HowTo – IPSec Roadwarrior mit PSK

Dieses Beispiel zeigt, wie zwei Netze via IPSec unter Verwendung eines Preshared Key miteinander verbunden werden, um beispielsweise eine Aussenstelle an eine Firmenzentrale anzubinden.

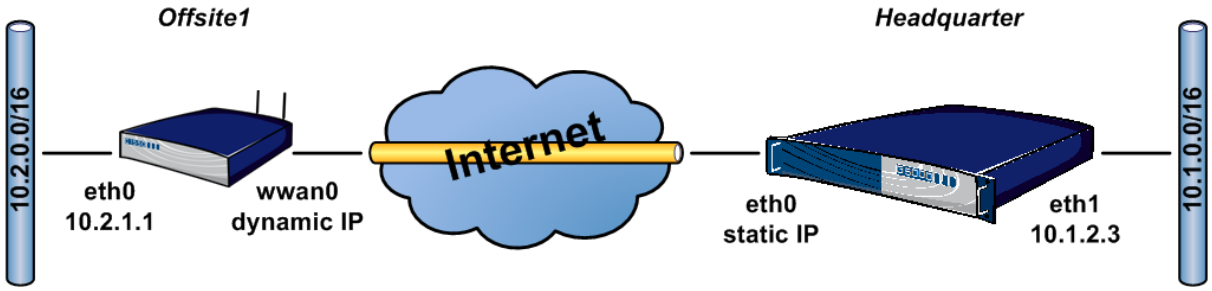

Abbildung 1: Beispiel Netzplan

1 IPSec Konfiguration auf der Zentralseite

Auf der Zentralseite wird von einer festen IP (z.B. CompanyConnect) an der Netzwerkschnittstelle ***eth0*** ausgegangen. Wird ein anders Interface verwendet muss dieses unter ***Networking > IPSec VPN > Global Settings*** angepasst werden. Dazu wird bei den IPSec-Interface-Mappings ***Use ipsec0 as defaultroute*** auf ***No*** gestellt und im Dropdownmenü ***Bind ipsec0 to*** die verwendete Schnitstelle ausgewählt.

1.1 Template erstellen

Auf der Zentralseite empfielt sich für die IPSec Konfiguration die Verwendung von Templates.

> Hinweis
> ➢ Templates vereinfachen die Konfiguration, da hier immer wiederkehrende Parameter global gesetzt werden können.

Um ein IPSec Template zu erstellen navigiert man in das Menü ***Networking > IPSec VPN*** und klickt dort auf den Button ***[Add Template]***.

In diesem Beispiel wurde die Konfiguration wie dem Screenshot und den Tabellen zu entnehmen ist, erstellt.

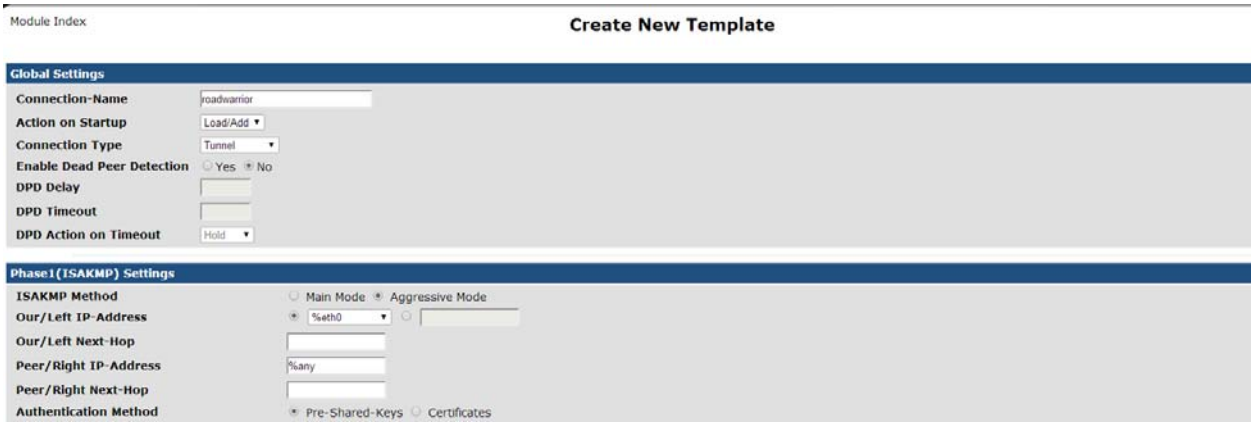

Abbildung 2: IPSec Template

1.1.1 Global Settings

Parameter	Wert
Connection-Name	roadwarrior
Action on Startup	Load/Add
Connection Type	Tunnel

1.1.2 Phase1(ISAKMP) Settings

Parameter	Wert
ISAKMP Method	Aggressive Mode
Our/Left IP-Address	%eth0
Peer/Right IP-Address	%any

1.1.2.1 IKE Settings

Parameter	Wert	
IKE algorithms	**Encryption:**	aes128
	Authentication:	sha1
	MODP-Group:	1024
IKE Lifetime	8h	

1.1.3 Phase2 Settings

Parameter	Wert	
Encapsulating Security Payload (ESP)	**Encryption:**	aes128
	Authentication:	sha1
	PFS-Group:	modp1024

Parameter	Wert	
SA Lifetime	8	hours

Mittels des ***[Create]*** Buttons wird das Template erstellt.

1.2 IPSec Verbindung mit Template erstellen

Um eine Verbindung unter Verwendung eines Templates zu erstellen, gibt es zwei Möglichkeiten.

Entweder man benutzt den ***Add Connection*** Link der am Ende der Tabellenzeile des gewünschten Templates steht, oder man wählt in dem DropDown Menü neben dem ***[Add Connection]*** Button das entsprechende Template aus.

> Hinweis
> ➢ Die Konfigurationsseite der Verbindung unterscheidet sich nicht von der Template Seite, allerdings werden die Parameter, die im Template gesetzt wurden, ausgegraut.

1.2.1 Global Settings

Parameter	Wert
Connection-Name	offsite1

1.2.2 Phase1(ISAKMP) Settings

Parameter	Wert
Our/Left ID	@headquarter_id
Peer/Right ID	@offsite1_id Achtung! ➢ muss für jeden Tunnel eindeutig sein

1.2.2.1 PSK-Settings

Parameter	Wert
Pre-Shared-Key	In diesem Feld den zu verwendenden PSK eintragen
Confirm Pre-Shared-Key	Hier den PSK zum verifizieren eintragen

1.2.1 Phase2 Settings

Parameter	Wert
Local Subnet	10.1.0.0/16 Achtung! ➢ muss für jeden Endpunkt eindeutig sein
Local Source IP	10.1.2.3
Remote Subnet	10.2.0.0/16 Achtung! ➢ muss für jeden Endpunkt eindeutig sein
Remote Source IP	10.2.1.1

Durch drücken des ***[Create]*** Buttons die Einstellungen Speichern.

1.3 IPSec Server starten

Im Menü ***Networking > IPSec VPN*** wird der Server mit dem Button ***[Start IPSec Server]*** gestartet.

Damit der IPSec auch nach einem Neustart aktiviert wird, wählt man bei ***[Start at boot time]*** ***yes*** und übernimmt diese Einstellung durch drücken des Buttons.

2 IPSec Konfiguration Aussenstelle

In diesem Anwendungsbeispiel ist die Aussenstelle über ppp0 unter Verwendung des Connection-Managers online. Der IPSec Tunnel nutzt die bestehende Verbindung und wird durch den Connection-Manager gestartet.

2.1 IPSec Interface Mapping

Unter dem Menüpunkt ***Networking > IPSec VPN > Global Settings*** wird der Parameter ***Use ipsec0 as defaultroute*** auf ***Yes*** gesetzt und die Änderung gespeichert.

2.2 IPSec Verbindung erstellen (ohne Template)

Bei der Aussenstellenkonfiguration ist es nicht nötig mit Templates zu arbeiten, darum wird in diesem Beispiel auf ein Template verzichtet.

Im Menü ***Networking > IPSec VPN*** auf den Button ***[Add Connection]*** klicken um die Verbindung anzulegen.

2.2.1 Global Settings

Parameter	Wert
Connection-Name	offsite1
Action on Startup	Ignore
Connection Type	Tunnel
Enable Dead Peer Detection	Yes
DPD Delay	30
DPD Timeout	120
DPD Action on Timeout	Clear

2.2.2 Phase1(ISAKMP) Settings

Parameter	Wert
ISAKMP Method	Aggressive Mode
Our/Left IP-Address	%ppp0
Peer/Right IP-Address	Öffentiche IP von headquater
Our/Left ID	@offsite1_id
Peer/Right ID	@headquarter_id

2.2.2.1 PSK-Settings

Parameter	Wert
Pre-Shared-Key	In diesem Feld den zu verwendenden PSK eintragen
Confirm Pre-Shared-Key	Hier den PSK zum verifizieren eintragen

2.2.2.2 IKE Settings

Parameter	Wert	
IKE algorithms	**Encryption:**	aes128
	Authentication:	sha1
	MODP-Group:	1024
IKE Lifetime	8h	

2.2.3 Phase2 Settings

Parameter	Wert	
Local Subnet	10.2.0.0/16 Achtung! ➢ muss für jeden Endpunkt eindeutig sein	
Local Source IP	10.2.1.1	
Remote Subnet	10.1.0.0/16 Achtung! ➢ muss für jeden Endpunkt eindeutig sein	
Remote Source IP	10.1.2.3	
Encapsulating Security Payload (ESP)	**Encryption:**	aes128
	Authentication:	sha1
	PFS-Group:	modp1024
SA Lifetime	8	hours

[Create] übernimmt die eingestellten Parameter.

2.3 IPSec mit dem Connection-Manager starten

Um die IPSec Verbindung über den Connection-Manager zu starten, öffnet man den Connection-Manager Eintrag, der das PPP-Interface verwaltet. In diesem Beispiel ist das ***Networking > Connection Management > Connection-Manager > Index 1***.

Hier wird in etwa in der Seitenmitte bei dem Parameter Use IPSec-Interface das verwendete Interface angepasst.

Parameter	Wert
Use IPSec-Interface	ipsec0 as defaultroute

Am Ende dieser Seite unter dem Punkt ***Logical Subordinated Connections*** wird der Button ***[Add Connection]*** gedrückt und eine Verbindung hinzugefügt.

Auf der Konfigurationsseite wird nun lediglich die angelegte IPSec Verbindung ausgewählt und die Parameter wie folgt gesetzt.

Abbildung 3: Connection-Manager - logische Verbindung

Parameter	Wert
Power Up Delay	2
Maximum Negotiation Timeout	15

Mit ***[Create]*** Speichern.

3 Firewall Regeln

Aus Sicherheitsgründen sollte der Zugriff von Aussen (aus dem Internet) auf die Router beschränkt werden.

> Achtung!
> ➢ Es ist zwingend erforderlich, dass der Zugriff über die lokal verwendete(n) Schnittstelle(n) erlaubt ist, da man sich sonst aussperrt.

Dazu wechselt man in das Menü ***Networking > Linux Firewall > Showing IPtable: Packet filtering (filter)***.

In dem Bereich ***Incoming packets (INPUT)*** werden mit ***[Add Rule]*** die Regeln mit den Parametern wie in den Tabellen hinzugefügt und mit ***[Create]*** angelegt.

Action to take	Comment	Network protocol	Destination TCP or UDP port
Accept	Allow Encapsulating Security Payload (ESP)	Equal – ESP	–
Accept	Allow Internet Key Exchange (IKE)	Equal – UDP	Port(s): 500
Accept	Allow NAT traversal (NAT-T)	Equal – UDP	Port(s): 4500

Action to take	Comment	Incoming interface
Accept	Allow traffic on ipsec0 interface	Equals –other - ipsec0

Nach Erstellen der Regeln werden die Einstellungen mit ***[Apply Configuration]*** übernommen.

3.1 Firewall Einstellungen Zentralseite

Eine Firewall die von aussen nur in IPSec verwendete Protokolle und Ports verwendet, könnte wie in dem Screenshot gezeigt aussehen.

Abbildung 4: Zentralseitige Firewall

3.2 Firewall bei der Aussenstelle

Wird der Router auch als Internet Gateway verwendet, benötigt man eine Established/Related und eine Masquerading Regel für das Öffentliche Interface, ansonsten genügt es das lokale Interface zu erlauben.

3.2.1 Established/Related Regel

Im Menü ***Networking > Linux Firewall > Showing IPtable: Packet filtering (filter)*** wird im Bereich ***Incoming packets (INPUT)*** mit ***[Add Rule]*** folgende Regel hinzugefügt.

Action to take	Comment	Connection states
Accept	Allow traffic if established or related	Equals – ESTABLISHED und RELATED Mehrfachauswahl ***[STRG]***+Klick

Abbildung 5: Aussenstellen Router, gleichzeitig Internet Gateway

3.2.2 Masquerading

Das Masquerading konfiguriert man unter ***Networking > Linux Firewall > Showing IPtable: Network address translation (nat)*** im Bereich ***Packets after routing (POSTROUTING)***.

Action to take	Outgoing interface
Masquerade	Equals – Other – ppp0 (hier das verwendete Interface eintragen)

Abbildung 6: Masquerading am Aussenstellen Router

4 Konfiguration abschließen

Um die Konfiguration abzuschließen, ist es nötig, die durchgeführten Änderungen dauerhaft zu speichern. Dazu wechselt man auf die Seite ***Permanent Save*** und drückt auf ***Save Config***.

> Achtung!
> ➢ Um die Änderungen dauerhaft zu übernehmen ist es nötig ***Permanent Save > Save Config*** auszuführen, da die Einstellungen sonst bei einem Router-Neustart verloren gehen.

5 Logfileauszug

Nachfolgend Logfileauszüge von einem erfolgreichen IPSec Verbindungsaufbau.

Verbindungsaufbau bei der Aussenstelle:

```
Jan 21 10:11:12 C1500 pluto[5372]: added connection description "offsite1"
Jan 21 10:11:12 C1500 pluto[5372]: "offsite1" #10: initiating Aggressive Mode #10,
connection "offsite1"
Jan 21 10:11:13 C1500 pluto[5372]: "offsite1" #10: received Vendor ID payload [Dead Peer
Detection]
Jan 21 10:11:13 C1500 pluto[5372]: "offsite1" #10: received Vendor ID payload [RFC 3947]
method set to=109
Jan 21 10:11:13 C1500 pluto[5372]: "offsite1" #10: Aggressive mode peer ID is ID_FQDN:
'@headquarter_id'
Jan 21 10:11:13 C1500 pluto[5372]: "offsite1" #10: NAT-Traversal: Result using RFC 3947
(NAT-Traversal): no NAT detected
Jan 21 10:11:13 C1500 pluto[5372]: "offsite1" #10: transition from state STATE_AGGR_I1 to
state STATE_AGGR_I2
Jan 21 10:11:13 C1500 pluto[5372]: "offsite1" #10: STATE_AGGR_I2: sent AI2, ISAKMP SA
established {auth=OAKLEY_PRESHARED_KEY cipher=aes_128 prf=oakley_sha group=modp1024}
Jan 21 10:11:13 C1500 pluto[5372]: "offsite1" #10: Dead Peer Detection (RFC 3706): enabled
Jan 21 10:11:13 C1500 pluto[5372]: "offsite1" #11: initiating Quick Mode
PSK+ENCRYPT+TUNNEL+PFS+DONTREKEY+UP+AGGRESSIVE+IKEv2ALLOW {using isakmp#10 msgid:fe8d1e4a
proposal=AES(12)_128-SHA1(2)_160 pfsgroup=OAKLEY_GROUP_MODP1024}
Jan 21 10:11:14 C1500 pluto[5372]: "offsite1" #11: Dead Peer Detection (RFC 3706): enabled
Jan 21 10:11:14 C1500 pluto[5372]: "offsite1" #11: transition from state STATE_QUICK_I1 to
state STATE_QUICK_I2
Jan 21 10:11:14 C1500 pluto[5372]: "offsite1" #11: STATE_QUICK_I2: sent QI2, IPsec SA
established tunnel mode {ESP=>0x08427414 <0x881c46b2 xfrm=AES_128-HMAC_SHA1 NATOA=none
NATD=none DPD=enabled}
Jan 21 10:11:15 C1500 Connection_Manager[30781]: Connection-Entry 1, Logical-Entry 1:
IPSec-connection established successfully!
```

Verbindungsaufbau auf der Zentralseite:

```
Jan 21 10:11:12 C1500 pluto[26437]: packet from 80.187.0.141:500: received Vendor ID
payload [Dead Peer Detection]
Jan 21 10:11:12 C1500 pluto[26437]: packet from 80.187.0.141:500: received Vendor ID
payload [RFC 3947] method set to=109
Jan 21 10:11:12 C1500 pluto[26437]: packet from 80.187.0.141:500: received Vendor ID
payload [draft-ietf-ipsec-nat-t-ike-03] meth=108, but already using method 109
Jan 21 10:11:12 C1500 pluto[26437]: packet from 80.187.0.141:500: received Vendor ID
payload [draft-ietf-ipsec-nat-t-ike-02_n] meth=106, but already using method 109
Jan 21 10:11:12 C1500 pluto[26437]: packet from 80.187.0.141:500: received Vendor ID
payload [draft-ietf-ipsec-nat-t-ike-02] meth=107, but already using method 109
Jan 21 10:11:12 C1500 pluto[26437]: packet from 80.187.0.141:500: received Vendor ID
payload [draft-ietf-ipsec-nat-t-ike-00]
Jan 21 10:11:12 C1500 pluto[26437]: "offsite1"[1] 80.187.0.141 #1: Aggressive mode peer ID
is ID_FQDN: '@offsite1_id'
Jan 21 10:11:12 C1500 pluto[26437]: "offsite1"[1] 80.187.0.141 #1: responding to
Aggressive Mode, state #1, connection "offsite1" from 80.187.0.141
Jan 21 10:11:12 C1500 pluto[26437]: "offsite1"[1] 80.187.0.141 #1: enabling possible NAT-
traversal with method 4
Jan 21 10:11:12 C1500 pluto[26437]: "offsite1"[1] 80.187.0.141 #1: transition from state
STATE_AGGR_R0 to state STATE_AGGR_R1
Jan 21 10:11:12 C1500 pluto[26437]: "offsite1"[1] 80.187.0.141 #1: STATE_AGGR_R1: sent
AR1, expecting AI2
Jan 21 10:11:13 C1500 pluto[26437]: "offsite1"[1] 80.187.0.141 #1: NAT-Traversal: Result
using RFC 3947 (NAT-Traversal): no NAT detected
Jan 21 10:11:13 C1500 pluto[26437]: "offsite1"[1] 80.187.0.141 #1: transition from state
STATE_AGGR_R1 to state STATE_AGGR_R2
Jan 21 10:11:13 C1500 pluto[26437]: "offsite1"[1] 80.187.0.141 #1: STATE_AGGR_R2: ISAKMP
SA established {auth=OAKLEY_PRESHARED_KEY cipher=aes_128 prf=oakley_sha group=modp1024}
Jan 21 10:11:13 C1500 pluto[26437]: "offsite1"[1] 80.187.0.141 #1: Dead Peer Detection
(RFC 3706): enabled
Jan 21 10:11:13 C1500 pluto[26437]: "offsite1"[1] 80.187.0.141 #1: the peer proposed:
10.1.0.0/16:0/0 -> 10.2.0.0/16:0/0
Jan 21 10:11:13 C1500 pluto[26437]: "offsite1"[1] 80.187.0.141 #2: responding to Quick
Mode proposal {msgid:d7e38d27}
Jan 21 10:11:13 C1500 pluto[26437]: "offsite1"[1] 80.187.0.141 #2:     us:
10.1.0.0/16===62.123.231.12<%eth0>[@headquarter_id,+S=C]
Jan 21 10:11:13 C1500 pluto[26437]: "offsite1"[1] 80.187.0.141 #2:   them:
80.187.0.141[@offsite1_id,+S=C]===10.2.0.0/16
Jan 21 10:11:13 C1500 pluto[26437]: "offsite1"[1] 80.187.0.141 #2: transition from state
STATE_QUICK_R0 to state STATE_QUICK_R1
Jan 21 10:11:13 C1500 pluto[26437]: "offsite1"[1] 80.187.0.141 #2: STATE_QUICK_R1: sent
QR1, inbound IPsec SA installed, expecting QI2
Jan 21 10:11:13 C1500 pluto[26437]: "offsite1"[1] 80.187.0.141 #2: up-client output:
/usr/local/lib/ipsec/_updown.klips: changesource `ip route change 10.2.0.0/16 dev ipsec0
src 10.1.2.3' failed (RTNETLINK answers: No such file or directory)
Jan 21 10:11:13 C1500 pluto[26437]: "offsite1"[1] 80.187.0.141 #2: Dead Peer Detection
(RFC 3706): enabled
Jan 21 10:11:13 C1500 pluto[26437]: "offsite1"[1] 80.187.0.141 #2: transition from state
STATE_QUICK_R1 to state STATE_QUICK_R2
Jan 21 10:11:13 C1500 pluto[26437]: "offsite1"[1] 80.187.0.141 #2: STATE_QUICK_R2: IPsec
SA established tunnel mode {ESP=>0x881c46b4 <0x20ec795f xfrm=AES_128-HMAC_SHA1 NATOA=none
NATD=none DPD=enabled}
```

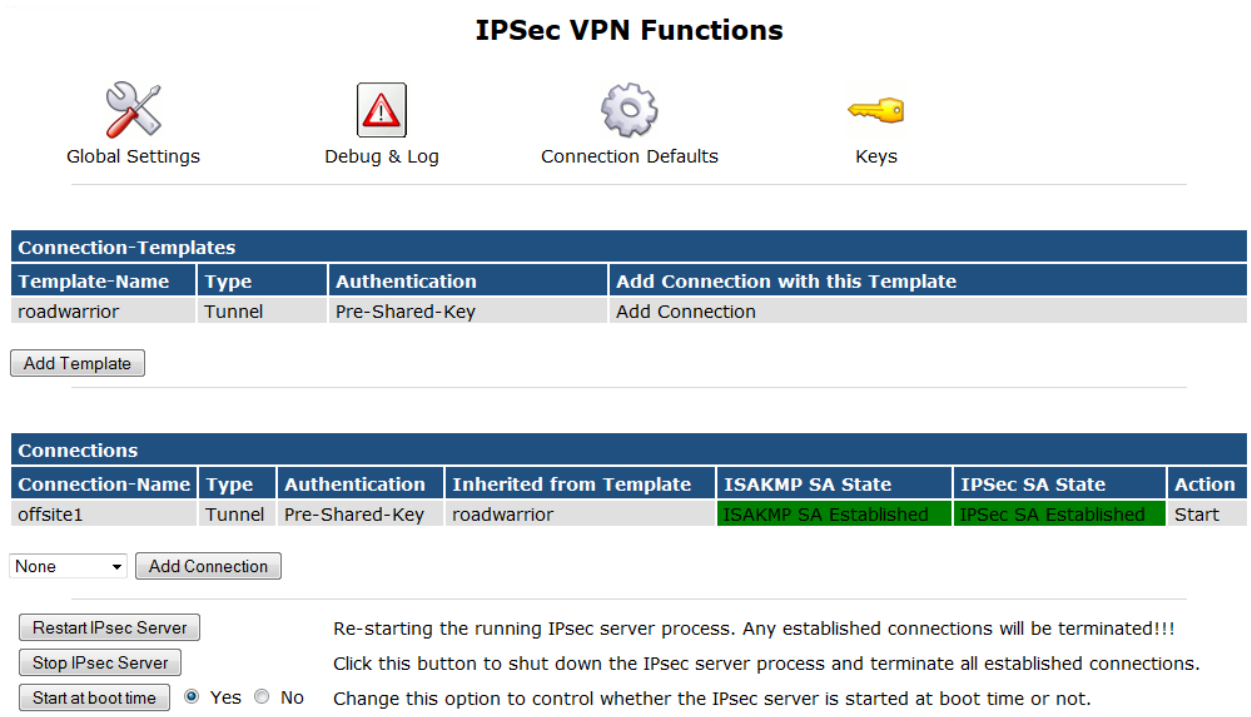

Abbildung 7: IPSec erfolgreich aufgebaut (Zentralseite)