HowTo – IPsec Site-2-Site-PSK zu LANCOM

Dieses Beispiel zeigt, wie zwei Netze, zwischen einem VR2020 und einem LANCOM, via IPsec unter Verwendung eines Pre-Shared Key miteinander verbunden werden, um beispielsweise eine **Außenstelle** (VR2020) an eine **Zentrale** (LANCOM) anzubinden.

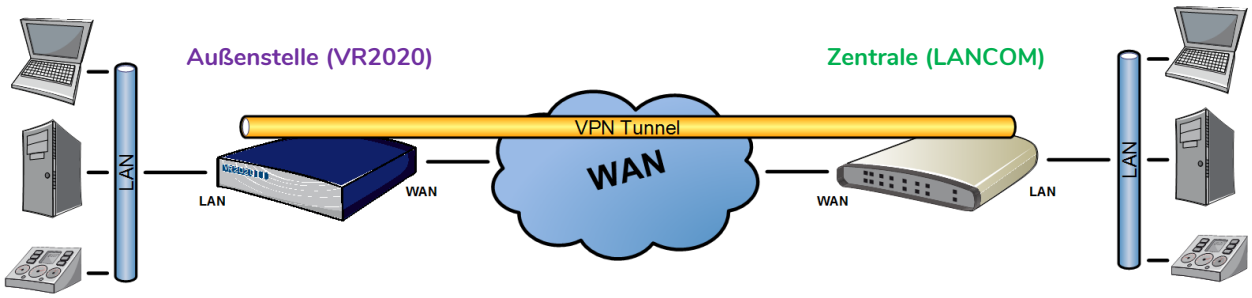

Abbildung 1: Netzplan-Beispiel

Hinweis

- In diesem Beispiel wird ein VR2020 mittels **WAN**-Schnittstelle direkt mit einem LANCOM verbunden. Die Verbindung kann natürlich auch über jeden anderen WAN-Weg etabliert werden, so sich die Geräte erreichen können.
- **Außenstelle** hat die IP ***10.99.99.2*** an Schnittstelle **WAN** und ***192.168.1.50/24*** an **LAN**.
- **Zentrale** hat die IP ***10.99.99.1*** an der als WAN konfigurierten Schnittstelle und an der als LAN genutzten Schnittstelle die IP ***192.168.0.50/24***.

1 Außenstelle TDT

1.1 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.

1.1.1 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.

1.2 IPsec-Instanz hinzufügen

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.

1.2.1 General

Auf der Seite **General** wird der Parameter **auto** auf den Wert ***start*** eingestellt.

© TDT AG

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) ***keyingtries*** (Anzahl der Aufbauversuche) hinzugefügt und konfiguriert.

Bei **closeaction** und **dpdaction** wird ***restart*** gewählt. Für DPD werden dann die default Werte **dpddelay** ***30*** Sekunden und **dpdtimeout** ***150*** Sekunden verwendet.

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

Die Änderung wird mit `Speichern` übernommen.

1.2.2 Phase 1

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

Der Wert ike bei **keyexchange** wird auf ***ikev1*** geändert.

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

Das Feld **ike** wird, im Beispiel mit ***aes128-sha-modp1536*** (modp1536 entspricht Diffie-Hellman Group 5), konfiguriert. `Speichern` und weiter mit...

1.2.3 Phase 2

Hier wird der Parameter **esp** mit dem Wert ***aes128-sha-modp1536*** konfiguriert. Mit Angeben der DH Group wird Perfect Forward Secrecy für das Rekeying der Child_SA verwendet. Mit `Speichern` werden die Änderungen übernommen.

1.2.4 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***
right	***10.99.99.1***	***10.99.99.2***
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.

© TDT AG

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.

1.2.5 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 der Wert eingetragen der am Gerät für **right**, konfiguriert wurde, im Beispiel ist das ***10.99.99.1***.

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.

1.3 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.

© TDT AG

2 Zentrale LANCOM

Beim LANCOM wird die Ipsec-Konfiguration über den Setup Wizard durchgeführt. Dazu wird der Assistent ***Zwei locale Netze verbinden*** ausgewählt und ausgeführt.

In dem Assistenten werden mehrere Schritte durchlaufen. Nach Konfiguration der genannten Parameter wird jeweils mit `Weiter >` zum nächsten Schritt gewechselt.

1. ***VPN über eine Internet-Verbindung*** auswählen.
2. **IPSEC over-HTTPS** wird nicht aktiviert!
3. Verfügt die Gegenseite über einen ISDN Anschluss? ***Nein***.
4. Auswählen von ***Beide Seiten haben eine feste IP-Adresse oder DNS-auflösbare Namen***.
5. Unter **Eigener Bezeichner** wir ein frei wählbarer Name vergeben (z.B. ***Zentrale***).
6. Als **Name der Gegenstelle** kann ein frei wählbarer Name verwendet werden (z.B. ***Aussenstelle***).
7. Zur Authentifizierung wird ***Gemeinsames Passwort (Preshared Key)*** gewählt.
8. Im nächsten Schritt wird ein ***Passwort*** und ***Preshared Key*** vergeben.
9. Die Diffie-Hellman Konfiguration wird für Phase 1 und 2 in diesem Schritt eingestellt. Hier wird ***Langsamerer Verbindungsaufbau (IKE- und PFS-Gruppe 5)*** gewählt.
10. ***Die Verbindung wird initial sowie bei einer Unterbrechung sofort wieder aufgebaut und unbegrenzt aufrecht erhalten*** auswählen.
11. In diesem Schritt werden folgende Parameter konfiguriert:
    a. **Gateway**, bezeichnet die **WAN** IP des TDT-Routers, im Beispiel ***10.99.99.2***.
    b. Das **LAN**-Netz des TDT-Routers, **Adresse** für die Netzadresse, im Beispiel ***192.168.1.0*** und die dazugehörige **Netzmaske** ***255.255.255.0***.
12. **Alle Stationen im lokalen Netz hinter der folgenden IP-Adresse maskieren (Extranet VPN)** wird bei deaktiviert belassen.
13. **NetBIOS über IP Routing aktivieren** wird nicht gesetzt.
14. Im letzten Schritt wird der Assistent mit `Fertigstellen` beendet. Dadurch wird die Konfiguration erzeugt und gespeichert.

© TDT AG