

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 als OpenVPN-Gateway nutzt, der hat schon eine CA erstellt.

Ansonsten zum Erstellen einer CA wie folgt vorgehen:

System: Certificate Authority Manager ?

CA's Certificates Certificate Revocation

Descriptive name:

Method:

Internal Certificate Authority

Key length: bits

Digest Algorithm:
NOTE: It is recommended to use an algorithm stronger than SHA1 when possible.

Lifetime: days

Distinguished name

Country Code: ex: DE

State or Province: ex: Texas

City: ex: Austin

Organization: ex: My Company Inc.

Email Address: ex: admin@mycompany.com

Common Name: ex: internal-ca

pfSense is © 2004 - 2013 by Electric Sheep Fencing LLC. All Rights Reserved. [\[view license\]](#)

2. Konfiguration als VPN-Client mit OpenVPN

Hier wird der OpenVPN-Client der pfSense analog zu den erhaltenen 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.

Diagnosics → 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!

Diagnosics: Edit file



```
-----BEGIN CERTIFICATE-----
MIIHtCCBbGgAwIBAgIBATANBgkqhkiG9w0BAQUFADB9MQswCQYDVQQGEwJJTDEW
MBQGA1UEChMNU3RhcncRDb20gTHRkLjErMCKGA1UECxMiU2VjdXJlIERpZ2l0YWw
Q2VydGlmawNhdGUGU2lnbmLuZzEpMCCGA1UEAxMgU3RhcncRDb20gQ2VydGlmawN
dGlvbiBBdXR0b3JpdHkwHhcNMDYwOTE3MTk0NjM2WhcNMzYwOTE3MTk0NjM2WjB9
MQswCQYDVQQGEwJJTDEWMBQGA1UEChMNU3RhcncRDb20gTHRkLjErMCKGA1UECxMi
U2VjdXJlIERpZ2l0YWwQ2VydGlmawNhdGUGU2lnbmLuZzEpMCCGA1UEAxMgU3Rhc
ncRDb20gQ2VydGlmawNhdGlvbiBBdXR0b3JpdHkwGgIiMA0GCsQGSIB3DQEBAQUA
A4ICDwAwggIKAoICAQDBiNsJvGxGFHiflXuIM5DycmLWwTYgIiRezUl38kMKogZk
pMy0Nvg45iPwbm2xPN1yo4UcodM9tDMR0y+v/uqwQVlntsQGfQqedIXWeUyAN3rf
OQVSwff0G0ZDPnkFhdLdcfN1YjS6LIp/Ho/u7TTQeEceWzVI9ujPW3U3eCztKS5/C
Ji/6tRYccjV3yjd5srhJosannZcAdt0FCX+7bWgiA/deMothWeXMAEtCnn6RtYT
Kqi5pquDSR3l8u/d5AG0GAqPYIMWhWkPdhk6zLVmvsJrdAfkk+F2PrRt2PZE4XNI
HzvEvqBTViVsUqn3qqvKv3b9bZvzndu/Pwa8DFaqr5hIlTpL36dYUNK4dalb6kMM
Av+Z6+hsTXBbKwWc3apdzK8BMewM69KN60qce+Zu9ydmDBpI125C4z/eIT574Q1w
+20qqGwaVLRcJXRJosmLfqa7LH4XXgVNWG4SHQHuehANxjJ/GP/89PrNbpHoNkm+
GkhpI8KwTRoSsmkXwQqQ1vp5Iki/untp+HJDH+no32NgN0nZPV/+Qt+0R0t3vwmC3
Zzrd/qqc8NSLf3Iizsaf17b4r4qqEKjZ+xjGtrVcUiyJthkqcwEKDw0zEmDyei+B
26Nu/yYwL/WL3YLXtq09s68rxbd2AvCl1iuaahhQqcvbjm4xdCUst37uMdBN5SwID
AQABo4ICUjCCAk4wDAYDVROTBaUwAwEB/zALBgnVHQ8EBAMCa4wHQYDVR00BBYE
FE4L7xqkQFuLF2mHMMo0aEPQ0a7yMGQGA1UdHwRdMFswLKAQoCiGJmh0dHA6Ly9j
ZXJ0LnN0YXJ0Y29tLm9yZy9zZnNjYS1jcmwuY3J3sMCugKaAnhiVodHRwOi8vY3J3
LnN0YXJ0Y29tLm9yZy9zZnNjYS1jcmwuY3J3sMIIBXQYDVROGBIIBVDCCAVAwggFM
BgsrBgEEAYG1NwEBATCCATswLwYIKwYBBQUHAgEWI2h0dHA6Ly9jZXJ0LnN0YXJ0
Y29tLm9yZy9zZnNjYS1jcmwuY3J3kucGRmMDU0GCCsGAQUFBwIBFiLodHRwOi8vY2VydC5zdGFy
dGlvbS5vcncvaW50ZXJtZWRRYXRLLnBkZjZjCB0AYIKwYBBQUHAgIwgcMwJxYU3Rhc
ncQ29tbnV5Y2lhbC AoU3RhcncRDb20pIEEx0ZC4wAwIBARqBl0xpbwL0ZWQgTGlh
YmlsaXR5LDBYjZWFkIHRoZSBzZWNoaW9uICpMZWhhbCBMaW1pdGF0aW9ucyogb2Yg
dGhlIFN0YXJ0Y29tIENlcnRpZmljYXRpb24gQXV0aG9yaXR5IFBvbGJjeSBhdFp
bGFiGUGYXQgaHR0cDovL2NlcnQuc3RhcncRDb20ub3JnL3BvbGJjeS5wZGYwEQYJ
YIZIAyb4QgEBBAQDAgAHMdgGCWCGSAGG+EIBDQQRFltdGFyYENvbnRlbnQvLm9yZy9z
ZnNjYS1jcmwuY3J3Zm90aW9uIEF1dGhvcml0eTANBgkqhkiG9w0BAQUFAAOCAGeAFmyZ
9GYMNPXQhV59CuzaEE44HF7fpiUFS5Eyweg78T3dRALbB0mKKctmArexmvclmAk8
jhvh3TaHK0u7aNM5Zj2gJsfy0ZEdUauCe37Vzlrk4gNXcGmXCPLewKYK34wGmkUW
FjgKXlf2Ysd6AgXmvB618p70qSmD+LIU424oh0TDkBre0Kk8rENNEX03SipXPJz
ewT4F+irsfMuXGRucZ6E6Eri8sxHkfy+BUZo7jYn0TZNmezWd7d0aHRzrZVD1oNB1
ny+v80qCQ5j4aZyJecRDjkZy42Q2Eq/3JR44iZB3fsNrnDy0RLrHiQi+fHLB5L
EUTINFInzQpdn4XBidUaePKVEFMy3YCEZnXZTgwo+2EuvoSoOMCZEoalHmdkrQYU
L6lwhceWD3jZzfwQ100q92lgDMUYMA0yZZwLKM59R9Ie70cfmu3nZD0Ijuu+Pwq
wvUldDvraTvkLrBtfa1i6w0tiYiRKGHIHVkt+VQF0a4DGTAM+L11AYSiCM7wRUC
```

in-berlin.auth

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

Diagnostics: Edit file



Save / Load from path:

```
SITENAME@in-vpn.de
unheimlichesPassw0rt|
```

in-berlin.tls-auth

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

Diagnostics: Edit file



Save / Load from path:

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
790e0fc1dlacc59f6c3b51f4e67eb5e9
8ae0600608f0b036dbcd471f262ba95b
c86e0ab12689c4ac287bc3e51ce64b31
2f205e59034aef1e89f7d55cd04385fb
ee6072f5cb0cad81f573f7f73fdc9150
2bbda2abd827f2cf31d906d922127409
010cefe3a28568f5bc19c148bf81bd07
f90a8395cd3be7967b2a7adb0d6932f3
49dda7d806461ed41d5a689823a27814
688a1252c42a587a4efdeb9f3ae84c75
d8f79ac5ad3c4741bfe8fa89ff2c0789
9868bfe78c4baca3dd596193253ff45b
2c42c30257ce5f5cc375c6922bb8b7c1
c607f4ae22e3295dd4263e179f18c705
d288e1f71afd084abd5a019adee1a9ac
0690d7fcf4de1334204841b95651110e
-----END OpenVPN Static key V1-----
```

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.

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:

```
remote openvpn2.in-berlin.de;
remote openvpn3.in-berlin.de;
mute-replay-warnings;
persist-tun;
persist-key;
ca /conf/startssl-chain.crt;
comp-lzo;
verify-x509-name openvpn.in-berlin.de name;
auth-user-pass /conf/in-berlin.auth;
tls-auth /conf/in-berlin.tls-auth;
```

Enter any additional options you would like to add to the OpenVPN client configuration here, separated by a semicolon
EXAMPLE: remote server.mysite.com 1194; or remote 1.2.3.4 1194;

Save

Wichtig: 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

| Interface | Network port |
|------------|-------------------------|
| TELEKOM | PPPOE1(ue0) - t-offline |
| LAN | vr0 (00:0d:b9:0d:85:a0) |
| BERLIN | PPPOE2(ue0) - in-berlin |
| BERLIN VPN | ovpnc2 () |
| OPT3 | ovpnc2 () |

Save

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.

Interfaces: **BERLIN_VPN**



General configuration

Enable **Enable Interface**

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC address
This field can be used to modify ("spoof") the MAC address of this interface (may be required with some cable connections)
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

MTU
If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.

MSS
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

Private networks

Block private networks
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.

Block bogon networks
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive.

Note: The update frequency can be changed under System->Advanced Firewall/NAT settings.

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

System: Gateways: Edit gateway group



Edit gateway group entry

| Group Name | <input type="text" value="InternetRouting"/> Group Name | | | | | | | | | | | | | | | | |
|-------------------------|---|-------------------|------------------------------------|------------|-------------|--------------|-------|-------------------|--------------------------------|---------------|--------|-------------------|--|------------------|--------|-------------------|------------------------------------|
| Gateway Priority | <table border="1"><thead><tr><th>Gateway</th><th>Tier</th><th>Virtual IP</th><th>Description</th></tr></thead><tbody><tr><td>BERLIN_PPPOE</td><td>Never</td><td>Interface Address</td><td>Interface BERLIN_PPPOE Gateway</td></tr><tr><td>TELEKOM_PPPOE</td><td>Tier 1</td><td>Interface Address</td><td></td></tr><tr><td>BERLIN_VPN_VPNV4</td><td>Tier 2</td><td>Interface Address</td><td>Interface BERLIN_VPN_VPNV4 Gateway</td></tr></tbody></table> <p>Link Priority The priority selected here defines in what order failover and balancing of links will be done. Multiple links of the same priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted we will use the next available link(s) in the next priority level.</p> <p>Virtual IP The virtual IP field selects what (virtual) IP should be used when this group applies to a local Dynamic DNS, IPsec or OpenVPN endpoint</p> | Gateway | Tier | Virtual IP | Description | BERLIN_PPPOE | Never | Interface Address | Interface BERLIN_PPPOE Gateway | TELEKOM_PPPOE | Tier 1 | Interface Address | | BERLIN_VPN_VPNV4 | Tier 2 | Interface Address | Interface BERLIN_VPN_VPNV4 Gateway |
| Gateway | Tier | Virtual IP | Description | | | | | | | | | | | | | | |
| BERLIN_PPPOE | Never | Interface Address | Interface BERLIN_PPPOE Gateway | | | | | | | | | | | | | | |
| TELEKOM_PPPOE | Tier 1 | Interface Address | | | | | | | | | | | | | | | |
| BERLIN_VPN_VPNV4 | Tier 2 | Interface Address | Interface BERLIN_VPN_VPNV4 Gateway | | | | | | | | | | | | | | |
| Trigger Level | <input type="text" value="Member Down"/> When to trigger exclusion of a member | | | | | | | | | | | | | | | | |
| Description | <input type="text"/> You may enter a description here for your reference (not parsed). | | | | | | | | | | | | | | | | |

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.