

# Interoperability Profile for D-Link DSR Router Series

Last updated: 2011-01-14

---

## Overview

This document describes how to configure the D-Link DSR-1000N to implement IPSec gateway to gateway with pre-shared secrets, specified in "Document Profiles for IPSec interoperability " by the VPN Consortium.

The following is a typical gateway-to-gateway IPSec VPN. This use case will go through IPSec VPN tunnel configuration between D-Link DSR-1000N router and DFL-800 firewall.

## [Topology]

(L:192.168.3.1)DSR-1000N(W1:192.168.40.2)----(192.168.40.1)Router(192.168.10.1)  
----(W1:192.168.10.254)DFL-800(Lan:192.168.1.1)

#####

## The settings of DFL-800

#####

```
set Interface Ethernet wan1 DHCPEnabled=No
```

```
set Interface Ethernet wan1 DefaultGateway=192.168.10.1
```

```
set Address IP4Address InterfaceAddresses/wan1_ip Address=192.168.10.254
```

```
set Address IP4Address InterfaceAddresses/wan1net Address=192.168.10.0/24
```

```
add PSK ipsec-psk Type=ASCII PSKAscii=testtest
```

```
add Interface IPsecTunnel ipsec-if AuthMethod=PSK IKEAlgorithms=Medium IPsecAlgorithms=Medium
```

```
PSK=ipsec-psk LocalNetwork=InterfaceAddresses/lannet RemoteNetwork=192.168.3.0/24
```

```
RemoteEndpoint=192.168.40.2
```

```
add Interface InterfaceGroup ipsec-lan Members=ipsec-if,lan
```

```
add IPRule Action=Allow SourceInterface=ipsec-lan SourceNetwork=all-nets
```

```
DestinationInterface=ipsec-lan DestinationNetwork=all-nets Service=all_services Index=1
```

```
LogEnabled=Yes Name=ipsec-lan-allow
```

#####

# The settings of DSR-1000N

#####

## 1. The settings of WAN1 IP address:

The screenshot displays the D-Link DSR-1000N web management interface. At the top, it shows 'Product Page: DSR-1000N' and 'Hardware Version: A1 Firmware Version: 1.02B07'. The D-Link logo is prominently displayed. The navigation menu includes 'DSR-1000N', 'SETUP', 'ADVANCED', 'TOOLS', 'STATUS', and 'HELP'. The 'Internet Settings' menu is expanded, showing options like Wizard, Internet Settings, Wireless Settings, Network Settings, DMZ Setup, VPN Settings, USB Settings, and VLAN Settings. The main content area is titled 'WAN1 SETUP' and includes a 'LOGOUT' link. A descriptive paragraph states: 'This page allows you to set up your Internet connection. Ensure that you have the Internet connection information such as the IP Addresses, account information, etc. This information is usually provided by your ISP or network administrator.' Below this are 'Save Settings' and 'Don't Save Settings' buttons. The configuration is organized into sections: 'ISP Connection Type' (Static), 'PPPoE Profile Name' (No PPPoE Profiles), 'User Name', 'Password', 'Secret', 'MPPE Encryption', 'Split Tunnel', 'Connectivity Type' (Keep Connected), 'Idle Time', 'My IP Address', 'Server Address', and 'Host Name'. The 'Internet (IP) Address' section shows 'IP Address Source' (Use Static IP Address), 'IP Address' (192.168.40.2), 'IP Subnet Mask' (255.255.255.0), and 'Gateway IP Address' (192.168.40.1). The 'Domain Name System (DNS) Servers' section shows 'DNS Server Source' (Use These DNS Servers), 'Primary DNS Server' (1.1.1.1), and 'Secondary DNS Server'. The 'Mac Address' section shows 'MAC Address Source' (Use Default Address) and 'MAC Address'. A 'Helpful Hints...' sidebar on the right provides additional context. The footer contains 'UNIFIED SERVICES ROUTER' and 'Copyright © 2010 D-Link Corporation.'

## 2. IPSec policy settings at DSR-1000N

IPSec General setting:

General	
<b>Policy Name:</b>	<input type="text" value="ipsec-if"/>
<b>Policy Type:</b>	<input type="text" value="Auto Policy"/>
<b>IPSec Mode:</b>	<input type="text" value="Tunnel Mode"/>
<b>Select Local Gateway:</b>	<input type="text" value="Dedicated WAN"/>
<b>Remote Endpoint:</b>	<input type="text" value="IP Address"/>
	<input type="text" value="192.168.10.254"/>
<b>Enable NetBIOS:</b>	<input type="checkbox"/>
<b>Enable RollOver:</b>	<input type="checkbox"/>
<b>Enable DHCP:</b>	<input type="checkbox"/>
<b>Local IP:</b>	<input type="text" value="Subnet"/>
<b>Local Start IP Address:</b>	<input type="text" value="192.168.3.0"/>
<b>Local End IP Address:</b>	<input type="text" value=""/>
<b>Local Subnet Mask:</b>	<input type="text" value="255.255.255.0"/>
<b>Remote IP:</b>	<input type="text" value="Subnet"/>
<b>Remote Start IP Address:</b>	<input type="text" value="192.168.1.0"/>
<b>Remote End IP Address:</b>	<input type="text" value=""/>
<b>Remote Subnet Mask:</b>	<input type="text" value="255.255.255.0"/>

IPSec Phase1 setting:

Phase1(IKE SA Parameters)	
Exchange Mode:	Main
Direction / Type:	Both
Nat Traversal:	
On:	<input checked="" type="radio"/>
Off:	<input type="radio"/>
NAT Keep Alive Frequency (in seconds):	20
Local Identifier Type:	Local Wan IP
Local Identifier:	
Remote Identifier Type:	Remote Wan IP
Remote Identifier:	
Encryption Algorithm:	3DES
Authentication Algorithm:	SHA-1
Authentication Method:	Pre-shared key
Pre-shared key:	testtest
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
Username:	
Password:	

IPSec Phase2 setting:

Phase2-(Manual Policy Parameters)	
SPI-Incoming:	<input type="text"/>
SPI-Outgoing:	<input type="text"/>
Encryption Algorithm:	3DES
Key Length:	<input type="text"/>
Key-In:	<input type="text"/>
Key-Out:	<input type="text"/>
Integrity Algorithm:	SHA-1
Key-In:	<input type="text"/>
Key-Out:	<input type="text"/>

  

Phase2-(Auto Policy Parameters)	
SA Lifetime:	3600 <input type="text"/> Seconds
Encryption Algorithm:	3DES
Key Length:	<input type="text"/>
Integrity Algorithm:	SHA-1
PFS Key Group:	<input type="checkbox"/> DH Group 1 (768 bit)

#####

**[Verification]:**

1. Check the IPSEC SAs database, both IKE and IPSEC SAs are established without problem.
2. To initial the ICMP traffic from DFL-800, DFL-800 is able to reach the LAN1 IP of DSR-1000N

#####

```
vpnstats -ike -ipsec -verbose
```

```
--- Active IKE SAs:
```

```
1 Remote peer: 192.168.40.2:500
```

```
Identities:
```

```
local : 192.168.10.254
```

```
remote: 192.168.40.2
```

```
# Negotiations in progress: 1
```

```
Bytes sent : 796
```

```
Created : 2010-09-16 07:12:08
```

Last used : 2010-09-16 07:12:18  
Expires : 2010-09-16 15:12:08  
Encryption alg : 3des-cbc  
Hash alg : sha1  
PRF alg : hmac-sha1

--- Active IPsec SAs:

2 IPsec Tunnel : ipsec-if  
Endpoints : 192.168.1.0/24 <--> 192.168.3.0/24  
Local IP : 192.168.1.1  
Remote gateway : 192.168.40.2  
Protocol : ESP: 3des-cbc hmac-sha1-96  
SPI (in) : 0x539d72e0  
SPI (out) : 0x2084729  
NAT information:  
Local end behind NAT : No  
Remote end behind NAT: No  
Authentication information:  
Auth method : Pre-shared key  
Local ID : 192.168.1.0/24  
Remote ID : 192.168.3.0/24

DFL-800:/> ping 192.168.3.1 -count=5  
Sending 5 4-byte ICMP pings to 192.168.3.1 from 192.168.1.1  
ICMP Reply from 192.168.3.1 seq=0 time=<10 ms TTL=64  
ICMP Reply from 192.168.3.1 seq=1 time=<10 ms TTL=64  
ICMP Reply from 192.168.3.1 seq=2 time=<10 ms TTL=64  
ICMP Reply from 192.168.3.1 seq=3 time=<10 ms TTL=64  
ICMP Reply from 192.168.3.1 seq=4 time=<10 ms TTL=64  
#####

End of document.