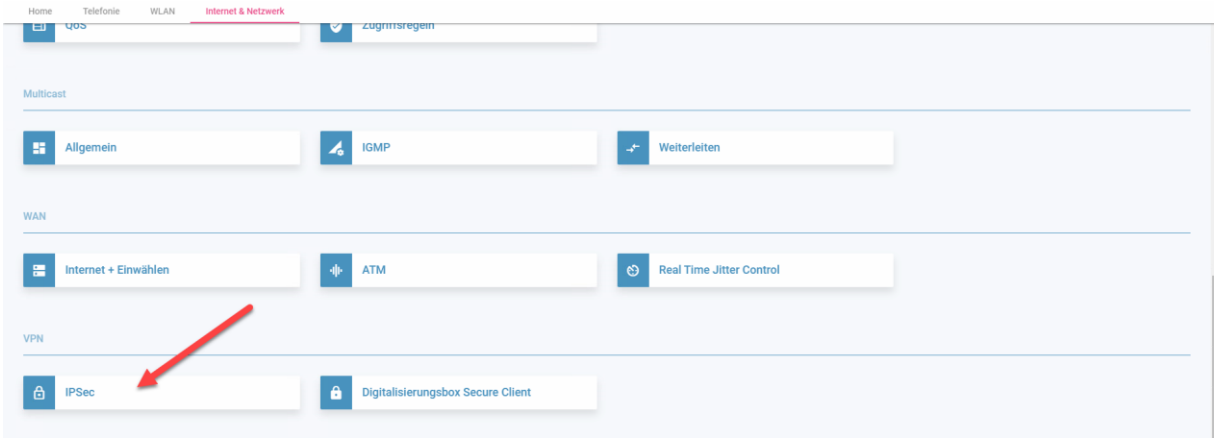
→Speichern

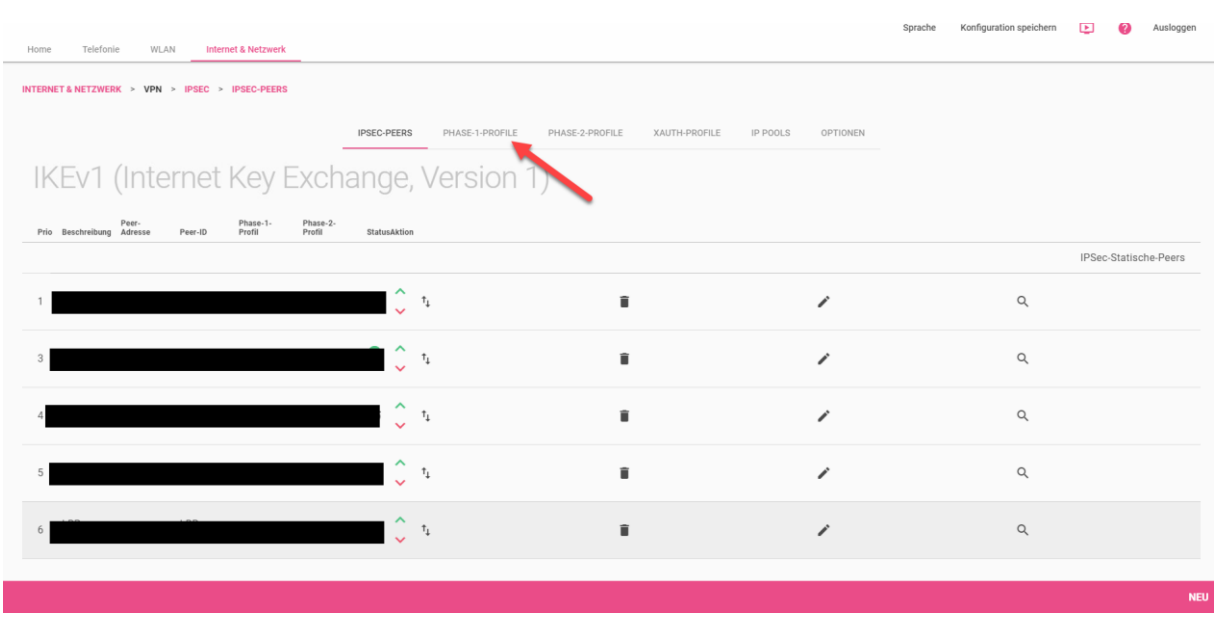

WAN | Regeln | Firewall | OPNsen
Nicht sicher | 172.25.0.1/firewall_rules.php?if=wan
root@OPNsense.localdomain
Lobby
Berichterstattung
System
Schnittstellen
Firewall
Aliase
Regeln
Fließend
IPsec
LAN
WAN
NAT
Shaper
Gruppen
Virtuelle IPs
Einstellungen
Protokolldateien
Diagnose
VPN
Dienste
Energie
Hilfe
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
10
IPv4 TCP
IPv4 UDP
IPv4 UDP
IPv4 ESP
WAN Adresse
443 (HTTPS)
500 (ISAKMP)
4500 (IPsec NAT-T)
Erlauben
erlauben (deaktiviert)
blockieren
blockieren (deaktiviert)
ablehnen
ablehnen (deaktiviert)
protokollieren
protokollieren (deaktiviert)
eingehend
ausgehend
erste Zuordnung
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.

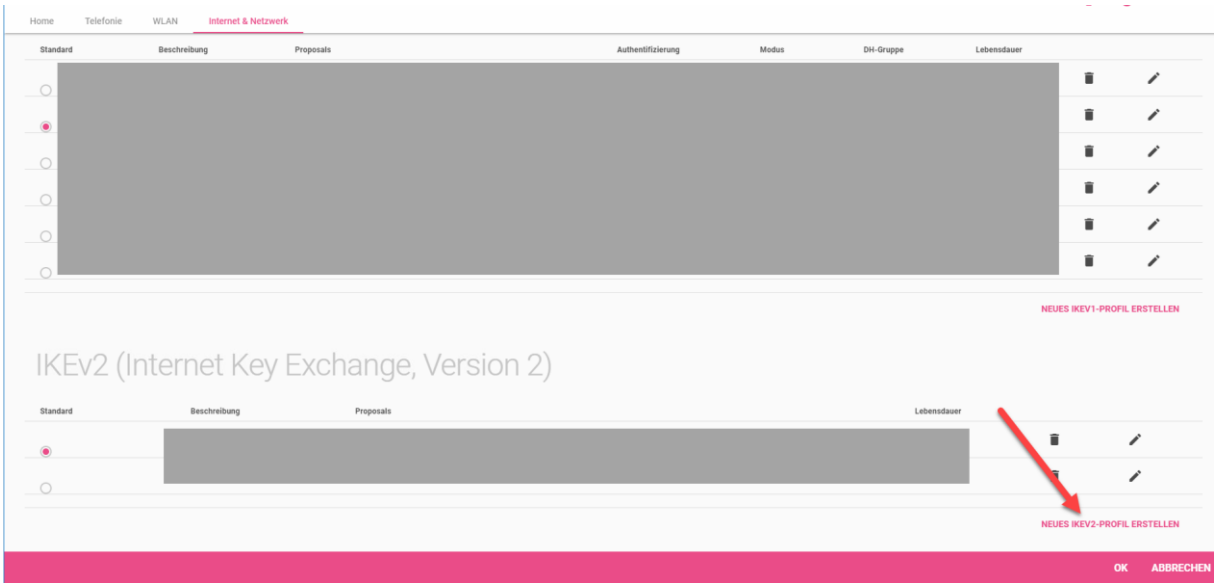
Teil 2: Kanzlei

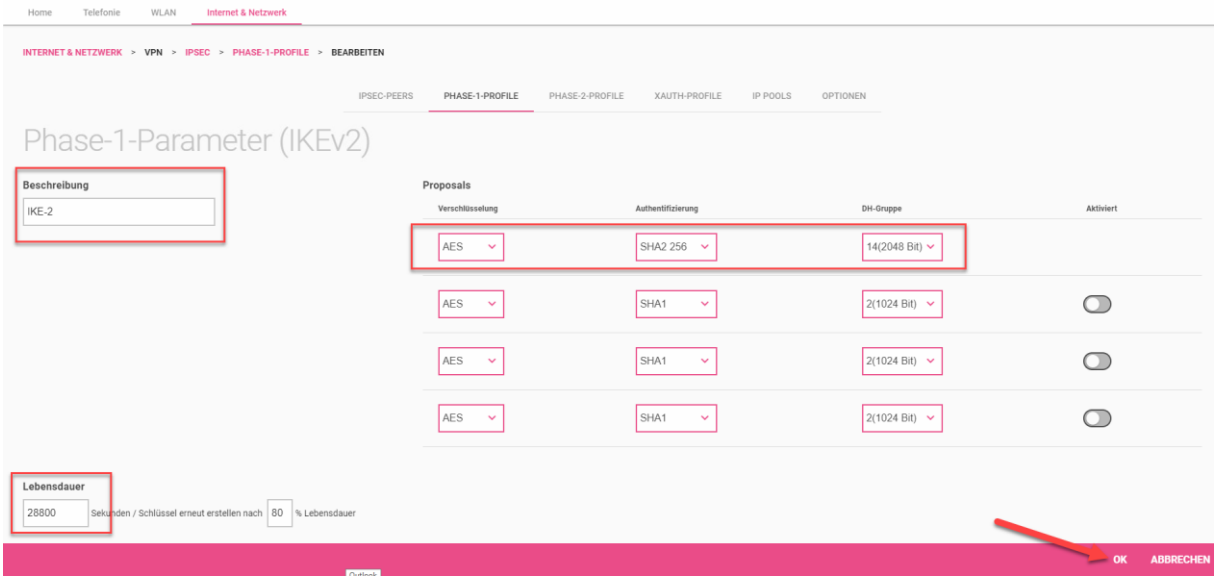


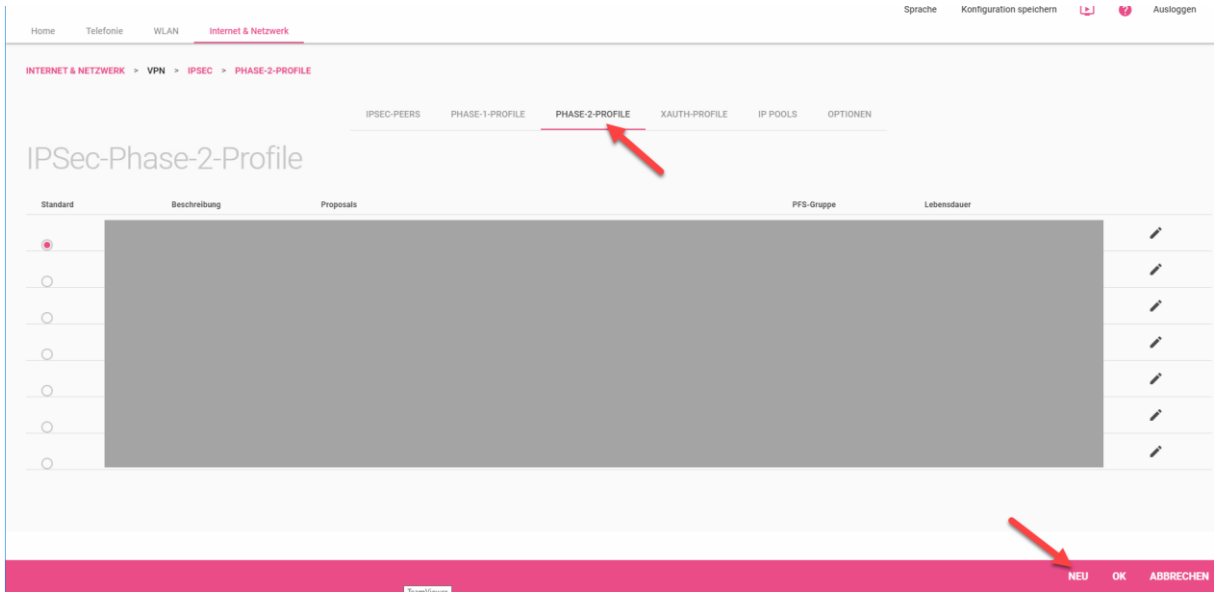


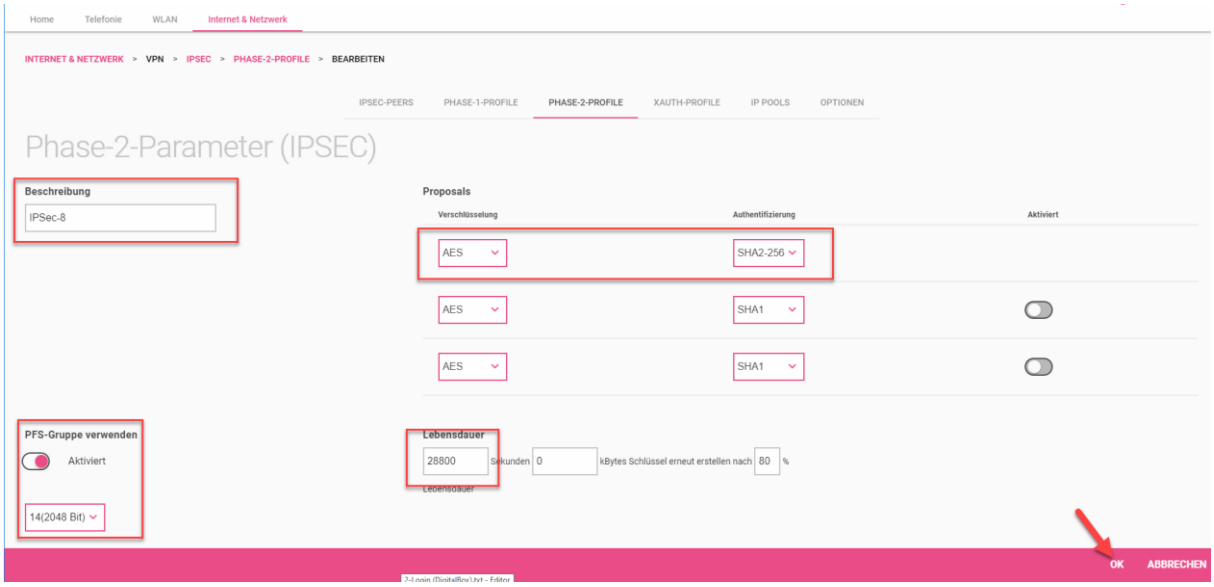

Home
Telefonie
WLAN
Internet & Netzwerk
Multicast
Allgemein
IGMP
Weiterleiten
WAN
Internet + Einwählen
ATM
Real Time Jitter Control
VPN
IPSec
Digitalisierungsbox Secure Client

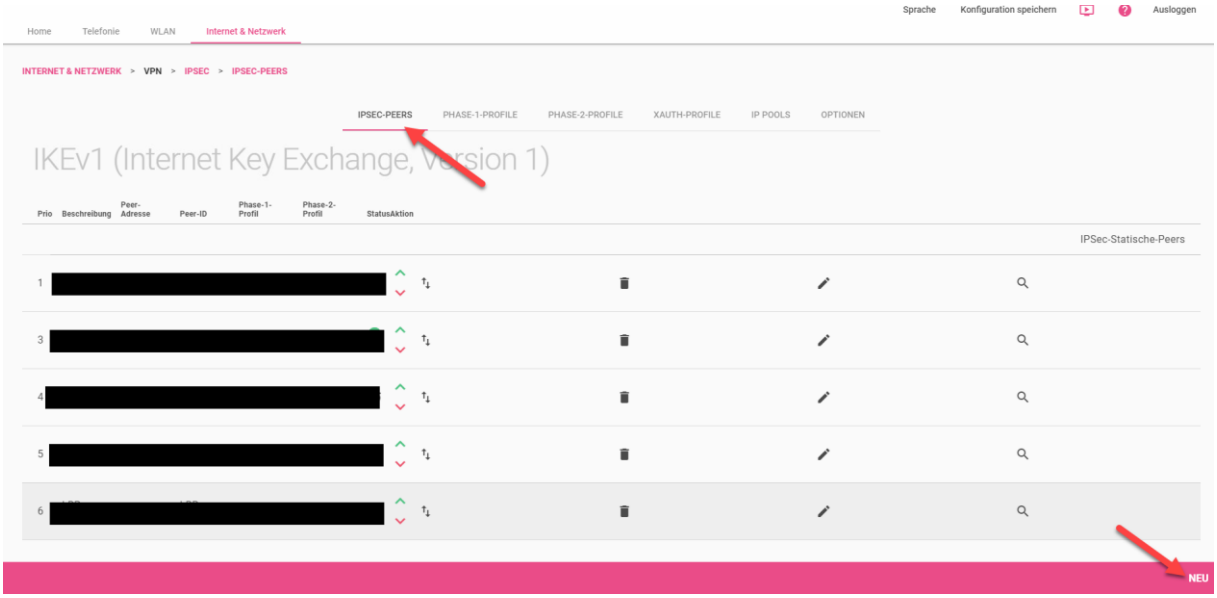

Sprache
Konfiguration speichern
Ausloggen
Home
Telefonie
WLAN
Internet & Netzwerk
INTERNET & NETZWERK > VPN > IPSEC > IPSEC-PEERS
IPSEC-PEERS
PHASE-1-PROFILE
PHASE-2-PROFILE
XAUTH-PROFILE
IP POOLS
OPTIONEN
IKEv1 (Internet Key Exchange, Version 1)
Prio
Beschreibung
Peer-Adresse
Peer-ID
Phase-1-Profil
Phase-2-Profil
StatusAktion
IPSec-Statische-Peers
NEU

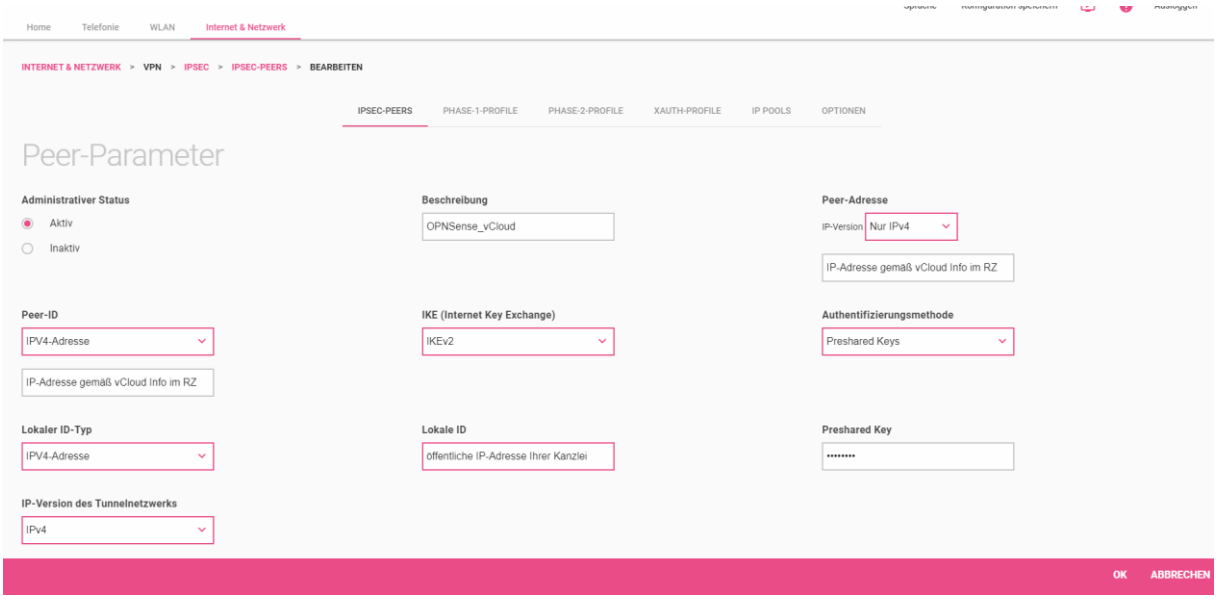

Home
Telefonie
WLAN
Internet & Netzwerk
Standard
Beschreibung
Proposals
Authentifizierung
Modus
DH-Gruppe
Lebensdauer
NEUES IKEV1-PROFIL ERSTELLEN
IKEv2 (Internet Key Exchange, Version 2)
Standard
Beschreibung
Proposals
Lebensdauer
NEUES IKEV2-PROFIL ERSTELLEN
OK
ABBRECHEN

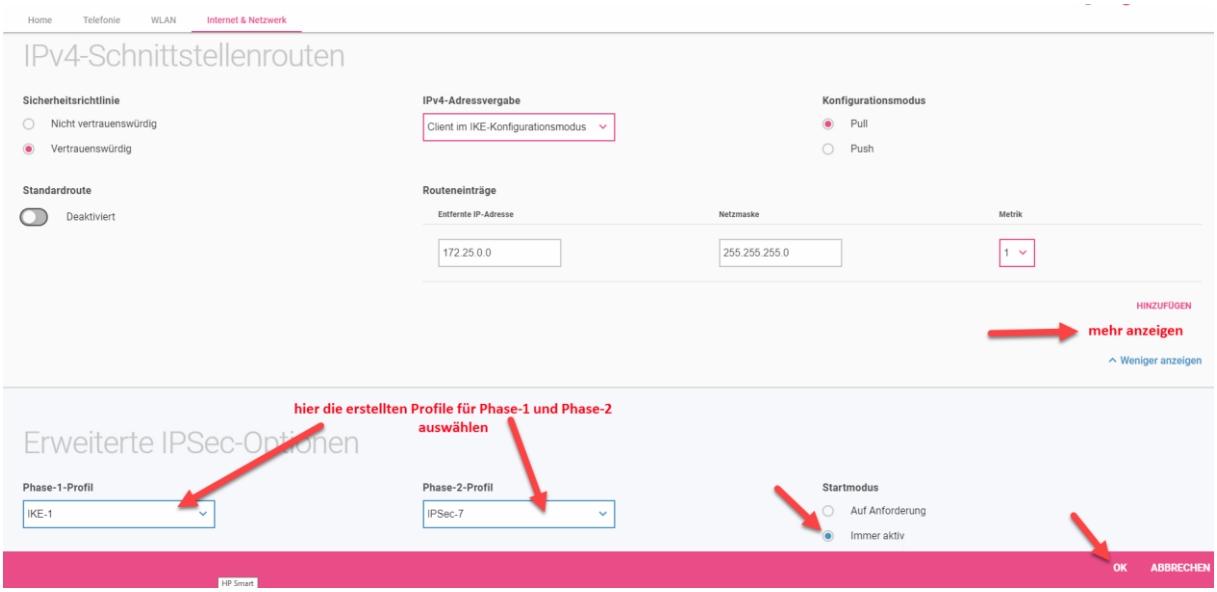

Home
Telefonie
WLAN
Internet & Netzwerk
INTERNET & NETZWERK > VPN > IPSEC > PHASE-1-PROFILE > BEARBEITEN
IPSEC-PEERS
PHASE-1-PROFILE
PHASE-2-PROFILE
XAUTH-PROFILE
IP POOLS
OPTIONEN
Phase-1-Parameter (IKEv2)
Beschreibung
IKE-2
Proposals
Verschlüsselung
Authentifizierung
DH-Gruppe
Aktiviert
AES
SHA2 256
14(2048 Bit)
AES
SHA1
2(1024 Bit)
AES
SHA1
2(1024 Bit)
AES
SHA1
2(1024 Bit)
Lebensdauer
28800
Sekunden / Schlüssel erneut erstellen nach
80
% Lebensdauer
OK
ABBRECHEN


Sprache
Konfiguration speichern
Ausloggen
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-Profile
Standard
Beschreibung
Proposals
PFS-Gruppe
Lebensdauer
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
AES
SHA1
AES
SHA1
PFS-Gruppe verwenden
Aktiviert
14(2048 Bit)
Lebensdauer
28800
Sekunden
0
kBytes Schlüssel erneut erstellen nach
80
%
OK
ABBRECHEN


Sprache
Konfiguration speichern
Ausloggen
Home
Telefonie
WLAN
Internet & Netzwerk
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
IPSec-Statische-Peers
NEU


Home
Telefonie
WLAN
Internet & Netzwerk
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
IKE (Internet Key Exchange)
IKEv2
Authentifizierungsmethode
Preshared Keys
Lokaler ID-Typ
IPV4-Adresse
Lokale ID
öffentliche IP-Adresse Ihrer Kanzlei
Preshared Key
IP-Version des Tunnelnetzwerks
IPv4
OK
ABBRECHEN


Home
Telefonie
WLAN
Internet & Netzwerk
IPv4-Schnittstellenrouten
Sicherheitsrichtlinie
Nicht vertrauenswürdig
Vertrauenswürdig
IPv4-Adressvergabe
Client im IKE-Konfigurationsmodus
Konfigurationsmodus
Pull
Push
Standardroute
Deaktiviert
Routeneinträge
Entfernte IP-Adresse
Netzmaske
Metrik
172.25.0.0
255.255.255.0
1
HINZUFÜGEN
mehr anzeigen
Weniger anzeigen
hier die erstellten Profile für Phase-1 und Phase-2 auswählen
Erweiterte IPSec-Optionen
Phase-1-Profil
IKE-1
Phase-2-Profil
IPSec-7
Startmodus
Auf Anforderung
Immer aktiv
OK
ABBRECHEN