

How to setup IPSec Hub-and-Spoke VPN between DFL series and DSR series? (DSR works as a Hub in the scenario)

[Prerequisite]

DFL Netdefend series x2 (Firmware version 2.27.02.11)

DSR 1000N x1 (Firmware version 1.03b09)

[Scenario]

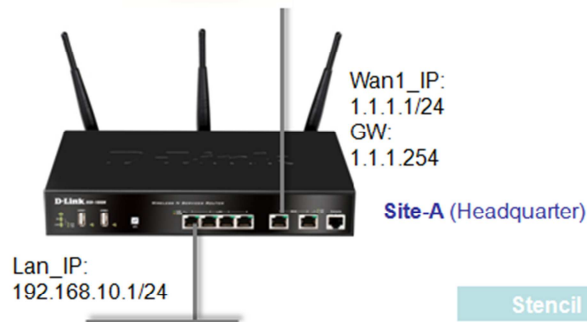
The DSR is in charge of all the VPN routing and centralizes management the VPN traffic to-and-from DFLs in the current scenario.

[Topology]



IPSEC paramaters:

1. IKE proposal(Phase1)
 - Encryption: AES-128
 - Authentication: SHA-1
 - Authentication Method: Pre-shared key
 - Key value: testtest
 - DH Group: Group2
 - SA-lifetime: 28800 seconds
 - DPD: Enable
2. IPSEC proposal(Phase2)
 - Encryption: 3DES
 - Integrity Algorithm: SHA-1
 - PFS: none
 - SA-lifetime: 3600 seconds



Stencil	Description
	FasterEthernet

[Configuration]

The settings of DSR-1000N

#####

1. In the **SETUP** page, go to **Internet Settings->WAN1 settings->WAN1 Setup**, configure the necessary information as following figure shown for WAN1 interface.

D-Link®

DSR-1000N //	SETUP	ADVANCED	TOOLS	STATUS	HELP
Wizard ▶	WAN1 SETUP LOGOUT				Helpful Hints... The setup page lets you configure the ISP settings to enable this router to connect to the Internet. This router supports multiple connections. Please select the appropriate connection to connect to the Internet. More...
Internet Settings ▷	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. <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/>				
Wireless Settings ▶	ISP Connection Type				
Network Settings ▶	ISP Connection Type: <input type="text" value="Static IP"/>				
DMZ Setup ▶	IP Address: <input type="text" value="1.1.1.1"/>				
VPN Settings ▶	IP Subnet Mask: <input type="text" value="255.255.255.0"/>				
USB Settings ▶	Gateway IP Address: <input type="text" value="1.1.1.254"/>				
VLAN Settings ▶	Domain Name System (DNS) Servers				
	Primary DNS Server: <input type="text" value="1.1.1.254"/>				
	Secondary DNS Server: <input type="text" value="1.1.1.254"/>				
	Mac Address				
	MAC Address Source: <input type="text" value="Use Default Address"/>				
	MAC Address: <input type="text" value="00:00:00:00:00:00"/>				

UNIFIED SERVICES ROUTER

Copyright © 2010 D-Link Corporation.

2. In the [SETUP](#) page, go to [VPN settings->IPSEC->IPSEC POLICIES](#), add a VPN policy here.

D-Link®

DSR-1000N //	SETUP	ADVANCED	TOOLS	STATUS	HELP																		
Wizard Internet Settings Wireless Settings Network Settings DMZ Setup VPN Settings USB Settings VLAN Settings	<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> <div style="background-color: #cccccc; padding: 2px;">List of VPN Policies</div> <div style="background-color: #cccccc; padding: 2px;">Auto Policy</div> <table border="1" style="width: 100%; border-collapse: collapse;"><thead><tr><th><input type="checkbox"/></th><th>Status</th><th>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 colspan="9" style="background-color: #cccccc; padding: 2px;">Manual Policy</td></tr></tbody></table> <div style="text-align: right; margin-top: 10px;"><input type="button" value="Edit"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/> <input style="border: 1px solid #ccc; background-color: #eee; padding: 2px 10px; cursor: pointer; color: #ccc; text-decoration: none; font-size: 0.9em; font-weight: normal; border-radius: 3px; box-shadow: 1px 1px 0px #ccc;" type="button" value="Add"/></div>				<input type="checkbox"/>	Status	Name	Type	IPSec Mode	Local	Remote	Auth	Encr	Manual Policy									Helpful Hints... <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> More...
<input type="checkbox"/>	Status	Name	Type	IPSec Mode	Local	Remote	Auth	Encr															
Manual Policy																							

UNIFIED SERVICES ROUTER

3. In the [IPSEC Configuration](#) page, fill in all the parameters as following figure shown, and then [Save Settings](#).



DSR-1000N	SETUP	ADVANCED	TOOLS	STATUS	HELP
-----------	-------	----------	-------	--------	------

Wizard	▶
Internet Settings	▶
Wireless Settings	▶
Network Settings	▶
DMZ Setup	▶
VPN Settings	▶
USB Settings	▶
VLAN Settings	▶

IPSEC CONFIGURATION

[LOGOUT](#)

This page allows user to add/edit VPN (IPSec) policies which includes Auto and Manual policies.

General

Policy Name:	<input type="text" value="ipsec-vpn"/>
Policy Type:	<input type="text" value="Auto Policy"/>
IPSec Mode:	<input type="text" value="Tunnel Mode"/>
Select Local Gateway:	<input type="text" value="Dedicated WAN"/>
Remote Endpoint:	<input type="text" value="FQDN"/>
	<input type="text" value="0.0.0.0"/>
Enable Mode Config:	<input type="checkbox"/>
Enable NetBIOS:	<input type="checkbox"/>
Enable RollOver:	<input type="checkbox"/>
Protocol:	<input type="text" value="ESP"/>
Enable DHCP:	<input type="checkbox"/>
Local IP:	<input type="text" value="Any"/>
Local Start IP Address:	<input type="text"/>
Local End IP Address:	<input type="text"/>
Local Subnet Mask:	<input type="text"/>
Remote IP:	<input type="text" value="Any"/>
Remote Start IP Address:	<input type="text"/>
Remote End IP Address:	<input type="text"/>
Remote Subnet Mask:	<input type="text"/>

Phase1(IKE SA Parameters)

Exchange Mode:	<input type="text" value="Main"/>
Direction / Type:	<input type="text" value="Both"/>
Nat Traversal:	
On:	<input checked="" type="radio"/>
Off:	<input type="radio"/>
NAT Keep Alive Frequency (in seconds):	<input type="text" value="20"/>
Local Identifier Type:	<input type="text" value="Local Wan IP"/>
Local Identifier:	<input type="text"/>
Remote Identifier Type:	<input type="text" value="Remote Wan IP"/>
Remote Identifier:	<input type="text"/>
Encryption Algorithm:	<input type="text" value="AES-128"/>
Key Length:	<input type="text" value="0"/>
Authentication Algorithm:	<input type="text" value="SHA-1"/>
Authentication Method:	<input type="text" value="Pre-shared key"/>
Pre-shared key:	<input type="text" value="testtest"/>

Helpful Hints...

Use Tunnel mode if you require communication to be secured between networks. Transport mode can be used if the requirement is to have secure communication between 2 hosts. Use Manual Policy parameters if you wish to specify the keys to be used for encryption/decryption (during communication). This is for advanced users who require more control over IPsec tunnel communication. For normal users, Auto Policy would do just fine. Enable Rollover only if the Port Mode is 'Auto-Rollover' in WAN MODE settings page. The active WAN will be used for setting up the tunnel, thus providing an uninterrupted VPN connection. Enable DHCP over IPsec checkbox to allow external users to form a VPN to DSR-1000N. Multiple users can connect as well.

[More...](#)

#####

The settings of DFL-SiteB

#####

```
set Interface Ethernet wan DHCPEnabled=No
set Device Name=DFL210-siteB
set Address IP4Address InterfaceAddresses/lan_ip Address=192.168.20.1
set Address IP4Address InterfaceAddresses/lannet Address=192.168.20.0/24
set Address IP4Address InterfaceAddresses/wan_ip Address=2.2.2.1
set Address IP4Address InterfaceAddresses/wannet Address=2.2.2.0/24
set Address IP4Address InterfaceAddresses/wan_gw Address=2.2.2.254
add PSK ipsec-psk Type=ASCII PSKAscii=testtest
add Address IP4Address DSR-lannet Address=192.168.10.0/24
add Address IP4Address DFL210-siteB-lannet Address=192.168.30.0/24
add Address IP4Group DSR-and-SiteB-lannets Members=DSR-lannet,DFL210-siteB-lannet

add Interface IPsecTunnel ipsec-to-DSR AuthMethod=PSK IKEAlgorithms=Medium
IPsecAlgorithms=Medium RemoteNetwork=DSR-and-SiteB-lannets
LocalNetwork=InterfaceAddresses/lannet PSK=ipsec-psk RemoteEndpoint=1.1.1.1

add Interface InterfaceGroup lan-ipsec Members=lan,ipsec-to-DSR

add IPRule Action=Allow SourceInterface=lan-ipsec SourceNetwork=all-nets
DestinationInterface=lan-ipsec DestinationNetwork=all-nets Service=all_services Index=1
LogEnabled=Yes Name=allow-ipsec-lan

set IPRule 2(ping_fw) SourceInterface=lan-ipsec SourceNetwork=all-nets
```

Save then Activate

#####

The settings of DFL-SiteC

#####

```
set Interface Ethernet wan DHCPEnabled=No
set Device Name=DFL210-siteC
set Address IP4Address InterfaceAddresses/lan_ip Address=192.168.30.1
set Address IP4Address InterfaceAddresses/lannet Address=192.168.30.0/24
set Address IP4Address InterfaceAddresses/wan_ip Address=3.3.3.1
set Address IP4Address InterfaceAddresses/wannet Address=3.3.3.0/24
set Address IP4Address InterfaceAddresses/wan_gw Address=3.3.3.254
add PSK ipsec-psk Type=ASCII PSKAscii=testtest
add Address IP4Address DSR-lannet Address=192.168.10.0/24
add Address IP4Address DFL210-siteC-lannet Address=192.168.20.0/24
add Address IP4Group DSR-and-SiteC-lannets Members=DSR-lannet,DFL210-siteC-lannet

add Interface IPsecTunnel ipsec-to-DSR AuthMethod=PSK IKEAlgorithms=Medium
IPsecAlgorithms=Medium RemoteNetwork=DSR-and-SiteC-lannets
LocalNetwork=InterfaceAddresses/lannet PSK=ipsec-psk RemoteEndpoint=1.1.1.1

add Interface InterfaceGroup lan-ipsec Members=lan,ipsec-to-DSR

add IPRule Action=Allow SourceInterface=lan-ipsec SourceNetwork=all-nets
DestinationInterface=lan-ipsec DestinationNetwork=all-nets Service=all_services Index=1
LogEnabled=Yes Name=allow-ipsec-lan

set IPRule 2(ping_fw) SourceInterface=lan-ipsec SourceNetwork=all-nets
```

Save then Activate

#####

[Expected result]

On the DFL-SiteA

1. Try to initial the PING to the LAN_IP of Site-B and Site-C respectively, both LAN_IPs shall be reachable.

On the DFL-SiteB

1. Check if both IPSEC tunnels have been established, one to Site-A(DSR,192.168.10.0/24), another one to Site-C(DFL,192.168.30.0/24).

```
DFL210-siteB:/> vpnstats
--- Active IPsec SAs:
Displaying one line per SA-bundle
IPsec Tunnel      Local Net          Remote Net          Remote Endpoint
-----
ipsec-to-DSR      192.168.20.0/24   192.168.10.0/24    1.1.1.1
ipsec-to-DSR      192.168.20.0/24   192.168.30.0/24    1.1.1.1
```

On the DFL-SiteC

2. Check if both IPSEC tunnels have been established, one to Site-A(DSR,192.168.10.0/24), another one to Site-B(DFL,192.168.20.0/24).

```
DFL210-siteC:/> vpnstats
--- Active IPsec SAs:
Displaying one line per SA-bundle
IPsec Tunnel      Local Net          Remote Net          Remote Endpoint
-----
ipsec-to-DSR      192.168.30.0/24   192.168.10.0/24    1.1.1.1
ipsec-to-DSR      192.168.30.0/24   192.168.20.0/24    1.1.1.1
DFL210-siteC:/> █
```

End of document.