HowTo – IPsec Site-2-Site-PSK

Dieses Beispiel zeigt, wie zwei Netze via IPsec unter Verwendung eines Pre-Shared Key miteinander verbunden werden, um beispielsweise eine **Außenstelle** an eine Firmenzentrale (**Zentrale**) anzubinden.

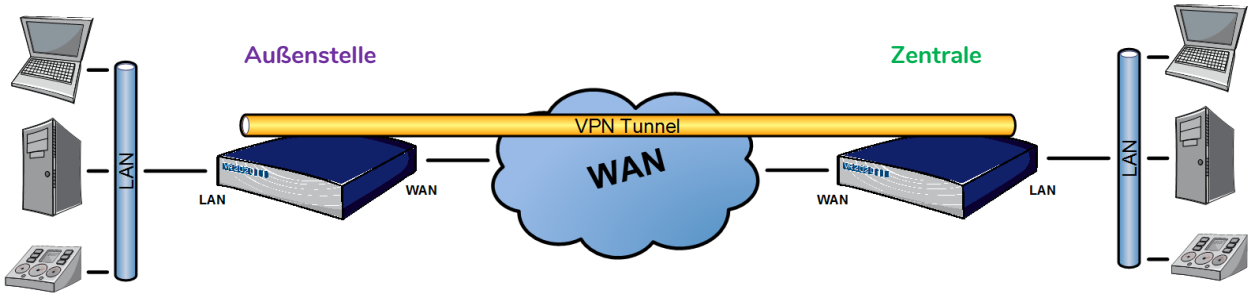

Abbildung 1: Netzplan-Beispiel

Hinweis

- In diesem Beispiel werden zwei VR2020 mittels **WAN**-Schnittstelle direkt miteinander verbunden. Die Verbindung kann natürlich auch über jeden anderen WAN-Weg etabliert werden, so sich die Geräte erreichen können.
- Außenstelle mit ***wechselnder IP*** an Schnittstelle **WAN** und ***192.168.1.50/24*** an **LAN**.
- Zentrale hat die IP ***10.99.99.1*** an Schnittstelle **WAN** und ***192.168.0.50/24*** an **LAN**.

1 Firewall anpassen

Um den Tunnelaufbau und die Datenkommunikation erfolgreich durchführen zu können sind noch Änderungen an der Firewall nötig. Diese werden im Menü ***Netzwerk*** > ***Firewall*** durchgeführt.

1.1 Verkehrsregeln

Hier wird auf den Tab **Verkehrsregeln** gewechselt und die drei bestehenden IPsec-Regeln aktiviert. Dazu wird bei den Einträgen ***Allow-IPsec-ESP-Input***, ***Allow-IPsec-IKE-Input*** und ***Allow-IPsec-NAT-T-Input*** das Häkchen in der Spalte **Aktivieren** gesetzt und die Änderung `Speichern & Anwenden` übernommen.

2 IPsec-Instanz hinzufügen

Hinweis

- Die angegebenen Parameter gelten, wenn nicht explizit anders angegeben, für beiden Seiten.

Auf der Konfigurationsseite **Dienste** > **IPSec** wird in dem Eingabefeld ein Name für den Tunnel eingegeben und der Button `Hinzufügen` gedrückt. Daraufhin erscheint eine Instanz in der Verbindungsübersicht. Um die neu angelegte Instanz zu konfigurieren wird `Bearbeiten` gewählt.

2.1 General

Auf der Seite **General** wird der Parameter **auto** bei der Außenstelle auf den Wert ***start*** eingestellt. Auf dem Router in der Zentrale wird hier ***add*** gewählt.

Um den Tunnel stabil aufgebaut zu halten, werden noch die Parameter ***closeaction*** (Aktion nachdem der Tunnel von der Gegenseite abgebaut wird), ***dpdaction*** (Dead Peer Detection: Aktion, wenn der Partner nicht ereichbar ist) und in der Außenstelle ***keyingtries*** (Anzahl der Aufbauversuche) hinzugefügt und konfiguriert.

Bei **closeaction** und **dpdaction** wird an der Außenstelle ***restart***, und am Router der Zentrale ***hold*** gewählt. Für DPD werden dann die default Werte **dpddelay** ***30*** Sekunden und **dpdtimeout** ***150*** Sekunden verwendet.

Die **keyingtries** werden am Router der Außenstelle auf ***%forever*** konfiguriert, dass entsprechend fortlaufend versucht wird den Tunnel aufzubauen.

Die Änderung wird mit `Speichern` übernommen.

2.2 Phase 1

Bei Phase 1 wird **authby** auf ***psk*** oder ***secret*** geändert. Beide Werte stehen für Pre-Shared Key.

Zur Info: Der Wert ***ike*** bei **keyexchange** steht bei der initiierenden Seite für IKEv2. Der Responder akzeptiert sowohl IKEv1, als auch IKEv2.

Im Dropdown `-- Zusätzliches Feld --` wird ***ike*** ausgewählt und mit `Hinzufügen` angehängt.

Das Feld **ike** wird, im Beispiel mit ***aes128-sha256-modp3072*** (modp3072 entspricht Diffie-Hellman Group 15), konfiguriert. `Speichern` und weiter mit...

2.3 Phase 2

Hier wird der Parameter **esp** mit dem Wert ***aes128-sha256-modp3072*** konfiguriert. Mit Angeben der DH Group wird Perfect Forward Secrecy für das Rekeying der Child_SA verwendet. Mit `Speichern` werden die Änderungen übernommen.

2.4 Left und Right

Bei IPsec steht Left für die Parameter der »lokalen« Seite, also den Einstellungen die für die Seite des Gerätes gelten. Wohingegen Right für den remote Peer, die Gegenseite verwendet wird.

Die Parameter werden dabei auf den beiden Routern entsprechend »seitenverkehrt« konfiguriert. Um dieses besser darstellen zu können werden die Werte in einer Tabelle gegenübergestellt.

Parameter	Außenstelle	Zentrale
leftsubnet	***192.168.1.0/24***	***192.168.0.0/24***
leftid	***@aussenstelle***	
right	***10.99.99.1***	
rightid		***@aussenstelle***
rightsubnet	***192.168.0.0/24***	***192.168.1.0/24***

Der Parameter **leftfirewall** erlaubt es, dass IPsec-Pakete die Forwarding-Firewall, unabhängig von der sonstigen Konfiguration, passieren dürfen. Dazu wird für jeden Tunnel, dynamisch eine Firewall-Regel erstellt. Wird der Zugriff durch eigene Firewall-Regeln gesteuert, ist der Parameter nicht nötig.

Zudem wird durch Aktivieren der Funktion **leftfirewall** auch das Maskieren der Datenpakete, die für IPsec bestimmt sind verhindert, was die Kommunikation in den meisten Fällen erst möglich macht.

Ähnlich verhält es sich mit dem optionalen Parameter **lefthostacces**. Ist dieser gesetzt, wird eine Firewall-Regel für den entsprechenden Tunnel gesetzt, die den Zugriff auf den Router über die VPN-Verbindung erlaubt.

Wie gehabt werden die Änderungen auf der Konfigurationsseite **Left** mittels `Speichern`-Button übernommen.

Da nach der Konfiguration der **Right** Parameter die Konfiguration abgeschlossen ist, wird an dieser Stelle `Speichern & Anwenden` geklickt. Dadurch werden die Änderungen aktiviert, die Konfiguration entsprechend erstellt und auf die Übersichtsseite gewechselt.

2.5 Secrets Settings

Von der Übersichtsseite aus wird auf den Tab **Secrets Settings** gewechselt.

Hier wird mit dem Button `Hinzufügen` ein neuer Eintrag erstellt.

Bei **ID/Selector** wird bei der Außenstelle der Wert eingetragen der am Gerät für **right**, konfiguriert wurde, im Beispiel ***10.99.99.1***. Bei der Zentrale wird hier die Info von **rightid** (***@aussenstelle***) verwendet.

Der Pre-Shared Key wird bei **Passphrase/Secret** eingetragen.

Name wird nur als Kommentar, zur einfacheren Zuordnung des Pre-Shared Key verwendet und kann daher freigelassen werden.

Mit `Speichern & Anwenden` werden die Änderungen übernommen und aktiviert.

3 IPsec Tunnel starten

Um den IPsec-Tunnel aufzubauen wird nochmals zur **Connection Overview** gewechselt und bei dem neu angelegten Tunnel auf `Start` gedrückt. Dieser Schritt muss nur auf einem Router durchgeführt werden, da die Konfiguration zuvor schon aktiviert wurde.