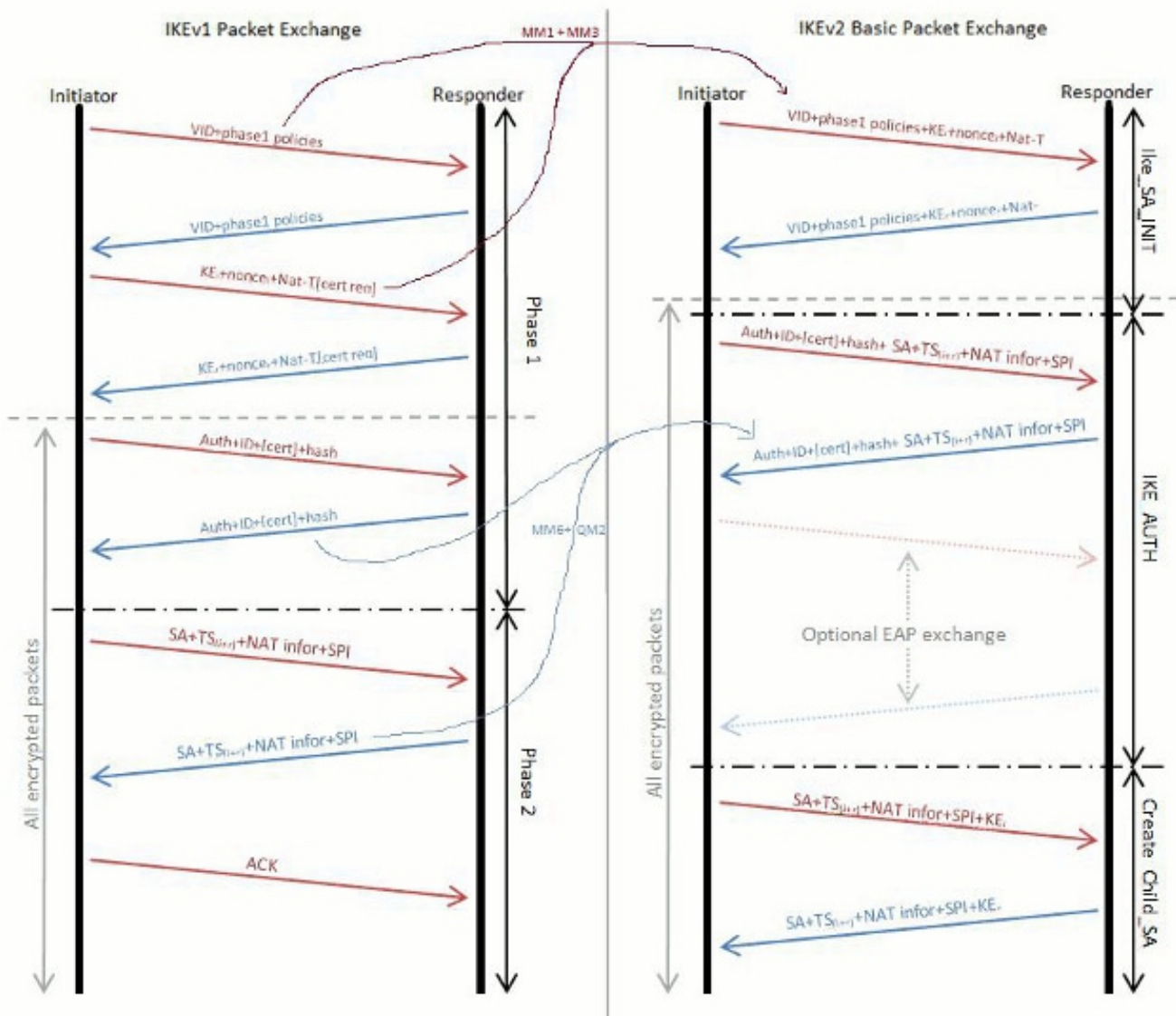


Netzwerk

VPN IPsec Tips (Lancom)

Phasen bei IPsec IKEv1 und IKEv2 (Quelle: [Cisco](#)):



Der VPN-Tunnelaufbau beim Einsatz von IKEv2/IPsec erfolgt mit 4 IKE-Telegramme.

- 2 Telegramme sind für die Aushandlung der Verschlüsselung (des Steuerkanals IKE) => IKE_SA_INIT-REQUEST + IKE_SA_INIT-RESPONSE.
- 2 Telegramme sind für die Authentifizierung der beiden VPN-Endpunkte => IKE_AUTH-REQUEST + IKE_AUTH-RESPONSE.

Zuerst erfolgt der Austausch der IKE_SA_INIT-Telegramme, danach kommen die IKE_AUTH-Telegramme.

Die IKE_SA_INIT-Telegramme werden unverschlüsselt übertragen.

Die IKE_AUTH-Telegramme sind bereits verschlüsselt.

Die REQUEST-Telegramme kommen immer vom Initiator (Client) des VPN-Tunnels.

Die RESPONSE-Telegramme werden immer vom Responder (Server) versendet.

Netzwerk

Main Mode - setzt feste IP auf beiden Seiten voraus

Aggressive Mode - erforderlich für dynam. IP

IP wird automatisch zugewiesen (IKE-CFG, bsp. Lancom Adv.VPN-Client) oder fest:

ike1: Routing-Tabelle: VPN-Verbindung in "Router" auswählen, feste IP-Adresse (Mask 255.255.255.255)

ike2: Lanconfig: VPN -> IKEv2 -> IPv4-Adressen: IP-Pool festlegen, VPN -> IKEv2 -> Verbindungsliste: IPv4-Adress-Pool auswählen (es darf kein fester IP-Eintrag in der Routing-Tabelle sein)

Local ID - Peer ID

Muss auf beiden Seiten gleich (gedreht natürlich) sein.

Als ID kommt Feste-IP oder FQDN in Frage. Der FQDN muss kein gültiger Domainname sein. Lange Zeichenkette ist besser.

PSK Preshared Key - möglichst 20-30 Zeichen lang, (bei Fritzbox und Lucom keine Sonderzeichen)

phase2localid - phase2remoteid

Proxy-IDs, definieren den Subnetzbereich, von und zu dem das VPN getunnelt wird. (Bsp.: 192.168.110.0/24)

PPP-Liste: Gegenstelle eintragen mit (Benutzer) + Passwort.

IPv4-Regeln:

RAS-WITH-NETWORK-SELECTION | 0.0.0.0/0 - 0.0.0.0/0 -> alle IPv4-Adressen (Default-Route) - bei Router-Router

RAS-WITH-CONFIG-PAYLOAD | 0.0.0.0/0 - 0.0.0.0/32 -> nur IPv4-Adresse des VPN-Clients - bei Clientverbindungen

Aktuelle und empfohlene Parameter:

- DH-Gruppe 14
- AES-256
- SHA-256
- Lifetime = 8 Std.

DEFAULT-Einträge nicht löschen!

- VPN IKE2 Verbindungsliste:

Bei fehlendem DEFAULT-Eintrag in /Setup/VPN/IKEv2/Gegenstellen/ verarbeitet das VPN-Modul des LANCOM-Router nur einkommende IKE_SA_INIT-REQUEST's, deren Absender-IP-Adresse in /Setup/VPN/IKEv2/Gegenstellen/Entferntes-Gateway eingetragen sind (=> statische IP-Adressen) ODER für welche die Absender-IP-Adresse einer in /Setup/VPN/IKEv2/Gegenstellen/Entferntes-Gateway eingetragen DNS-Adresse entspricht (=> dynamische IP-Adresse). Vom LANCOM-Router nicht akzeptierte IKE_SA_INIT-REQUEST's werden mit Fehlermeldung (Peer <UNKNOWN>: Received an IKE_SA_INIT-REQUEST of 632 bytes) unverarbeitet verworfen.

Netzwerk

DEFAULT-Eintrag in Verbindungsliste ist **wichtig** für alle Geräte, deren IP der Router nicht kennt (Mobilfunk, dyn. IP)!

Es werden Verschlüsselungen zugewiesen und PSK oder Zertifikat entschieden.

Der Default-Eintrag darf keinen Eintrag in IPv4-CFG-Pool und IPv4-Regeln aufweisen.

Ab LCOS Fw 10.50 ändert sich das Verhalten der Actionstabellen bei IP v6.

Ein "gerne" gemachter Fehler dabei ist, daß das IPv6-Modul eingeschaltet ist, obwohl es nicht genutzt wird.

Konfiguration einer Fritzbox (entsprechend langsam und ohne detaillierte Filter) in CT 2017/15 S.160ff.

Die Fritzbox kann nur IPSec (IKE v.1) + neuerdings Wireguard, kein PPTP oder SSL.

Für zertifikatsbasierte VPN sollte der Router mit der festen IP einen gültigen FQDN besitzen.

Alternativ: X509v3 Subjekt Alternative Name: IP-Adresse oder DNS

Kontrolle der Zertifikate in SSH-Konsole mittels "show vpn cert" und "show vpn ca".

VPN siehe auch:

- VPN zu Android: https://uwe-kernchen.de/phpmyfaq/index.php?solution_id=1120
- VPN Zertifikate erstellen: https://uwe-kernchen.de/phpmyfaq/index.php?solution_id=1393
- Adv.VPN Client für Windows lizenzieren: https://uwe-kernchen.de/phpmyfaq/index.php?solution_id=1376
- VPN über Router hinweg: https://uwe-kernchen.de/phpmyfaq/index.php?solution_id=1111
- Lancom Router: https://uwe-kernchen.de/phpmyfaq/index.php?solution_id=1159
- IPSec erklärt: <https://administrator.de/tutorial/ipsec-protokoll-einsatz-aufbau-benoetigte-ports-und-begriffserlaeuterungen-73117.html>

Eindeutige ID: #1238

Verfasser: Uwe Kernchen

Letzte Änderung: 1970-01-01 01:00