Bijlage 22: Rijkswaterstaat IPSEC TUNNEL SETTINGS

Klant naam (TP)	<TP naam>
TP Peer IP adres	<ip address>
PHASE 1 Protocol	IKE Version 2
PHASE 1 Authentication Mode	Pre-shared key
Pre-Shared Key	
PHASE 1 Authentication Algorithm	SHA - 512 / 384 / 256bit
PHASE 1 Encryption Algorithm	AES - 256bit
PHASE 1 Diffie-Hellman Group	Group 20
PHASE 1 Psuedo-random function (PRF)	SHA - 512 / 384 / 256bit
PHASE 1 Lifetime Measurement	Time
PHASE 1 Time Lifetime	28800s (8 hours)
PHASE 1 DPD	Disabled
PHASE 1 Mode	Main
PHASE 2 Protocol	ESP (Tunnel Mode)
PHASE 2 Authentication Algorithm	SHA - 512 / 384 / 256bit
PHASE 2 Encryption Algorithm	ESP-AES 256
PHASE 2 Encapsulation Mode	Tunnel mode
PHASE 2 Perfect Forward Secrecy	Yes, DH group 20
PHASE 2 Lifetime Measurement	Time & Kilobytes
PHASE 2 Time Lifetime	3600s (1 hour)
PHASE 2 Kilobytes amount	4.608.000 KB (10Mb per seconde voor 1 uur)
TP Net 0	<ip address,subnet>
RWS Net 0	<ip address, subnet>