VPN Netscreen Remote zu Netscreen 25/5GT mit Xauth und minimaler Konfiguration pro User

1. IP-Pool eröffnen: Netz darf nicht innerhalb des trust-Netzes sein (kein ARP-Proxy auf Netscreen-Device, siehe nskb6425)
2. user eröffnen für alle:neuer user (z.B. „VPN-Users“, IKE-User, simultanous logins z.B. 40 (bei NS5GT max. 10 wegen Lizenz), simple identity, identity eingeben (z.B. „vpnusers@domain.ch“)
3. Xauth-Users eröffnen ohne IKE-ID: user, xauth-user ankreuzen, PW eingeben, IP-Pool etc. nicht ändern
4. neu dialup-usergroup erstellen („VPNuser_gruppe“), User aus Schritt 2 hinzufügen („VPN-Users“, nicht die einzelnen User!)
5. globale xauth-settings konfigurieren: VPN- Autokey advanced – xauth-settings: „Reserve Private IP for XAuth User“ sollte länger als phase 1 rekey-Zeit sein, z.B. 600 Minuten, CHAP funktioniert mit aktuellem Netscreen-Remote-Client nicht, IP-Pool auswählen, DNS konfigurieren
6. phase 1 gateway konfigurieren: custom security level, neues gateway, dialup group, gruppe wählen, key eingeben, advanced: proposal wählen (pre-g2-3des-sha), aggressive, NAT-Traversal, udp-checksum, XAuth Server auswählen, use default
7. phase 2 konfigurieren: neues autoike, gateway wählen, advanced, phase2 proposal wählen nopfs-esp-3des-sha, kein replay protection
8. policy erstellen: neu untrust-trust, dialup-VPN zu internes Netz, tunnel, tunnel wählen, logging

zusätzliche user: nur neuer xauth-user

Client:
1. neue Verbindung
2. Name geben
3. „only connect manually“ sonst connected der Client auch im internen Netz sofort
4. Remote Party Identity and Addressing: Netz eingeben
5. gateway eingeben
6. aggressive mode
7. kein perfect forward secrecy, kein replay detection
8. ID type email, email eingeben (bei allen die gleiche)
9. virtual adapter preferred
10. preshared key eingeben
11. authentication method: preshared key, extended authentication

falls Hostname (dyndns) für Gateway verwendet: ID Type: Any, Gateway Hostname

siehe auch juniper-netscreen-knowledgebase: ns10133, ns5202

Vorteile:
- interne IP zugewiesen aus Pool
- dns und WINS-Server werden automatisch zugewiesen
- login nötig
- dafür keine eigenen keys pro user
- logins ersichtlich im log mit username
- als auth-server könnte per radius oder ldap auch interner server benutzt werden
- ohne „connect manually“ wäre wohl auch login während boot möglich

conf-file sollte gelocked sein