How to create IPsec backup policy

[Voraussetzungen]

1. DSR-500N/1000N mit Firmware Version: v1.06B43 und höher
2. Kompatibler 3G USB Stick oder redundante WAN Verbindung

[Szenario]

DSR-1 (1.1.1.1) ---------- Router ---------- (3.3.3.1) (wan1) DSR-2
---------- (4.4.4.1) (wan2)

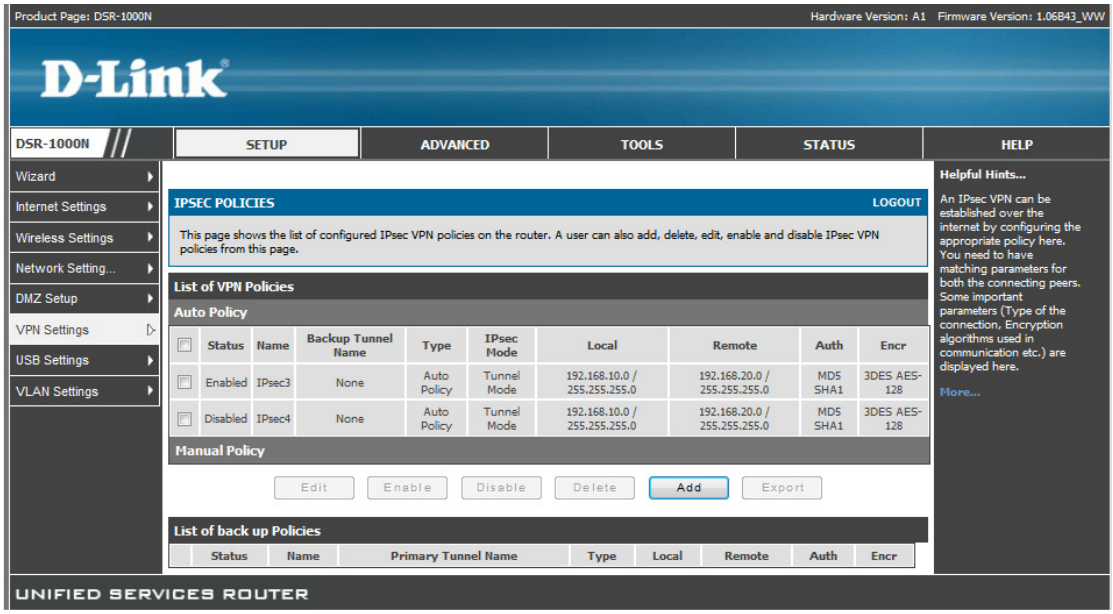
DSR 1 benutzt primäre IPSEC-Policy um einen Tunnel zu DSR 2 aufzubauen.
Wenn der primäre Tunnel ausfällt schwenkt DSR1 auf den Backup Tunnel.

[Vorgehensweise]

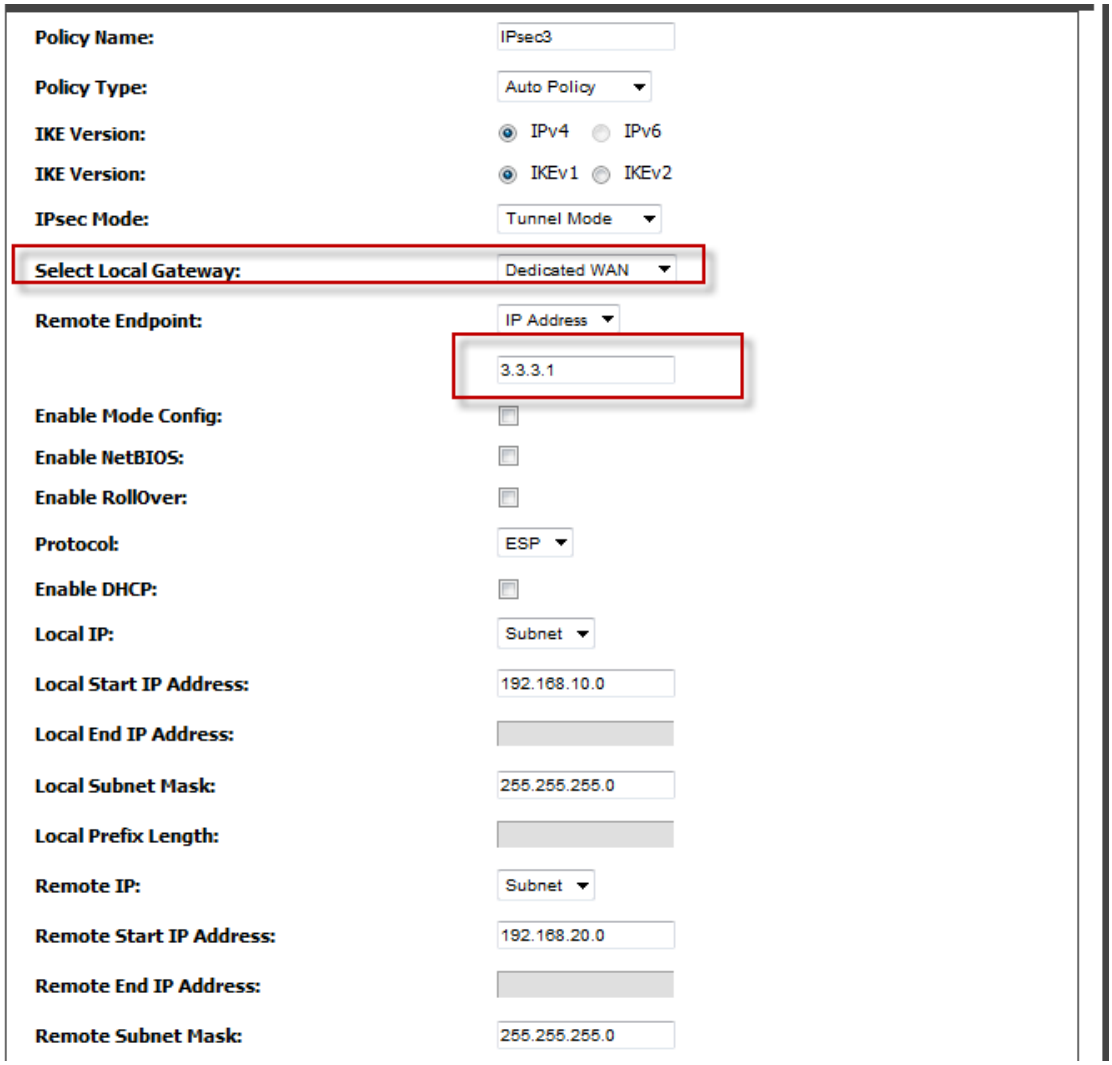
DSR-1:

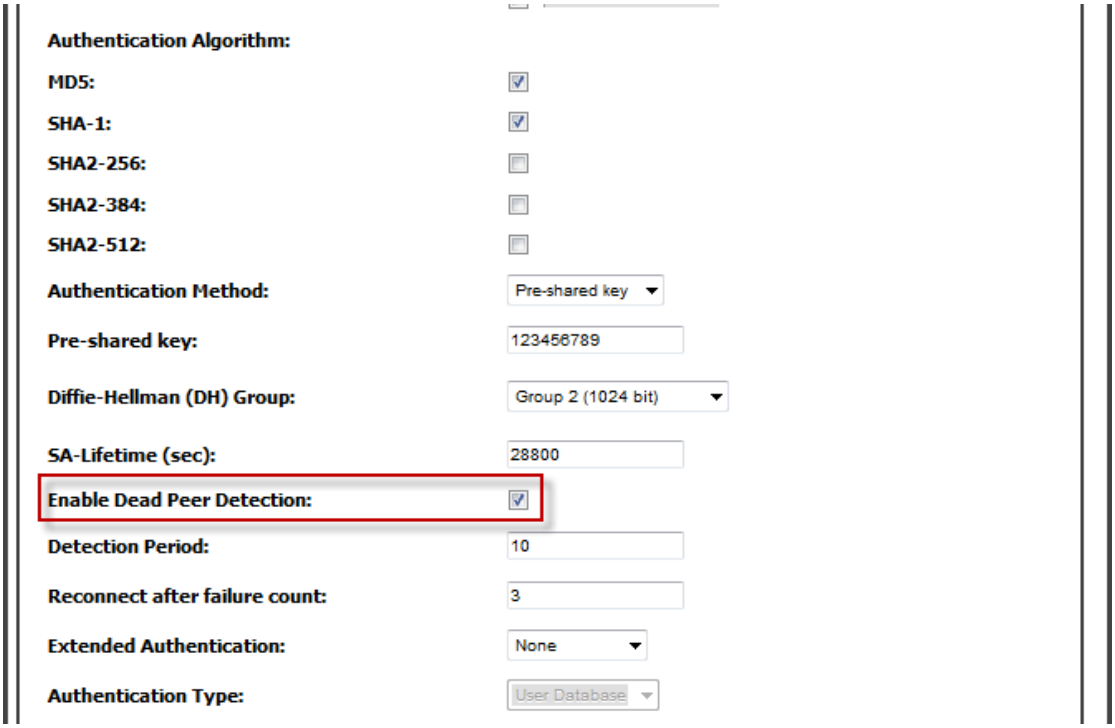
(1) Konfigurieren der WAN IP Adresse des DSR-1 als z.B. statisch 1.1.1.1/24 und der LAN IP Addresse ist 192.168.10.1/24

(2) Erstellung von 2 IPSec Policies (IPSec3 = Primär & IPSEC4 = Backup Policy)



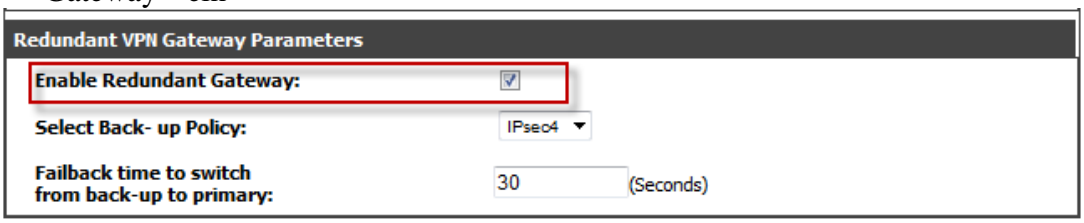
(3) Bitte schalten Sie unter der primären IPSec Policy (IPSec3) das Dead-Peer-Detection ein um einen eventuellen Tunnelausfall automatisch erkennen lassen zu können

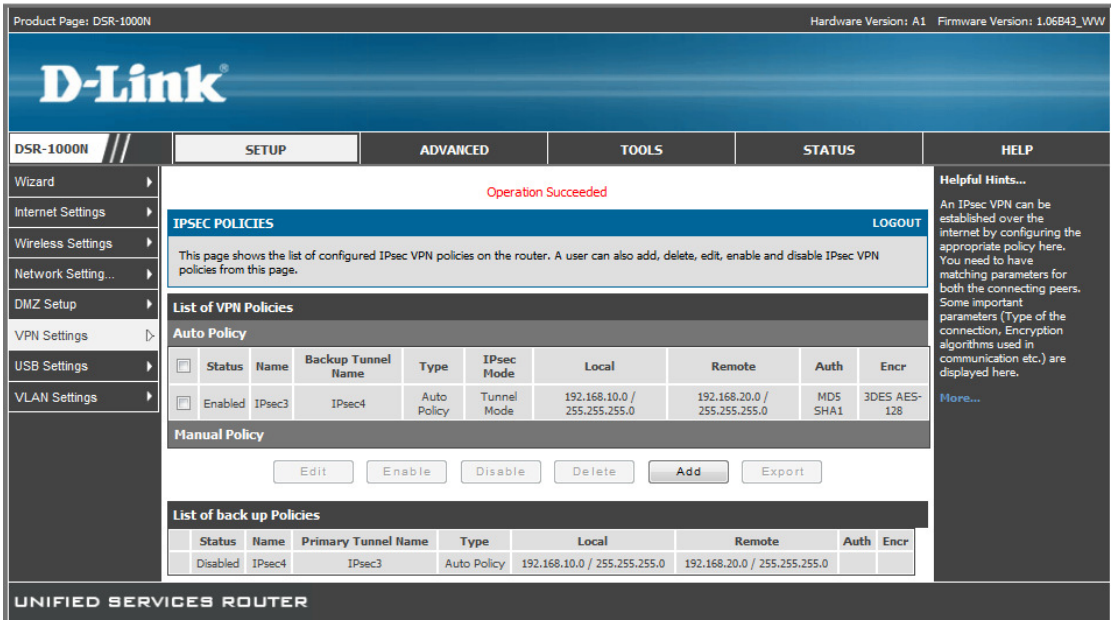




(4) Bitte schalten Sie unter der sekundären IPSec Policy (IPSec4) das Dead-Peer-Detection ein um einen eventuellen Tunnelausfall automatisch erkennen lassen zu können

(5) Anschliessend schalten Sie unter der primären IPSec Policy (IPSec3) das „Redundante Gateway“ ein

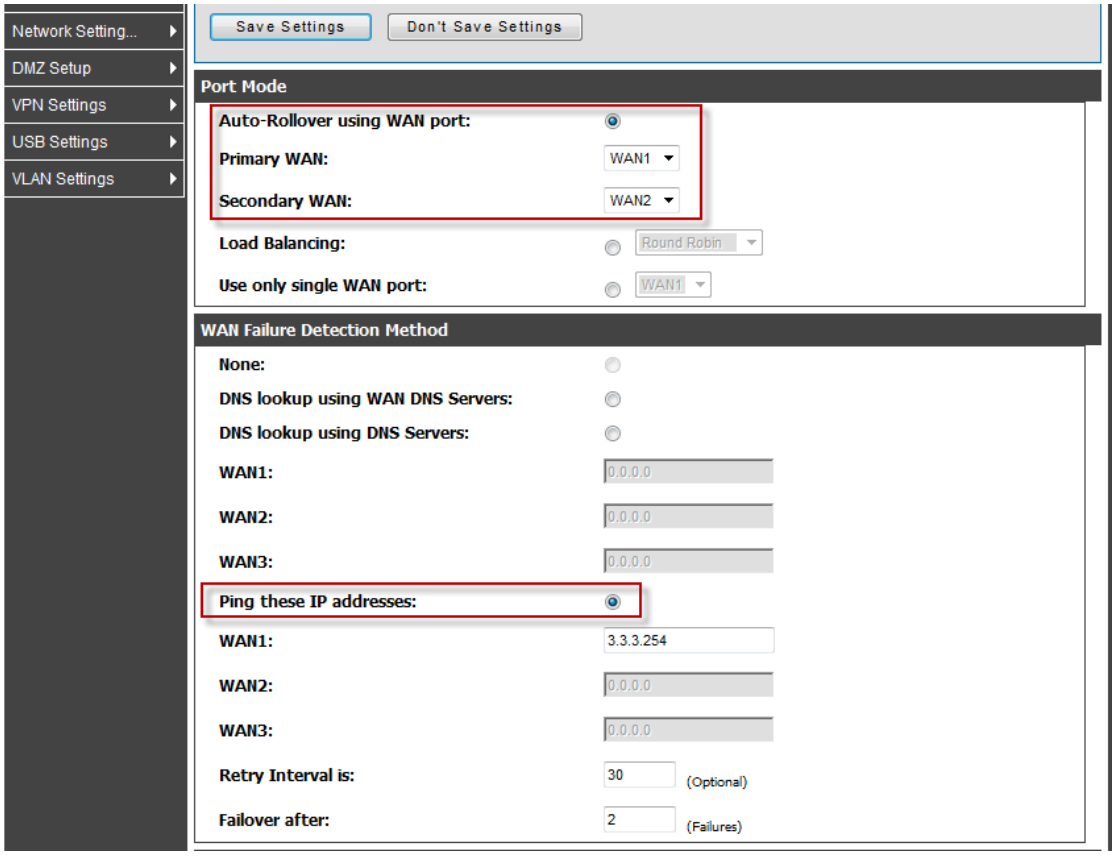



Product Page: DSR-1000N
Hardware Version: A1 Firmware Version: 1.06B43_WW
D-Link
DSR-1000N
SETUP
ADVANCED
TOOLS
STATUS
HELP
Wizard
Internet Settings
Wireless Settings
Network Setting...
DMZ Setup
VPN Settings
USB Settings
VLAN Settings
Operation Succeeded
IPSEC POLICIES
LOGOUT
This page shows the list of configured IPsec VPN policies on the router. A user can also add, delete, edit, enable and disable IPsec VPN policies from this page.
List of VPN Policies
Auto Policy
Status Name Backup Tunnel Name Type IPsec Mode Local Remote Auth Encr
Enabled IPsec3 IPsec4 Auto Policy Tunnel Mode 192.168.10.0 / 255.255.255.0 192.168.20.0 / 255.255.255.0 MD5 SHA1 3DES AES-128
Manual Policy
Edit Enable Disable Delete Add Export
List of back up Policies
Status Name Primary Tunnel Name Type Local Remote Auth Encr
Disabled IPsec4 IPsec3 Auto Policy 192.168.10.0 / 255.255.255.0 192.168.20.0 / 255.255.255.0
Helpful Hints...
An IPsec VPN can be established over the internet by configuring the appropriate policy here. You need to have matching parameters for both the connecting peers. Some important parameters (Type of the connection, Encryption algorithms used in communication etc.) are displayed here.
More...
UNIFIED SERVICES ROUTER

DSR-2:

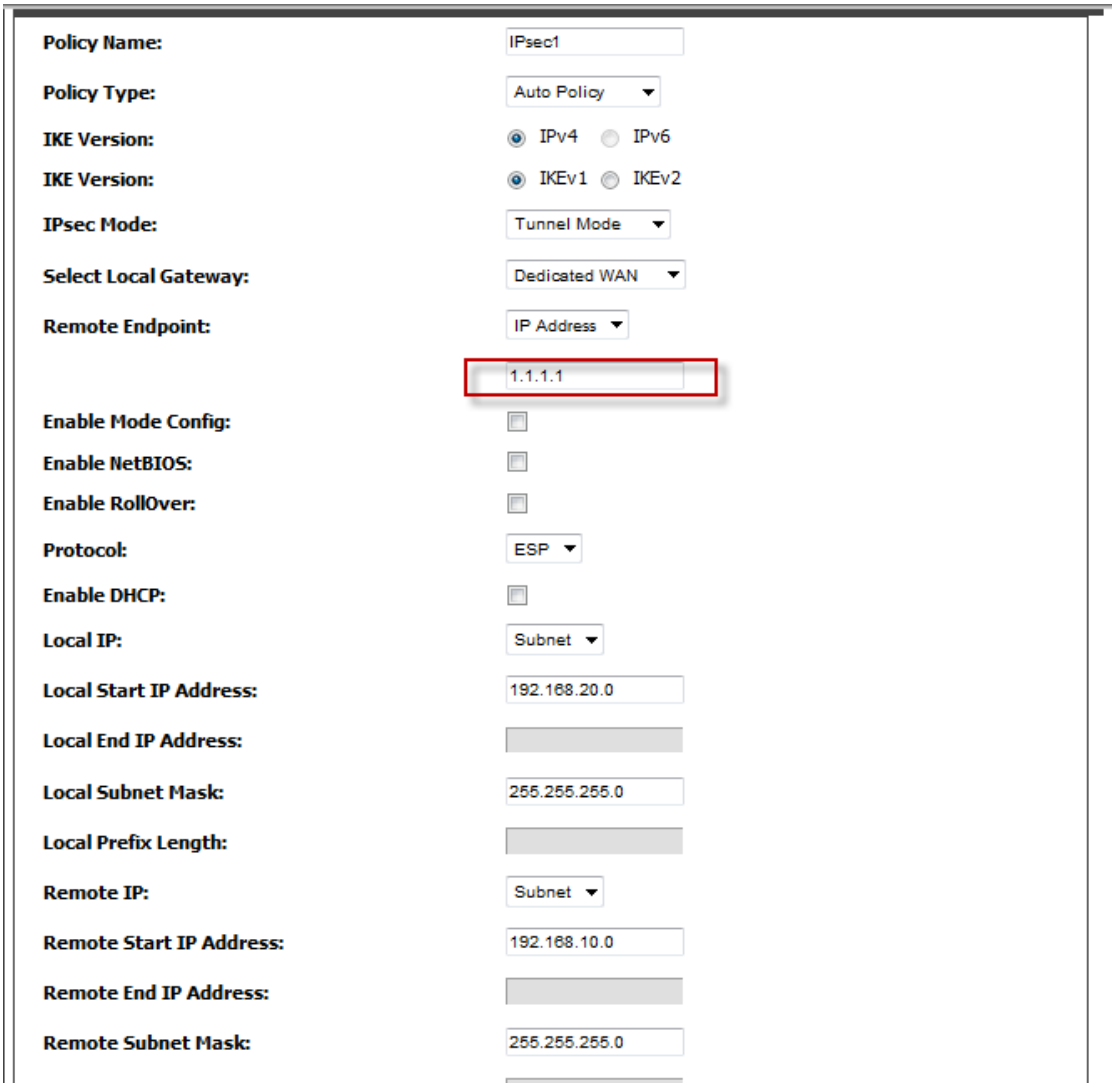
(6) Konfigurieren der WAN-1 IP Adresse des DSR-2 als z.B. statisch 3.3.3.1/24 sowie die WAN-2 IP Adresse des DSR-2 als z.B. statisch 4.4.4.1/24 und der LAN IP Addresse ist 192.168.20.1/24

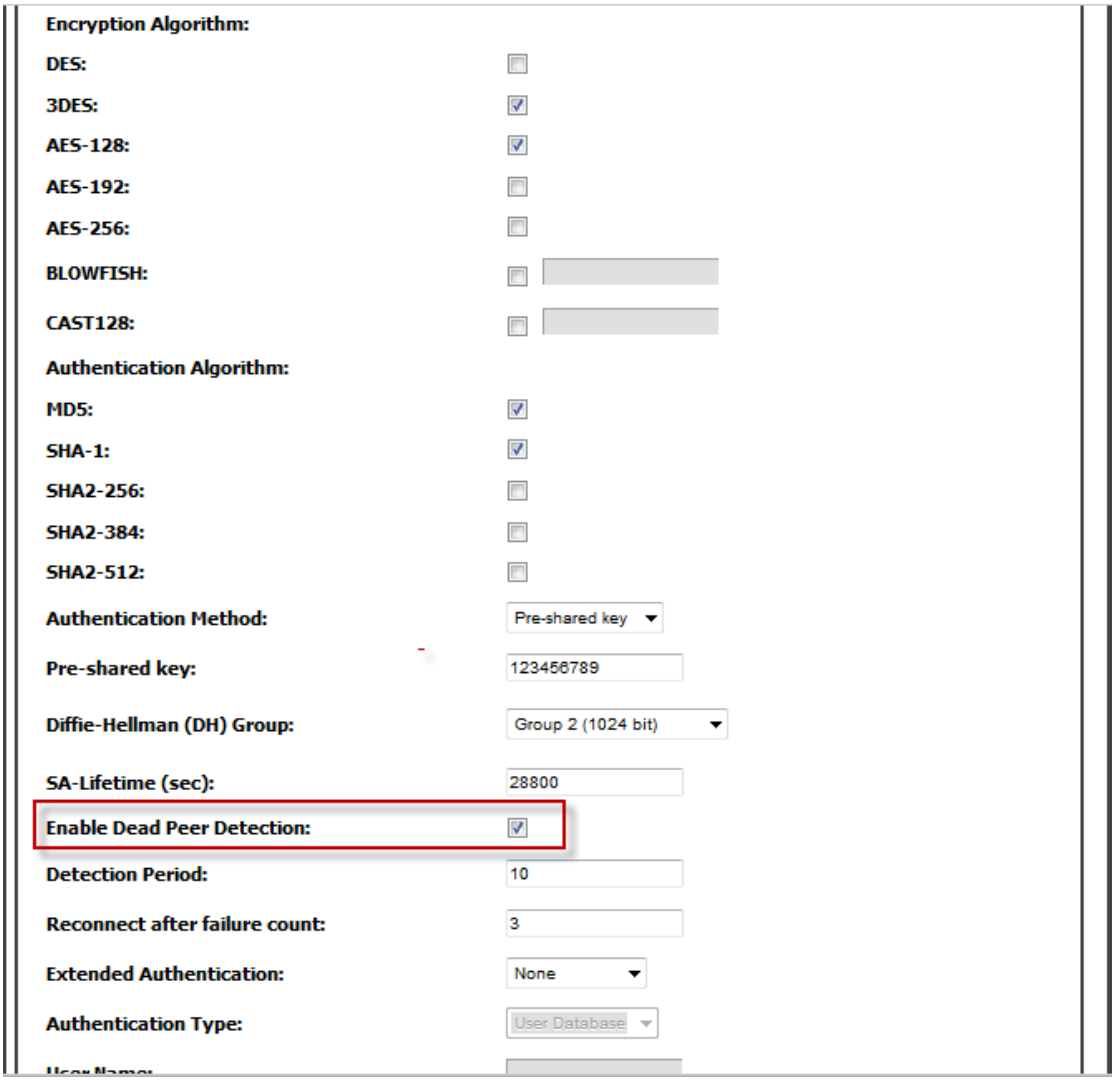
(7) Einschalten der "Auto-Rollover" Funktion und Auswahl der Erkennungsmethode z.B. „ping"



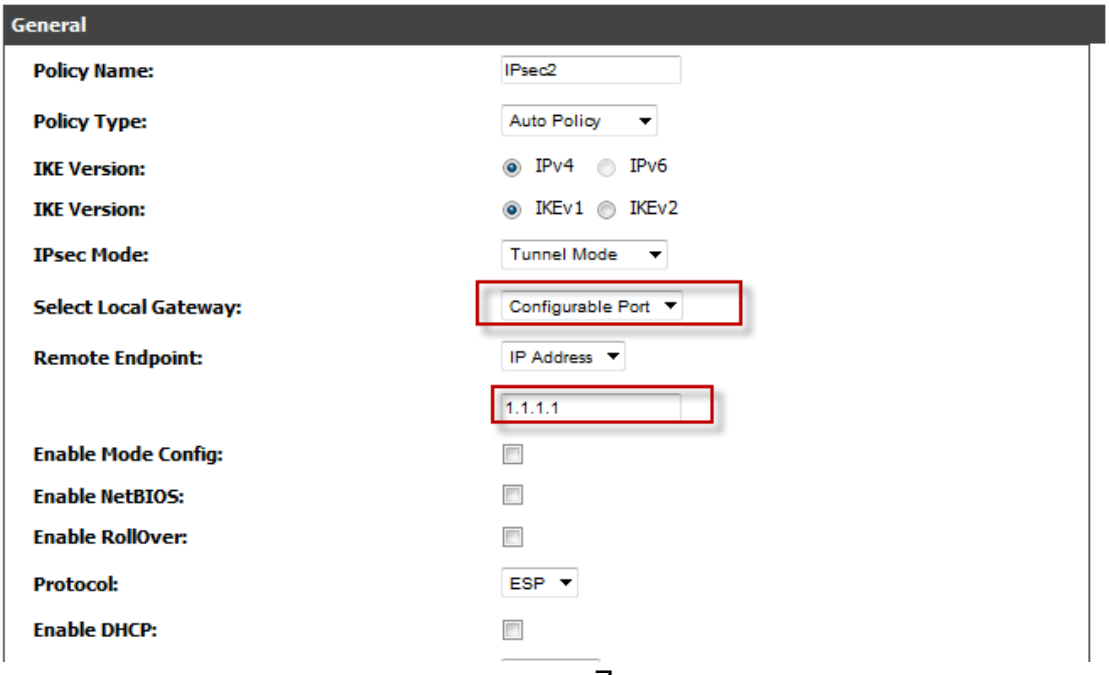
(8) Erstellung von 2 IPSec Policies (IPSec1 = Primär & IPSEC2 = Backup Policy)

(9) Bitte schalten Sie unter der primären IPSec Policy (IPSec1) das Dead-Peer-Detection ein um einen eventuellen Tunnelausfall automatisch erkennen lassen zu können

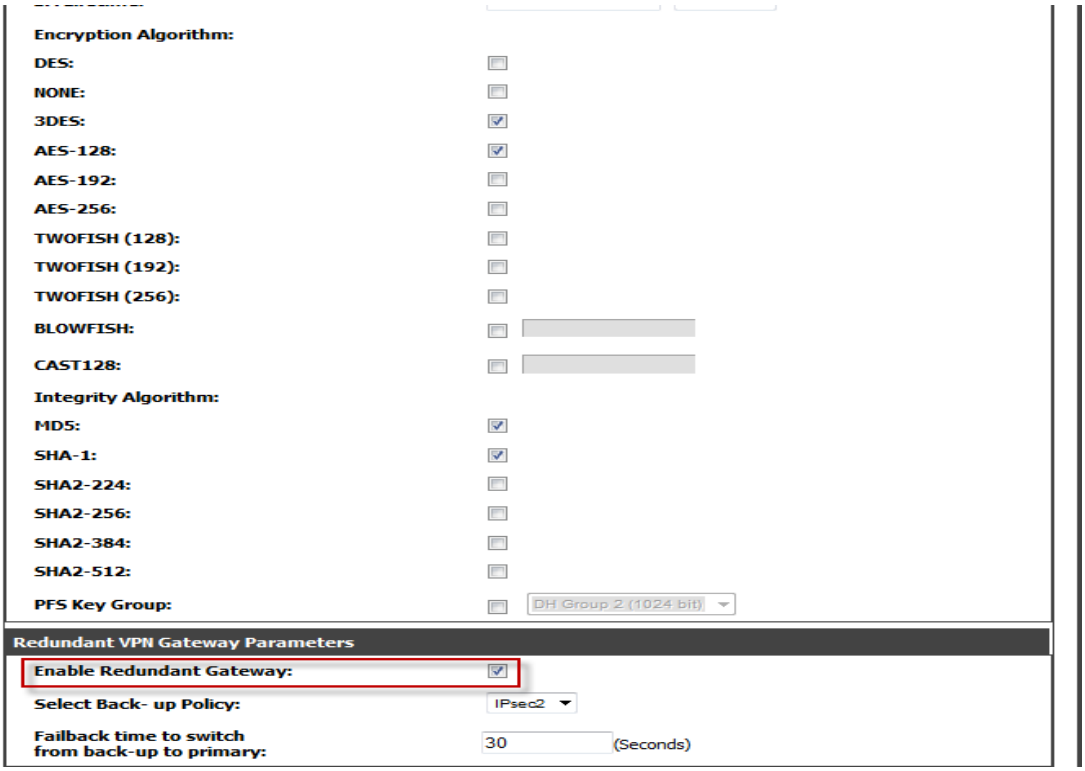




(10) Bitte schalten Sie unter der sekundären IPSec Policy (IPSec2) das Dead-Peer-Detection ein und wählen Sie als lokal Gateway Ihr „WAN2/3G“ Interface



(11) Anschliessend schalten Sie unter der primären IPSec Policy (IPSec3) das „Redundante Gateway“ ein



In diesem Screenshot können Sie am DSR-1 erkennen, dass der Backup Tunnel aktiv ist.