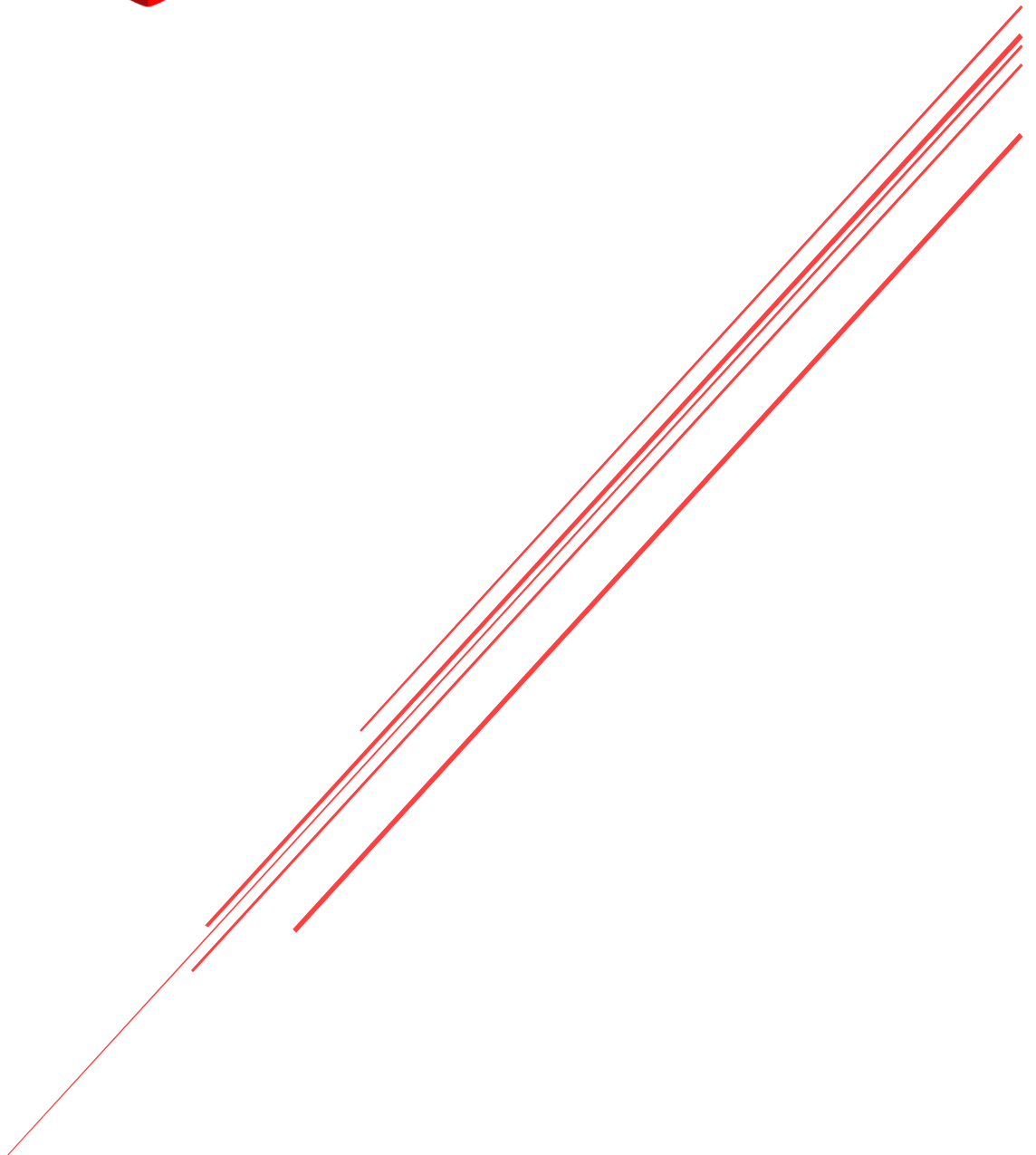


# OPNSENSE

SSL VPN Tunnel zwischen OPNsense und Sophos UTM



FreeSOC  
Peter Leibling

## Inhaltsverzeichnis

Vorwort.....	2
Voraussetzungen .....	2
Vorbereitungen.....	2
Hinweis .....	3
Einrichten des OpenVPN SSL VPN Tunnels .....	3
Einrichtung Sophos UTM (VPN Server) .....	3
Extrahieren der benötigten Zugangsdaten und Zertifikate.....	5
Anmeldepasswort extrahieren .....	5
Kennwort extrahieren.....	5
Root Zertifikat extrahieren .....	5
Verbindungszertifikat extrahieren .....	5
Privaten Schlüssel extrahieren .....	5
Einrichtung OPNsense (VPNClient).....	6
Erstellen der Firewallregeln .....	6
Einrichten CA Zertifikat.....	6
Einrichten Zertifikat mitsamt privaten Schlüssel .....	6
Erstellen des Tunnels .....	7

## Vorwort

In dieser Anleitung wird beschrieben, wie ein VPN Tunnel zwischen einer OPNsense (Community License) und einer Sophos UTM 9.7 (Network Protection oder Home License erforderlich) per OpenVPN mit SSL eingerichtet wird.

Einen IPSec Tunnel verwende ich nicht, da es einige Voraussetzungen gibt, die dagegen sprechen – zum einen hat die OPNsense Probleme mit Double NAT (Router vor der Firewall), dann kann sie nicht mit dynamischen Adressen umgehen (z.B. DynDNS usw.) und was noch problematischer ist, das IPSec langsamer ist als SSL Tunnel – da ich über diese Verbindung Backups in ein Rechenzentrum mache, wäre dies nicht sinnvoll.

Diese Anleitung wurde basierend auf dem Youtube Video von SysopsTV erstellt: <https://www.youtube.com/watch?v=RVWiXe4LhUo>

## Voraussetzungen

Die Sophos UTM Serverseite muss erreichbar sein (IP, DNS oder DynDNS) auf einem Port, welcher nicht schon anderweitig belegt ist. Die OPNsense muss eine Verbindung nach außen haben – die sie als Client fungiert, muss diese nicht von extern erreichbar sein (kein Portforwarding benötigt) und könnte sogar hinter einem Proxy positioniert sein. Für beide Systeme werden administrative Zugangsdaten benötigt.

## Vorbereitungen

Solltet ihr mehrere Sophos UTM Tunnel benötigen, so müssen wir auf den Sophos UTM's den SSL VPN Pool die Netzwerkadresse im weiteren Verlauf verlegen, da alle Sophos UTM den selben Adressbereich verwenden (10.242.2.0/24).

Ich habe mir angewöhnt, das 3. Oktet des Sophos UTM Adressbereich zu verwenden, da es oft eindeutig ist – sollte die Sophos UTM Netzwerkadresse 192.168.123.0/24 sein, so ändere den SSL VPN Pool auf 10.242.123.0/24 – wir werden diese im späteren Verlauf als **Neuer SSL Pool Adressbereich** bezeichnen.

Weiterhin benötigen wir eine IP aus dem Bereich, z.B. die erste – somit 10.242.123.1. Diese werden im späteren Verlauf **Neue SSL Pool Adresse** bezeichnen.

## Hinweis

Achtet bitte darauf, welchen Editor ihr verwendet – die Konfigurationsdatei, welche auf der Sophos UTM geniert wird, enthält Steuerzeichen welche die Editoren durcheinander bringen. Am besten ihr verwendet Windows und Notepad.

Wundert euch nicht, das wir erst die Neue SSL Pool Adresse einrichten und dann erst den Neuer SSL Pool Adressbereich – solltet ihr andersherum vorgehen, so wird die Einstellung des Neuer SSL Pool Adressbereich nicht gespeichert werden können.

Beachtet bitte, das sobald ihr die VPN Pool (SSL) Netzwerkadresse geändert habt, kurz alle VPN Verbindungen unterbrochen und neu gestartet werden, danach bekommen die Geräte Adressen aus den neu definierten Adressbereich. Gegebenenfalls müsst ihr auch DNS und Firewallregeln (bei bestehenden anderen Tunneln eventuell sogar die Gegenseiten) sowie Static IP Zuordnungen anpassen.

Am besten erstellt ihr vorher ein Backup eurer Firewall unter Management > Backup/Restore > Create Backup.

## Einrichten des OpenVPN SSL VPN Tunnels

### Einrichtung Sophos UTM (VPN Server)

Meldet euch auf der Sophos UTM an und geht zu Site-to-Site VPN > SSL.

Wechselt zum Registerreiter Advanced.

Kontrolliert bitte, ob die Einstellungen wie folgt sind:



The image shows a screenshot of the Sophos UTM configuration interface for SSL VPN settings. It features five rows of configuration options, each with a label, a value, and a dropdown arrow:

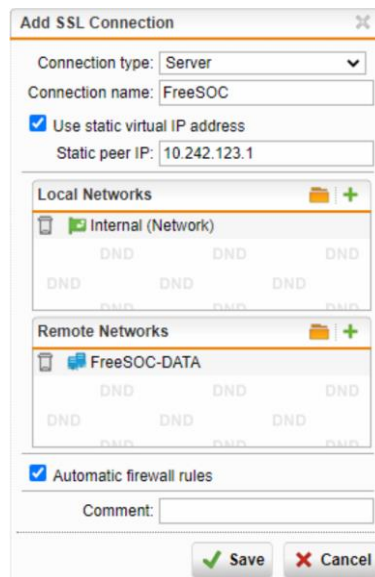
- Encryption algorithm: AES-128-CBC
- Authentication algorithm: SHA1
- Key size: 2048 bit
- Server certificate: Local X509 Cert
- Key lifetime: 28800 seconds

Stellt das protokoll auf UDP um und Deaktiviert bitte den Punkt Compress SSL VPN traffic - danach speichert mit Apply.

In dem Registerreiter Settings, seht ihr die Adresse und den Port welchen wir später benötigen.

Wechselt nun in den Registerreiter Connections und drückt den Button **New SSL Connection**.

Fügt eine neue Verbindung wie folgt hinzu:



Verwendet bitte bei Use static virtual IP address die **Neue SSL Pool Adresse** aus den Vorbereitungen.

Wenn ihr die Einstellungen mit den Button Save gesichert habt, dann könnt ihr den Download Button drücke in der Übersicht und die Konfigurationsdatei sichern. Diese benötigen wir gleich für den nächsten Abschnitt.

Als letztes müssen wir noch den SSL VPN Pool Addressbereich ändern, geht dazu nach Definitions &Users > Network Definitions.

Sucht nun bitte nach VPN Pool (SSL) und bearbeitet diesen wie folgt:



Speichert nun die Änderung mit Save (beachtet auch hier bitte oben den Hinweis-Bereich oben).

## Extrahieren der benötigten Zugangsdaten und Zertifikate

Öffnet nun die heruntergeladene Datei (beachtet bitte den Hinweis-Bereich oben).

In dieser Datei sind drei lange Zeichenkettenblöcke (uns interessieren nur die mit Zahlen, Buchstaben und Zeichen – die Zahlenkolonnen interessieren uns nicht).

### Anmeldepasswort extrahieren

Im dritten Zeichenblock ganz am Anfang der Zeile wo --- BEGINN PRIVATE KEY ---- steht, steht eine Zeichenkette wie REF\_AaaUse1 – diese ist der **Anmeldename**, dieser wird gleich benötigt. Am besten kopiert ihr ihn euch in eine neue Datei (zur späteren Verwendung und Dokumentation).

### Kennwort extrahieren

Nun benötigen wir das Kennwort – das kommt nach nach dem Verschlüsselungsalgorithmus (z.B. AES-128-CBC ..... compression), womöglich habt ihr dort noch ein Sonderzeichen (z.B. >), dieses dann nicht mit kopieren – der Bereich endet wieder mit einem Sonderzeichen, der benötigte Bereich beginnt mit REF\_ oder DREF\_ - notiert auch bitte diesen Bereich als **Passwort**. Achtet auch bitte darauf, das tatsächlich nur das Passwort kopiert wird – bei einigen Editoren wurde auch noch mehr angehängt.

### Root Zertifikat extrahieren

Nun erstellen wir das benötigte RootCA der Sophos, sucht dazu nach dem zweiten Zeichenkettenblock (direkt überhalb der Bezeichnung ca\_cert)– wir benötigen den Bereich zwischen -----BEGIN CERTIFICATE----- und -----END CERTIFICATE-----. Kopiert diesen inklusive der vorgenannten Zeichenketten in eine neue Datei und nennt diese z.B. Tunnelname\_CA.cert

Nun benötigen wir das Zertifikat für die Verbindung mitsamt dem privaten Schlüssel als einzelne Zertifikate.

### Verbindungszertifikat extrahieren

Kopiert für das Zertifikat den Inhalt vom ersten Zeichenblock (inklusive der nun genannten Zeichen) beginnend mit -----BEGIN CERTIFICATE----- bis einschließlich -----END CERTIFICATE----- in eine neue Datei und speichert diese als Tunnelname\_Cert.crt

### Privaten Schlüssel extrahieren

Zuletzt benötigen wir nun noch den privaten Schlüssel, geht dazu zum dritten Zeichenkettenblock und kopiert diesen von (einschließlich) -----BEGIN PRIVATE KEY----- bis hin zu (einschließlich) -----END PRIVATE KEY----- in eine neue Datei und speichert diese unter Tunnelname\_key.crt .

Nun haben wir alle benötigten Informationen und können nun mit diesen den Tunnel auf der OPNsense einrichten.

## Einrichtung OPNsense (VPNClient)

### Erstellen der Firewallregeln

Geht zu Firewall > Rules > WAN und klickt oben rechts auf das Plus.

Erstellt dazu eine Regeln wie folgt für den OpenVPN ausgehenden Verkehr:

- Action: Pass
- Interface: WAN
- Direction: out
- TCP/IP Version IPv4
- Protocol: UDP
- Source: any
- Destination: any
- Destination Port Range: from OpenVPN / to OpenVPN
- Description: Allow OpenVPN traffic
- Speichert mit Apply Changes.

Dann noch eine weitere Regeln für den ausgehenden Verkehr in den Tunnel unter Firewall > Rules > OpenVPN – wieder durch klicken auf das Plus oben rechts:

- Action: Pass
- Interface: OpenVPN
- Direction: out
- TCP/IP Version IPv4
- Protocol: any
- Source: Single host or Network und dann das entsprechende **Neue SSL Pool Adressbereich** z.B. 10.242.123.0/24
- Destination: any
- Destination any
- Description: Allow Tunnelname traffic

### Einrichten CA Zertifikat

Meldet euch auf der OPNsense an und geht zu System > Trust > Authorities.

Klickt oben rechts auf das Plus.

Gebt nun bei Descriptive Name einen Namen ein wie z.B. Tunnelname CA, lasst bei method Import an existing Certificate Authority stehen und gebt bei Certificate data den Inhalt der Datei Tunnelname\_CA.crt

### Einrichten Zertifikat mitsamt privaten Schlüssel

Geht nun zu System > Trust > Certificates und geht ebenfalls wieder auf das Plus oben rechts.

Wählt nun bei Method Import an existing Certificate, vergebte eine Beschreibung (Descriptive Name) wie z.B. Tunnelname Certificate und kopiert den Inhalt eurer Tunnelname\_Cert.crt Datei in das Feld Certificate Data und in das Feld Privatekey data den Inhalt der Tunnelname\_key.crt Datei. Danach speichert dies mit Save.

## Erstellen des Tunnels

Wenn ihr das nun habt, geht bitte zu VPN > OpenVPN > Clients und klickt wieder oben rechts das Plus an.

Stellt nun folgendes ein:

- Vergebt einen Name (Description) wie z.B. Tunnelname.
- Lasst bei Server mode Peer to Peer /SSL/TLS) stehen.
- Bei Protocol wählt bitte TCP.
- Bei Device Model bitte tun.
- Bei Interface any.
- Bei Host und Port die entsprechenden Daten (in der Sophos UTM zu finden unter Site-to-Site VPN > SSL > Settings).
- Sofern ihr keinen Proxy benötigt, geht es direkt weiter bei User name/pass – gebt dort die entsprechenden extrahierten Daten ein.
- Tragt bei Renegotiation time den Wert aus der Sophos UTM unter Site-to-Site > SSL > Advanced Key Lifetime ein (bei mir ist dies der Standardwert 28800).
- TLS Authentication bitte auf Disabled.
- Lasst bei Automatic generate a shared TLS authentication key den Hacken aktiv.
- Wählt bei Peer Certificate Authority das Zertifikat Tunnelname CA.
- Wählt bei Client Certificate bitte das Tunnelname Cert.
- Wählt bei Encryption Algorithm (depricated) das entsprechende aus – die Einstellungen findet ihr bei der Sophos UTM unter Site-to-Site > SSL > Encryption algorithm – bei mir ist dies AES-128-CBC.
- Unter Auth Digits Algorithm den entsprechenden Wert aus der Sophos UTM unter Site-to-Site > SSL > Authentication algorithm – bei mir SHA1 bzw. SHA1 (160) auf der OPNsense.
- Tragt bei IPv4 Tunnel Network den **Neuen SSL Pool Adressbereich** ein z.B. 10.242.123.0/24
- Tragt bei IPv4 Remote Network das lokale Netz der UTM ein (z.B. 192.168.33.0/24
- Macht einen Hacken bei Don't pull routes.
- Speichert das ganze nun und starten den Tunnel, kontrolliert bei der Sophos UTM unter Site-to-Site VPN > SSL im Live Log ob die Verbindung zustande kommt.