

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 Adresse ist 192.168.10.1/24
- (2) Erstellung von 2 IPsec Policies (IPSec3 = Primär & IPSEC4 = Backup Policy)

The screenshot shows the D-Link web interface for a DSR-1000N router. The top navigation bar includes 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'HELP'. The left sidebar lists various settings like Wizard, Internet Settings, Wireless Settings, etc. The main content area is titled 'IPSEC POLICIES' and contains a 'List of VPN Policies' table. The table has columns for Status, Name, Backup Tunnel Name, Type, IPsec Mode, Local, Remote, Auth, and Encr. Two policies are listed: IPsec3 (Enabled) and IPsec4 (Disabled). Below the table are buttons for 'Edit', 'Enable', 'Disable', 'Delete', 'Add', and 'Export'. A 'List of back up Policies' table is also visible at the bottom of the main content area.

| Status | Name | Backup Tunnel Name | Type | IPsec Mode | Local | Remote | Auth | Encr |
|-------------------------------------|--------|--------------------|-------------|-------------|------------------------------|------------------------------|----------|--------------|
| <input checked="" type="checkbox"/> | IPsec3 | None | 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 |
| <input type="checkbox"/> | IPsec4 | None | 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 |

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

| | |
|---------------------------------|--|
| Policy Name: | IPsec3 |
| Policy Type: | Auto Policy ▾ |
| IKE Version: | <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 |
| IKE Version: | <input checked="" type="radio"/> IKEv1 <input type="radio"/> IKEv2 |
| IPsec Mode: | Tunnel Mode ▾ |
| Select Local Gateway: | Dedicated WAN ▾ |
| Remote Endpoint: | IP Address ▾ 3.3.3.1 |
| Enable Mode Config: | <input type="checkbox"/> |
| Enable NetBIOS: | <input type="checkbox"/> |
| Enable RollOver: | <input type="checkbox"/> |
| Protocol: | ESP ▾ |
| Enable DHCP: | <input type="checkbox"/> |
| Local IP: | Subnet ▾ |
| Local Start IP Address: | 192.168.10.0 |
| Local End IP Address: | |
| Local Subnet Mask: | 255.255.255.0 |
| Local Prefix Length: | |
| Remote IP: | Subnet ▾ |
| Remote Start IP Address: | 192.168.20.0 |
| Remote End IP Address: | |
| Remote Subnet Mask: | 255.255.255.0 |

| | |
|---------------------------------------|-------------------------------------|
| Authentication Algorithm: | |
| MD5: | <input checked="" type="checkbox"/> |
| SHA-1: | <input checked="" type="checkbox"/> |
| SHA2-256: | <input type="checkbox"/> |
| SHA2-384: | <input type="checkbox"/> |
| SHA2-512: | <input type="checkbox"/> |
| Authentication Method: | Pre-shared key ▾ |
| Pre-shared key: | 123456789 |
| Diffie-Hellman (DH) Group: | Group 2 (1024 bit) ▾ |
| SA-Lifetime (sec): | 28800 |
| Enable Dead Peer Detection: | <input checked="" type="checkbox"/> |
| Detection Period: | 10 |
| Reconnect after failure count: | 3 |
| Extended Authentication: | None ▾ |
| Authentication Type: | User Database ▾ |

- (4) Bitte schalten Sie unter der sekundären IPsec Policy (IPsec4) das Dead-Peer-Detection ein um einen eventuellen Tunnelausfall automatisch erkennen lassen zu können

| | |
|------------------------------|--|
| General | |
| Policy Name: | IPsec4 |
| Policy Type: | Auto Policy ▾ |
| IKE Version: | <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 |
| IKE Version: | <input checked="" type="radio"/> IKEv1 <input type="radio"/> IKEv2 |
| IPsec Mode: | Tunnel Mode ▾ |
| Select Local Gateway: | Dedicated WAN ▾ |
| Remote Endpoint: | IP Address ▾ 4.4.4.1 |
| Enable Mode Config: | <input type="checkbox"/> |
| Enable NetBIOS: | <input type="checkbox"/> |
| Enable RollOver: | <input type="checkbox"/> |
| Protocol: | ESP ▾ |

- (5) Anschliessend schalten Sie unter der primären IPsec Policy (IPsec3) das „Redundante Gateway“ ein

| | |
|---|-------------------------------------|
| Redundant VPN Gateway Parameters | |
| Enable Redundant Gateway: | <input checked="" type="checkbox"/> |
| Select Back-up Policy: | IPsec4 ▾ |
| Failback time to switch from back-up to primary: | 30 (Seconds) |

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.06B43_VW

D-Link®

| DSR-1000N | SETUP | ADVANCED | TOOLS | STATUS | HELP | | | | | | | | | | | | | | | | | | | | |
|---|---------------------|----------|---------------------|-------------|---|------------------------------|------------------------------|---------------------|--------------------|-------|------------|-------|--------|--------------------------|----------|--------------------------|---------|-------------|------------------------------|------------------------------|-------------|------------------------------|------------------------------|----------|--------------|
| <ul style="list-style-type: none"> Wizard ▶ Internet Settings ▶ Wireless Settings ▶ Network Setting... ▶ DMZ Setup ▶ VPN Settings ▶ USB Settings ▶ VLAN Settings ▶ | Operation Succeeded | | | | <p>Helpful Hints...</p> <p>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.</p> <p>More...</p> | | | | | | | | | | | | | | | | | | | | |
| <div style="background-color: #0056b3; color: white; padding: 2px;"> IPSEC POLICIES LOGOUT </div> <p>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.</p> | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>List of VPN Policies</p> <p>Auto Policy</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th><input type="checkbox"/></th> <th>Status</th> <th>Name</th> <th>Backup Tunnel Name</th> <th>Type</th> <th>IPsec Mode</th> <th>Local</th> <th>Remote</th> <th>Auth</th> <th>Encr</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>Enabled</td> <td>IPsec3</td> <td>IPsec4</td> <td>Auto Policy</td> <td>Tunnel Mode</td> <td>192.168.10.0 / 255.255.255.0</td> <td>192.168.20.0 / 255.255.255.0</td> <td>MD5 SHA1</td> <td>3DES AES-128</td> </tr> </tbody> </table> <p>Manual Policy</p> <p style="text-align: center;"> <input type="button" value="Edit"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/> <input type="button" value="Add"/> <input type="button" value="Export"/> </p> | | | | | | <input type="checkbox"/> | Status | Name | Backup Tunnel Name | Type | IPsec Mode | Local | Remote | Auth | Encr | <input type="checkbox"/> | 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 |
| <input type="checkbox"/> | Status | Name | Backup Tunnel Name | Type | | IPsec Mode | Local | Remote | Auth | Encr | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | 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 | | | | | | | | | | | | | | | | |
| <p>List of back up Policies</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th><input type="checkbox"/></th> <th>Status</th> <th>Name</th> <th>Primary Tunnel Name</th> <th>Type</th> <th>Local</th> <th>Remote</th> <th>Auth</th> <th>Encr</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>Disabled</td> <td>IPsec4</td> <td>IPsec3</td> <td>Auto Policy</td> <td>192.168.10.0 / 255.255.255.0</td> <td>192.168.20.0 / 255.255.255.0</td> <td></td> <td></td> </tr> </tbody> </table> | | | | | <input type="checkbox"/> | Status | Name | Primary Tunnel Name | Type | Local | Remote | Auth | Encr | <input type="checkbox"/> | Disabled | IPsec4 | IPsec3 | Auto Policy | 192.168.10.0 / 255.255.255.0 | 192.168.20.0 / 255.255.255.0 | | | | | |
| <input type="checkbox"/> | Status | Name | Primary Tunnel Name | Type | Local | Remote | Auth | Encr | | | | | | | | | | | | | | | | | |
| <input type="checkbox"/> | Disabled | IPsec4 | IPsec3 | Auto Policy | 192.168.10.0 / 255.255.255.0 | 192.168.20.0 / 255.255.255.0 | | | | | | | | | | | | | | | | | | | |

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 Adresse ist 192.168.20.1/24
- (7) Einschalten der “Auto-Rollover” Funktion und Auswahl der Erkennungsmethode z.B. „ping“

The screenshot displays the configuration page for the DSR-2 device. The left sidebar contains navigation options: Network Setting..., DMZ Setup, VPN Settings, USB Settings, and VLAN Settings. The main content area is divided into two sections: "Port Mode" and "WAN Failure Detection Method".

Port Mode

- Auto-Rollover using WAN port: (highlighted with a red box)
- Primary WAN: WAN1 (dropdown menu)
- Secondary WAN: WAN2 (dropdown menu)
- Load Balancing: Round Robin (dropdown menu)
- Use only single WAN port: WAN1 (dropdown menu)

WAN Failure Detection Method

- None:
- DNS lookup using WAN DNS Servers:
- DNS lookup using DNS Servers:
- WAN1: 0.0.0.0 (text input)
- WAN2: 0.0.0.0 (text input)
- WAN3: 0.0.0.0 (text input)
- Ping these IP addresses: (highlighted with a red box)
- WAN1: 3.3.3.254 (text input)
- WAN2: 0.0.0.0 (text input)
- WAN3: 0.0.0.0 (text input)
- Retry Interval is: 30 (Optional) (text input)
- Failover after: 2 (Failures) (text input)

At the top of the configuration area, there are two buttons: "Save Settings" and "Don't Save Settings".

- (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

| | |
|---------------------------------|--|
| Policy Name: | IPsec1 |
| Policy Type: | Auto Policy |
| IKE Version: | <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 |
| IKE Version: | <input checked="" type="radio"/> IKEv1 <input type="radio"/> IKEv2 |
| IPsec Mode: | Tunnel Mode |
| Select Local Gateway: | Dedicated WAN |
| Remote Endpoint: | IP Address |
| | 1.1.1.1 |
| Enable Mode Config: | <input type="checkbox"/> |
| Enable NetBIOS: | <input type="checkbox"/> |
| Enable RollOver: | <input type="checkbox"/> |
| Protocol: | ESP |
| Enable DHCP: | <input type="checkbox"/> |
| Local IP: | Subnet |
| Local Start IP Address: | 192.168.20.0 |
| Local End IP Address: | |
| Local Subnet Mask: | 255.255.255.0 |
| Local Prefix Length: | |
| Remote IP: | Subnet |
| Remote Start IP Address: | 192.168.10.0 |
| Remote End IP Address: | |
| Remote Subnet Mask: | 255.255.255.0 |

| | |
|----------------------------------|---|
| Encryption Algorithm: | |
| DES: | <input type="checkbox"/> |
| 3DES: | <input checked="" type="checkbox"/> |
| AES-128: | <input checked="" type="checkbox"/> |
| AES-192: | <input type="checkbox"/> |
| AES-256: | <input type="checkbox"/> |
| BLOWFISH: | <input type="checkbox"/> <input type="text"/> |
| CAST128: | <input type="checkbox"/> <input type="text"/> |
| Authentication Algorithm: | |
| MD5: | <input checked="" type="checkbox"/> |
| SHA-1: | <input checked="" type="checkbox"/> |
| SHA2-256: | <input type="checkbox"/> |
| SHA2-384: | <input type="checkbox"/> |
| SHA2-512: | <input type="checkbox"/> |
| Authentication Method: | Pre-shared key ▾ |
| Pre-shared key: | <input type="text" value="123456789"/> |
| Diffie-Hellman (DH) Group: | Group 2 (1024 bit) ▾ |
| SA-Lifetime (sec): | <input type="text" value="28800"/> |
| Enable Dead Peer Detection: | <input checked="" type="checkbox"/> |
| Detection Period: | <input type="text" value="10"/> |
| Reconnect after failure count: | <input type="text" value="3"/> |
| Extended Authentication: | None ▾ |
| Authentication Type: | User Database ▾ |
| User Name: | <input type="text"/> |

- (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

| | |
|-----------------------|--|
| General | |
| Policy Name: | <input type="text" value="IPsec2"/> |
| Policy Type: | Auto Policy ▾ |
| IKE Version: | <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 |
| IKE Version: | <input checked="" type="radio"/> IKEv1 <input type="radio"/> IKEv2 |
| IPsec Mode: | Tunnel Mode ▾ |
| Select Local Gateway: | Configurable Port ▾ |
| Remote Endpoint: | IP Address ▾ <input type="text" value="1.1.1.1"/> |
| Enable Mode Config: | <input type="checkbox"/> |
| Enable NetBIOS: | <input type="checkbox"/> |
| Enable RollOver: | <input type="checkbox"/> |
| Protocol: | ESP ▾ |
| Enable DHCP: | <input type="checkbox"/> |

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

Encryption Algorithm:

DES:

NONE:

3DES:

AES-128:

AES-192:

AES-256:

TWOFISH (128):

TWOFISH (192):

TWOFISH (256):

BLOWFISH: _____

CAST128: _____

Integrity Algorithm:

MD5:

SHA-1:

SHA2-224:

SHA2-256:

SHA2-384:

SHA2-512:

PFS Key Group: DH Group 2 (1024 bit) ▼

Redundant VPN Gateway Parameters

Enable Redundant Gateway:

Select Back- up Policy: IPSec2 ▼

Failback time to switch from back-up to primary: 30 (Seconds)

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

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.06B43_WW

D-Link

DSR-1000N // SETUP ADVANCED TOOLS STATUS HELP

Device Info | Logs | Traffic Monitor | Active Sessions | Wireless Clients | LAN Clients | Active VPNs

ACTIVE VPN LOGOUT

The page will auto-refresh in 1 seconds

This page displays the active VPN connections, IPSEC as well as SSL.

Active IPsec SAs

| Policy Name | Endpoint | tx (KB) | tx (Packets) | State | Action |
|-------------|----------|-----------|----------------|--------------------------|---------|
| IPsec1 | 1.1.1.1 | 0.00 | 0 | IPsec SA Not Established | Connect |
| IPsec2 | 1.1.1.1 | 806013.05 | 1002634 | IPsec SA Established | Drop |

Active SSL VPN Connections

| User Name | IP Address | Local PPP Interface | Peer PPP Interface IP | Connect Status |
|-----------|------------|---------------------|-----------------------|----------------|
| | | | | |

Active PPTP VPN connections

| Connection Status | Action |
|-------------------|---------|
| Disconnected | Connect |

Poll Interval: 10 (Seconds) Start Stop

UNIFIED SERVICES ROUTER

Helpful Hints... This page lists current established IPsec Security Associations and SSL VPN tunnels. More...