Netzwerk

VPN IPSec (Client -> LAN) zwischen Android und Lancom Router

Vor der nachfolgenden Erstellung der VPN-Verbindung müssen die » Zertifikate erstellt werden «.

VPN-Verbindung zwischen Lancom Router und Android Client (IPSec IKE.v2 mit Zertifikat)
mit StrongSwan VPN-Client

Lancom-Router:

- Verschlüsselung: DH28, DH14, kein PFS, AES-CBC-256, AES-CGM-256, SHA-256
- Authentifizierung: 2x RSA-Signatur, lokale Identität: IPv4-Adresse, entfernte Identität: ASN.1-Distinguished-Name, VPN1, CRL-Check: Ja
  (Variante 2: Authentifizierung: 2x RSA-Signatur, lokale Identität: IPv4-Adresse, entfernte Identität: FQDN (DNS aus Zertifikat und Client-ID), VPN1, CRL-Check: Ja)
- Verbindungsparameter: Default (30 sek, keine)
- Gültigkeitsdauer: Default (86.400 sek, 0 kB, 14.400 sek, 2.000.000 kB)
- Regelerzeugung: Manuell
- IKE-CFG: Server
- IPv4-Adress-Pool eintragen

StrongSwan VPN-Client:

- CA-Zertifikat und Client-Zertifikatskette auf Android übertragen
  (muss als X509v3 Subjekt Alternative Name -> IP des Routers enthalten)
- CA-Zertifikate: Zertifikat importieren (ca.crt)
- Verbindungsprotil erstellen
- Server: IP-Adresse
- VPN-Typ: IKEv2 Zertifikat
- Benutzer-Zertifikat: client.pfx
- CA-Zertifikat: auswäheln -> importiert -> ca.crt
- Erweitert: Server-Identität ist per Default = Server-IP (passt: X509v3 SAN -> IP)
- Erweitert: Client-Identität: Identität aus Client-Zertifikat -> Inhaber -> RFC-2253 (CN=... , ggf. gedreht!)
  (Variante 2: Client-Identität: Identität aus Client-Zertifikat -> X509v3 SAN -> DNS)
- Erweitert: NAT-T Keepalive-Interval: 15
- Erweitert: RSA/PSS-Signaturen verwenden: on

Netzwerk

Fehlersuche:

- SSH Fehlersuche: trace # vpn status (mit "Cursor-hoch" -> "ENTER" kann man on/off umschalten)
- trace + vpn - Auswerten mit Putty: Copy-All-To-Clipboard
- SSH: show vpn long - zeigt VPN-Tunnel Regeln, Verschlüsselung und Einstellungen

- SSH: show vpn rules- zeigt VPN Security Policies

- SSH: show vpn sadb - zeigt ausgehandelte SA
- Trace (LanConfig oder LanMonitor): vpn-debug / vpn-ike / vpn-status laufen lassen und Verbindung aufbauen

Typischer Fehler:
• DEFAULT-Eintrag in Verbindungsliste bis zum letzten Parameter prüfen!
• im Trace:
Compare: -Received-ID C=de,O=netdesign,CN=tw-pls-tw-client:DER_ASN1_DN != Expected-ID CN=tw-pls-hdf-client,O=netdesign,C=de:DER_ASN1_DN
-> die Geräte drehen die Reihenfolge!

Tip:
• VPN/Allgemein/Flexiber Identitätsvergleich aktivieren
• VPN IKEv1 Default-Parameter: alle 3 Defaults von Gruppe 2 (1024) auf Gruppe 14 (2048) stellen

Quellen und Links:

- VPN mit NCP-VPN-Client ohne Zertifikat: https://uwe-kernchen.de/phpmyfaq/index.php?solution_id=1120
- zertifikatsbasierte VPN-Verbindung IKEv.2 mit Lancom Adv.VPN-Client https://support.lancom-systems.com/knowledge/pages/viewpage.action?pageId=32983599
- VPN StrongSwan mit Zertifikaten: https://www.lancom-forum.de/aktuelle-lancom-router-serie-f41/1781vaw-vpn-verbindung-klappt-nicht-t16074.html#p90462
- Linkliste Lancom VPN zu Android: https://www.lancom-forum.de/fragen-zum-thema-vpn-f14/vpn-via-android-client-t17229.html#p97795
- Strongswan Connection Parameter: https://wiki.strongswan.org/projects/strongswan/wiki/ConnSection

Netzwerk

Eindeutige ID: #1398
Verfasser: Uwe Kernchen
Letzte Änderung: 2022-12-03 19:24