

Anleitung zur Herstellung einer IPSec/Ikev2 Site-to-Site Verbindung mit der OPNSense Option zu einer Securepoint UTM in der Kanzlei

RA Thomas Schmidt – RA-MICRO Vertriebs GmbH – Stand 07.01.2021 – Alle Angaben ohne Gewähr

1. Teil: Rechenzentrum:

The screenshot shows the OPNSense web interface for configuring IPsec tunnels. The left sidebar has 'VPN' selected, with 'IPsec' and 'Tunneleinstellungen' highlighted. The main content area is titled 'VPN: IPsec: Tunneleinstellungen'. It features a table with columns: Typ, Ferner Gateway, Modus, Phase 1 Vorschlag, Authentifizierung, and Beschreibung. The table contains one entry: 'Lokales Subnetz' (Typ), 'Fernes Subnetz' (Ferner Gateway), 'Phase 2 Proposal' (Modus), and 'Phase 2 Proposal' (Phase 1 Vorschlag). Below the table, there is a checkbox for 'IPsec aktivieren' and a 'Speichern' button. A red arrow points to a '+' icon in the top right corner of the table, indicating the option to add a new tunnel entry.

The screenshot shows the configuration page for a specific IPsec tunnel. The left sidebar is the same as in the previous screenshot. The main content area is titled 'VPN: IPsec: Tunneleinstellungen' and is divided into sections: 'Allgemeine Information' and 'Phase 1 Vorschlag (Authentifizierung)'. The 'Allgemeine Information' section includes fields for: 'Deaktiviert' (checkbox), 'Anschlussart' (dropdown: 'Nur antworten'), 'Schlüsselaustauschversion' (dropdown: 'V2'), 'Internet Protokoll' (dropdown: 'IPv4'), 'Schnittstelle' (dropdown: 'WAN'), 'Ferner Gateway' (text: '0.0.0.0'), 'Dynamic gateway' (checkbox: 'Allow any remote gateway to connect'), and 'Beschreibung' (text: 'Kanzlei_ohne_feste_oeffentliche_IP-Adresse'). The 'Phase 1 Vorschlag (Authentifizierung)' section includes: 'Authentifizierungsmethode' (dropdown: 'Mutual PSK'), 'Meine Kennung' (dropdown: 'Meine IP-Adresse'), 'Peer-Identifizierer' (dropdown: 'KeyID Tag'), and 'Pre-Shared Schlüssel' (text: 'das_ist_das_sichere_Kennwort_fuer_die_VPN-Bruecke'). A red box highlights the 'Deaktiviert' checkbox and the 'Deaktiviere diesen Phase 1 Eintrag' checkbox, which is currently unchecked.

Tunneleinstellungen | IPsec | VPN | x +

Nicht sicher | 172.25.0.1/vpn_ipsec_phase1.php

root@OPNsense.localdomain

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

Pre-Shared Schlüssel:

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:

10 Sekunden

5 Wiederholungen

Restart the tunnel

DPD action

Inactivity timeout

Margintime

Rekeyfuzz

Speichern

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

Tunneleinstellungen | IPsec | VPN | x +

Nicht sicher | 172.25.0.1/vpn_ipsec.php

root@OPNsense.localdomain

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

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

IPsec aktivieren

Speichern

Tunneleinstellungen | IPsec | VPN | x +

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

root@OPNsense.localdomain

VPN: IPsec: Tunneleinstellungen

[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

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

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: 28800 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

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
<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

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	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.

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 +

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									
<input type="checkbox"/>	IPv4 TCP	*	*	WAN Adresse	443 (HTTPS)	*	*		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	IPv4 UDP	*	*	WAN Adresse	500 (ISAKMP)	*	*		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	IPv4 UDP	*	*	WAN Adresse	4500 (IPsec NAT-T)	*	*		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	IPv4 ESP	*	*	WAN Adresse	*	*	*		<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

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 Securepoint-Router z.B. BlackDwarf G3

← → ↻ ▲ Nicht sicher | <https://192.168.175.1:11115>

SECUREPOINT IT-Security made in Germany

Konfiguration Netzwerk Firewall Anwendungen **VPN** Authentifizierung Extras Alerting Center Log

INFO

Gerätetyp: UTM v11.8 - 11.8.10 (Final)
Lizenz: RAMICRO Software AG
RA-MICRO Software AG
5 Benutzer

Läuft ab:
Uptime: 00 Tage, 00:20
Viruspattern: ClamAV: Invalid date
Cyren: 03.11.2020 14:06 Uhr

Konfigurationen: Start: configuration-wizard-03.11.20-01:40:27
Aktuell: configuration-wizard-03.11.20-01:40:27

APPLIANCE

CPU: Intel(R) Atom(TM) CPU E3815 @ 1.466GHz
Speicher: 4.02 GByte

LOAD

ANWENDUNGSSTATUS

Dienst
admin-ui
admin-ui
ipsec

SECUREPOINT IT-Security made in Germany

Konfiguration Netzwerk Firewall Anwendungen **VPN** Authentifizierung Extras Ale

INFO

Gerätetyp: UTM v11.8 - 11.8.10 (Final)
Lizenz: RAMICRO Software AG
RA-MICRO Software AG
5 Benutzer

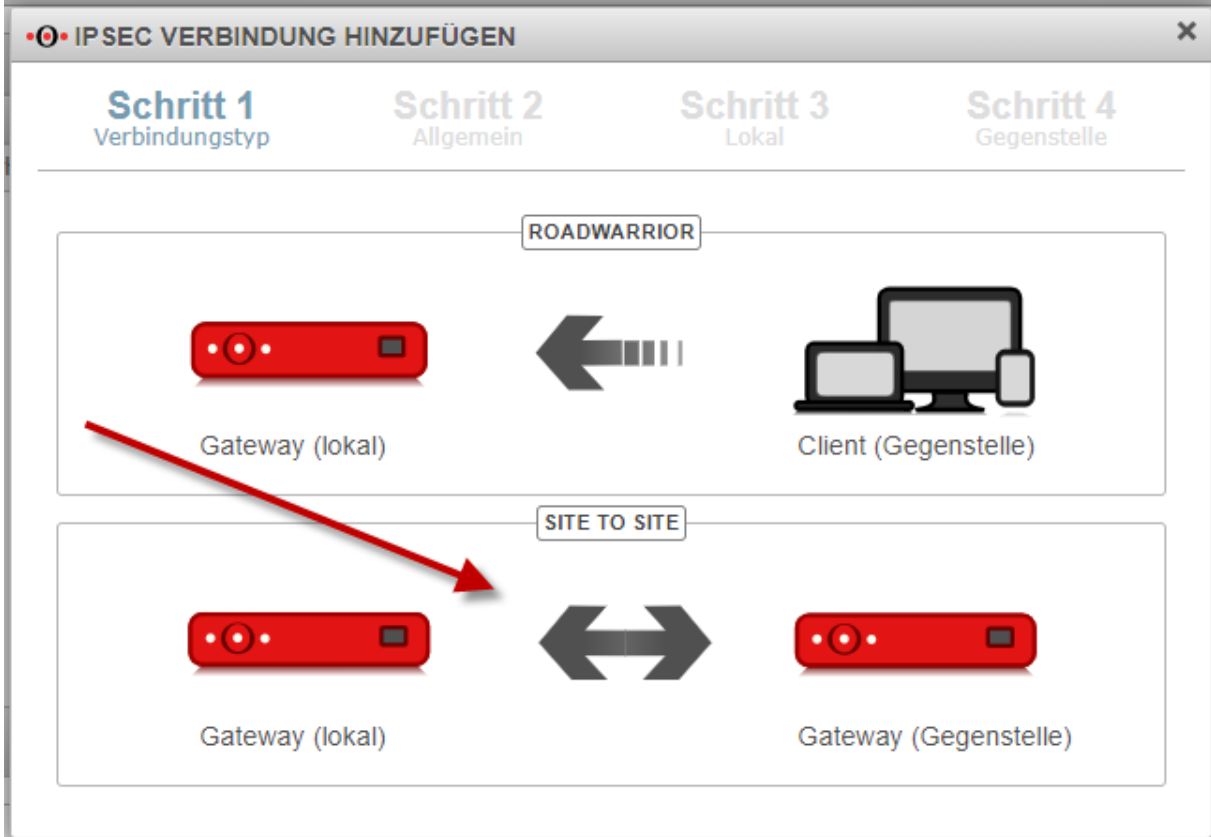
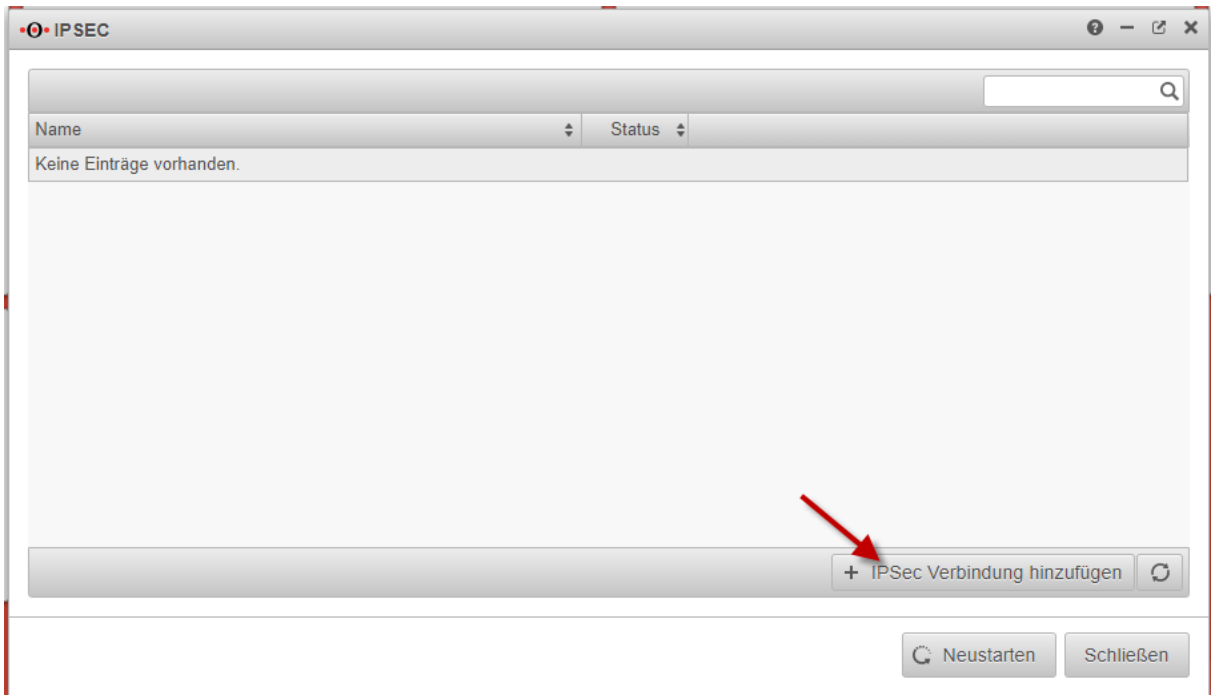
Läuft ab: **in einem Monat (03.12.2020)**
Uptime: 00 Tage, 00:21
Viruspattern: ClamAV: Invalid date
Cyren: 03.11.2020 14:06 Uhr

Konfigurationen: Start: configuration-wizard-03.11.20-01:40:27
Aktuell: configuration-wizard-03.11.20-01:40:27

Globale VPN Einstellungen

- IPSec**
- SSL-VPN
- L2TP
- Clientless VPN

CPU: Intel(F)
Speicher: 4.02 C



• IPSEC VERBINDUNG HINZUFÜGEN

Schritt 1 Verbindungstyp Schritt 2 Allgemein Schritt 3 Lokal Schritt 4 Gegenstelle

Name:

Authentifizierungsmethode: PSK X.509 Zertifikat RSA

Pre-Shared Key: Sehr stark

IKE Version: IKE v1 IKE v2

• IPSEC VERBINDUNG HINZUFÜGEN

Schritt 1 Verbindungstyp Schritt 2 Allgemein Schritt 3 Lokal Schritt 4 Gegenstelle

Local Gateway ID:

Netzwerke freigeben:

• IPSEC VERBINDUNG HINZUFÜGEN

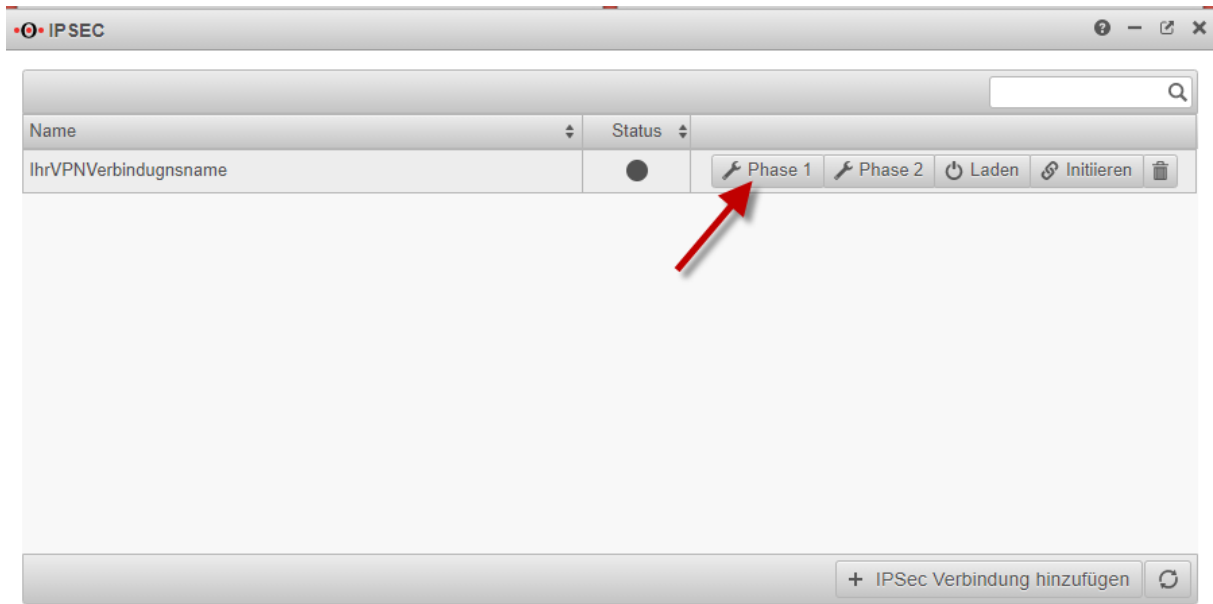
Schritt 1 Verbindungstyp Schritt 2 Allgemein Schritt 3 Lokal Schritt 4 Gegenstelle

Remote Gateway:

Remote Gateway ID:

Netzwerke freigeben:

die mitgeteilte öffentliche OPNSense IP eintragen



Neustarten Schließen



Falls die Securepoint hinter einem Router steht/nicht selbst eine externe öffentliche IP-Adresse hat:

Hier die Key-ID eintragen, die Sie in der OpnSense als Peer-ID eingetragen haben

Name

opnsense

ALLGEMEIN

IKE

Name:	opnsense
IKE Version:	ikev2
Local Gateway:	eth0
Local Gateway ID:	der_Name_kann_frei_gewaehlt_werd...
Remote Host / Gateway:	55.55.55.55
Remote Host / Gateway ID:	55.55.55.55
Authentifizierung:	Pre-Shared Key
Pre-Shared Key:	das_ist_das_sichere_Ke <input type="password"/> Sehr stark
Startverhalten:	Outgoing
Dead Peer Detection:	<input checked="" type="checkbox"/> Ein
Compression:	<input type="checkbox"/> Aus

Speichern

Schließen

PHASE 1 BEARBEITEN

ALLGEMEIN | IKE

Verschlüsselung:


Authentifizierung:

Diffie-Hellman Group:






Strict: Ein


IKE Lifetime:

Rekeying:



IPSEC

Name	Status	
IhrVPNVerbindungsname	●	 Phase 1  Phase 2  Laden  Initiieren 



PHASE 2 BEARBEITEN

ALLGEMEIN SUBNETZE

Name: IhrVPNVerbindungsname

Verschlüsselung: aes256

Authentifizierung: sha2_512

DH-Gruppe (PFS): modp2048

Schlüssel-Lebensdauer: 8 Stunden

Neustart nach Abbruch: Ja

Speichern Schließen

IPSEC

Name	Status	
IhrVPNVerbindungsname	●	Phase 1 Phase 2 Laden Initiieren

+ IPsec Verbindung hinzufügen

Neustarten Schließen

SECUREPOINT IT-Security, Made in Germany

Konfiguration Netzwerk Firewall **Anwendungen** VPN Authentifizierung Extras Alerting Center Log

INFO

Gerätetyp: UTM v11.8 - 11.8.10 (Final)
 Lizenz: RAMICRO Software AG
 RA-MICRO Software AG
 5 Benutzer

Läuft ab:
 Uptime: 00 Tage, 00:20
 Viruspattern: ClamAV: Invalid date
 Cyren: 03.11.2020 14:06 Uhr
 Konfigurationen: Start: configuration-wizard-03.11.20-01:40:27
 Aktuell: configuration-wizard-03.11.20-01:40:27

APPLIANCE

VGA LAN 1 LAN 2 LAN 3 USB DC Input

CPU: Intel(R) Atom(TM) CPU E3815 @ @ 1.466GHz
 Speicher: 4.02 GByte

ANWENDUNGSSTATUS

Name Status

NETZWERKOBJEKT BEARBEITEN

Name:

Zone:

Adresse:

Schnittstelle:

PORTFILTER

REGEL HINZUFÜGEN

AKTIV: Ein

AKTION:

LOGGING:

GRUPPE:

QUELLE:

ZIEL:

DIENST:

[-] NAT

TYP:

NETZWERKOBJEKT:

DIENST:

[+] EXTRAS

[+] BESCHREIBUNG

REGEL BEARBEITEN

AKTIV Ein

AKTION ACCEPT

LOGGING NONE - Nicht

GRUPPE default

QUELLE

- external-interface
- internal-interface
- internal-network
- internal-networks
- internet
- vCloudVPN
- VPN

ZIEL

- external-interface
- internal-interface
- internal-network
- internal-networks
- internet
- vCloudVPN
- VPN

DIENST

- any
- archie
- bgp
- blackberry
- cvs
- default-internet
- dhcp

[-] NAT

TYP HIDE NAT

NETZWERKOBJEKT internal-interface

DIENST

[+] EXTRAS

[+] BESCHREIBUNG

Speichern Schließen