

# Konfiguration pfSense FireWall VPN zu Watchguard

Ersteller: System-Clinch IT Servcies – [www.MiaTel.ch](http://www.MiaTel.ch)  
Author: Manuel Magnin, [MMagnin@Clinch.ch](mailto: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 Beispiel wie es am Schluss ausschauen könnte (Bitte die Farben gem. Legende oben beachten)

VPN / IPsec / Tunnel

Tunnel Mobile Clients Pre-Shared Keys Erweiterte Einstellungen

### IPsec Tunnel

IKE	Gegenstelle	Modus	P1 Protokoll	P1 Transformationen	P1 DH-Group	P1 Beschreibung	Aktionen
<input type="checkbox"/> Disable V1	WAN 55.66.77.88	main	AES (256 Bits)	SHA256	14 (2048 bit)	SOCA-SCIS	

	Modus	lokales Subnetz	entferntes Subnetz	P2 Protokoll	P2 Transformationen	P2 Authentifizierungsarten	P2 Aktionen
<input type="checkbox"/> Disable	tunnel	192.168.1830/24	192.168.10.0/24	ESP	AES (256 Bits)	SHA256	

+ P2 hinzufügen

+ P1 hinzufügen P1 löschen

# pfSense Phase1 Konfiguration:

System ▾ Schnittstellen ▾ Firewall ▾ Dienste ▾ VPN ▾ Status ▾ Diagnose ▾ Hilfe ▾

VPN / IPsec / Tunnel / Phase 1 editieren

Tunnel Mobile Clients Pre-Shared Keys Erweiterte Einstellungen

### Allgemeine Informationen

Deaktiviert  Diesen Phase 1 Eintrag deaktivieren, ohne ihn aus der Liste zu entfernen.

**Key Exchange Version** IKEv1  
Wählen Sie die zu benutzende Internet Key Exchange (IKE) Protokollversion. Als Initiator (die Verbindung aktiv Aufbauender) wird IKEv2 verwendet, als Responder (auf eine Verbindung Wartender) wird IKEv1 oder IKEv2 akzeptiert.

**Internet Protokoll** IPv4  
Wählen Sie die Internet-Protokollfamilie aus.

**Schnittstelle** WAN  
Wählen Sie die Schnittstelle, auf der dieser Phase 1 Eintrag lokal terminiert werden soll.

**Gegenstelle** 55.66.77.88  
Geben sie die Public-IP-Adresse oder den Hostnamen der Gegenstelle ein.

**Beschreibung** SOCA-SCIS  
Hier kann eine Beschreibung zu administrativen Zwecken eingetragen werden (wird nicht intern verarbeitet).

### Phase 1 Vorschlag (Authentifizierung)

**Authentifizierungsmethode** Einvernehmliches PSK  
Muss mit den Einstellungen der Gegenseite übereinstimmen.

**Vereinbarungs Modus** Main  
\*Aggressiv\* ist anpassungsfähiger, aber weniger sicher

**Meine Identifizierungsart** IP-Adresse 11.22.33.44

**Gegenstellen Identifizierungsart** IP-Adresse 55.66.77.88

**Pre-Shared Key** Mein geheimer Schlüssel  
Enter the Pre-Shared Key string. This key must match on both peers.

### Phase 1 Proposal (Encryption Algorithm)

**Verschlüsselungsalgorithmus** AES 256 bits SHA256 14 (2048 bit) Löschen  
Algorithm Schlüssellänge Hash DH Group

Note: Blowfish, 3DES, CAST128, MD5, SHA1, and DH groups 1, 2, 22, 23, and 24 provide weak security and should be avoided.

**Add Algorithm** + Add Algorithm

### OHNETITEL

**Gültigkeitsdauer (in Sekunden)** 28800

### Erweiterte Optionen

**Schlüssel Neugenerierung deaktivieren**  Deaktiviert die Neuverhandlung bei bevorstehendem Ablauf der Verbindung.

**Zeitspanne (Sekunden)**  
Wie lange vor Ablauf der Verbindung oder des Verfall des Schlüsselkanals sollte versucht werden, einen Ersatz zu verhandeln.

**Nur Responder**  Aktivieren Sie diese Option um nur eingehende Verbindungen zu beantworten und nie selbst eine Verbindung aufzubauen.

**NAT Traversal** Erzwingen  
Wählen Sie diese Option, um falls nötig NAT-T (die Verkapselung von ESP in UDP Paketen) zu aktivieren, was bei Clients hinter restriktiven Firewalls nützlich sein kann.

**Entdeckung 'toter' Gegenstellen**  Aktiviere DPD (Erkennung inaktiver Gegenstellen)

**Verzögerung** 20  
Verzögerung der Anforderung von Rückmeldungen der Gegenstelle.

**max. Anzahl Fehlschläge** 5  
Anzahl der erlaubten aufeinanderfolgenden Fehlschläge, bevor die Verbindung abgebrochen wird.

Allgemeine Informationen

**Deaktiviert**  Deaktiviere diesen Phase 2 Eintrag, ohne ihn aus der Liste zu entfernen.

**Modus** Tunnel IPv4

**Lokales Netzwerk** Netzwerk 192.168.183.0 / 24

Typ Adresse  
Local network component of this IPsec security association.

**NAT/BINAT Übersetzung** Kein

Typ Adresse  
Falls für dieses Netzwerk NAT/BINAT benötigt wird, geben Sie hier die zu übersetzende Adresse an.

**Entferntes Netzwerk** Netzwerk 192.168.10.0 / 24

Typ 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

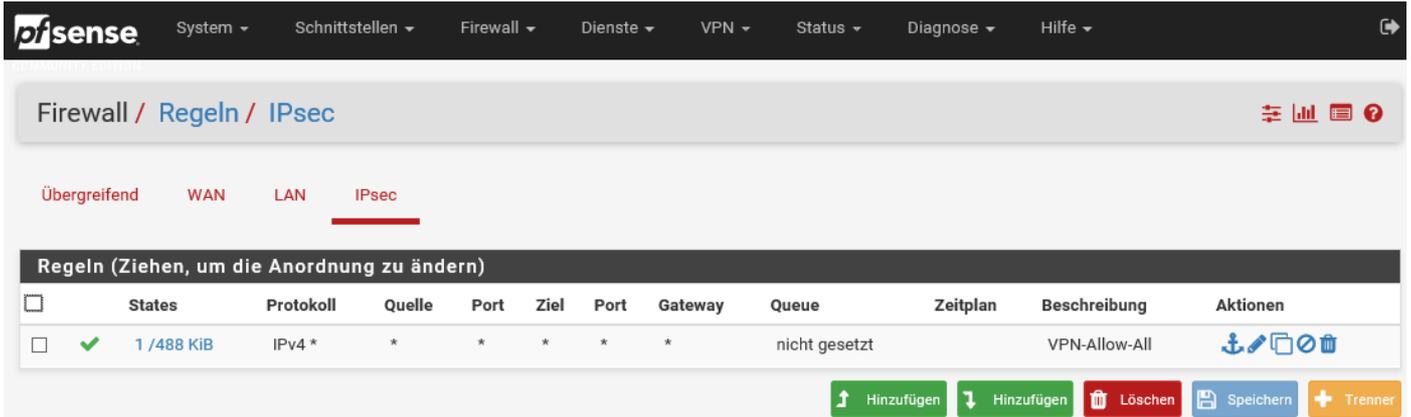
Note: MD5 and SHA1 provide weak security and should be avoided.

**PFS-Schlüsselgruppe** 14 (2048 bit)

Note: Groups 1, 2, 22, 23, and 24 provide weak security and should be avoided.

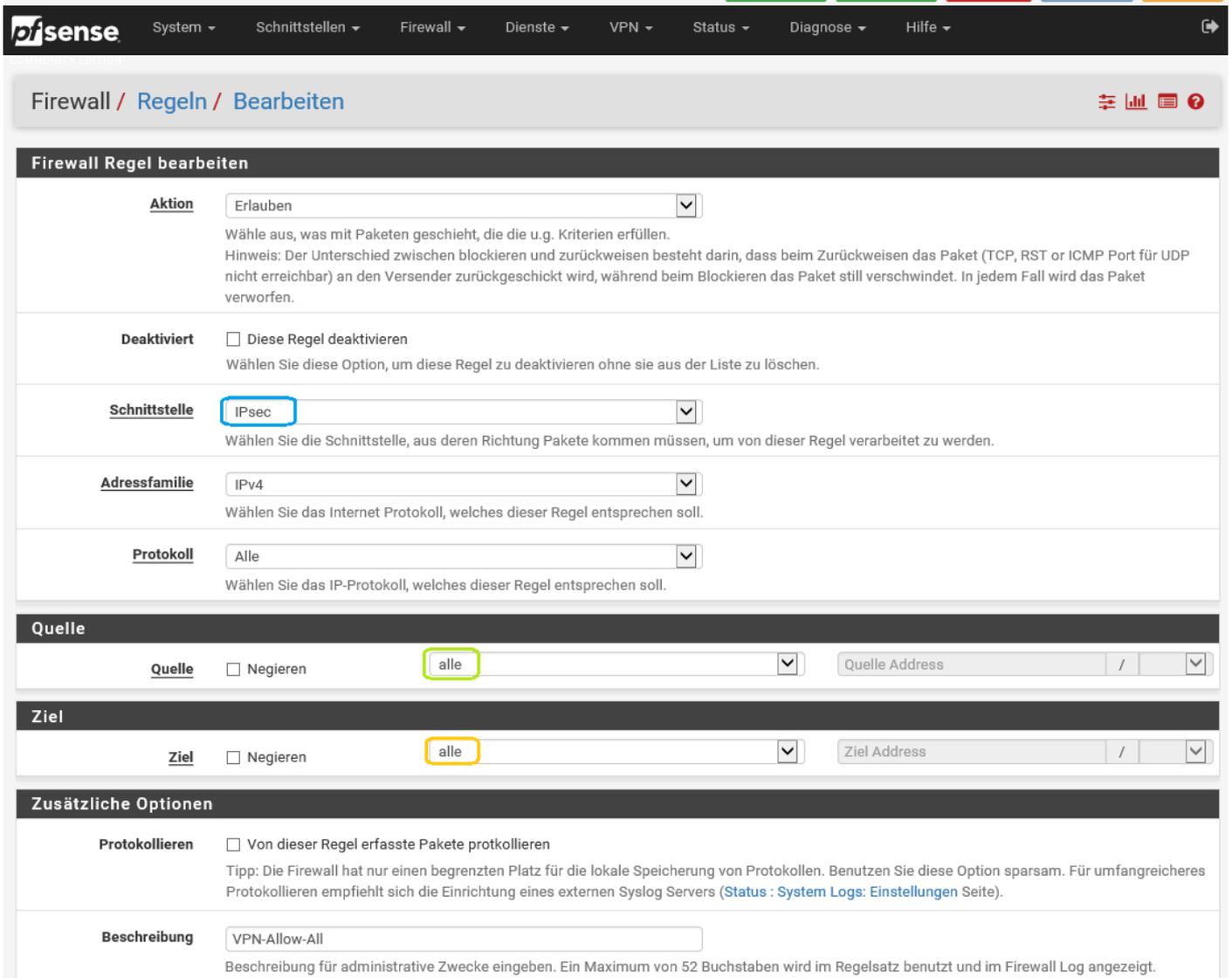
**Gültigkeitsdauer** 3600  
Specifies how often the connection must be rekeyed, in seconds

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!



The screenshot shows the pfSense web interface for Firewall Rules. The breadcrumb navigation is "Firewall / Regeln / IPsec". The "IPsec" tab is selected. Below the navigation, there is a table of rules. The table has columns: States, Protokoll, Quelle, Port, Ziel, Port, Gateway, Queue, Zeitplan, Beschreibung, and Aktionen. One rule is listed with a green checkmark, 1/488 KiB, IPv4 protocol, and description "VPN-Allow-All". Below the table are buttons for "Hinzufügen", "Hinzufügen", "Löschen", "Speichern", and "Trenner".

	States	Protokoll	Quelle	Port	Ziel	Port	Gateway	Queue	Zeitplan	Beschreibung	Aktionen
<input type="checkbox"/>	✓	1/488 KiB	IPv4 *	*	*	*	*	nicht gesetzt		VPN-Allow-All	  



The screenshot shows the "Firewall Regel bearbeiten" page in pfSense. The breadcrumb navigation is "Firewall / Regeln / Bearbeiten". The "Aktion" is set to "Erlauben". The "Schnittstelle" is set to "IPsec". The "Adressfamilie" is set to "IPv4". The "Protokoll" is set to "Alle". The "Quelle" is set to "alle" and the "Ziel" is set to "alle". The "Beschreibung" is "VPN-Allow-All".

**Aktion** Erlauben  
Wähle aus, was mit Paketen geschieht, die die u.g. Kriterien erfüllen.  
Hinweis: Der Unterschied zwischen blockieren und zurückweisen besteht darin, dass beim Zurückweisen das Paket (TCP, RST or ICMP Port für UDP nicht erreichbar) an den Versender zurückgeschickt wird, während beim Blockieren das Paket still verschwindet. In jedem Fall wird das Paket verworfen.

**Deaktiviert**  Diese Regel deaktivieren  
Wählen Sie diese Option, um diese Regel zu deaktivieren ohne sie aus der Liste zu löschen.

**Schnittstelle** IPsec  
Wählen Sie die Schnittstelle, aus deren Richtung Pakete kommen müssen, um von dieser Regel verarbeitet zu werden.

**Adressfamilie** IPv4  
Wählen Sie das Internet Protokoll, welches dieser Regel entsprechen soll.

**Protokoll** Alle  
Wählen Sie das IP-Protokoll, welches dieser Regel entsprechen soll.

**Quelle**  
**Quelle**  Negieren **alle**  /

**Ziel**  
**Ziel**  Negieren **alle**  /

**Zusätzliche Optionen**

**Protokollieren**  Von dieser Regel erfasste Pakete protokollieren  
Tipp: Die Firewall hat nur einen begrenzten Platz für die lokale Speicherung von Protokollen. Benutzen Sie diese Option sparsam. Für umfangreicheres Protokollieren empfiehlt sich die Einrichtung eines externen Syslog Servers ([Status : System Logs: Einstellungen Seite](#)).

**Beschreibung** VPN-Allow-All  
Beschreibung für administrative Zwecke eingeben. Ein Maximum von 52 Buchstaben wird im Regelsatz benutzt und im Firewall Log angezeigt.

# Die Konfiguration der Watchguard:

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

**General Settings**

Gateway Name: SCIS-SOCA

**Credential Method**

Use Pre-Shared Key

Use IPsec Firebox Certificate

Select the certificate to be used for the Gateway.

ID	Certificate Name	Algorithm
----	------------------	-----------

Show All Certificates

**Gateway Endpoints**

#	Local Gateway			Remote Gateway		
	Interface	Type	ID	IP Address	Type	ID
1	WAN-ZU12	IP Address	56.66.77.88	11.22.33.44	IP Address	11.22.33.44

Use modem for failover

Start Phase 1 tunnel when Firebox starts

OK Cancel Help

**Phase 1 Settings**

Gateway Name: SCIS-SOCA

Version: IKEv1

**Options**

Mode: Main

NAT Traversal Keep-alive interval: 20 seconds

IKE Keep-alive Message interval: 30 seconds

Max failures: 5

Dead Peer Detection (RFC3706)

Traffic idle timeout: 20 seconds

Max retries: 5

**Transform Settings**

To add a new Phase 1 Transform to the list, click Add. To change the order preference of a Phase 1 Transform, select the transform and click Up or Down.

Phase 1 Transform	Key Group
SHA2-256-AES (256-bit)	Diffie-Hellman Group14

Add... Edit... Remove Up Down

The order of transform represents preference from high to low.

OK Cancel Help

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

**General Settings**

Tunnel Name: SCIS-SOCA

Gateway: SCIS-SOCA

**Addresses** Phase 2 Settings Multicast Settings

**Addresses**

Configure tunnel routes for the tunnel.

Local	Dir	Remote
192.168.10.0/24	<==>	192.168.183.0/24

Helper Addresses

Local IP: . . .

Remote IP: . . .

Add this tunnel to the BOVPN-Allow policies

OK Cancel Help

**Phase 2 Settings**

Tunnel Name: SCIS-SOCA

Gateway: SCIS-SOCA

**Perfect Forward Secrecy**

PFS Diffie-Hellman Group14

**IPsec Proposals**

To add a new Phase 2 Proposal to the list, click Add. To change the order preference of a Phase 2 Proposal, select the proposal and click Up or Down.

ESP-AES256-SHA256 Add...

The order preference is from top to bottom.

OK Cancel Help