VPN-tunnel beleid Gooise Meren

Werkwijze

Voor het verkrijgen van toestemming en het inrichten van VPN-tunnels hanteert Gooise Meren de volgende werkwijze:

1. Aanmelden bij Netwerkbeheer
2. Review/Dialoog met CISO(s) -> Identificatie risico's
3. Opstellen/aanpassen overeenkomst leverancier (hierin worden de eisen voor Fase 1 en Fase 2 verbindingen zoals hieronder beschreven vastgelegd).
4. Ondertekening overeenkomst
5. Inrichting VPN-tunnel door GM/Leverancier
6. Toetsing op borging verbindingseisen

Uitangspunten

- no-tunnel, tenzij er echt geen alternatieven zijn;
- servers/applicaties die gebruik maken van VPN-tunnels dienen passend te worden *hardened* door de leverancier;
- servers/applicaties die voorzien zijn van een vpn-tunnel worden zo veel mogelijk in een afgescheiden netwerkzone/vlan geplaatst;
- tunnels worden vormgegeven op applicatieniveau en niet op poortniveau.

Phase 1 Technische eisen/configuratie:

MODE: IKEv2 Only
DH-GROEP: Diffie-Hellman group 19 - 256 bit elliptic curve
Diffie-Hellman group 20 - 384 bit elliptic curve

ENCRYPTIE-ALGORITME: AES256 (CBC)
Zie ook 'ICT-beveiligings- richtlijnen voor Transport Layer Security (TLS)'
HASH: SHA384/512
LIFETIME: 8 uur
PSK: 40 karakters, wordt niet gedeeld via e-mail

Phase 2 Technische eisen/configuratie:

IPSEC Protocol: ESP
Perfect Forward Secrecy (PFS): Ja, enabled
FPS DH-GROEP: Diffie-Hellman group 19 - 256 bit elliptic curve
Diffie-Hellman group 20 - 384 bit elliptic curve
ENCRYPTIE-ALGORITME: AES256 (CBC/GBC)
HASH: SHA384 (of hoger)
LIFETIME: 8 uur