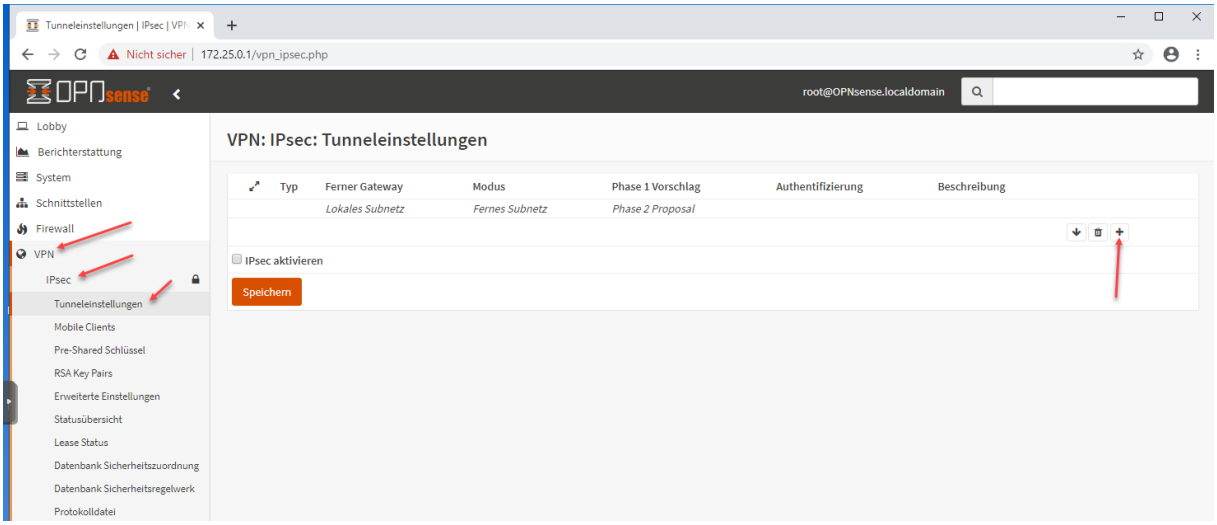
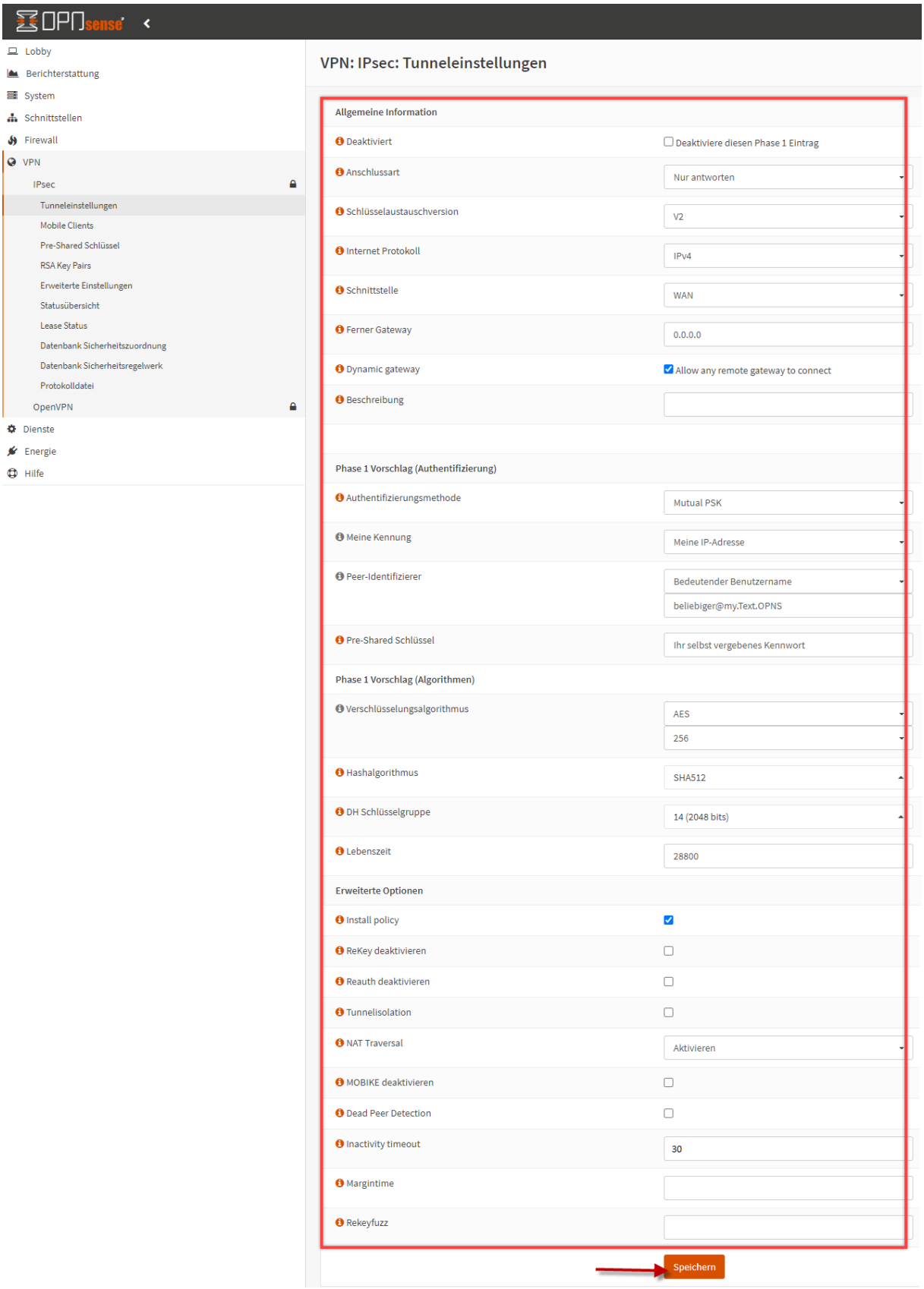
Anleitung zur Herstellung einer IPSec/IKev2 Site-to-Site Verbindung mit der OPNSense Option und einem Lancom-Router z.B. 1781EF+

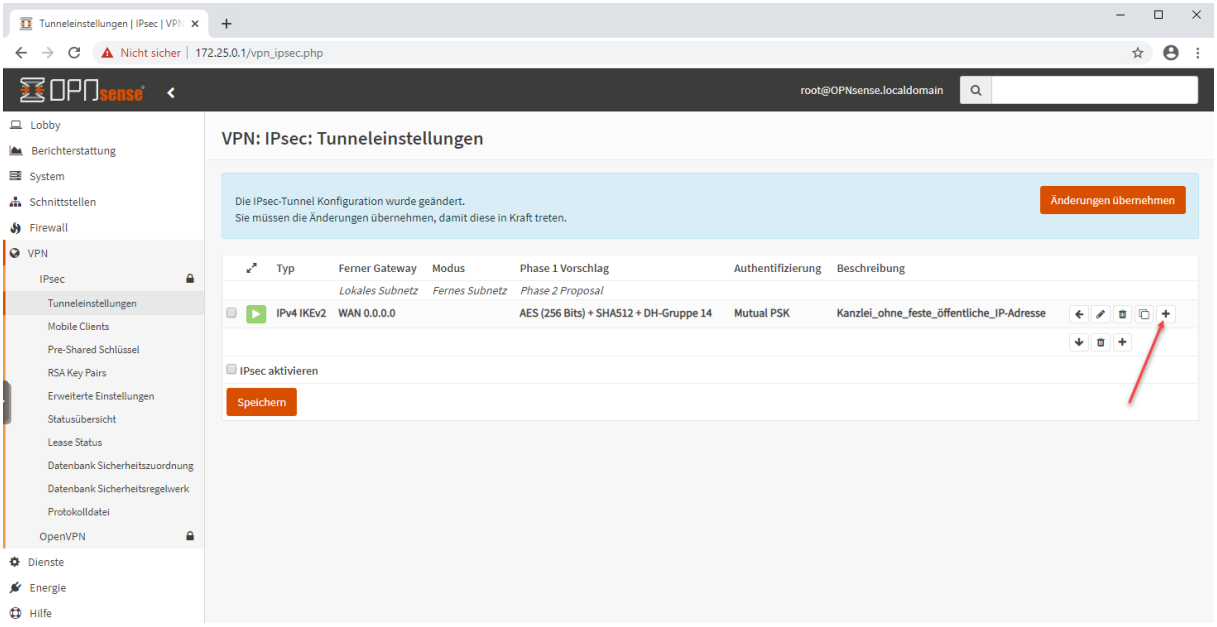
RA Thomas Schmidt – RA-MICRO Vertriebs GmbH – Stand 03.02.2021 – Alle Angaben ohne Gewähr

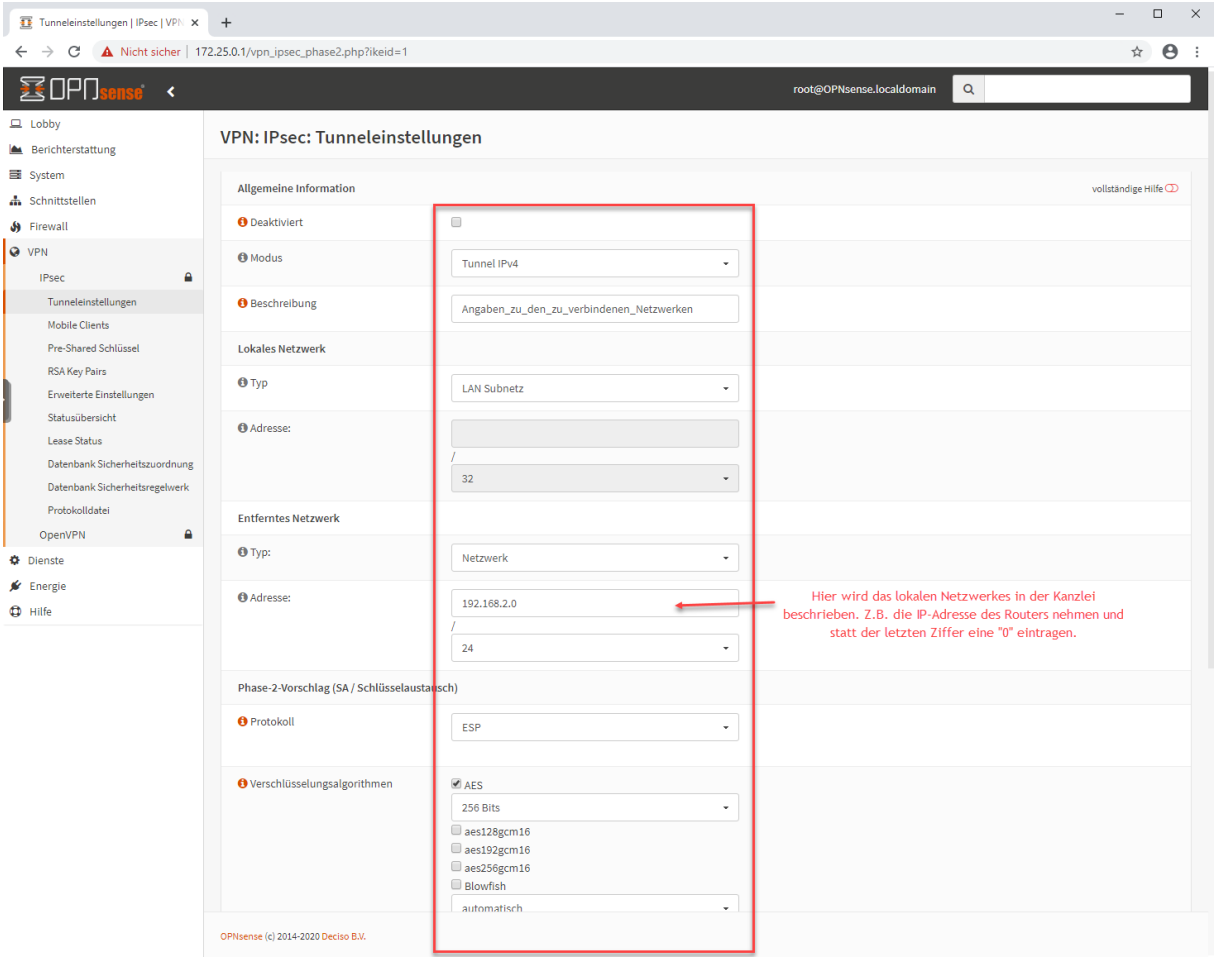
---

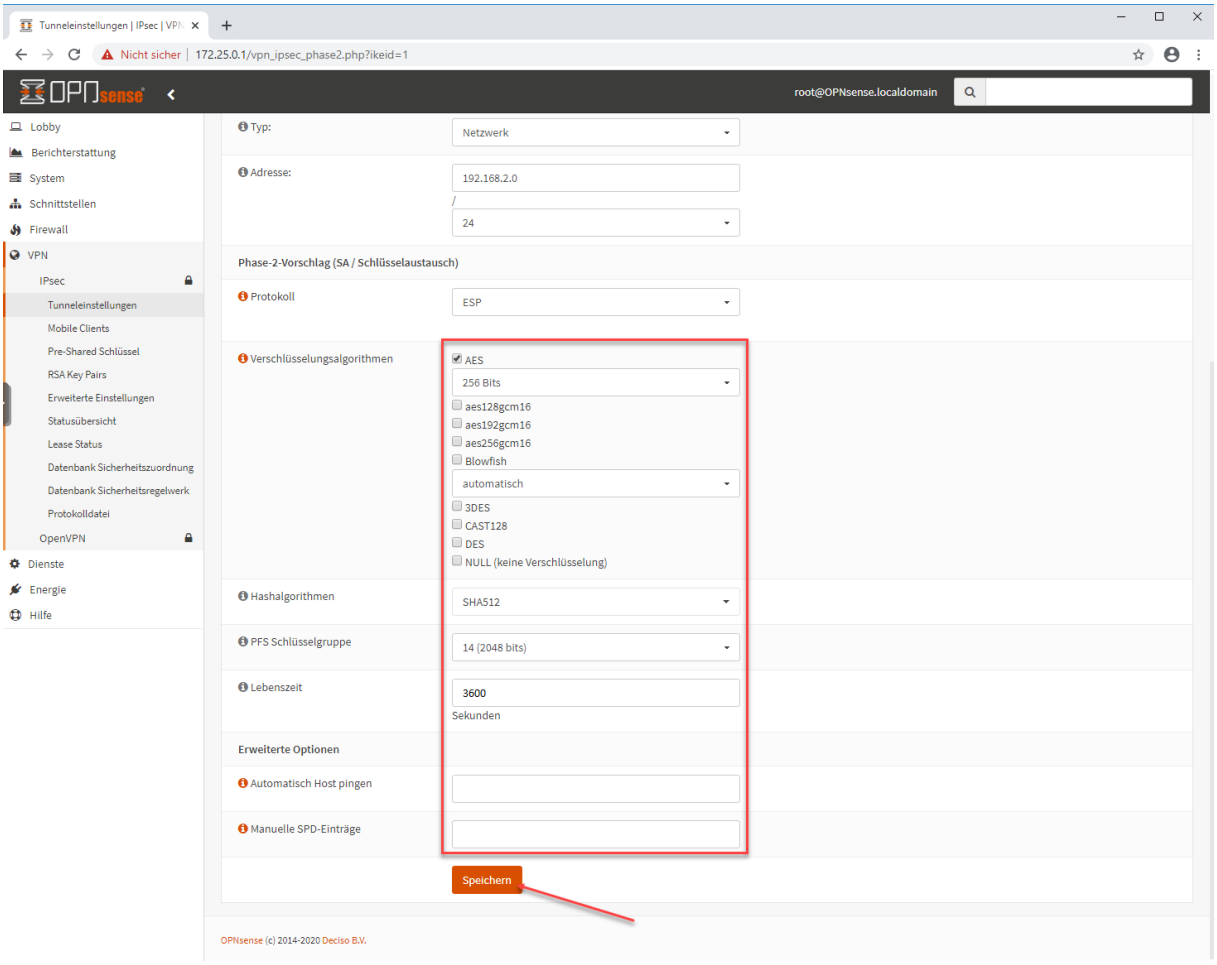
1. Teil: Rechenzentrum:

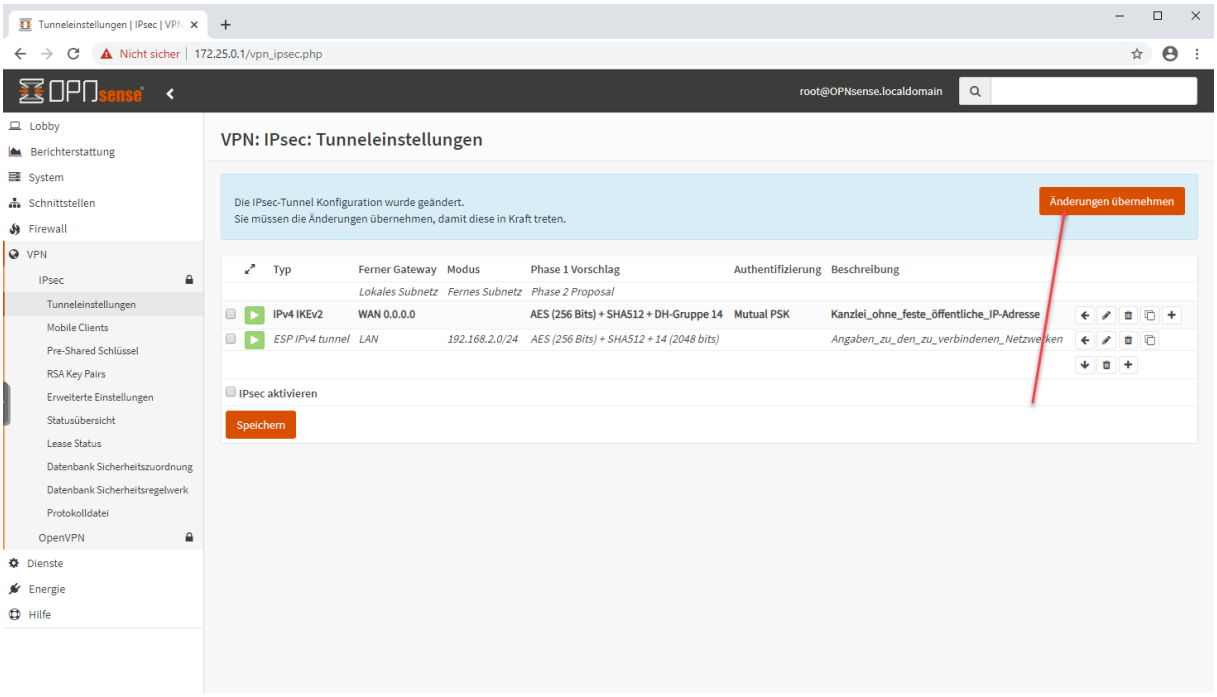


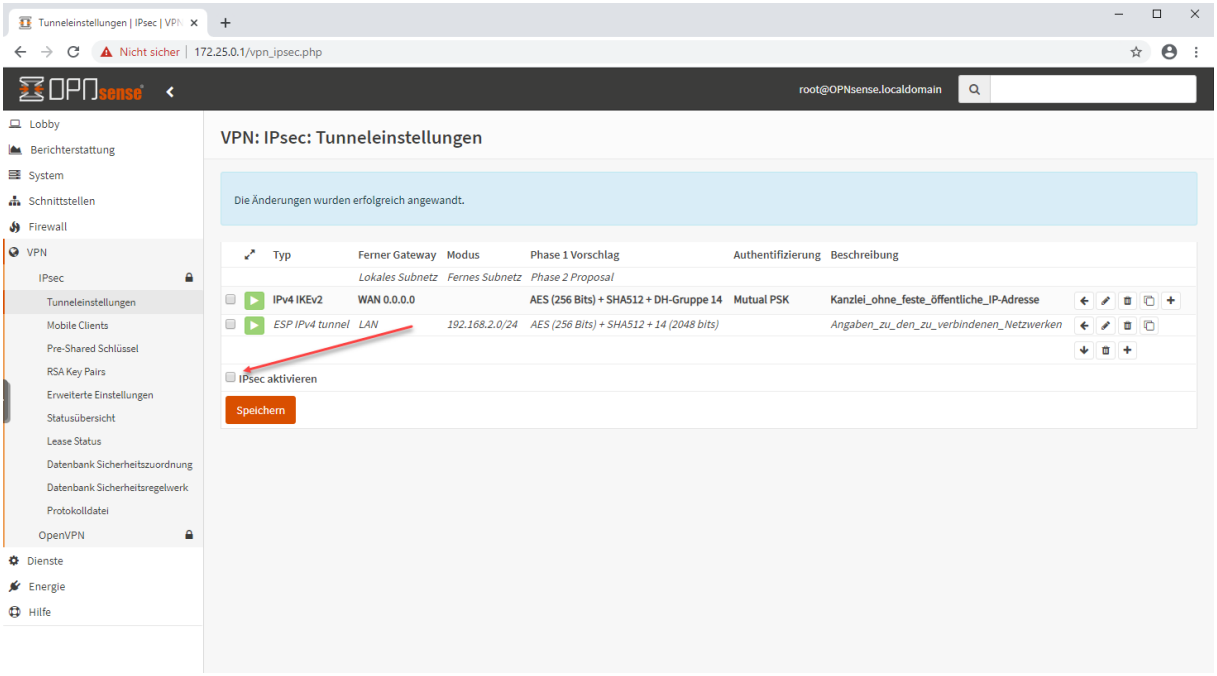

Lobby
Berichterstattung
System
Schnittstellen
Firewall
VPN
IPsec
Tunneleinstellungen
Mobile Clients
Pre-Shared Schlüssel
RSA Key Pairs
Erweiterte Einstellungen
Statusübersicht
Lease Status
Datenbank Sicherheitszuordnung
Datenbank Sicherheitsregelwerk
Protokolldatei
OpenVPN
Dienste
Energie
Hilfe
VPN: IPsec: Tunneleinstellungen
Allgemeine Information
Deaktiviert
Deaktiviere diesen Phase 1 Eintrag
Anschlussart
Nur antworten
Schlüsselaustauschversion
V2
Internet Protokoll
IPv4
Schnittstelle
WAN
Ferner Gateway
0.0.0.0
Dynamic gateway
Allow any remote gateway to connect
Beschreibung
Phase 1 Vorschlag (Authentifizierung)
Authentifizierungsmethode
Mutual PSK
Meine Kennung
Meine IP-Adresse
Peer-Identifizierer
Bedeutender Benutzername
beliebiger@my.Text.OPNS
Pre-Shared Schlüssel
Ihr selbst vergebenes Kennwort
Phase 1 Vorschlag (Algorithmen)
Verschlüsselungsalgorithmus
AES
256
Hashalgorithmus
SHA512
DH Schlüsselgruppe
14 (2048 bits)
Lebenszeit
28800
Erweiterte Optionen
Install policy
ReKey deaktivieren
Reauth deaktivieren
Tunnelisolation
NAT Traversal
Aktivieren
MOBIKE deaktivieren
Dead Peer Detection
Inactivity timeout
30
Margintime
Rekeyfuzz
Speichern

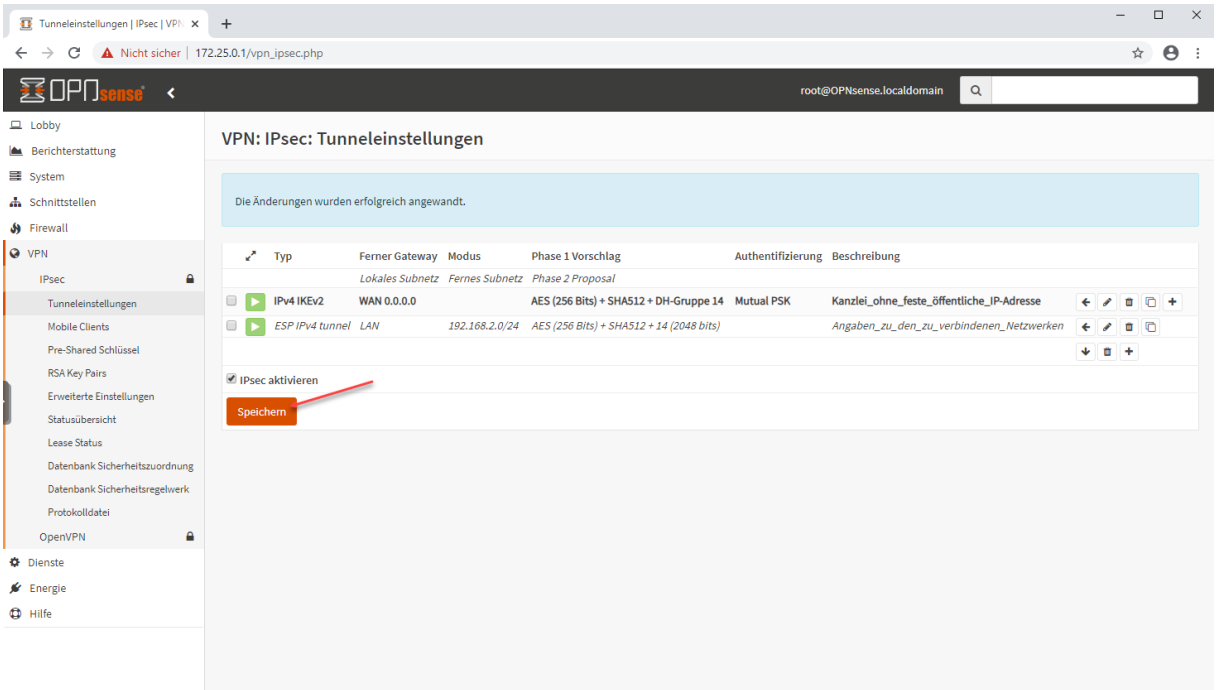

Tunneleinstellungen | IPsec | VPN
Nicht sicher | 172.25.0.1/vpn_ipsec.php
root@OPNsense.localdomain
Lobby
Berichterstattung
System
Schnittstellen
Firewall
VPN
IPsec
Tunneleinstellungen
Mobile Clients
Pre-Shared Schlüssel
RSA Key Pairs
Erweiterte Einstellungen
Statusübersicht
Lease Status
Datenbank Sicherheitszuordnung
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

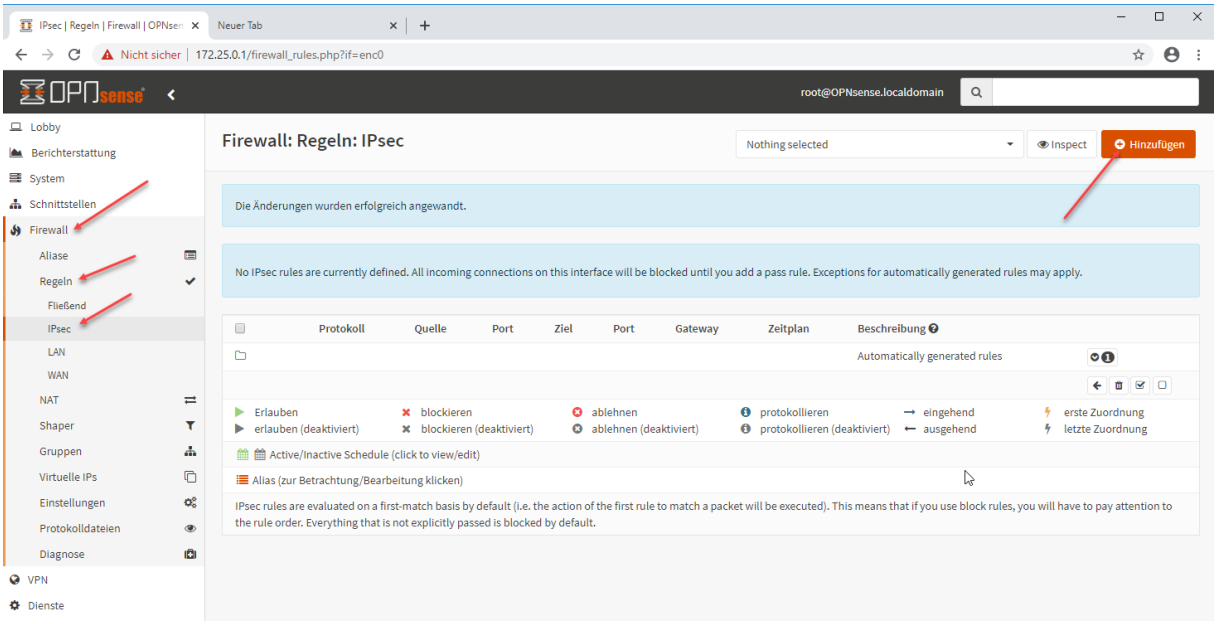

Tunneleinstellungen | IPsec | VPN
Nicht sicher | 172.25.0.1/vpn_ipsec_phase2.php?ikeid=1
root@OPNsense.localdomain
VPN: IPsec: Tunneleinstellungen
Allgemeine Information
vollständige Hilfe
Deaktiviert
Modus
Tunnel IPv4
Beschreibung
Angaben_zu_den_zu_verbindenen_Netzwerken
Lokales Netzwerk
Typ
LAN Subnetz
Adresse:
32
Entferntes Netzwerk
Typ:
Netzwerk
Adresse:
192.168.2.0
24
Hier wird das lokalen Netzwerkes in der Kanzlei beschrieben. Z.B. die IP-Adresse des Routers nehmen und statt der letzten Ziffer eine "0" eintragen.
Phase-2-Vorschlag (SA / Schlüsselaustausch)
Protokoll
ESP
Verschlüsselungsalgorithmen
AES
256 Bits
aes128gcm16
aes192gcm16
aes256gcm16
Blowfish
automatisch
OPNsense (c) 2014-2020 Deciso B.V.

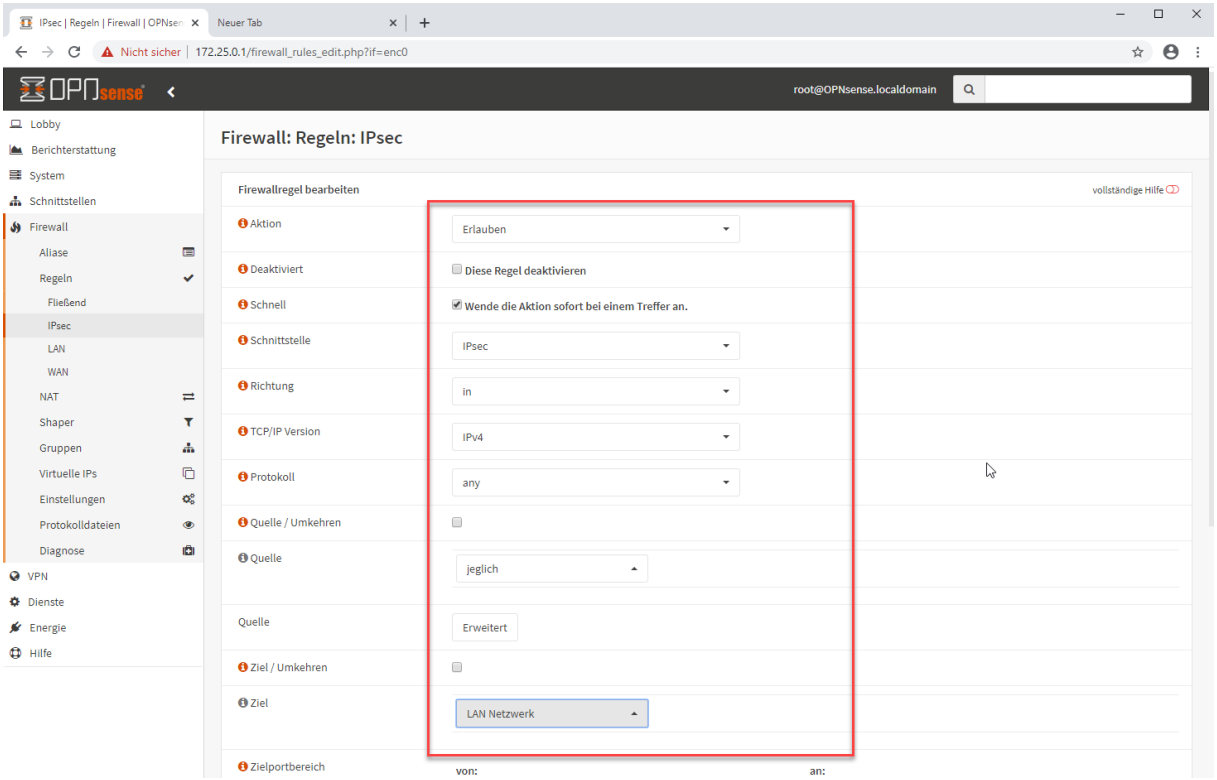

Tunneleinstellungen | IPsec | VPN
Nicht sicher | 172.25.0.1/vpn_ipsec_phase2.php?ikeid=1
root@OPNsense.localdomain
Lobby
Berichterstattung
System
Schnittstellen
Firewall
VPN
IPsec
Tunneleinstellungen
Mobile Clients
Pre-Shared Schlüssel
RSA Key Pairs
Erweiterte Einstellungen
Statusübersicht
Lease Status
Datenbank Sicherheitszuordnung
Datenbank Sicherheitsregelwerk
Protokolldatei
OpenVPN
Dienste
Energie
Hilfe
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
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
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

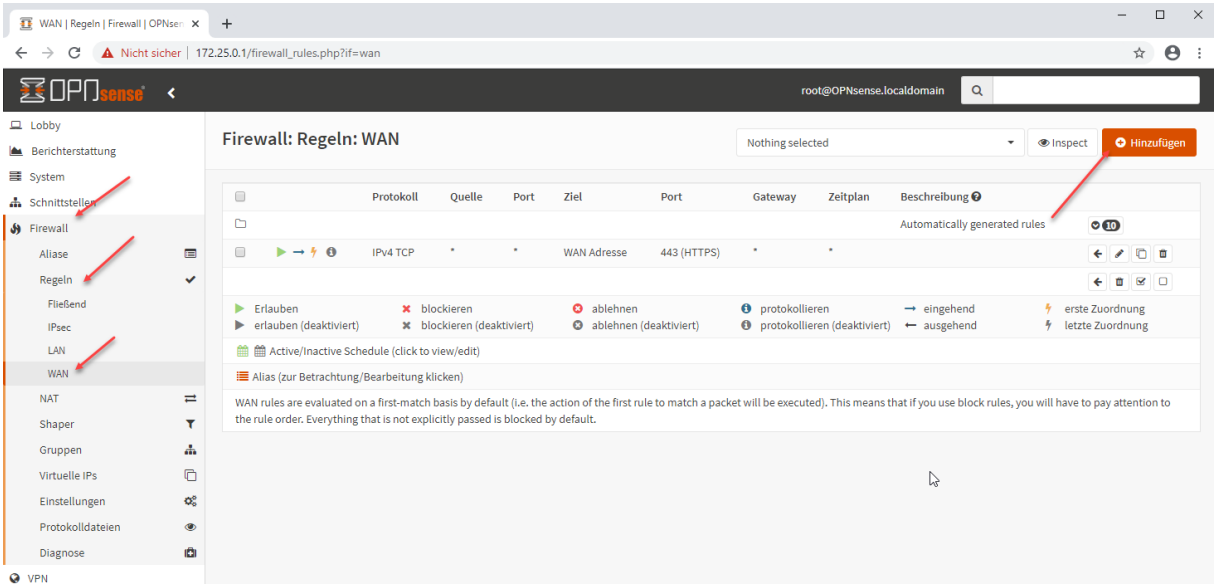

Tunneleinstellungen | IPsec | VPN
Nicht sicher | 172.25.0.1/vpn_ipsec.php
root@OPNsense.localdomain
Lobby
Berichterstattung
System
Schnittstellen
Firewall
VPN
IPsec
Tunneleinstellungen
Mobile Clients
Pre-Shared Schlüssel
RSA Key Pairs
Erweiterte Einstellungen
Statusübersicht
Lease Status
Datenbank Sicherheitszuordnung
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

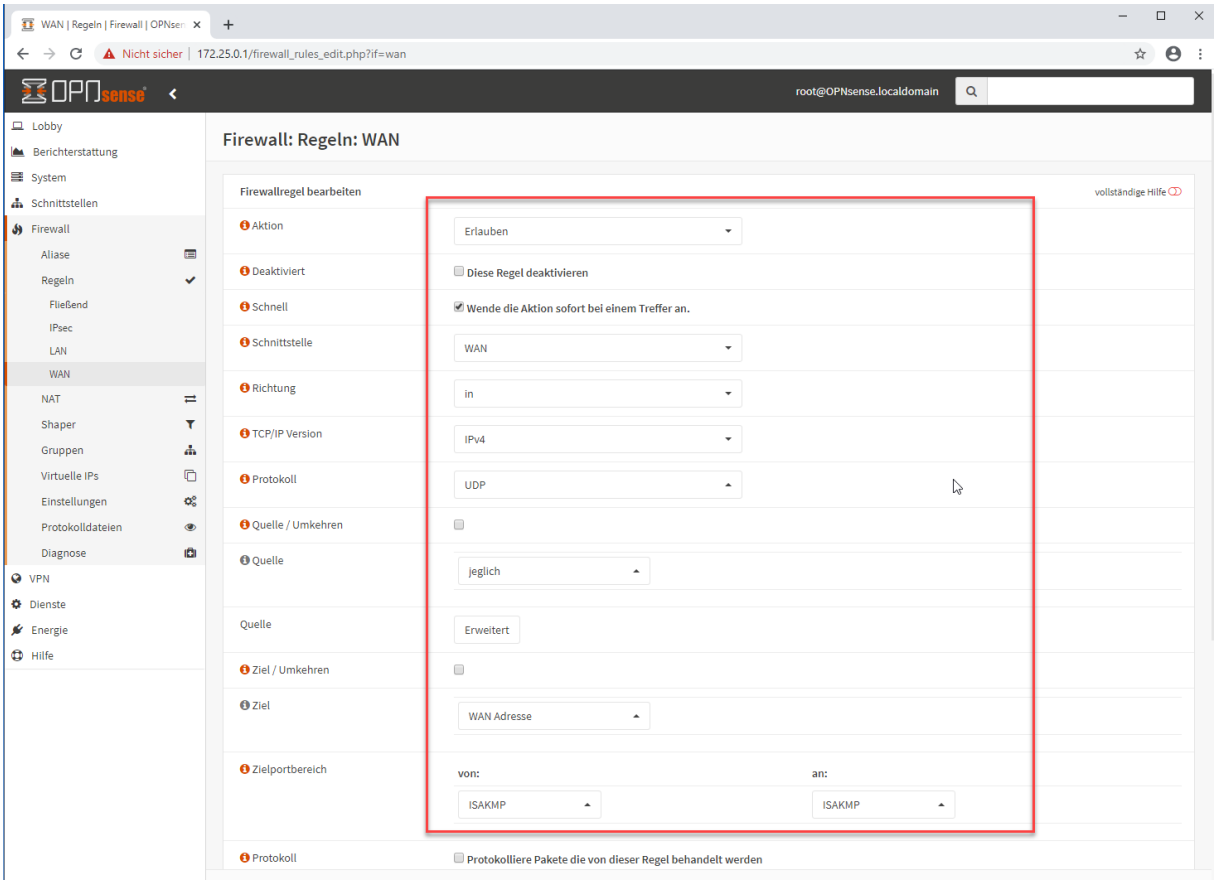




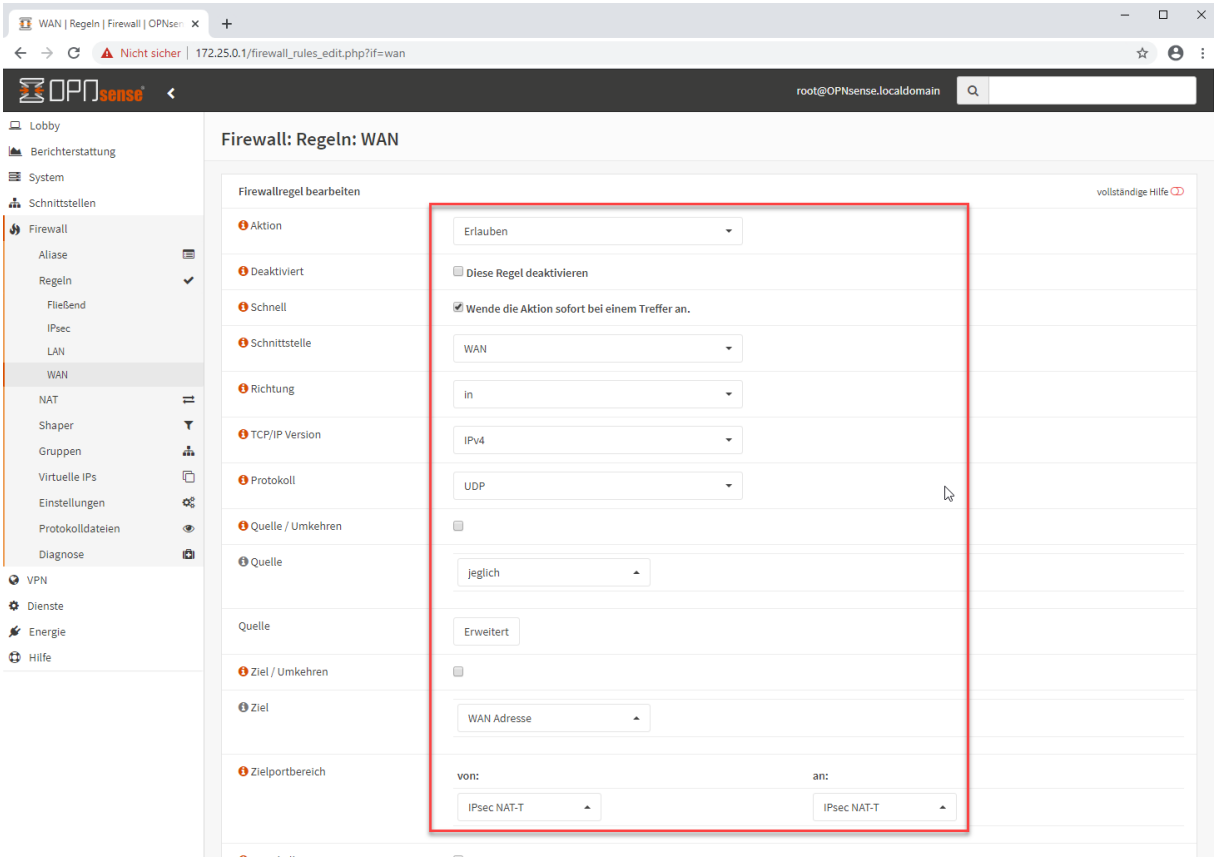
→ auf *Speichern* klicken

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:

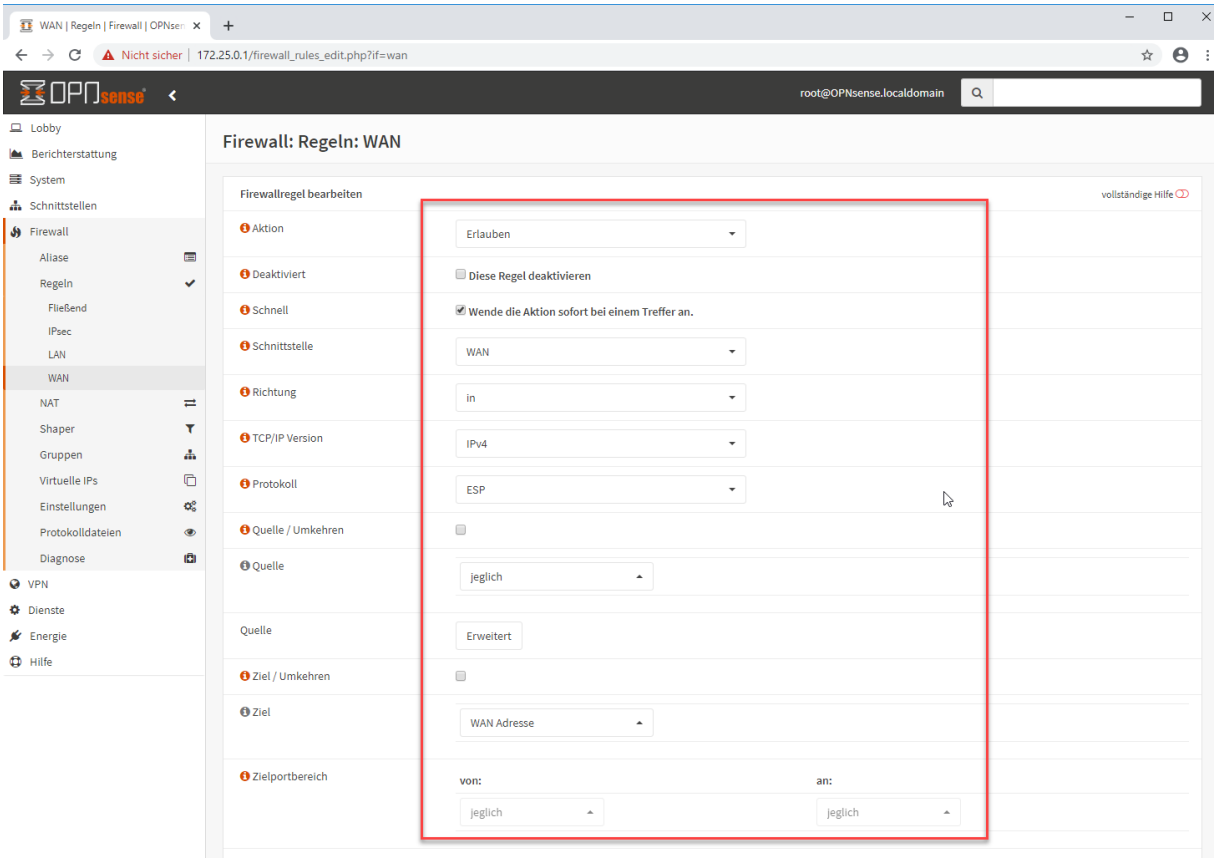




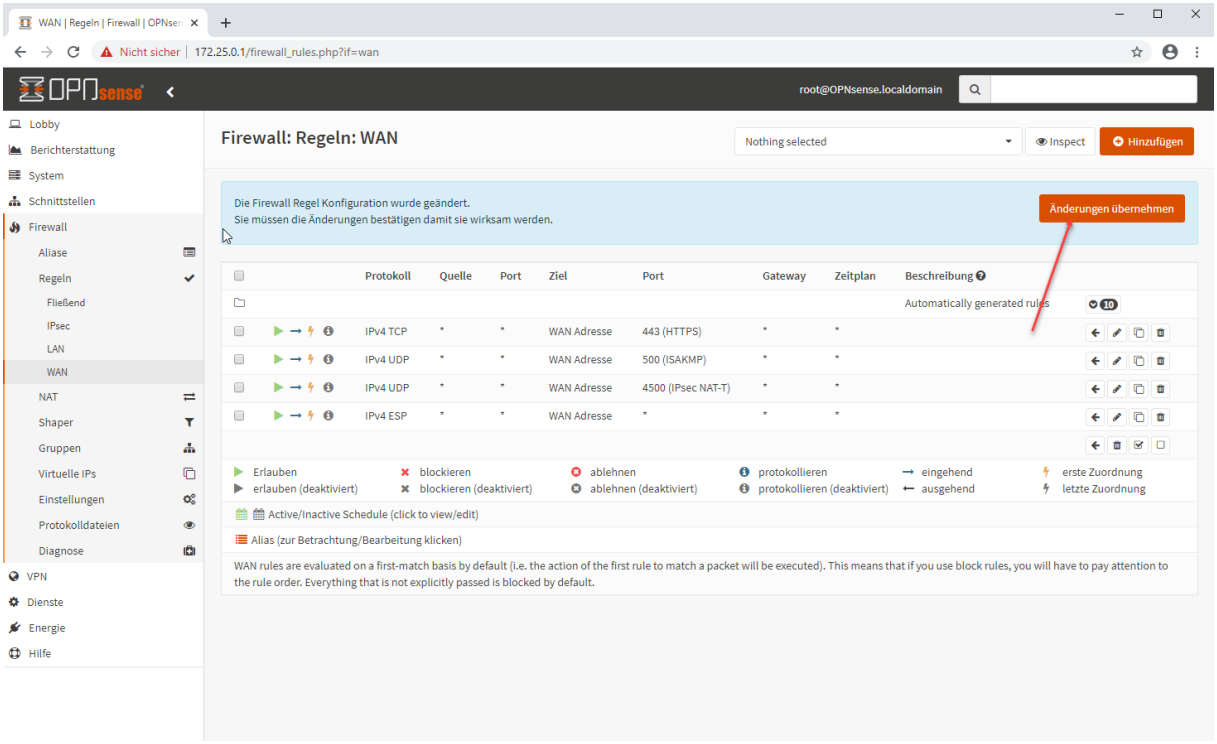
→ Speichern und wieder auf Hinzufügen klicken



→ Speichern und wieder auf Hinzufügen klicken

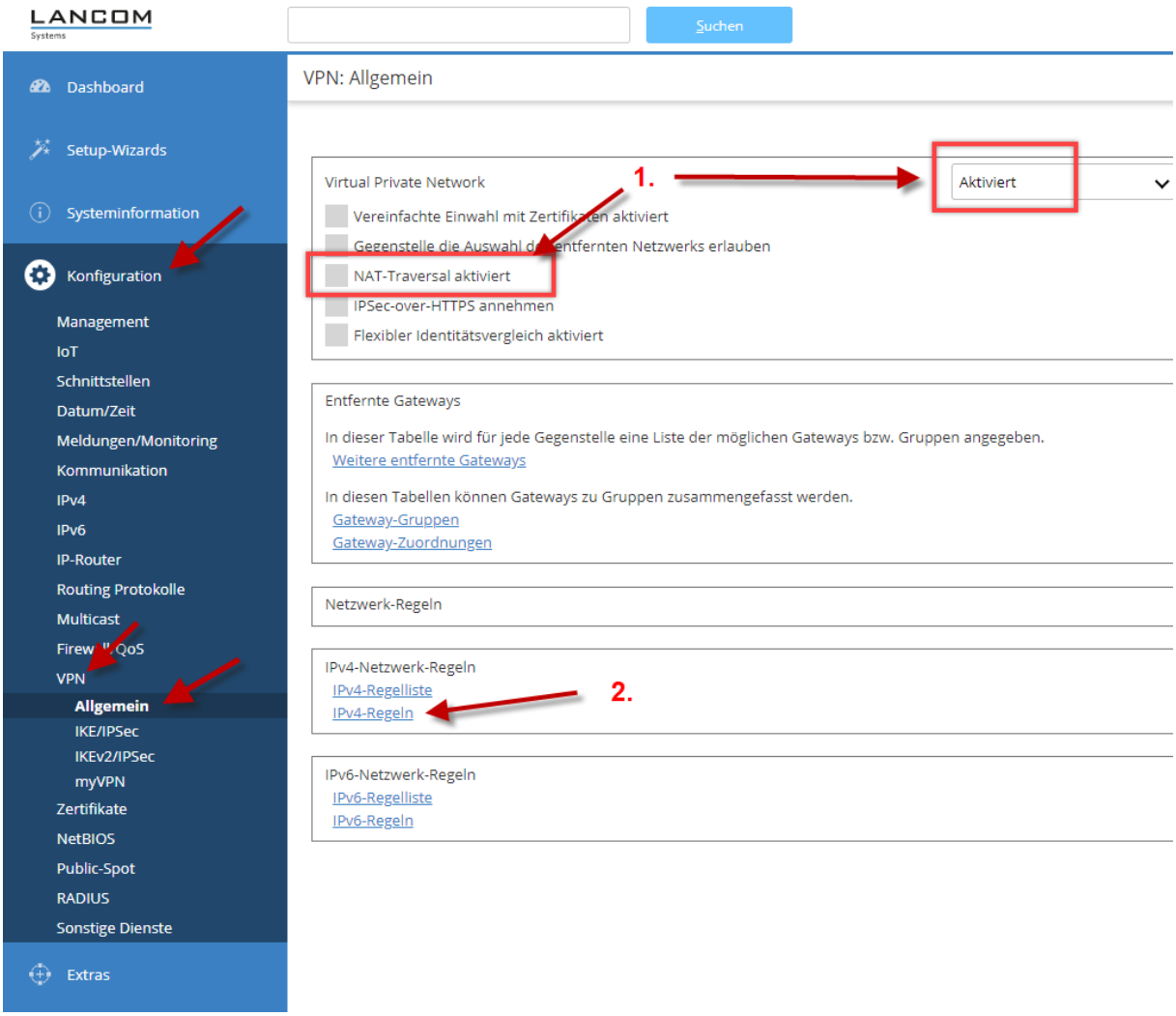


→Speichern


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 * * WAN Adresse 443 (HTTPS) * *
IPv4 UDP * * WAN Adresse 500 (ISAKMP) * *
IPv4 UDP * * WAN Adresse 4500 (IPsec NAT-T) * *
IPv4 ESP * * WAN Adresse * * *
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 mit Lancom-Router z.B. 1781EF+

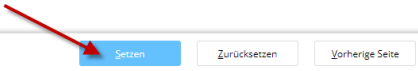
Die VPN LAN-zu-LAN Verbindung kann entweder manuell oder mit Hilfe des Assistenten erstellen werden. Wichtig ist, dass im Ergebnis die nachfolgend angezeigten Einstellungen entsprechend gesetzt sind.



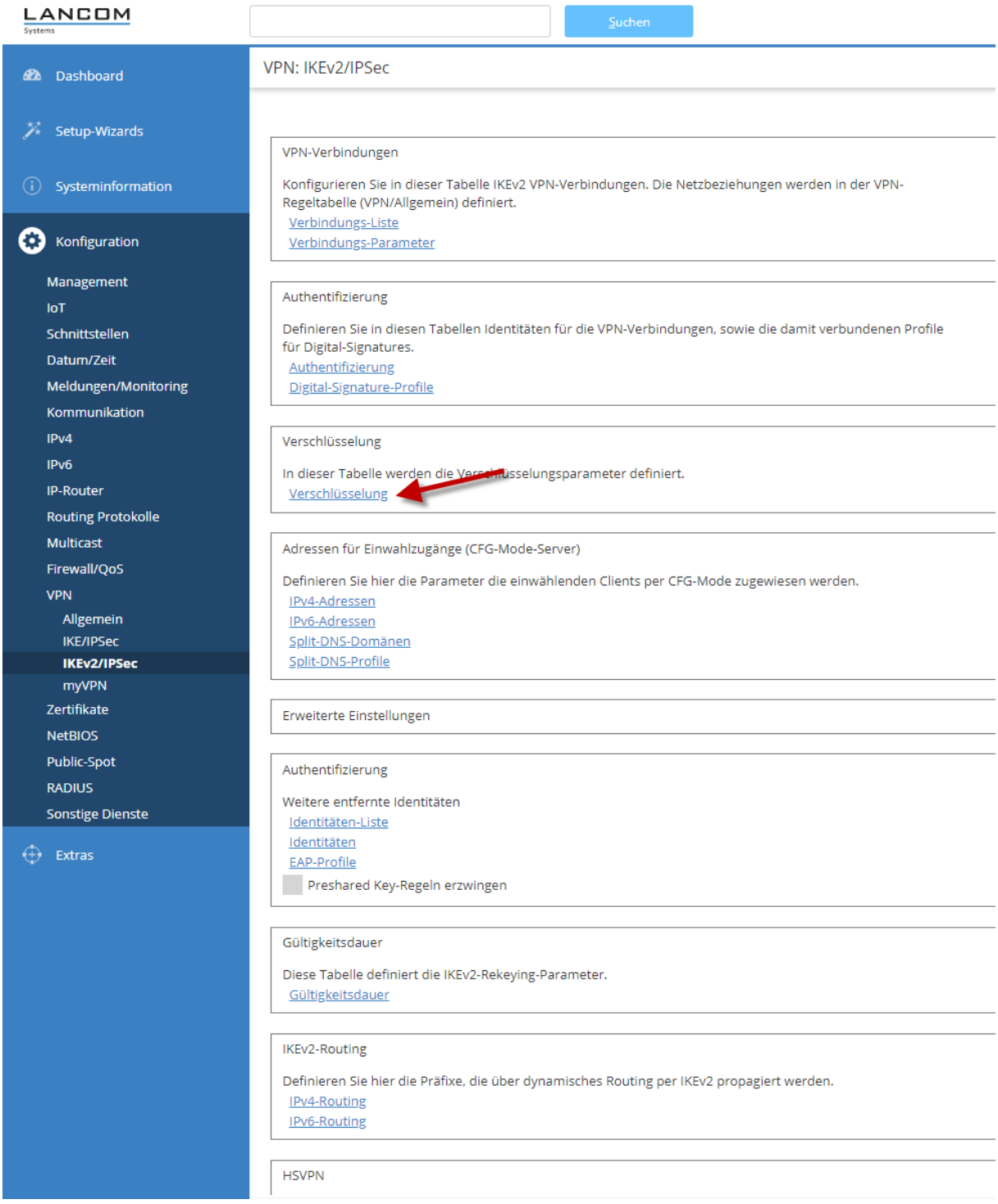
VPN: Allgemein

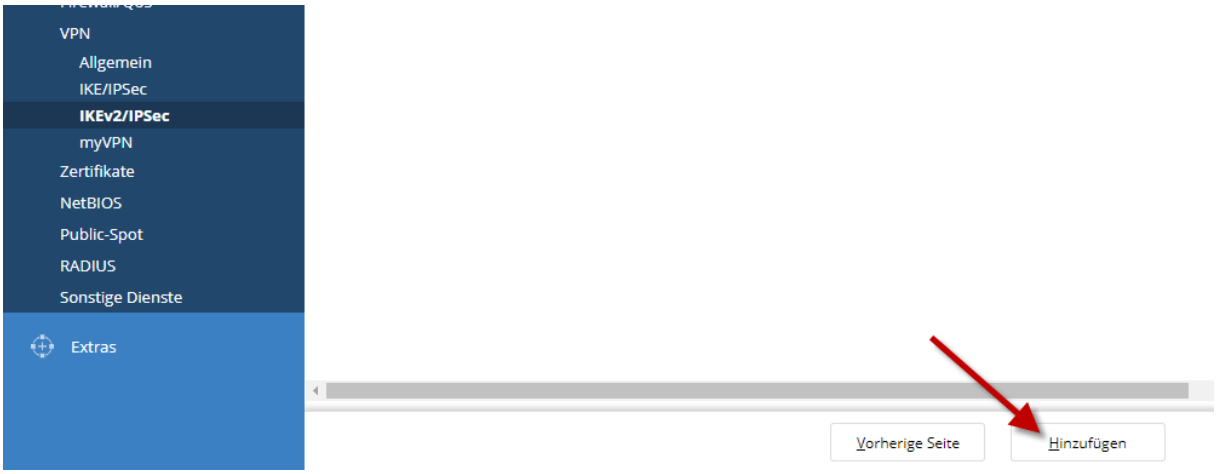
IPv4-Regeln
- Hinzufügen

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




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


LANCOM
Systems
Suchen
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: IKEv2/IPSec

Verschlüsselung
- Hinzufügen

Name: OPNS (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)
- [x] DH14 (MODP-2048)
- [ ] DH5 (MODP-1536)
- [ ] DH2 (MODP-1024)

PFS: Ja

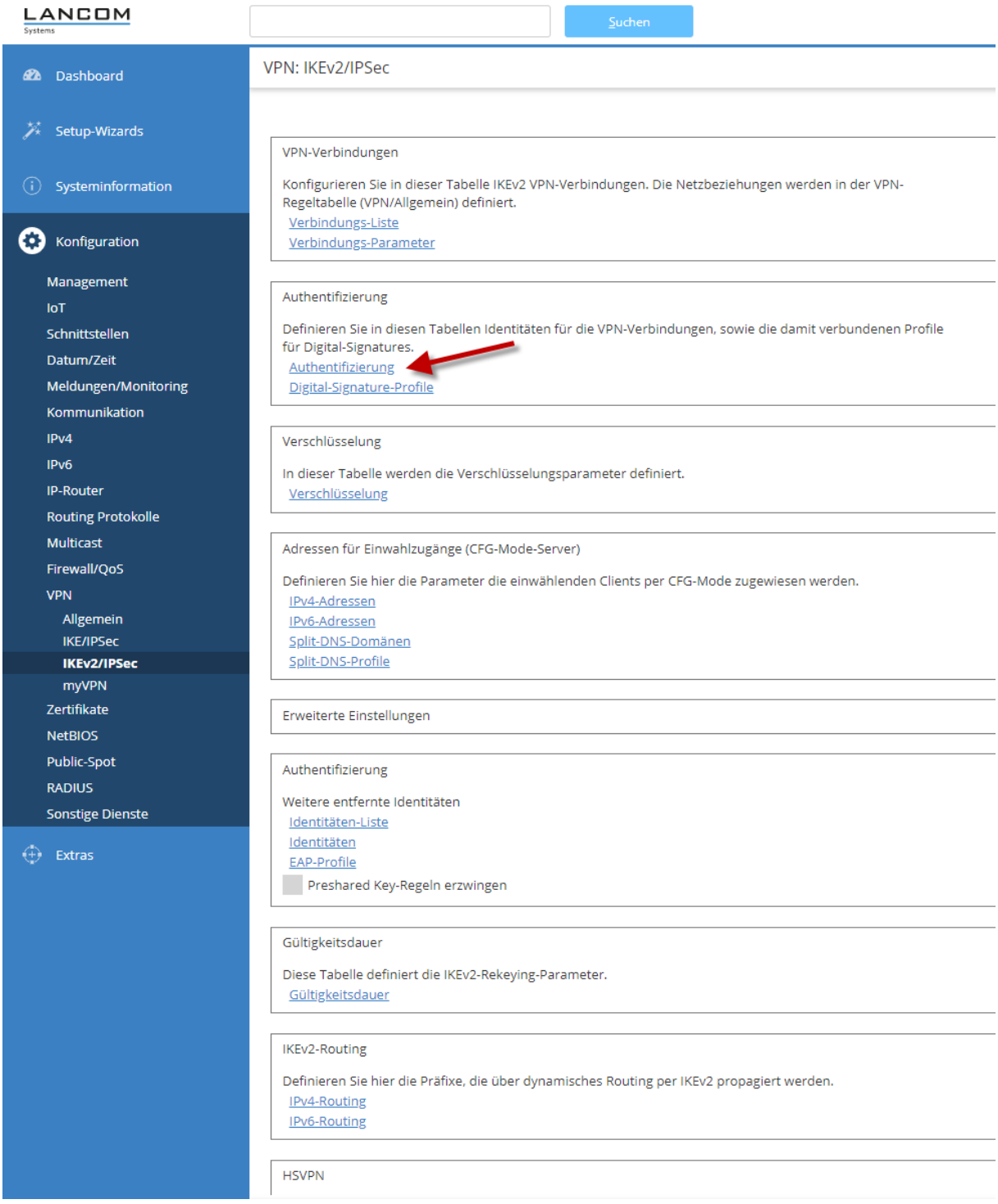
IKE-SA
Verschlüsselungsliste
- [x] AES-CBC-256
- [ ] AES-CBC-192
- [ ] AES-CBC-128
- [ ] 3DES
- [ ] AES-GCM-256
- [ ] AES-GCM-192
- [ ] AES-GCM-128
- [ ] CHACHA20-POLY1305

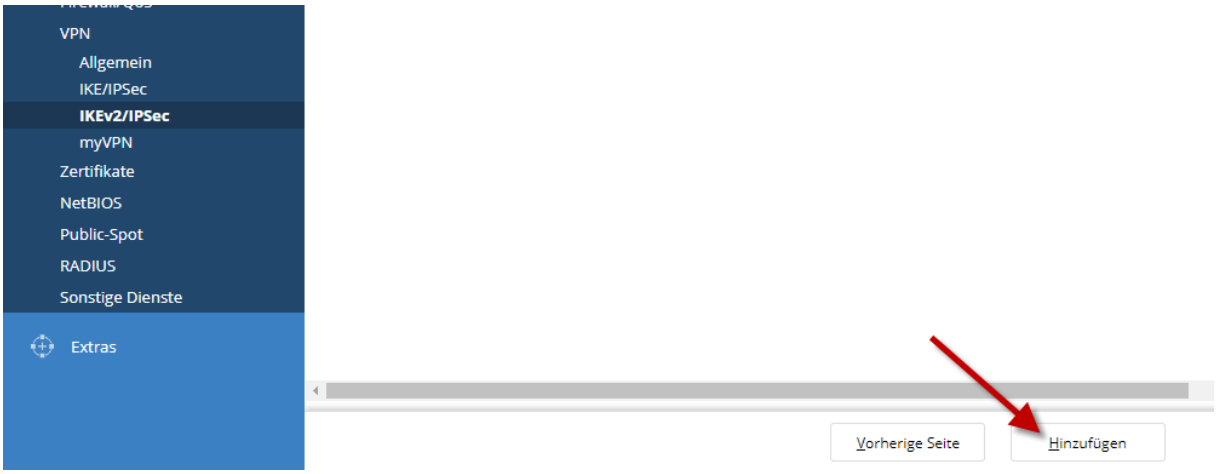
Hash-Liste
- [x] SHA-512
- [ ] SHA-384
- [ ] SHA-256
- [ ] SHA1
- [ ] MD5

Child-SA
Verschlüsselungsliste
- [x] AES-CBC-256
- [ ] AES-CBC-192
- [ ] AES-CBC-128
- [ ] 3DES
- [ ] AES-GCM-256
- [ ] AES-GCM-192
- [ ] AES-GCM-128
- [ ] CHACHA20-POLY1305

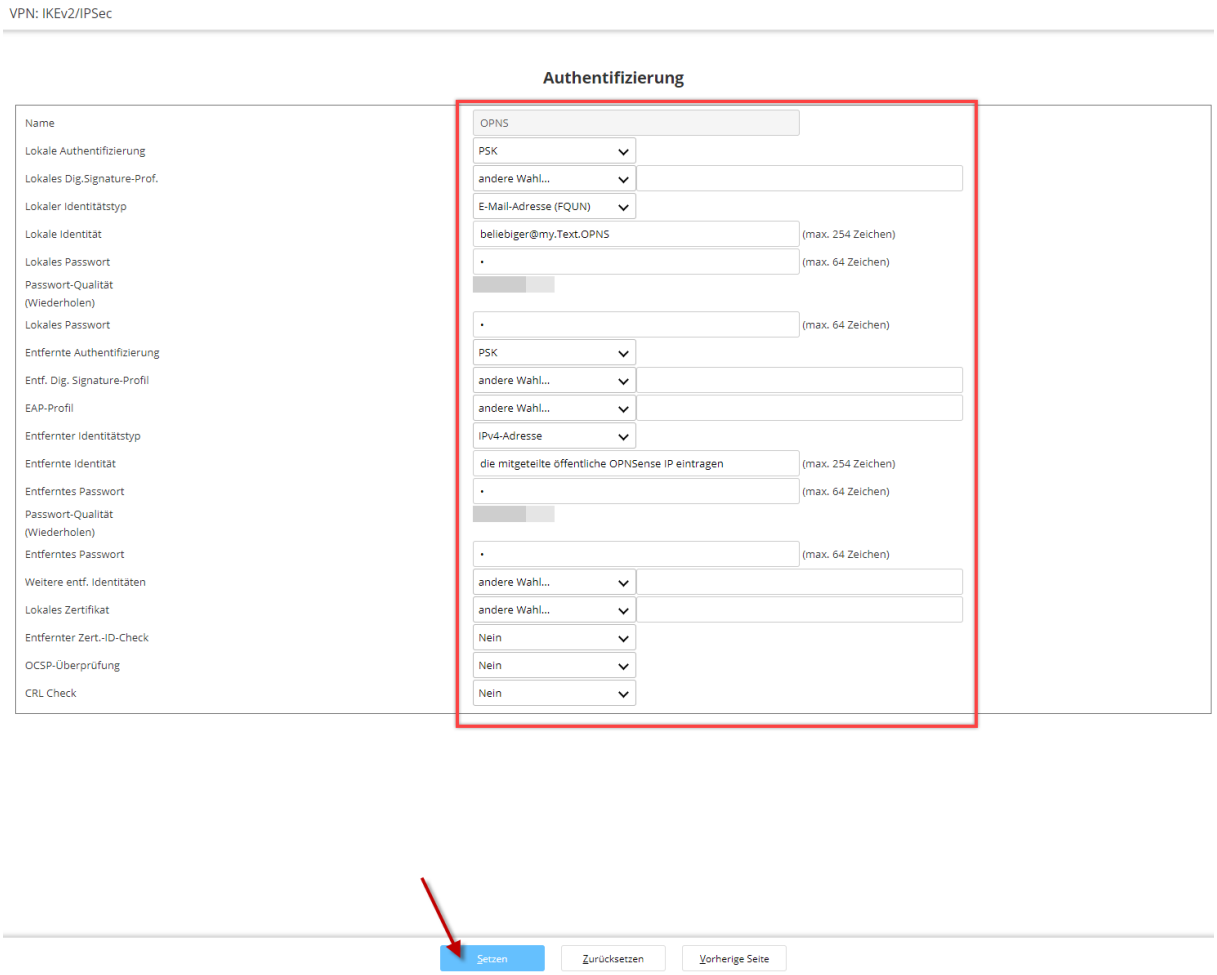
Hash-Liste
- [x] SHA-512
- [ ] SHA-384
- [ ] SHA-256
- [ ] SHA1
- [ ] MD5

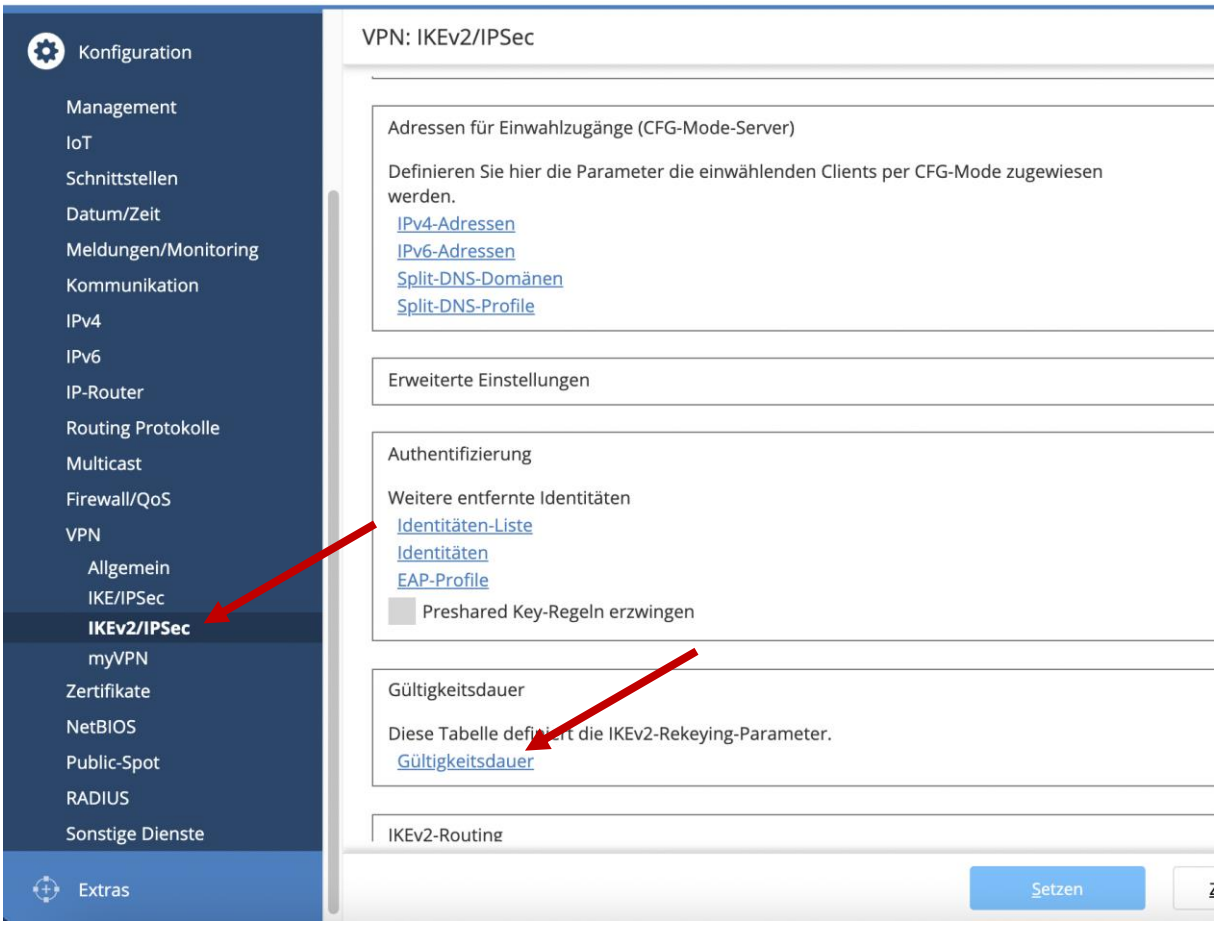
Setzen | Zurücksetzen | Vorherige Seite


LANCOM
Systems
Suchen
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

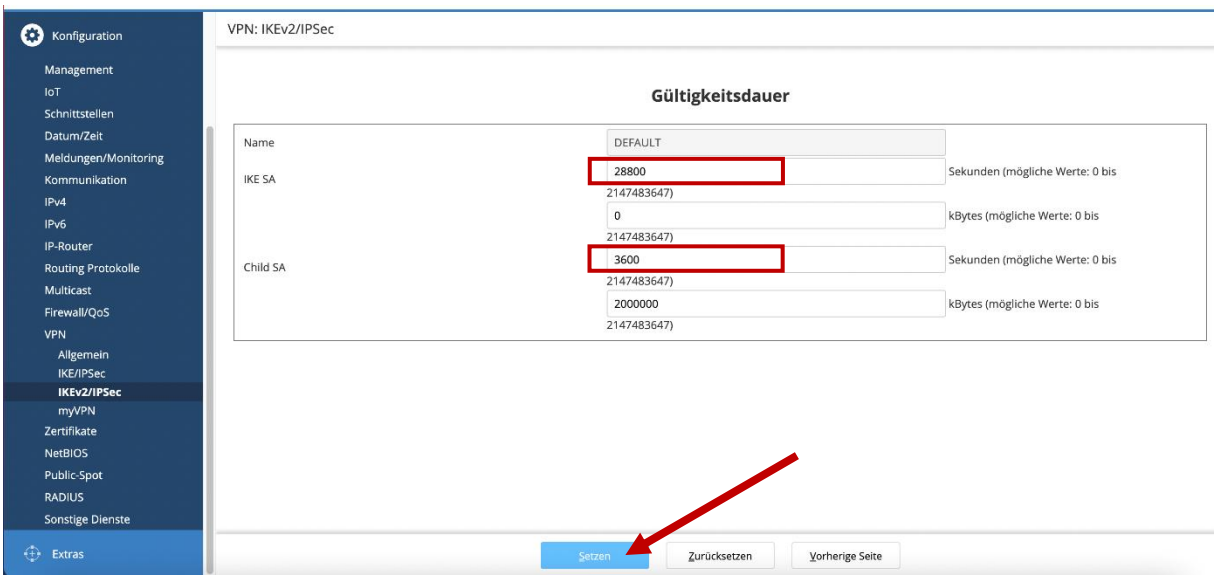


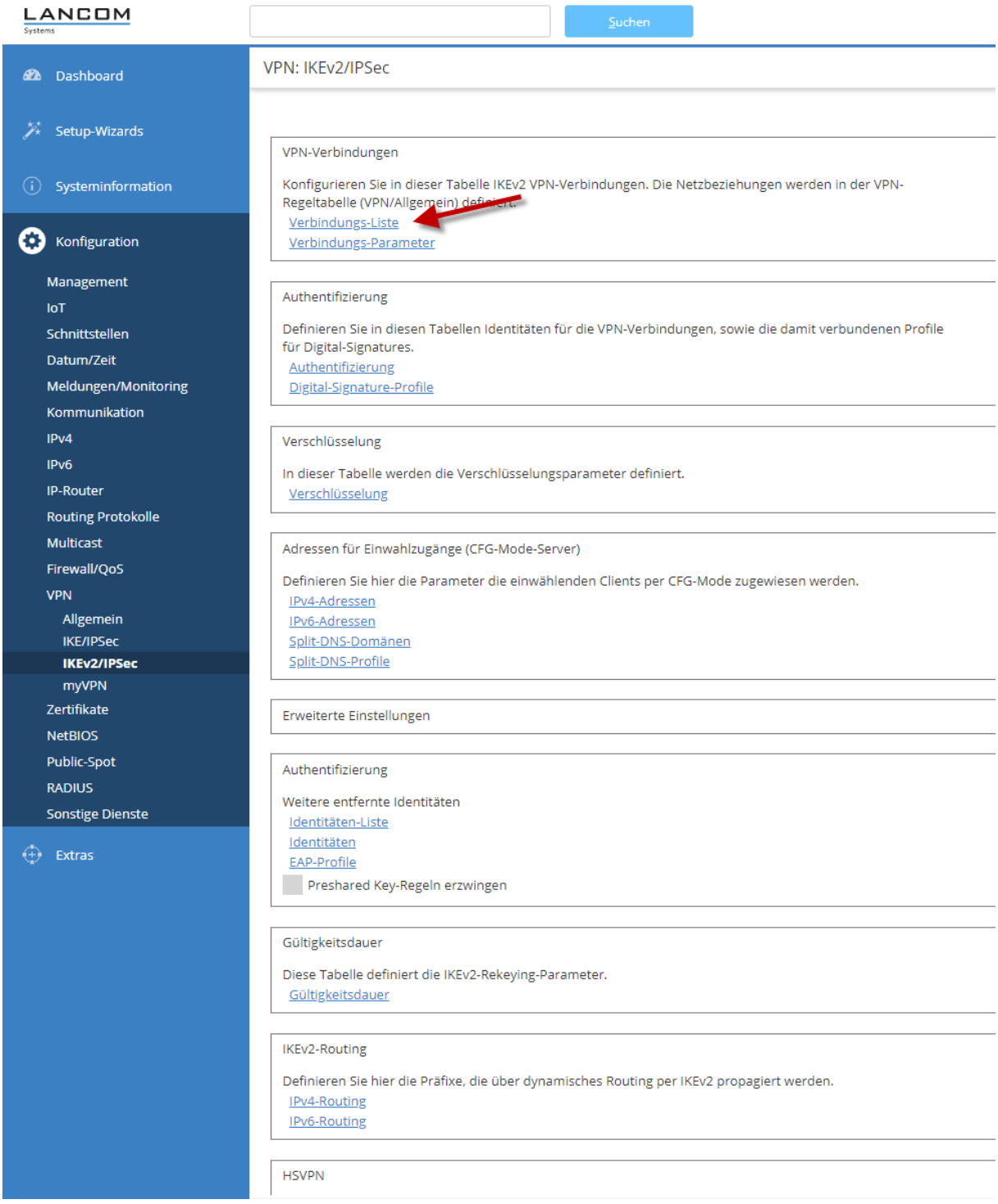
Bei **Lokales** und **Entferntes Passwort** das in der OPNSense im Rechenzentrum vergebene Kennwort unter „Pre-Shared Schlüssel" eintragen.

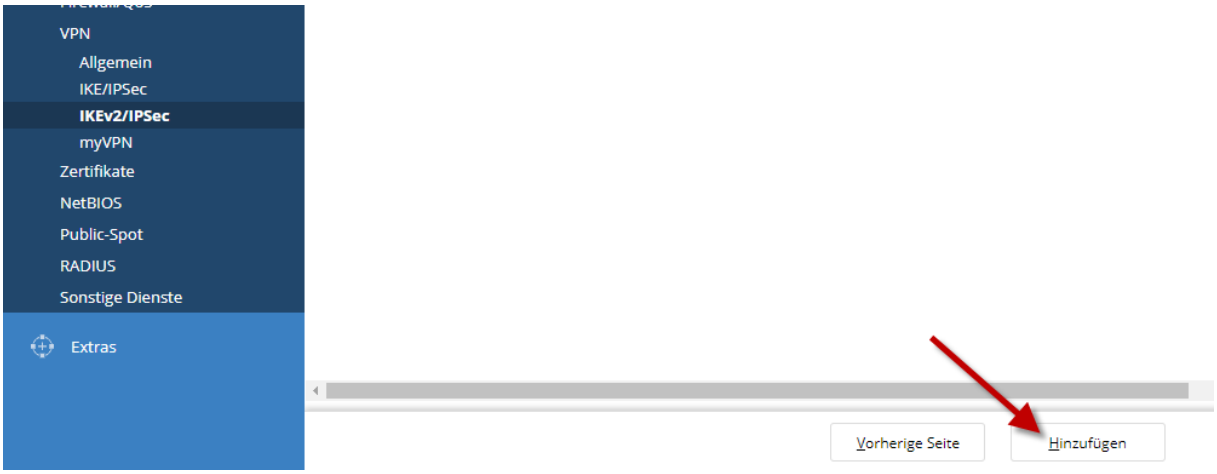



Konfiguration
Management
IoT
Schnittstellen
Datum/Zeit
Meldungen/Monitoring
Kommunikation
IPv4
IPv6
IP-Router
Routing Protokolle
Multicast
Firewall/QoS
VPN
Allgemein
IKE/IPSec
IKEv2/IPSec
myVPN
Zertifikate
NetBIOS
Public-Spot
RADIUS
Sonstige Dienste
Extras
VPN: IKEv2/IPSec
Adressen für Einwahlzugänge (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
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
28800
Sekunden (mögliche Werte: 0 bis 2147483647)
0
kBytes (mögliche Werte: 0 bis 2147483647)
Child SA
3600
Sekunden (mögliche Werte: 0 bis 2147483647)
2000000
kBytes (mögliche Werte: 0 bis 2147483647)
Setzen
Zurücksetzen
Vorherige Seite


LANCOM
Systems
Suchen
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: IKEv2/IPSec

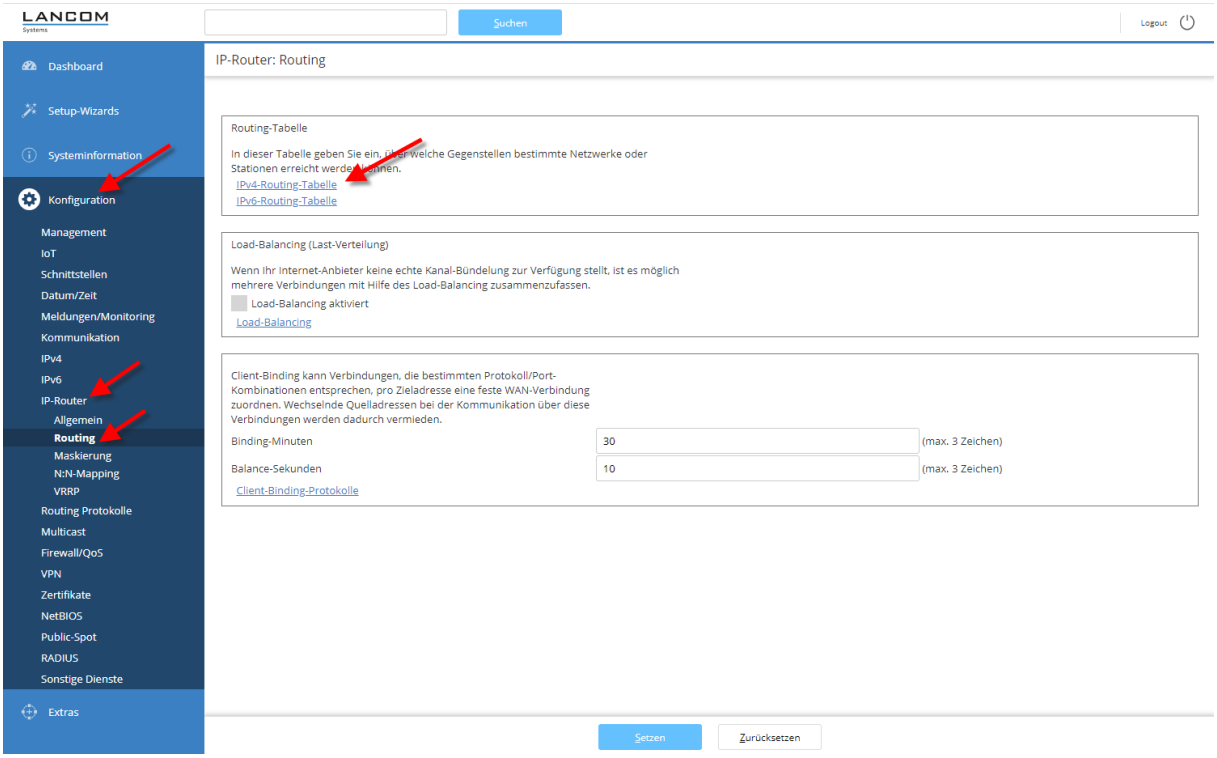
Verbindungs-Liste
- Hinzufügen

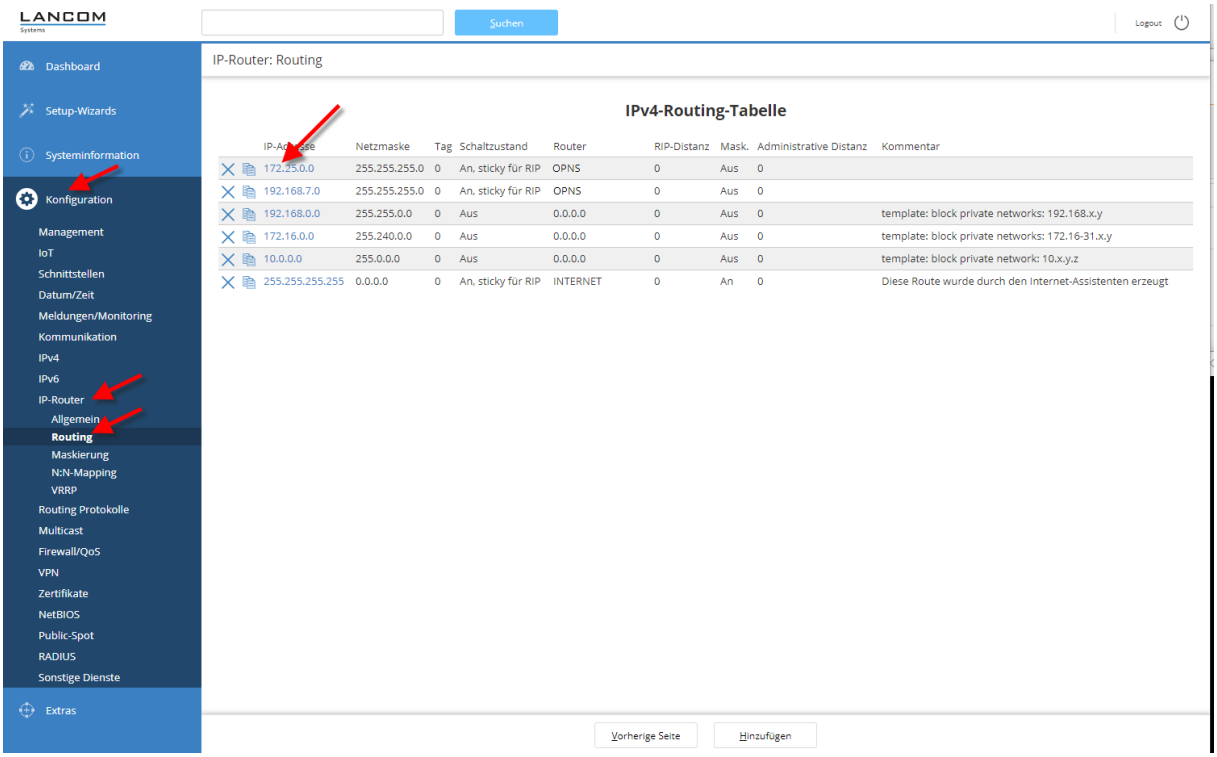
Name der Verbindung	OPNS	
Eintrag aktiv		
Haltezeit	9999	Sekunden (mögliche Werte: 0 bis 9999
Entferntes Gateway	die mitgeteilte öffentliche OPNSense IP Adresse eintragen	(max. 64 Zeichen)
Routing-Tag	0	(mögliche Werte: 0 bis 65535)
Verschlüsselung	OPNS	
Authentifizierung	OPNS	
Verbindungs-Parameter	DEFAULT	
Gültigkeitsdauer	DEFAULT	

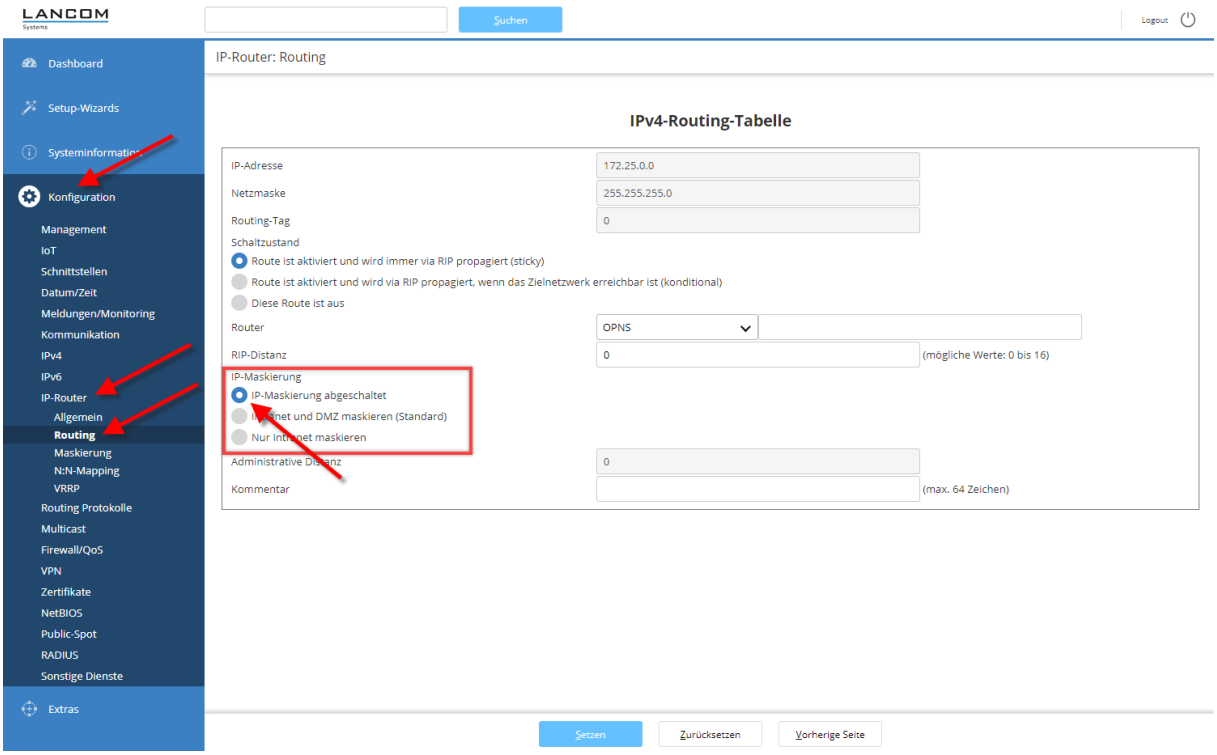
VPN-Regelerzeugung		
Regelerzeugung	Manuell	
IPv4-Regeln	OPNS	
IPv6-Regeln	andere Wahl...	

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	andere Wahl...	
RADIUS-Auth.-Server	andere Wahl...	
RADIUS-Acc.-Server	andere Wahl...	
IPv6-Profil	DEFAULT	
Kommentar		(max. 63 Zeichen)


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
30
(max. 3 Zeichen)
Balance-Sekunden
10
(max. 3 Zeichen)
Client-Binding-Protokolle
Setzen
Zurücksetzen


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
172.25.0.0 255.255.255.0 0 An, sticky für RIP OPNS 0 Aus 0
192.168.7.0 255.255.255.0 0 An, sticky für RIP OPNS 0 Aus 0
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
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
10.0.0.0 255.0.0.0 0 Aus 0.0.0.0 0 Aus 0 template: block private network: 10.x.y.z
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
Vorherige Seite
Hinzufügen


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
172.25.0.0
Netzmaske
255.255.255.0
Routing-Tag
0
Schaltzustand
Route ist aktiviert und wird immer via RIP propagiert (sticky)
Route ist aktiviert und wird via RIP propagiert, wenn das Zielnetzwerk erreichbar ist (konditional)
Diese Route ist aus
Router
OPNS
RIP-Distanz
0
(mögliche Werte: 0 bis 16)
IP-Maskierung
IP-Maskierung abgeschaltet
Nur Internet und DMZ maskieren (Standard)
Nur Internet maskieren
Administrative Distanz
0
Kommentar
(max. 64 Zeichen)
Setzen
Zurücksetzen
Vorherige Seite