

How to configure the IPSec backup on DSR series

The firmware version later than 1.06B62, DSR-500, 1000 series start to support IPSec backup.

Test Topology:

PC1-----(lan)DSR1(wan1)-----
(wan2)-----
(P1)Router(P3)-----
(P4)-----
(wan1)DSR2(lan)-----PC2
(wan2)

DSR1 info

Lan IP:192.168.10.1/24

Wan1 IP:1.1.1.1/24, Gateway:1.1.1.254/24

Wan2 IP:2.2.2.1/24, Gateway:2.2.2.254/24

DSR2 info

Lan IP:192.168.20.1/24

Wan1 IP:3.3.3.1/24, Gateway:3.3.3.254/24

Wan2 IP:4.4.4.1/24, Gateway:4.4.4.254/24

Router info

P1:1.1.1.254/24, P2:2.2.2.254/24,

P3:3.3.3.254/24, P4:4.4.4.254/24

PC1:192.168.10.100/24, Gateway:192.168.10.1

PC2:192.168.20.100/24, Gateway:192.168.20.1

Setup Procedure:

.

DSR1 Setting

1. Configure the IP address on DSR1 as above info
2. Configure the Port mode as Auto-Rollover
SETUP/Internet Settings/WAN MODE

<ul style="list-style-type: none"> Internet Settings > Wireless Settings > Network Setting... > DMZ Setup > VPN Settings > USB Settings > VLAN Settings > 	WAN MODE LOGOUT
<p>This page allows user to configure the policies on the two WAN ports for Internet connection.</p> <p style="text-align: center;"> <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/> </p>	
Port Mode	
<p>Auto-Rollover using WAN port: <input checked="" type="radio"/></p> <p>Primary WAN: <input type="text" value="WAN1"/></p> <p>Secondary WAN: <input type="text" value="WAN2"/></p> <p>Load Balancing: <input type="radio"/> <input type="text" value="Round Robin"/></p> <p>Use only single WAN port: <input type="radio"/> <input type="text" value="WAN1"/></p>	
WAN Failure Detection Method	
<p>None: <input type="radio"/></p> <p>DNS lookup using WAN DNS Servers: <input type="radio"/></p> <p>DNS lookup using DNS Servers: <input type="radio"/></p> <p>WAN1: <input type="text" value="0.0.0.0"/></p> <p>WAN2: <input type="text" value="0.0.0.0"/></p> <p>WAN3: <input type="text" value="0.0.0.0"/></p> <p>Ping these IP addresses: <input checked="" type="radio"/></p> <p>WAN1: <input type="text" value="3.3.3.1"/></p> <p>WAN2: <input type="text" value="0.0.0.0"/></p> <p>WAN3: <input type="text" value="0.0.0.0"/></p> <p>Retry Interval is: <input type="text" value="10"/> (Optional)</p> <p>Failover after: <input type="text" value="3"/> (Failures)</p>	

3. Add a IPsec policy : ipsec-1 as below
 - Policy Name:**ipsec-1**
 - Select Local Gateway:**Dedicated WAN**
 - Remote Endpoint:IP Address, **3.3.3.1**
 - Local IP:Subnet
 - Local start IP Address:192.168.10.0
 - Local Subnet Mask:255.255.255.0
 - Remote IP:Subnet
 - Remote Start IP Address:192.168.20.0
 - Remote Subnet Mask:255.255.255.0
 - Phase1
 - Encryption Algorithm:AES-128
 - Authentication Algorithm:SHA-1
 - Authentication method:Pre-shared key
 - Pre-shared key:dlink12345
 - Enable Dead Peer Detection**
 - Phase2
 - Encryption Algorithm:AES-128
 - Authentication Algorithm:SHA-1

4. Add a IPsec policy : ipsec-2 as below
Policy Name:**ipsec-2**
Select Local Gateway:**Configurable WAN**
Remote Endpoint:IP Address, **4.4.4.1**
Local IP:Subnet
Local start IP Address:192.168.10.0
Local Subnet Mask:255.255.255.0
Remote IP:Subnet
Remote Start IP Address:192.168.20.0
Remote Subnet Mask:255.255.255.0
Phase1
Encryption Algorithm:AES-128
Authentication Algorithm:SHA-1
Authentication method:Pre-shared key
Pre-shared key:dlink12345
Enable Dead Peer Detection
Phase2
Encryption Algorithm:AES-128
Authentication Algorithm:SHA-1
5. Back to configure the IPsec policy:ipsec-1,
Enable Redundant Gateway, and select “ipsec-2”

Redundant VPN Gateway Parameters	
Enable Redundant Gateway:	<input checked="" type="checkbox"/>
Select Back- up Policy:	ipsec-2 ▾
Failback time to switch from back-up to primary:	30 (Seconds)

6. Enable WAN interface respond to ping
ADVANCED/Advanced network/WAN Port Setup

DSR-1000N	SETUP	ADVANCED	TOOLS
Application Rules	<h3>WAN PORT SETUP</h3> <p>This page allows user to configure advanced WAN options for the router.</p> <p>Save Settings Don't Save Settings</p> <h4>WAN Ping</h4> <p>Respond to Ping: <input checked="" type="checkbox"/></p> <h4>WAN1 Port Setup</h4> <p>MTU Size: Default</p> <p>Custom MTU: 1500</p> <p>Port Speed: Auto Sense</p>		
Website Filter			
Firewall Setting...			
Wireless Settings			
Advanced Network...			
Routing			
Certificates			
External Authentica			
Users			
IP/MAC Binding			
IPv6			

DSR2 Setting

1. Configure the IP address on DSR2 as previous info
2. Configure the Port mode as Auto-Rollover

SETUP/Internet Settings/WAN MODE

Internet Settings	<h3>WAN MODE</h3> <p>This page allows user to configure the policies on the two WAN ports for Internet connection.</p> <p>Save Settings Don't Save Settings</p> <p>LOGOUT</p>
Wireless Settings	<h4>Port Mode</h4> <p>Auto-Rollover using WAN port: <input checked="" type="radio"/></p> <p>Primary WAN: WAN1</p> <p>Secondary WAN: WAN2</p> <p>Load Balancing: Round Robin</p> <p>Use only single WAN port: WAN1</p> <h4>WAN Failure Detection Method</h4> <p>None: <input type="radio"/></p> <p>DNS lookup using WAN DNS Servers: <input type="radio"/></p> <p>DNS lookup using DNS Servers: <input type="radio"/></p> <p>WAN1: 0.0.0.0</p> <p>WAN2: 0.0.0.0</p> <p>WAN3: 0.0.0.0</p> <p>Ping these IP addresses: <input checked="" type="radio"/></p> <p>WAN1: 1 1 1 1</p> <p>WAN2: 0.0.0.0</p> <p>WAN3: 0.0.0.0</p> <p>Retry Interval is: 10 (Optional)</p> <p>Failover after: 3 (Failures)</p>
Network Setting...	
DMZ Setup	
VPN Settings	
USB Settings	
VLAN Settings	

3. Add a IPsec policy : ipsec-1 as below
Policy Name:**ipsec-1**
Select Local Gateway:**Dedicated WAN**
Remote Endpoint:IP Address, **1.1.1.1**
Local IP:Subnet
Local start IP Address:192.168.20.0
Local Subnet Mask:255.255.255.0
Remote IP:Subnet
Remote Start IP Address:192.168.10.0
Remote Subnet Mask:255.255.255.0
Phase1
Encryption Algorithm:AES-128
Authentication Algorithm:SHA-1
Authentication method:Pre-shared key
Pre-shared key:dlink12345
Enable Dead Peer Detection
Phase2
Encryption Algorithm:AES-128
Authentication Algorithm:SHA-1

4. Add a IPsec policy : ipsec-2 as below
Policy Name:**ipsec-2**
Select Local Gateway:**Configurable WAN**
Remote Endpoint:IP Address, **2.2.2.1**
Local IP:Subnet
Local start IP Address:192.168.20.0
Local Subnet Mask:255.255.255.0
Remote IP:Subnet
Remote Start IP Address:192.168.10.0
Remote Subnet Mask:255.255.255.0
Phase1
Encryption Algorithm:AES-128
Authentication Algorithm:SHA-1
Authentication method:Pre-shared key
Pre-shared key:dlink12345
Enable Dead Peer Detection
Phase2

Encryption Algorithm: AES-128
Authentication Algorithm: SHA-1

5. Back to configure the IPsec policy: ipsec-1, Enable Redundant Gateway, and select "ipsec-2"

Redundant VPN Gateway Parameters	
Enable Redundant Gateway:	<input checked="" type="checkbox"/>
Select Back-up Policy:	ipsec-2 ▾
Failback time to switch from back-up to primary:	30 (Seconds)

6. Enable WAN interface respond to ping
ADVANCED/Advanced network/WAN Port Setup

DSR-1000H	SETUP	ADVANCED	TOOLS	
Application Rules ▾	WAN PORT SETUP This page allows user to configure advanced WAN options for the router. <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/>			
Website Filter ▾				
Firewall Setting... ▾				
Wireless Settings ▾				
Advanced Network... ▾				
Routing ▾				WAN Ping
Certificates				Respond to Ping: <input checked="" type="checkbox"/>
External Authentica ▾				WAN1 Port Setup
Users ▾				MTU Size: Default ▾
IP/MAC Binding				Custom MTU: 1500
IPv6 ▾	Port Speed: Auto Sense ▾			

End of this document.