Einstellungen für Experten

Bei den Experteneinstellungen handelt es sich um Konfigurationsmöglichkeiten der mp-Firewall, die es erlauben Dienste einzubeziehen, die nicht primär auf der mp-Firewall laufen. So können unter den Experteneinstellungen E-Mail Weiterleitungen eingestellt werden, OpenVPN-Verbindungen konfiguriert oder eigene Firewall-Regeln gesetzt werden. Diese Einstellungen sollten nur von Experten vorgenommen werden.

DNS-Slave- oder DNS-Forward-Server

Ein DNS-Server, der als direkte Quelle für die Synchronisation einer Zonendatei dient, wird als Master DNS Server bezeichnet. Einen DNS-Server, der die Zonendaten von einem Master bezieht, nennt man DNS-Slave-Server oder DNS-Forward-Server. Die TightGate-Firewall bietet die Möglichkeit, als DNS-Slave-Server und als DNS-Forward-Server für verschiedene Domains zu arbeiten. Dies ist besonders vorteilhaft bei größeren VPN-Netzwerken oder wenn in Netzwerken verschiedene DNS Master Server zum Einsatz kommen (z.B. Windows 2003 Server). Wir unterscheiden diese beiden Arten wie folgt. Als Erstes der DNS-Slave-Server, er speichert eine lokale Kopie der DNS-Einträge des DNS-Master-Servers. Der Zweite, der DNS-Forward-Server, holt sich die Antworten auf die DNS-Anfragen immer direkt vom Master.

Um neue DNS-Slave-Servern oder DNS-Forward-Server auf der mp-Firewall anzulegen oder bestehende zu ändern melden Sie sich bitte als Benutzer *config* an. Wählen Sie dann bitte aus den Menüpunkt *Einstellungen>DNS Slave/Forward* aus. So legen Sie einen neuen Eintrag an:

Wählen sie den Menüpunkt *Neu* aus. Geben Sie die Domain an, für welche die mp-Firewall als DNS Slave Server arbeiten soll, und anschließend noch den DNS Master Server für diese Domain.

Die mp-Firewall aktualisiert automatisch ihre DNS-Einträge vom eingestellten DNS Master Servern.

ACHTUNG: Wenn Sie alle Einstellungen vorgenommen haben, verlassen Sie das Menü. Speichern Sie nun alle Änderungen über den Menüpunkt *Speichern* ab und wenden Sie diese mit dem Menüpunkt *Sanft Anwenden* an. Erst nach dem Anwenden werden die Einstellungen wirksam.

OpenVPN

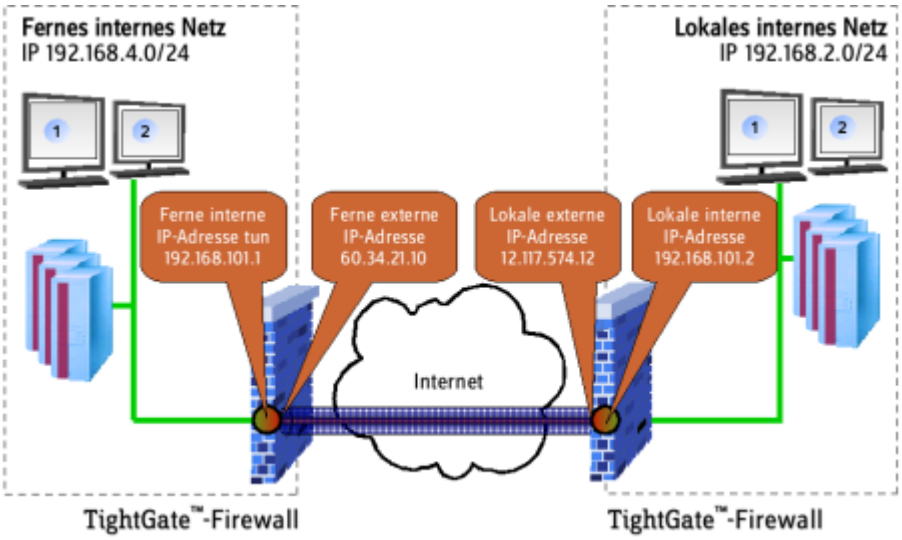
OpenVPN ist ein Werkzeug zum Aufbau eines virtuellen privaten Netzwerks über eine SSL-Verbindung, welche eine flexible Klienten-Authentifizierung ermöglicht. In der mp-Firewall wird OpenVPN mit einer SSL-Verschlüsselung ermöglicht. OpenVPN ist keine Web-Applikation und verfügt nicht über eine Web-Oberfläche.

Grundlagen zu OpenVPN

Funktionsweise des OpenVPN

Grundlage des OpenVPN-Tunnels ist der OpenVPN-Dienst, welcher sowohl auf dem Server als auch auf der Klientenseite auf einem Port läuft und mit Hilfe eines Treibers eine virtuelle Netzwerkschnittstelle

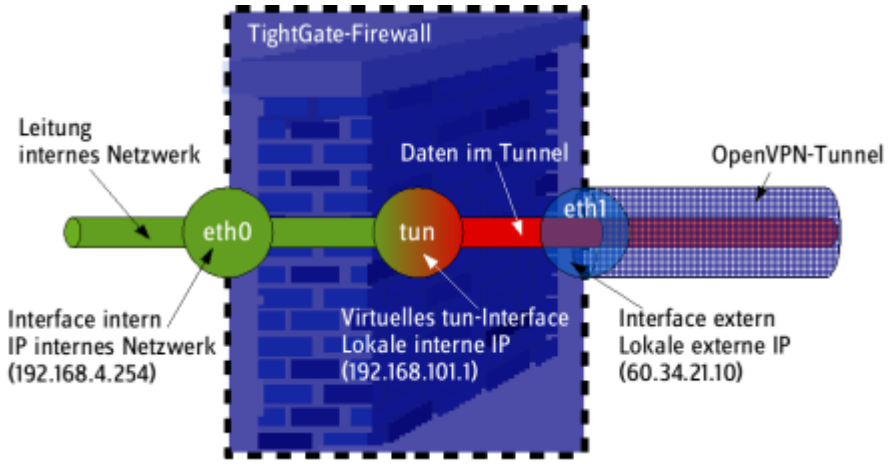
(tun-Interface) anlegt, welche jeweils ein Ende des Tunnels darstellt. Der gesamte Netzwerkverkehr kann dabei mit OpenSSL verschlüsselt werden. Beispiel einer OpenVPN-Verbindung:



Zum Aufbau eines OpenVPN-Netzwerkes (wie in obiger Abbildung dargestellt) werden drei Netzwerke benötigt. Es müssen zur Einrichtung der Verbindung die IP-Adressen für alle Netzwerke bekannt sein. Das sind im einzelnen:

1. Lokales internes Netz (das eigene interne Netzwerk)
2. Fernes internes Netz (das Netzwerk, welches sich intern hinter der fernen Firewall befindet)
3. Virtuelles OpenVPN-Netz (Das virtuelle Netzwerk, in welchem OpenVPN kommuniziert)

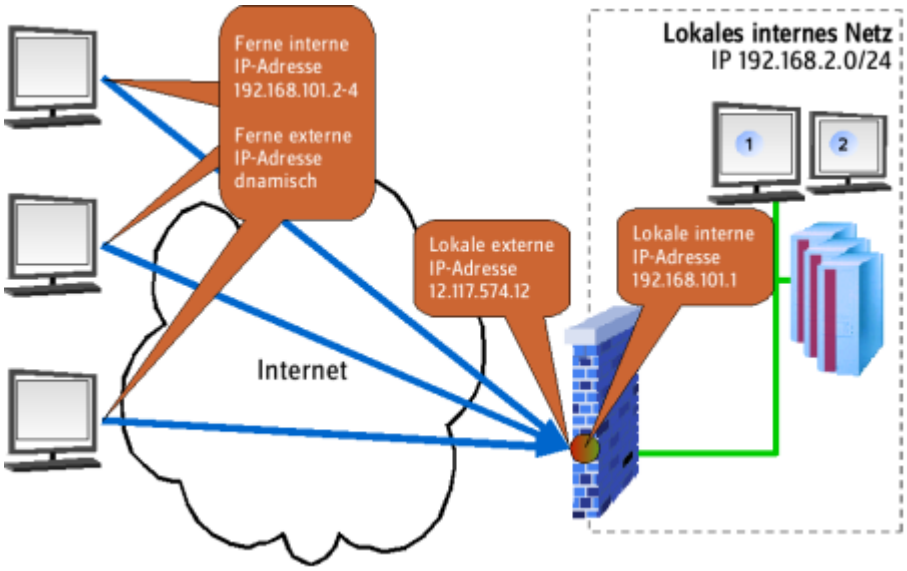
Beteiligte Schnittstellen
An der Konfiguration einer OpenVPN-Verbindung sind an der jeweiligen Firewall drei Interfaces beteiligt. Das nachfolgende Schaubild verdeutlicht dies noch einmal:



Es wird deutlich, dass neben den physikalischen Schnittstellen (eth0 und eth1) ein zusätzliches Interface (tun) auftaucht. Dies ist Teil des virtuellen OpenVPN-Netzes, welches zwischen den beteiligten Firewalls für das OpenVPN aufgebaut wird. Das virtuelle Netzwerk (tun) darf in keinem Fall im IP-Bereich eines beteiligten Netzwerks liegen.

Multi-Klienten
Eine weitere Anwendungsmöglichkeit neben der Firewall zu Firewall Verbindung ist die Verbindung von mehreren mobilen Klienten (Außenstellen, Notebooks etc.) hin zu einer mp-Firewall. Diese Möglichkeit sollte nur verwendet werden, wenn mobile Endgeräte an eine mp-Firewall angeschlossen

werden. Werden zwei mp-Firewalls oder Geräte mit fester IP-Adresse verbunden, so ist die Shared-Key-Authentifizierung vorzuziehen. Die nachfolgende Abbildung zeigt beispielhaft, wie eine solche aussehen könnte:



Authentifizierung
Zur Authentifizierung der Gegenstellen können grundsätzlich zwei Verfahren verwendet werden:

1. Shared-Key-Authentifizierung (zu empfehlen bei statischen Verbindungspunkten)
2. Zertifikat-basierte Authentifizierung (zu empfehlen bei Verbindungen mit mobilen Klienten)

Die mp-Firewall unterstützt beide Authentifizierungsverfahren.

Statische Verbindungen mit Shared-Key

Einsatzgebiet
Das Shared-Key Verfahren wird empfohlen zum Einsatz, wo zwei feste Gegenstellen eine sichere Tunnelverbindung untereinander aufbauen sollen. Dies kann z.B. die Anbindung von Außenstellen an eine Zentrale.

Einrichtung
Zum Einrichten einer neuen OpenVPN-Verbindung benötigen Sie die IP-Informationen für die beteiligten Netzwerke, sowie einen Überblick der für die Verbindung benutzen Schnittstellen. Sie haben die Möglichkeit die Schlüsseldatei für die Gegenstelle von der mp-Firewall erzeugen zu lassen. Diese kann dann exportiert werden oder, sofern die Gegenstelle auch eine mp-Firewall ist, einfach auf die Gegenstelle übertragen werden.

Zur Erstellung einer neuen OpenVPN-Verbindung mit Shared-Keys melden Sie sich bitte als Benutzer *config* an und wählen dann den Menüpunkt *Einstellungen>OpenVPN>Neu* aus.

Geben Sie der neuen OpenVPN-Verbindung eine Nummer. Diese dient nur der eindeutigen Identifizierung und hat im Gegensatz zu selbst definierten Firewall-Regeln keinen Einfluss auf eine priorisierende Ausführung. Nehmen Sie die Einstellungen auf der mp-Firewall entsprechend der nachfolgenden Tabelle vor. Es müssen die Optionen mit den laufenden Nummern 1 bis 13 geeignet eingestellt werden, wobei sich die einzutragenden Werte aus der Beschreibung und der Bemerkung dazu ergeben.

Lfd. Nr.	Beschreibung	Wert	Bemerkung
1	VPN-Modus	p2p	P2P ist einzustellen für Shared-Key Verbindungen, client/server für Zertifikate.
2	Transportprotokoll	udp	UDP sollte immer dann verwendet werden, wenn beide Partner vollen Internetzugang haben und über feste IP-Adressen verfügen. Ebenfalls ist dieses Verfahren einzusetzen, wenn beide Gegenstellen DSL-Zugang haben und über dynamische IP-Adressen angesprochen werden können. Ist dieses nicht der Fall, verwenden Sie bitte tcp-client am eingeschränkteren und tcp-server am anderen Ende der Verbindung.
3	Lokale externe IP (Externe IP der Firewall)	a.b.c.d	IP-Adresse des Interfaces an der mp-Firewall, welches mit dem Internet verbunden ist. Bei dynamischen Adressen lassen Sie dieses Feld leer.
4	Lokaler externer Tunnel-Port (Externer Port der Firewall)	'1200+x'	Es wird empfohlen den Port nach der Formel "1200 + Nummer der Verbindung" auszuwählen. Also für die erste OpenVPN-Verbindung: 1200 + 1 = Port 1201. Beim Protokoll tcp-server kann es nötig sein, den HTTPS-Port 443 zu verwenden, damit die Gegenstelle sich über einen HTTPS-Proxy verbinden kann.
5	Ferne externe Adresse	a.b.c.d	IP-Adresse des Interfaces der Gegenstelle, welches mit dem Internet Verbunden ist. Ist die IP-Adresse der Gegenstelle dynamisch lassen Sie dieses Feld leer.
6	Ferner externer Port (Externer Port der Gegenstelle)	= Lfd. Nr.4	Leer lassen, wenn dynamische Adressen und Ports vergeben werden, ansonsten den konfigurierten Port der Gegenstelle übernehmen.
7	Lokale interne Tunnel-IP-Adresse (tun-Interface der mp-Firewall)	a.b.c.d	IP-Adresse des virtuellen tun-Interface auf der mp-Firewall. Das virtuelle tun-Netzwerk darf in keinem anderen beteiligten Netzwerk liegen. Vergeben Sie die tun-Interface-Adresse z.B. nach folgender Formel: 192.168.(200+Verbindung).1, wobei die mp-Firewall lokal immer die a.b.c.1 bekommen sollte.
8	Ferne interne Tunnel-IP-Adresse (tun-Interface der Gegenstelle)	a.b.c.d	IP-Adresse des virtuellen tun-Interface der Gegenstelle. Die IP Adresse wird analog der Lfd. Nr. 7 vergeben nach folgender Formel: 192.168.(200+Verbindung).2, wobei die Gegenstelle immer die a.b.c.2 bekommen sollte (dort natürlich entsprechend anders herum eintragen).
9	Ferne interne Netze (Netzwerk hinter der Gegenstelle)	a.b.c.d./n	IP-Adresse/Valid-Bit des Netzwerks, das hinter der Gegenstelle erreichbar sein soll. Leer lassen, wenn keine weiteren Netzwerke hinter der Gegenstelle zu erreichen sind.
10	Sende-Rate	0	Möglichkeit, die Sende-Rate für die VPN-Verbindung zu beschränken. Dies wird im Normalfall nicht nötig sein. Um keine Beschränkung der Sende-Rate vorzunehmen, bitte 0 eintragen.
11	Weitere Optionen	comp-lzo comp-noadapt keepalive passtos	Bitte alle Optionen anschalten.
12	Voller Firewallzugriff	Ja/Nein	Erlaubt der Gegenstelle über die OpenVPN-Verbindung alle auf der mp-Firewall laufenden Dienste zu nutzen (z.B. Mailserver, interner FTP- oder Web-Server)*.

Lfd. Nr.	Beschreibung	Wert	Bemerkung
13	Voller Zugriff auf intern	Ja/Nein	Erlaubt der Gegenstelle über die OpenVPN-Verbindung auf alle Ressourcen des lokalen Netzwerks zuzugreifen. (z.B. TightGate-Pro)*.

*Soll kein allgemeiner Zugriff auf die Firewall oder das interne Netz freigegeben werden, so sind die Einträge für die Lfd. Nr. 12 + 13 auf *Nein* zu setzen. Es können aber einzelne Dienste gezielt und kontrolliert freigeschaltet werden. Per Custom-Regel kann für das jeweilige Interface der Zugriffe geregelt werden. z.B. für die OpenVPN-Verbindung Nr. 5 ist das Interface tun5 zuständig.
Wenn man für alle Tunnel gemeinsame Regeln setzen möchte, muss man als Interface in der Custom-Regel tun+ eintragen.

Wenn alle Einstellungen vorgenommen sind, ist der erste Schritt der Konfiguration abgeschlossen. Sie sehen nun eine Liste der von Ihnen konfigurierten OpenVPN-Verbindungen. Wählen Sie bitte Ihre Konfiguration aus. Um die Konfiguration abzuschließen ist noch die Erzeugung oder der Import eines Schlüssels notwendig. Wählen Sie zum Erzeugen den Menüpunkt *Schlüsseldatei erzeugen* aus.

ACHTUNG: Nur wenn hinter dem Menüpunkt *Schlüsseldatei erzeugen* ein nicht vorhanden steht hat die OpenVPN-Verbindung keinen Schlüssel. Steht hinter dem Menüpunkt Schlüsseldatei erzeugen ein vorhanden, so existiert bereits eine Schlüsseldatei. Durch wiederholtes Anklicken auf eine vorhandene Schlüsseldatei wird diese überschrieben. Es muss dann ebenfalls die Schlüsseldatei auf der Gegenstelle neu eingespielt werden. Ist eine Schlüsseldatei vorhanden, so kann diese über den Menüpunkt Schlüsseldatei ansehen zur Anzeige gebracht werden. Das Beenden der Anzeige geschieht mit der taste q.

Zum Export der Schlüsseldatei und zur Einrichtung der Gegenstelle/Klienten gehen Sie bitte vor, wie im Abschnitt Schlüssel- und Zertifikats-Management beschrieben.

ACHTUNG: Wenn Sie alle Einstellungen vorgenommen haben, verlassen Sie das Menü. Speichern Sie nun alle Änderungen über den Menüpunkt *Speichern* ab und wenden Sie diese mit dem Menüpunkt *Voll Anwenden* an. Erst nach dem Anwenden werden die Einstellungen wirksam.

Multi-Klienten Verbindungen mit Zertifikat

Einsatzgebiet
Das Zertifikats-Verfahren wird empfohlen, falls zu einer mp-Firewall von mehreren mobilen Klienten aus eine sichere Tunnelverbindung aufgebaut werden soll. Das kann z.B. die Anbindung von AußendienstmitarbeiterInnen mit Notebooks an eine Zentrale sein.

Einrichtung
Zum Einrichten einer neuen OpenVPN-Verbindung benötigen Sie die IP-Informationen für die beteiligten Netzwerke sowie einen Überblick der für die Verbindung benutzen Schnittstellen. Mit der mp-Firewall können Sie problemlos die OpenVPN-Verbindung einrichten. Sie haben auch die Möglichkeit, die Konfigurationen für die Gegenstellen (Notebooks) von der mp-Firewall mit erzeugen zu lassen. Diese können dann auf einfache Weise exportiert werden. Somit sparen Sie Zeit und Mühe, da keine doppelte Konfiguration vorgenommen werden muss.

Zur Erstellung einer neuen zertifikatsbasierten OpenVPN-Verbindung melden Sie sich bitte als Benutzer *config* an und wählen dann den Menüpunkt *Einstellungen>OpenVPN>Neu* aus. Geben Sie der neuen OpenVPN-Verbindung eine Nummer. Diese dient nur der eindeutigen Identifizierung und

hat im Gegensatz zu selbst definierten Firewall-Regeln keinem Einfluss auf eine priorisierende Ausführung.
Nehmen Sie die Einstellungen auf der mp-Firewall entsprechend der nachfolgenden Tabelle vor. Es müssen die Optionen mit den laufenden Nummern 1 bis 13 eingestellt werden, wobei sich die einzutragenden Werte aus der Beschreibung und der Bemerkung dazu ergeben.

Lfd. Nr.	**Beschreibung**	**Wert**	**Bemerkung**
1	VPN-Modus	server	P2P ist einzustellen für *Shared-Key* Verbindungen, *server* für Zertifikate, *client*, wenn die mp-Firewall die Gegenstelle einer Verbindung ist.
2	Transportprotokoll	tcp-server	UDP sollte immer dann verwendet werden, wenn alle Partner unbeschränkten Internetzugang haben. Ist dieses nicht der Fall, verwenden Sie bitte tcp-server im VPN-Modus server und tcp-client im VPN-Modus client.
3	Lokale externe IP (Externe IP der Firewall)	a.b.c.d	IP-Adresse des Interfaces an der mp-Firewall, welches mit dem Internet Verbunden ist.
4	Lokaler externer Tunnel-Port (Externer Port der Firewall)	'1200+x'	Es wird empfohlen den Port nach der Formel "1200 + Nummer der Verbindung" auszuwählen. Also für die erste OpenVPN-Verbindung: 1200 + 1 = Port 1201. Beim Protokoll tcp-server kann es nötig sein, den HTTPS-Port 443 zu verwenden, damit die Gegenstelle sich über einen HTTPS-Proxy verbinden kann.
5	Ferne externe Adresse	a.b.c.d	IP-Adresse des Interfaces der Gegenstelle, welches mit dem Internet Verbunden ist. Ist die IP-Adresse der Gegenstelle dynamisch lassen Sie dieses Feld leer.
6	Ferner externer Port (Externer Port der Gegenstelle)	= Lfd. Nr.4	Leer lassen, wenn dynamische Adressen und Ports vergeben werden, ansonsten den konfigurierten Port der mp-Firewall übernehmen.
7	Lokale interne Tunnel-IP-Adresse (tun-Interface der mp-Firewall)	a.b.c.d	IP-Adresse des virtuellen tun-Interface auf der mp-Firewall. Das virtuelle tun-Netzwerk darf in keinem anderen beteiligten Netzwerk liegen. Vergeben Sie die tun-Interface-Adressen z.B. nach folgender Formel: 192.168.(100+Verbindung).1, wobei die mp-Firewall lokal immer die a.b.c.1 und die ferne .2 bekommen sollte.
8	Ferne interne Tunnel-IP-Adresse (tun-Interface der Gegenstelle)	a.b.c.d	IP-Adresse des virtuellen tun-Interface der Gegenstelle. Die IP Adresse wird analog der Lfd. Nr. 7 vergeben nach folgender Formel: 192.168.(100+Verbindung).2, wobei die Gegenstelle immer die a.b.c.2 bekommen sollte.
9	Ferne interne Netze (Netzwerk hinter der Gegenstelle)	a.b.c.d./n	IP-Netzwerk/Valid-Bits der Netzwerke, die hinter der Gegenstelle erreichbar sein sollen. Leer lassen, wenn keine weiteren Netzwerke hinter der Gegenstelle zu erreichen sind. Achtung: Dieses funktioniert nicht im VPN-Modus *server* mit Multi-Klienten.
10	Sende-Rate	0	Möglichkeit Sende-Raten für die VPN-Verbindung zu beschränken. Dies wird im Normalfall nicht nötig sein. Um keine Beschränkung der Sende-Rate vorzunehmen bitte 0 eintragen.

Lfd. Nr.	Beschreibung	Wert	Bemerkung
11	Weitere Optionen	comp-lzo comp-noadapt keepalive passtos	Bitte alle Optionen anschalten.
12	Voller Firewallzugriff	Ja/Nein	Erlaubt dem Klienten über die OpenVPN-Verbindung alle auf der Firewall laufenden Dienste zu nutzen (z.B. Mailserver, interner FTP- oder Web-Server)*.
13	Voller Zugriff auf intern	Ja/Nein	Erlaubt dem Klienten über die OpenVPN-Verbindung auf alle Ressourcen des lokalen Netzwerks zuzugreifen. (z.B. TightGate-Pro)*.

*Soll kein allgemeiner Zugriff auf die Firewall oder das interne Netz freigegeben werden, so sind die Einträge für die Lfd. Nr. 12 + 13 auf Nein zu setzen. Es können aber einzelne Dienste gezielt und kontrolliert freigeschaltet werden. Per Custom-Regel kann für das jeweilige Interface der Zugriffe geregelt werden. Z.B. für die OpenVPN-Verbindung Nr. 5 ist das Interface tun5 zuständig.
Wenn man für alle Tunnel gemeinsame Regeln setzen möchte, muss man als Interface in der Custom-Regel tun+ eintragen.

Wenn alle Einstellungen vorgenommen sind ist der erste Schritt der Konfiguration abgeschlossen. Sie sehen nun eine Liste der von Ihnen konfigurierten OpenVPN-Verbindungen. Wählen Sie bitte Ihre Konfiguration aus. Bevor die einzelnen Zertifikate erzeugt werden können, sind ein ein paar weitere Einstellungen notwendig. Bitte tragen Sie die entsprechenden Werte laut der unten stehenden Tabelle für Ihre OpenVPN-Verbindung ein.

Wert	Beschreibung
Server-CN	Die Server CN sollte dem vollständigen Namen + Domain entsprechen, unter dem die mp-Firewall von den VPN-Gegenstellen angesprochen wird. Bsp. Heißt Ihre mp-Firewall gateway und befinden Sie sich in der Domäne m-privacy.de, so lautet die Server-CN gateway.m-privacy.de. Sollen mobile Klienten angebunden werden, so ist die Eintragung der korrekten Server-CN zwingend erforderlich.
Anzahl Klienten	Anzahl der Gegenstellen, die sich über das Zertifikat mit der mp-Firewall verbinden sollen. Es sind pro OpenVPN-Zertifikat maximal 63 Klienten zugelassen (Beschränkung durch die Größe des Klienten-Netzwerkes mit 24 Bit, falls Sie mehr benötigen, fragen Sie bitte den Support der m-privacy GmbH nach der korrekten Konfiguration).
Klienten-Netzwerk	IP-Adresse des Klienten Netzwerkes. Das Netzwerk ist in der Form a.b.c.d/n anzugeben. Das Klienten-Netzwerk entspricht dem unter der Lfd. Nr.7 festgelegten tun-Netzwerk. In dem Beispiel vom Anfang würde das Klienten-Netzwerk so aussehen: 192.168.101.0/24
Erste Klienten-IP	IP-Adresse des ersten Klienten, der sich verbinden soll. Diese muss aus dem Klienten-Netzwerk stammen und sollte als hintere Stelle die .4 haben. In dem Beispiel vom Anfang würde die erste Klienten-IP die 192.168.101.4 sein. (Anmerkung: Die IP-Adressen a.b.c.1/2/3 sind schon durch die tun-Interfaces und die Broadcast-Adresse vergeben. Daher beginnt die erste Klienten-IP mit der a.b.c.4).

Wert	Beschreibung
Letzte Klienten-IP	IP-Adresse des letzten Klienten, der sich verbinden soll. Diese muss aus dem Klienten-Netzwerk stammen und sollte als hintere Stelle die .252 haben. In dem Beispiel vom Anfang würde die letzte Klienten-IP die 192.168.101.252 sein. (Anmerkung. Die IP-Adressen der Klienten werden als 2-Bit-/4-Adressen-Blöcke vergeben, daher hat die letzte Klienten-IP die a.b.c.252).
Push Route	Mit dieser Funktion können Sie den Gegenstellen automatisch Routen mitgeben, wie diese die Netzwerke hinter Ihrer mp-Firewall erreichen können.
Push DNS	Mit dieser Funktion können Sie auf den Gegenstellen automatisch einstellen, dass alle DNS-Anfragen der Gegenstellen nur über die mp-Firewall beantwortet werden.
Benutzeranmeldung fordern	Mit der Anforderung einer Benutzeranmeldung haben Sie einen weiteren Sicherheitsbaustein für die OpenVPN-Verbindungen. Die Benutzeranmeldung ergänzt das Prinzip "Etwas haben" um das Prinzip "Etwas wissen". Ohne die Benutzeranmeldung werden zum Aufbau einer OpenVPN-Verbindung nur die von der Firewall bereitgestellten Zertifikate und Schlüssel benötigt. Das heißt, dass ein Nutzer sich allein durch den Besitz der notwendigen Dateien an der mp-Firewall anmelden kann. Gelangt jemand unberechtigtes in den Besitz dieser Dateien (z.B. Diebstahl eines Notebooks) so kann er damit eine Verbindung aufbauen. Mit einer geforderten Benutzeranmeldung ist zusätzlich zum Besitz der notwendigen Dateien noch der Benutzername und das Passwort eines gültigen Benutzers der mp-Firewall notwendig.

Sind alle Einstellungen aus der Liste vorgenommen, müssen beim VPN-Modus *server* nun noch die Certification Authority (CA) und die Zertifikate für die Klienten erzeugt werden.

SSL-CA erzeugen
Um das CA-Zertifikat der OpenVPN-Verbindung zu erzeugen, gehen Sie bitte auf den Menüpunkt SSL-CA erzeugen und wählen Sie diesen aus. Das Erzeugen des SSL-CA kann ein wenig Zeit in Anspruch nehmen. Bitte haben Sie etwas Geduld.

Klienten-Zertifikate erzeugen
Um die Klienten-Zertifikate zu erzeugen, gehen Sie bitte auf den Menüpunkt Klienten-Zertifikate erzeugen und wählen Sie diesen aus. Das Erzeugen der Zertifikate dauert ebenfalls etwas, da für jeden Klienten ein eigenes Zertifikat erzeugt wird. Haben Sie 3 oder mehr Klienten eingestellt, könnte die Zeit für einen Kaffee reichen.

Zum Export der Schlüsseldateien und zur Einrichtung der Gegenstelle/Klienten gehen Sie bitte vor, wie in den nachfolgenden Abschnitten beschrieben.

ACHTUNG: Wenn Sie alle Einstellungen vorgenommen haben, verlassen Sie das Menü. Speichern Sie nun alle Änderungen über den Menüpunkt *Speichern* ab und wenden Sie diese mit dem Menüpunkt *Voll Anwenden* an. Erst nach dem Anwenden werden die Einstellungen wirksam.

Schlüssel- und Zertifikats-Management

In diesem Kapitel wird Ihnen gezeigt, welche Möglichkeiten es gibt die erzeugten Dateien für Pre-Shared-Key oder Zertifikats-Verbindungen von der mp-Firewall zu exportieren.

Schlüsselmanagement
Es ist sicherzustellen, dass für den Aufbau des OpenVPN-Tunnels für Server und Client der gleiche

Schlüssel hinterlegt wird.

Pre-Shared Schlüsseldatei exportieren:
Zur Übertragung der Schlüsseldatei gibt es für Pre-Shared Key Verbindungen verschiedene Möglichkeiten:

1. Direktes Kopieren der Schlüsseldatei auf die Gegenstelle.
   Zum Exportieren der Schlüsseldatei den Menüpunkt *Schlüsseldatei hochladen* auswählen. Über einen Dialog kann per SSH-verschlüsselter Verbindung die Schlüsseldatei auf die Gegenstelle kopiert werden. Dazu muss die IP-Adresse, der Benutzername sowie der Zielpfad auf der Gegenstelle bekannt sein. Die Datei wird dabei in das angegebene Verzeichnis des Zielservers kopiert.
2. Schlüsseldatei über Transfer-Verzeichnis exportieren und dann auf der Gegenstelle einspielen.

Zum Exportieren der Schlüsseldatei auf eine Gegenstelle, die nicht per SSH von der mp-Firewall aus erreicht werden kann, bitte den Menüpunkt Schlüsseldatei in Transfer auswählen. Über diesen Menüpunkt wird die Schlüsseldatei in das Transfer-Verzeichnis des Benutzers config geschrieben. Dabei sind die Schlüssel je nach definierter Verbindungsnummer benannt; z.B. 5.key = Key der Verbindung Nr. 5.
Um die Schlüsseldatei von der mp-Firewall zu holen wird von einem Rechner, der SSH-Zugriff auf die mp-Firewall hat, eine Verbindung als Benutzer *config* per Secure Copy (unter Windows mit dem Programm WinSCP) auf die mp-Firewall aufgebaut. Die benötigte Schlüsseldatei kann nun aus dem Verzeichnis */home/config/transfer* / kopiert werden.

Zertifikate für zertifikatsbasierte OpenVPN-Verbindungen exportieren
Zur Übertragung der Zertifikate gibt es die Möglichkeit die Klienten-Zertifikate über das Transfer-Verzeichnis zu exportieren und dann auf den Gegenstellen einzuspielen.
Zum Exportieren der Klienten-Zertifikate samt Gegenstellen-Konfiguration bitte den Menüpunkt *Klienten-Zertifikate in Transfer* auswählen. Über diesen Menüpunkt werden die Zertifikatsdateien in das Transfer-Verzeichnis des Benutzers *config* geschrieben. Dabei wird für jeden Klienten ein Ordner je nach definierter Verbindungsnummer angelegt; z.B.im Ordner 1 = Verbindungsdateien für den Klienten Nr. 1.
In dem Ordner befinden sich alle benötigten Zertifikate und Konfigurationsdateien für die Gegenstelle. Diese müssen von der mp-Firewall extrahiert werden und auf der Gegenstelle eingespielt werden. Um die Dateien von der mp-Firewall zu holen wird von einem Rechner, der SSH-Zugriff auf die mp-Firewall hat eine Verbindung als Benutzer *config* per Secure Copy (Für Windows mit dem Programm WinSCP) auf die mp-Firewall aufgebaut. Die benötigten Schlüsseldateien können nun aus dem Verzeichnis */home/config/transfer/[OpenVPN-Nummer]/[Klienten-Nummer]* kopiert werden. Am besten kopieren Sie einfach das gesamte Verzeichnis.

Einrichtung der Gegenstelle

Um die Gegenstelle für die erstelle OpenVPN-Verbindung richtig zu konfigurieren muss sicher gestellt sein, dass auf der mp-Firewall wie auch auf der Gegenstelle die entsprechenden Schlüsseldateien verwendet werden. Weiterhin sind alle Einstellungen der mp-Firewall analog auch auf der Gegenstelle vorzunehmen.

Die Einrichtung der OpenVPN-Konfiguration mit Pre-Shared Key muss für die Gegenstelle geschieht manuell. Den benötigten Schlüssel können Sie sich wie unter dem vorigen Kapitel Schlüssel- und Zertifikats-Management beschrieben von der mp-Firewall holen.

Zur Einrichtung einer Gegenstelle für eine OpenVPN-Verbindung mit Zertifikaten wird die komplette Konfiguration für die Gegenstelle von der mp-Firewall bereit gestellt. Diese kann ebenfalls wie unter Schlüssel- und Zertifikats-Management beschrieben extrahiert werden.

Eigene Firewall-Regeln

Die mp-Firewall generiert für alle Menüeinträge automatisch alle notwendigen Firewall-Regeln. Diese können jedoch um individuelle Regelsätze erweitert werden. Um eine neue Firewall-Regel zu erstellen oder eine bestehende zu konfigurieren, melden Sie sich bitte als Benutzer *config* an und wählen dann den Menüpunkt *Einstellungen>Custom Settings* aus. Dort finden Sie Untermenüs für weitere Netzwerkanschlüsse, eigene Durchleitungs-, Eingangs- und Ausgangsregeln, sowie für eigene Routingregeln.

Um eine neue Regel zu erstellen wählen Sie bitte jeweils den Menüpunkt *Neu* aus. Um eine bestehende Regel zu konfigurieren navigieren Sie bitte auf die zu ändernde Regel und wählen Sie diese aus. Es erscheint ein Menü, wo Sie einzelne Änderungen vornehmen können.

Anleitung zu Erstellung einer neuen Firewall-Durchleitungs-Regel:

- Wählen Sie bitte aus dem Custom Settings-Menü Custom Forward Rules den Menüpunkt Neu aus. Sie werden nun nach der Nummer der neuen Regel gefragt. Bitte beachten Sie, dass die Nummerierung der Regel gleichzeitig die Priorität der Ausführung festlegt.
  Die Regeln werden immer in Reihenfolge ihrer Nummern abgearbeitet, und zwar vor allen anderen FORWARDING-Regeln, aber nach den ESTABLISHED-Regeln. Das bedeutet, dass nur neue Verbindungen über diese Regeln kontrolliert werden.
  Hinweis: Es ist nicht ratsam die erste Regel mit 1 zu nummerieren, da sonst keine Regeln mehr mit höherer Priorität angelegt werden können. Beginnen Sie die Nummerierung mit 100. Die höchste erlaubte Nummer ist 1000. Sie können die Nummern selbstverständlich auch nachträglich ändern.
- Geben Sie der Regel einen Namen. Dieser sollte so gewählt werden, dass Sie an Hand des Namens erkennen können, welche Regelung Sie getroffen haben.
- Wählen Sie ein Protokoll aus, für welches die Regel gelten soll. Wenn die Regel für alle Protokolle gelten soll, so wählen Sie bitte all (Alle Pakete) aus.
- Als nächstes werden Sie nach der IP-Adresse des Absenders der Pakete gefragt. Die IP-Adresse wird in der Form a.b.c.d/validbits angegeben. Wenn Sie diese Eingabe leer lassen, gilt die Regel für alle Absender.
  Beispiel:

Adressen im Netzwerk	IP-Adresse	Valid Bits	Eintragung in Firewall-Regel
0.0.0.1 – 255.255.255.254	alle	0	0.0.0.0/0 oder leer
192.0.0.1 bis 192.255.255.254	192.0.0.1	8	192.0.0.1/8
192.168.0.1 bis 192.168.255.254	192.168.1.1	16	192.168.0.1/16
192.168.0.1 bis 192.168.0.254	192.168.0.1	24	192.168.0.1/24
192.168.7.12	192.168.7.12	32	192.168.7.12/32 oder 192.168.7.12

- Im nächsten Eingabefeld werden Sie nach der IP-Adresse des Empfängers gefragt. Tragen Sie diese bitte in analoger Form zur Absender IP-Adresse ein. Wenn Sie diese Eingabe leer lassen, gilt die Regel für alle Empfänger.
- Absender-Ports für das jeweilige Protokoll. Wenn Sie diese Eingabe leer lassen, gilt die Regel für alle Absender-Ports. Einige Protokolle kennen keine Ports, dort werden keine Ports abgefragt.

- Empfänger Ports für das jeweilige Protokoll. Wenn Sie diese Eingabe leer lassen, gilt die Regel für alle Empfänger-Ports.
- Bitte die Regelwirkung auswählen. Folgende Behandlungsweisen stehen zur Auswahl:
  - Accept » Alle Pakete werden durchgelassen
  - Drop » Die Pakete werden ignoriert und fallen gelassen
  - Reject » Die Pakete werden zurückgewiesen
  - Log » Die Pakete werden protokolliert, jedoch nur die Pakete, die eine neue Verbindung öffnen. Achtung: Bei der Wirkung Log geht es anschließend weiter zur nächsten Regel!
  - Redirect (nur Input-Regel für tcp und udp): Umleitung auf einen lokalen Port, z.B. für transparente Proxies.

Wenn Sie Pakete protokollieren und dann ablehnen möchten, benötigen Sie zwei Regeln: Die erste Regel protokolliert, die zweite lehnt ab.

ACHTUNG: Wenn Sie alle Einstellungen vorgenommen haben, verlassen Sie das Menü. Speichern Sie nun alle Änderungen über den Menüpunkt *Speichern* ab und wenden Sie diese mit dem Menüpunkt *Sanft Anwenden* an. Erst nach dem Anwenden werden die Einstellungen wirksam.