Konfiguration pfSense FireWall VPN zu Watchguard

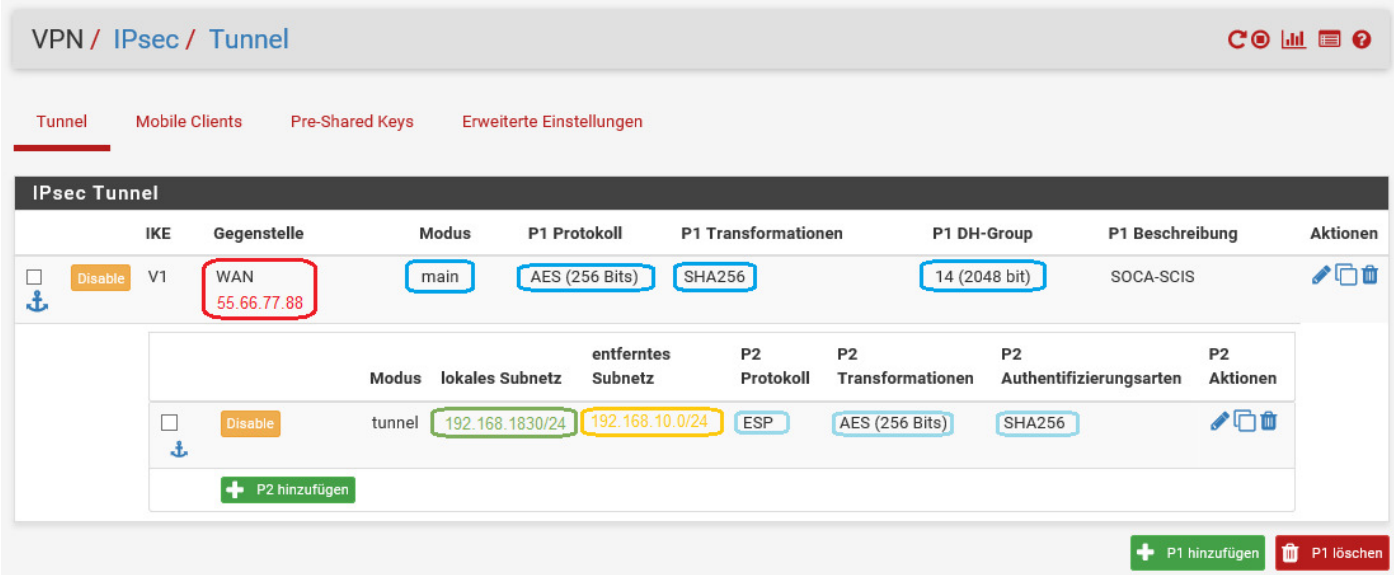
Ersteller: System-Clinch IT Servcies – www.MiaTel.ch
Author: Manuel Magnin, MMagnin@Clinch.ch

Datum: 09.04.2019

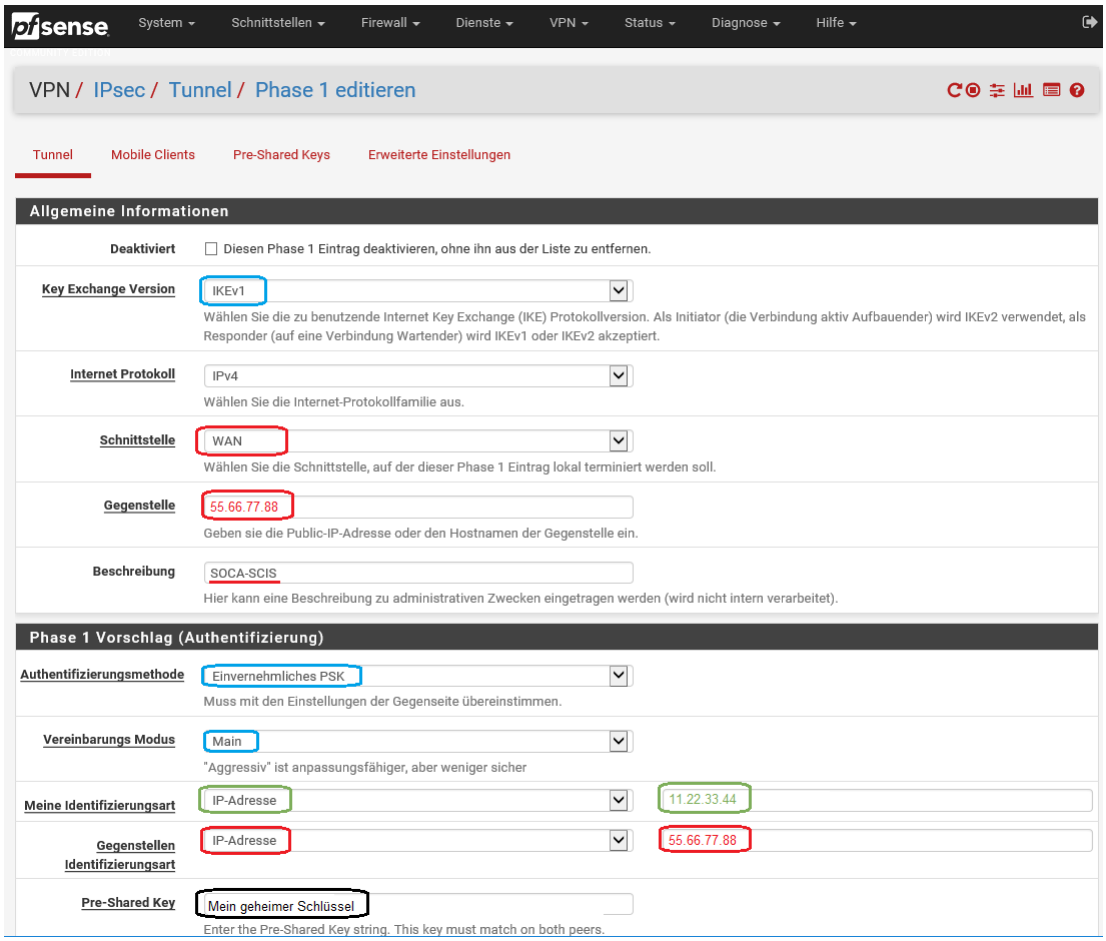
Konfigurationsbeispiel VPN Verbindung pfSense (OS:2.4.4) zu Watchguard (OS:12.2).

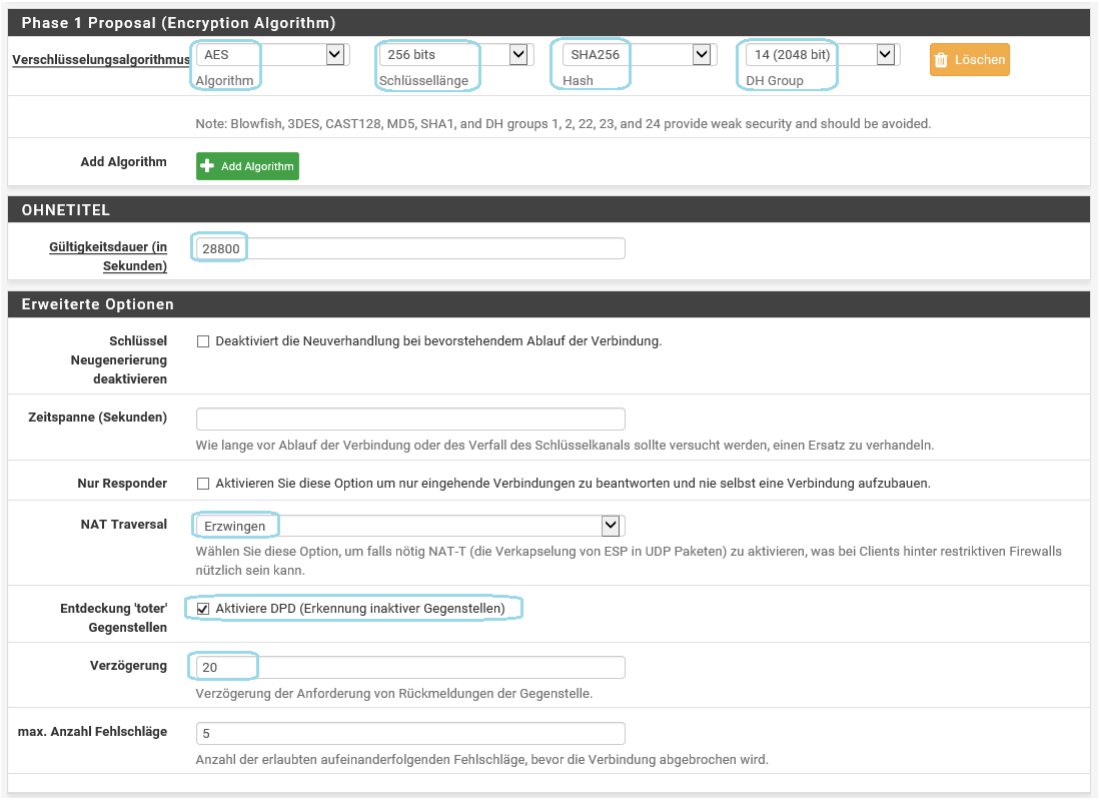
pfSense WAN: 11.22.33.44 LAN: 192.168.183.1/24
Watchguard WAN: 55.66.77.88 LAN: 192.168.10.1/24
Gemeinsam: WAN: Phase1 LAN: Phase2
Main, IKEV1, NAT-Traversal, DPD, AES256, SHA256 DH14,IP-WAN ESP, AES256,SHA256,DH14, IP-LAN

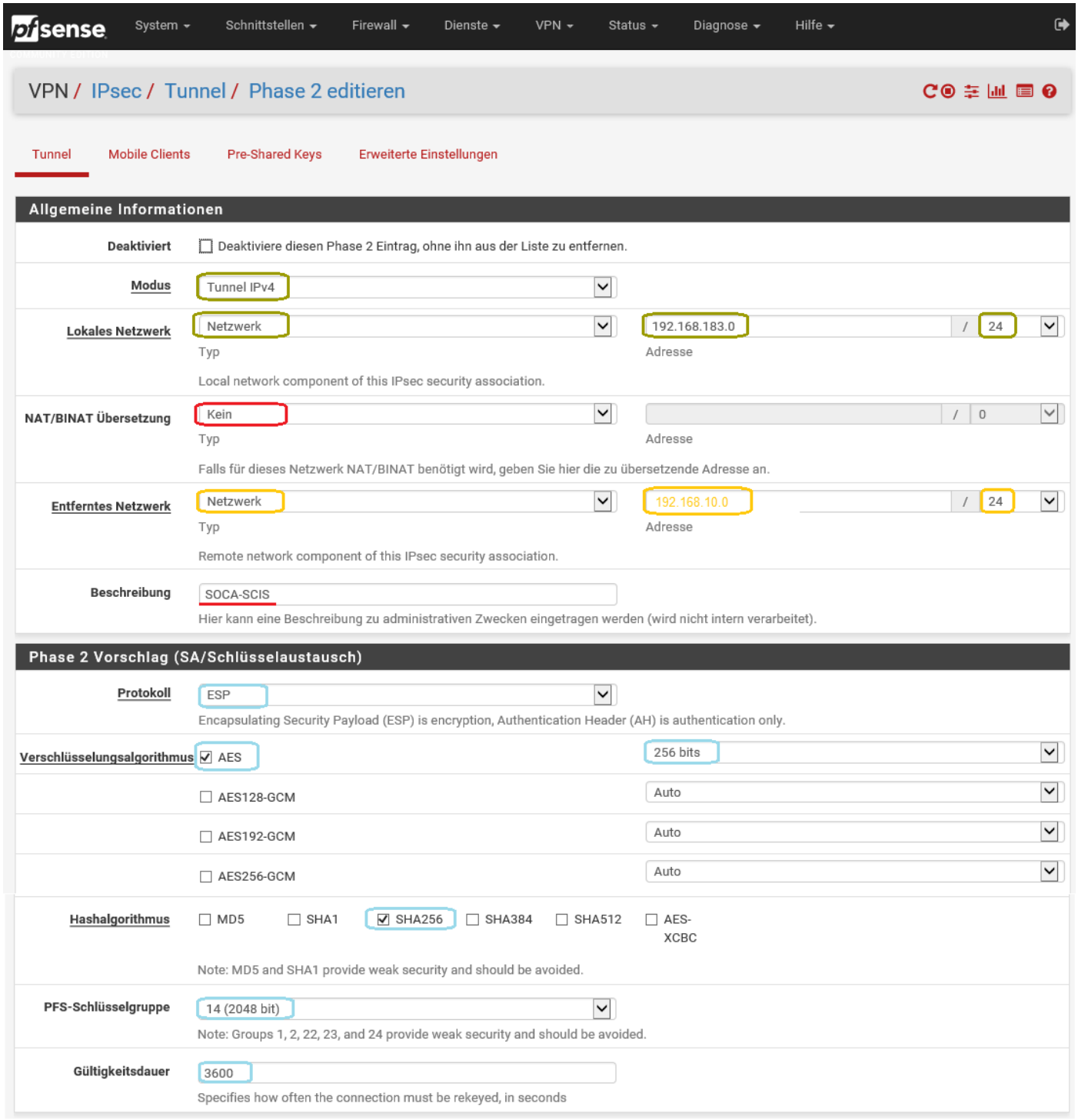
Ein Beilspiel wie es am Schluss ausschauen könnte (Bitte die Farben gem. Legende oben beachten)



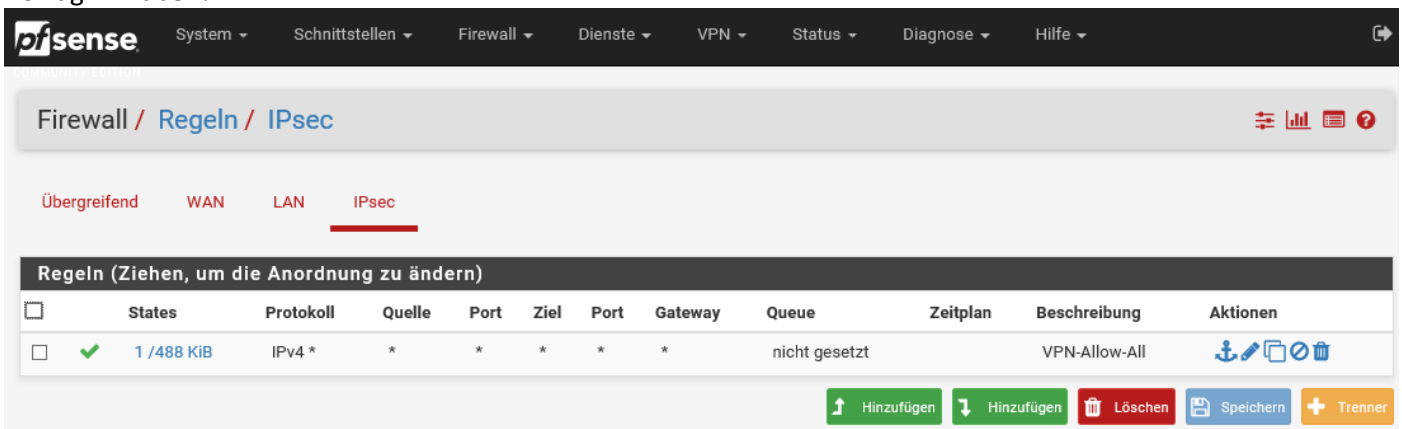
pfSense Phase1 Konfuguration:

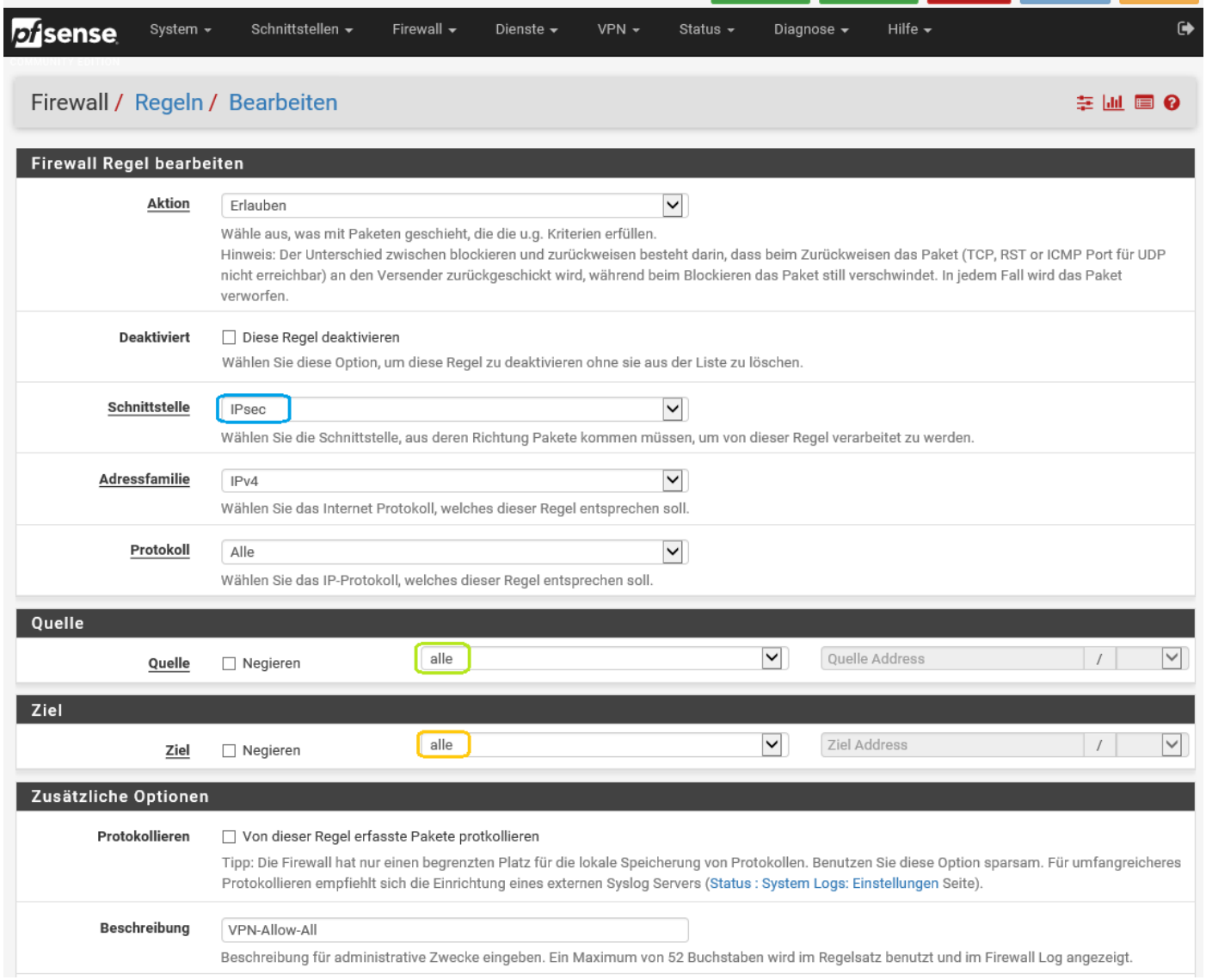





pfsense
System
Schnittstellen
Firewall
Dienste
VPN
Status
Diagnose
Hilfe
VPN / IPsec / Tunnel / Phase 2 editieren
Tunnel
Mobile Clients
Pre-Shared Keys
Erweiterte Einstellungen
Allgemeine Informationen
Deaktiviert
Deaktiviere diesen Phase 2 Eintrag, ohne ihn aus der Liste zu entfernen.
Modus
Tunnel IPv4
Lokales Netzwerk
Netzwerk
Typ
192.168.183.0
/ 24
Adresse
Local network component of this IPsec security association.
NAT/BINAT Übersetzung
Kein
Typ
/ 0
Adresse
Falls für dieses Netzwerk NAT/BINAT benötigt wird, geben Sie hier die zu übersetzende Adresse an.
Entferntes Netzwerk
Netzwerk
Typ
192.168.10.0
/ 24
Adresse
Remote network component of this IPsec security association.
Beschreibung
SOCA-SCIS
Hier kann eine Beschreibung zu administrativen Zwecken eingetragen werden (wird nicht intern verarbeitet).
Phase 2 Vorschlag (SA/Schlüsselaustausch)
Protokoll
ESP
Encapsulating Security Payload (ESP) is encryption, Authentication Header (AH) is authentication only.
Verschlüsselungsalgorithmus
AES
256 bits
AES128-GCM
Auto
AES192-GCM
Auto
AES256-GCM
Auto
Hashalgorithmus
MD5
SHA1
SHA256
SHA384
SHA512
AES-XCBC
Note: MD5 and SHA1 provide weak security and should be avoided.
PFS-Schlüsselgruppe
14 (2048 bit)
Note: Groups 1, 2, 22, 23, and 24 provide weak security and should be avoided.
Gültigkeitsdauer
3600
Specifies how often the connection must be rekeyed, in seconds

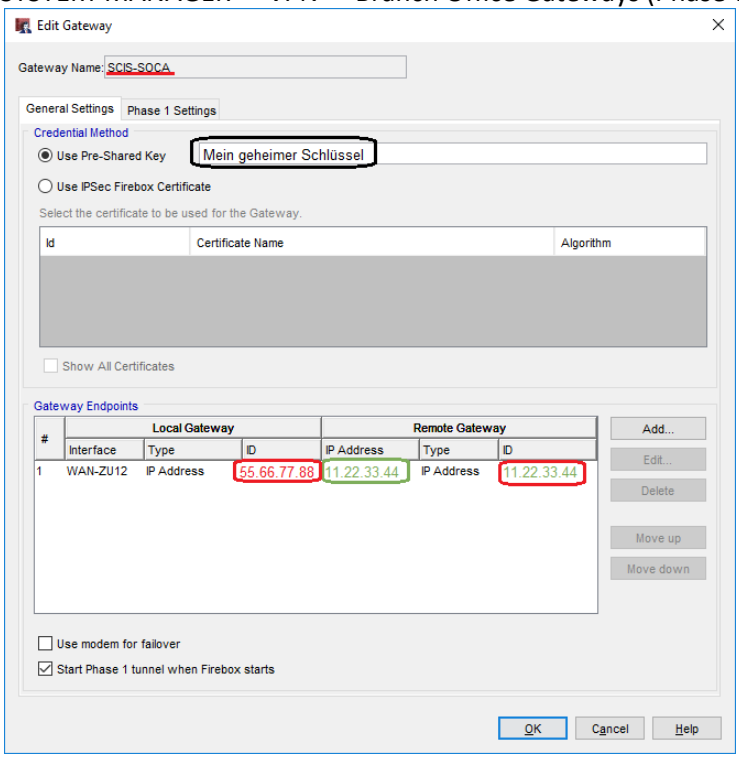
Die pfSense benötigt zum Schluss noch eine Firewall Regel damit der VPN Zugriff auf das Netzwerk funktioniert. Hier im Beispiel ein Zugriff auf das ganze Netzwerk. Der VPN Zugang sollte aus Sicherheitsgründen nur auf die benötigten IPs Zugriff haben!

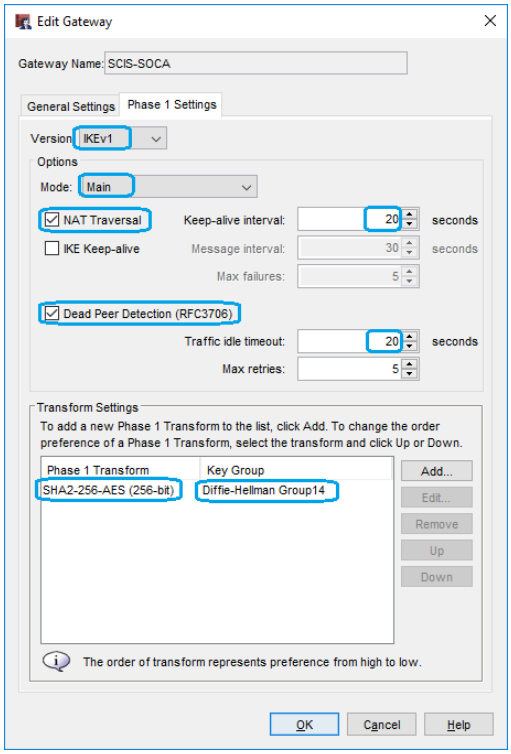




Die Konfiguration der Watchguard:

SYSTEM-MANAGER -> VPN -> Branch Office Gateways (Phase-I)





SYSTEM-MANAGER -> VPN -> Branch Office Tunnels (Phase-II)