IN-VPN via pfSense

Ersteller: Georg Schilling <in-berlin@george.in-dsl.de>

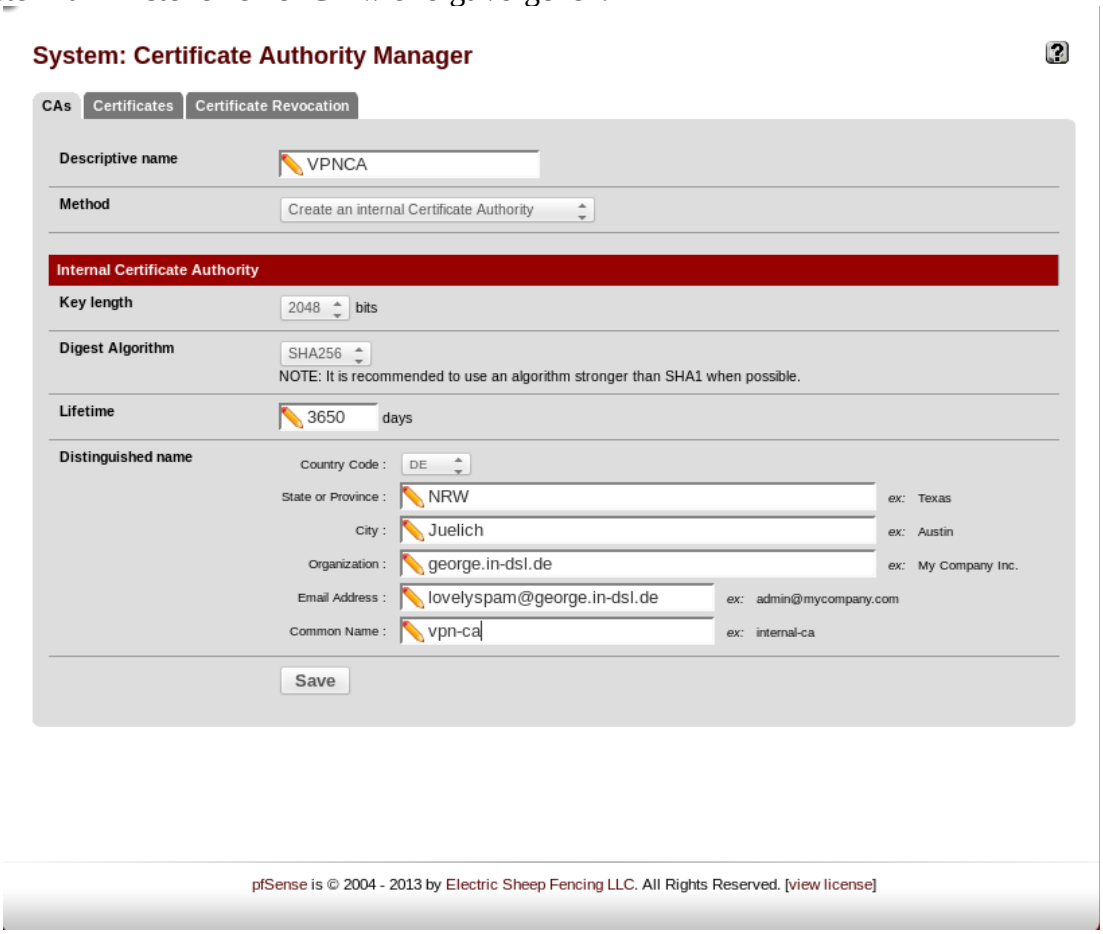
Stand: 22.07.15

1. Erstellen einer CA

System → Cert Manager → add or import cert

Aktuell kann ich nicht sagen, ob eine CA erstellt werden muss. Hier sind die HowTos gegenläufig. Mit dem vorgestellten Weg wird jedoch das startssl-Zertifikat aus dem ZIP-File auf Dateiebene importiert. Wer die Firewall eh schon asl OpenVPN-Gateway nutzt, der hat schon eine CA erstellt.

Ansonsten zum Erstellen einer CA wie folgt vorgehen:



2. Konfiguration als VPN-Client mit OpenVPN

Hier wird der OpenVPN-Client der pfSense analog zu den erhaltenden Daten konfiguriert. Im ersten Schritt müssen Teile der Dateien auf die Firewall „kopiert“ werden, die im weiteren Verlauf vom OpenVPN-Client genutzt werden. Analog zu dem hier vorgestellten Vorgehen können die

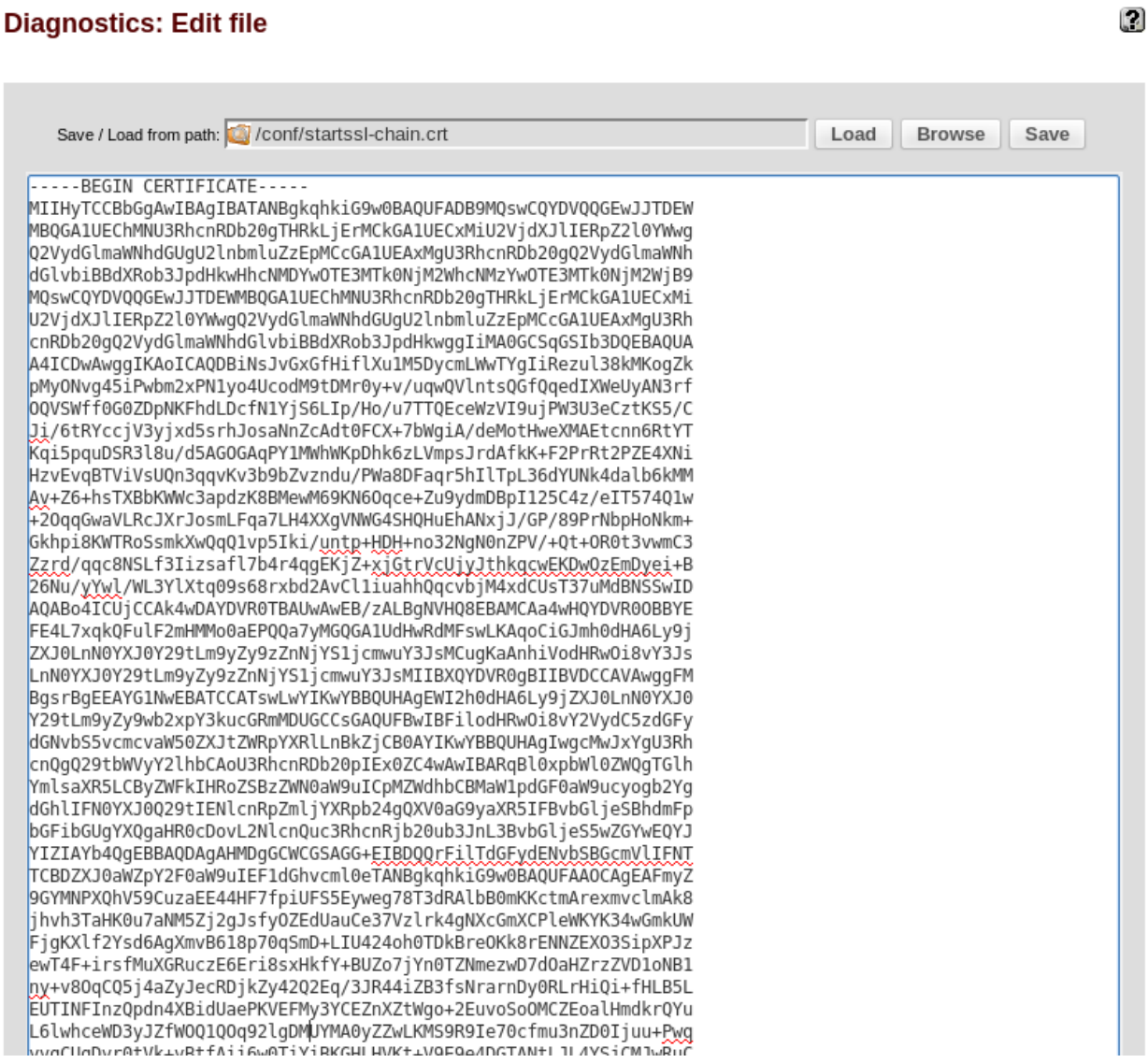
Informationen allerdings auch im Webinterface eingepflegt werden.

Diagnostics → Edit File

An dieser Stelle werden die Dateien **startssl-chain.crt**, **in-berlin.auth** und **in-berlin.tls-auth** aus dem dir übermittelten ZIP-File auf der Firewall für die weitere Verwendung abgespeichert. Alternativ zu der Erstellung über die Weboberfläche kann auch SSH/SCP genutzt werden, was jedoch nur für erfahrene Benutzer geeignet ist.

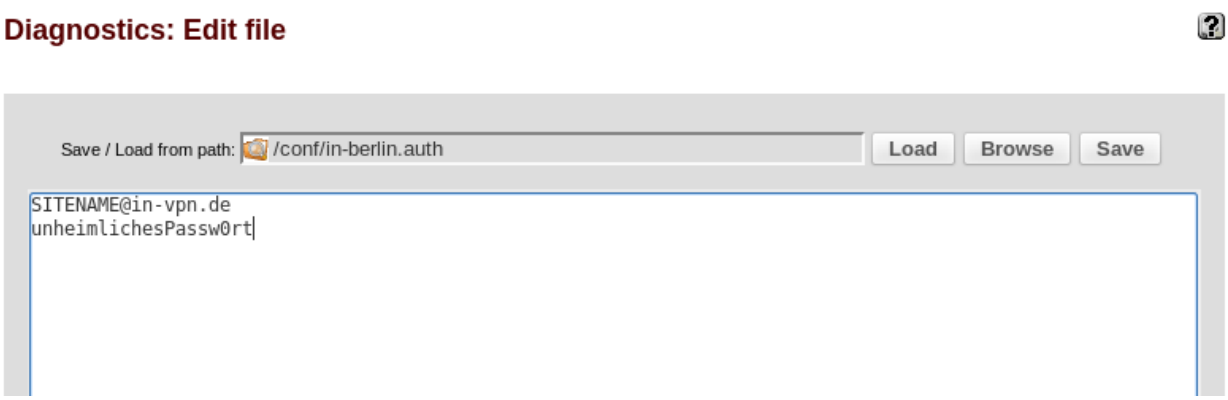
startssl-chain.crt

Nach Eingabe des gewünschten Pfads und dem Inhalt der Datei auf der Firewall den Button „Save“ drücken!



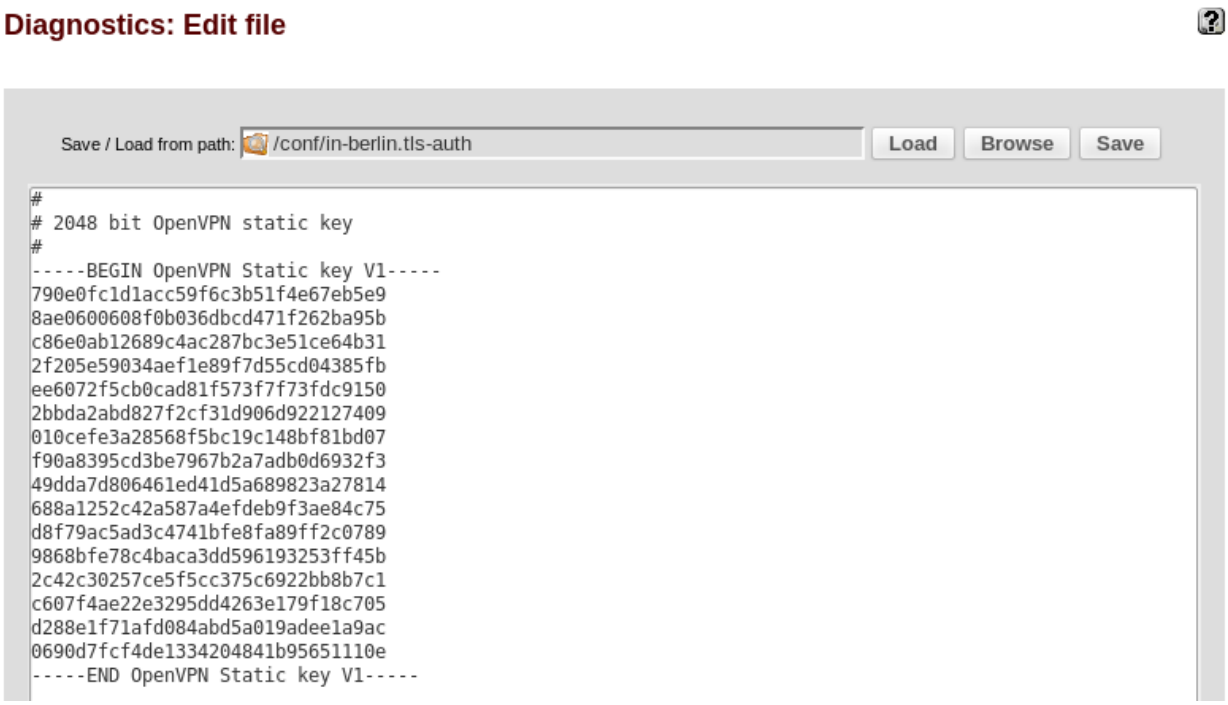
in-berlin.auth

Nach Eingabe des gewünschten Pfads und dem Inhalt der Datei auf der Firewall den Button „Save“ drücken!



in-berlin.tls-auth

Nach Eingabe des gewünschten Pfads und dem Inhalt der Datei auf der Firewall den Button „Save“ drücken!



VPN → OpenVPN → Client → add client

Auf der folgenden Seite wird der OpenVPN-Client der Firewall konfiguriert.

- Als Interface ist das WAN-Interface (also das, welches ins Internet zeigt) anzugeben.

- Es muss zwingend ein Server oder eine IP angegeben werden.

OpenVPN: Client

Server | Client | Client Specific Overrides | Wizards | Client Export | Shared Key Export

General information

Disabled	☐ **Disable this client** Set this option to disable this client without removing it from the list.
Server Mode	Peer to Peer (SSL/TLS)
Protocol	UDP
Device mode	tun
Interface	TELEKOM
Local port	 Set this option if you would like to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.
Server host or address	openvpn1.in-berlin.de
Server port	1194
Proxy host or address	
Proxy port	
Proxy authentication extra options	Authentication method : none
Server host name resolution	☑ Infinitely resolve server Continuously attempt to resolve the server host name. Useful when communicating with a server that is not permanently connected to the Internet.
Description	 You may enter a description here for your reference (not parsed).

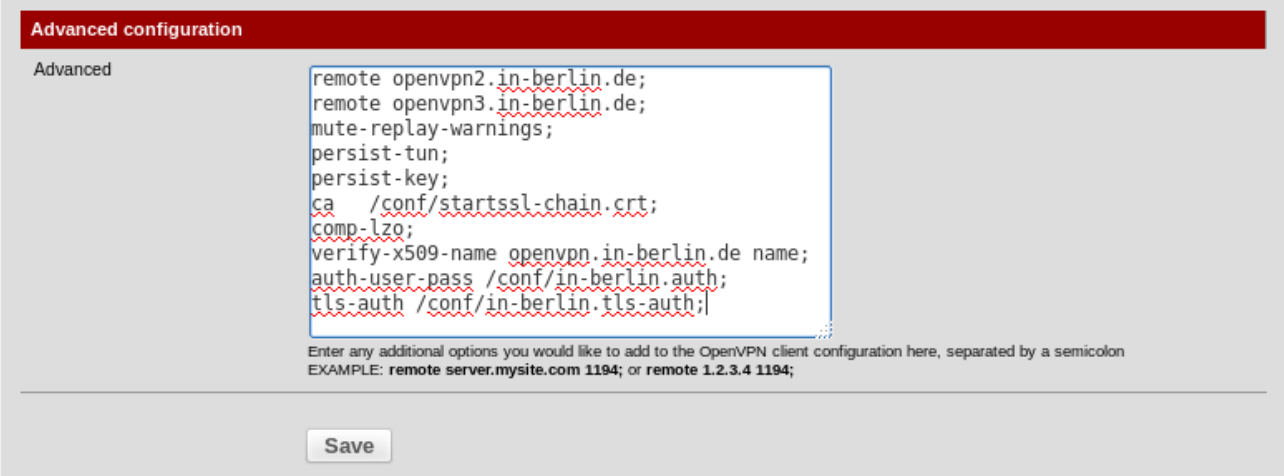
Cryptographic Settings

TLS Authentication	☐ Enable authentication of TLS packets.
Peer Certificate Authority	VPNCA
Client Certificate	webConfigurator default *In Use
Encryption algorithm	AES-128-CBC (128-bit)
Hardware Crypto	No Hardware Crypto Acceleration

Tunnel Settings

IPv4 Tunnel Network	 This is the virtual network used for private communications between this client and the server expressed using CIDR (eg. 10.0.8.0/24). The first network address is assumed to be the server address and the second network address will be assigned to the client virtual interface.
IPv6 Tunnel Network	 This is the IPv6 virtual network used for private communications between this client and the server expressed using CIDR (eg. fe80::/64). The first network address is assumed to be the server address and the second network address will be assigned to the client virtual interface.
IPv4 Remote Network/s	 These are the IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges. If this is a site-to-site VPN, enter the remote LAN/s here. You may leave this blank to only communicate with other clients.
IPv6 Remote Network/s	 These are the IPv6 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more IP/PREFIX. If this is a site-to-site VPN, enter the remote LAN/s here. You may leave this blank to only communicate with other clients.
Limit outgoing bandwidth	 Maximum outgoing bandwidth for this tunnel. Leave empty for no limit. The input value has to be something between 100 bytes/sec and 100 Mbytes/sec (entered as bytes per second).
Compression	☐ Compress tunnel packets using the LZO algorithm.
Type-of-Service	☐ Set the TOS IP header value of tunnel packets to match the encapsulated packet value.

Nun müssen noch die relevanten Dateien aus der **in-berlin-vpn.conf** in den Advanced-Bereich der Konfiguration eingetragen werden:



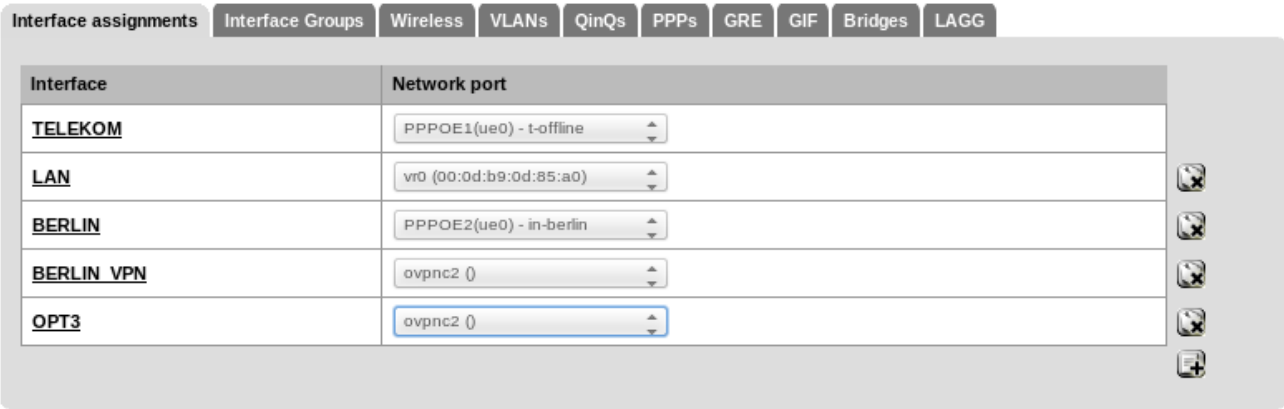
<u>Wichtig:</u> Die einzelnen Zeilen im Advanced-Fenster müssen entgegen der Textdatei mit einem „;“ abschließen!

Die VPN-Konfiguration mit „Save“ abschließen.

3. Erstellen eines Interfaces

Nachdem der Aufbau des VPN-Tunnels konfiguriert ist, muss nun noch ein passendes Interface auf der Firewall eingerichtet werden. Dank dieses Interfaces ist später eine Konfiguration möglich, wie man sie von anderen Interfaces kennt.

Interfaces → (assign) → add interface



Hier wird nun ein weiteres Interface hinzugefügt, welches als Netzwerk-Port die vorher konfigurierte OpenVPN-Verbindung nutzt. Den wenig sprechenden Namen „OPT3“ kann man im nächsten Schritt ändern.

„Save“ und „Apply changes“, fast fertig.

Interfaces → Interface-Name aus vorherigem Schritt

Zum Abschluss der Konfiguration nun noch das Interface einrichten. Achte auf einen sprechenden Namen.

4. Gateway-Groups

Mit der bisherigen Konfiguration hat die Firewall neben der oder den bestehenden Verbindungen eine weitere Verbindung ins Internet. Damit wurde allerdings noch keine weitere Regelung des Routings übernommen, was natürlich problematisch ist. Abschließend sollte nun eine Gateway-Gruppe eingerichtet werden, die ein sauberes Routing der einzelnen Pakete sicherstellt.

Wichtig dabei sind zwei Punkte, die aus dem aktuellen Beispiel hervorgehen sollen:

1. Ich nutze auf der pfSense zwei Internet-Zugänge. Der eine („normaler Provider“) wird im Haushalt zum Surfen im Internet genutzt, da hier keine Volumenbeschränkung besteht.

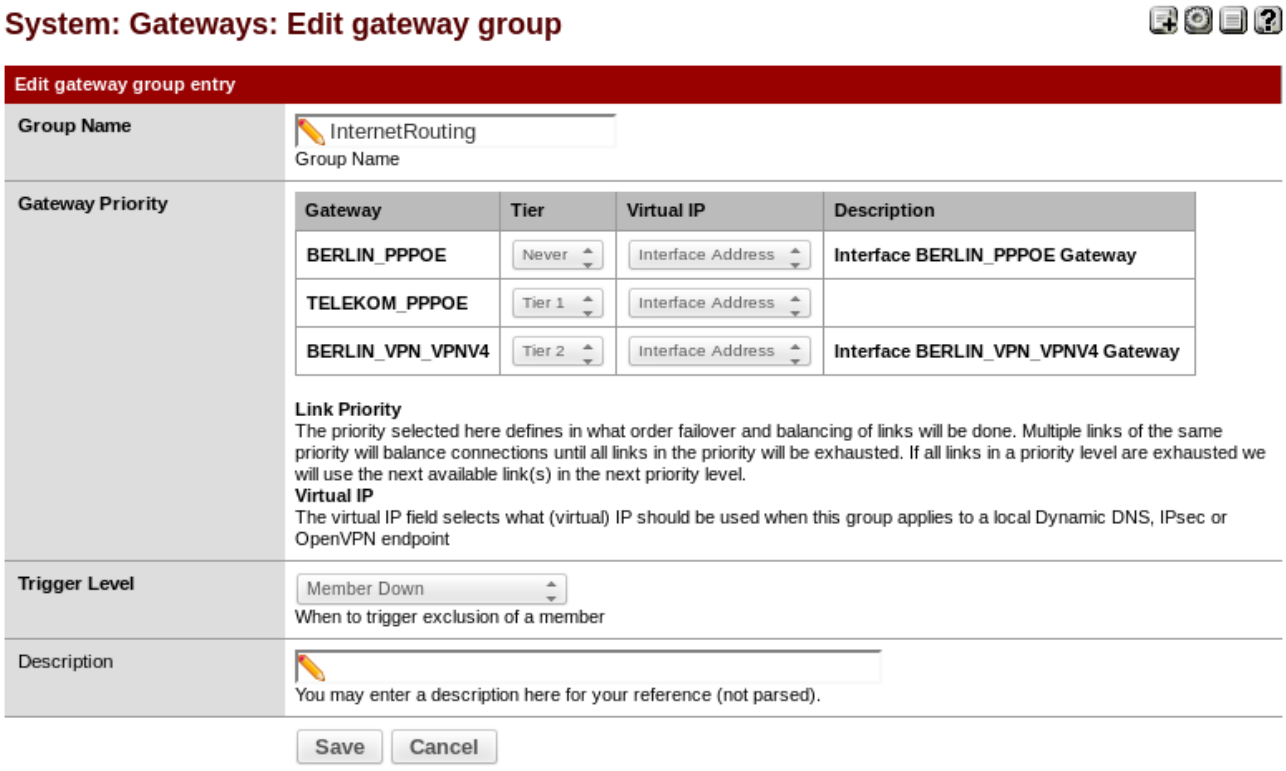
   Weiterhin wird die VPN-Verbindung zu IN-BERLIN über diesen Anschluss sichergestellt.

2. Die feste IP des IN_BERLIN nutze ich (beispielhaft) für meinen Mailserver

Aus diesen beiden Punkten ergeben sich also Firewall-Regeln, sowie Routingeinträge.
In der hier vorgestellten Kombination werden jedoch keine Failover-Mechanismen greifen, das bei Ausfall der Provider-Verbindung auch keine VPN-Verbindung mehr besteht.

Auf diese Art entsteht ein Routing auf Quell-Basis.

System → Routing → Groups → add group



Zur Erklärung:
Auf dem oberen Bild den Gateway „BERLIN_PPPOE“ bitte ausblenden, da in meinem Fall dieser Zugang abgelöst werden soll.
Je höher der Tier-Level, desto häufiger wird dieser Zugang genutzt.
Der „Trigger-Level“ definiert das Verhalten, welches zu einem Ausschluss aus der Routing-Gruppe führt.

Im weiteren Verlauf der Regeleinrichtung muss nun nur noch die hier eingerichtete Gateway-Gruppe in den Regeln definiert werden. Dies geschieht im Unterpunkt Gateway unterhalb der Advanced Features einer Firewall-Regel.