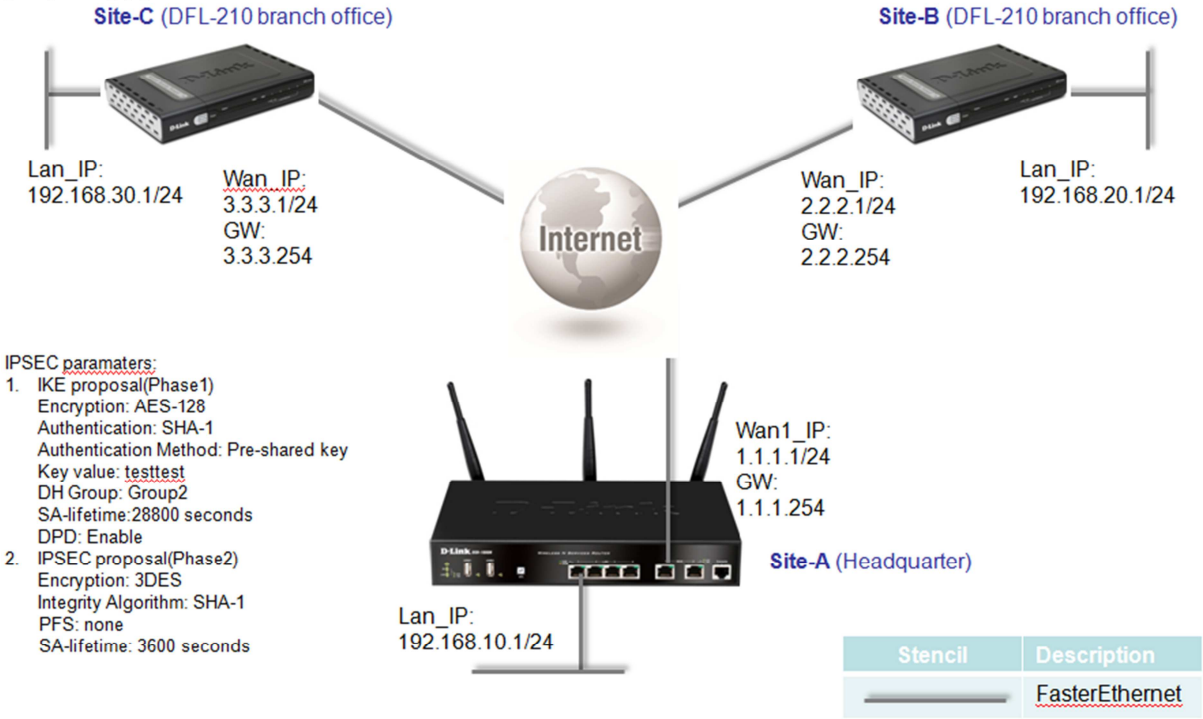
How to setup IPSec Hub-and-Spoke VPN between DFL series and DSR series? (DSR works as a Hub in the scenario)

[Prerequisite]
DFL Netdefend series x2 (Firmware version 2.27.02.11)
DSR 1000N x1 (Firmware version 1.03b09)

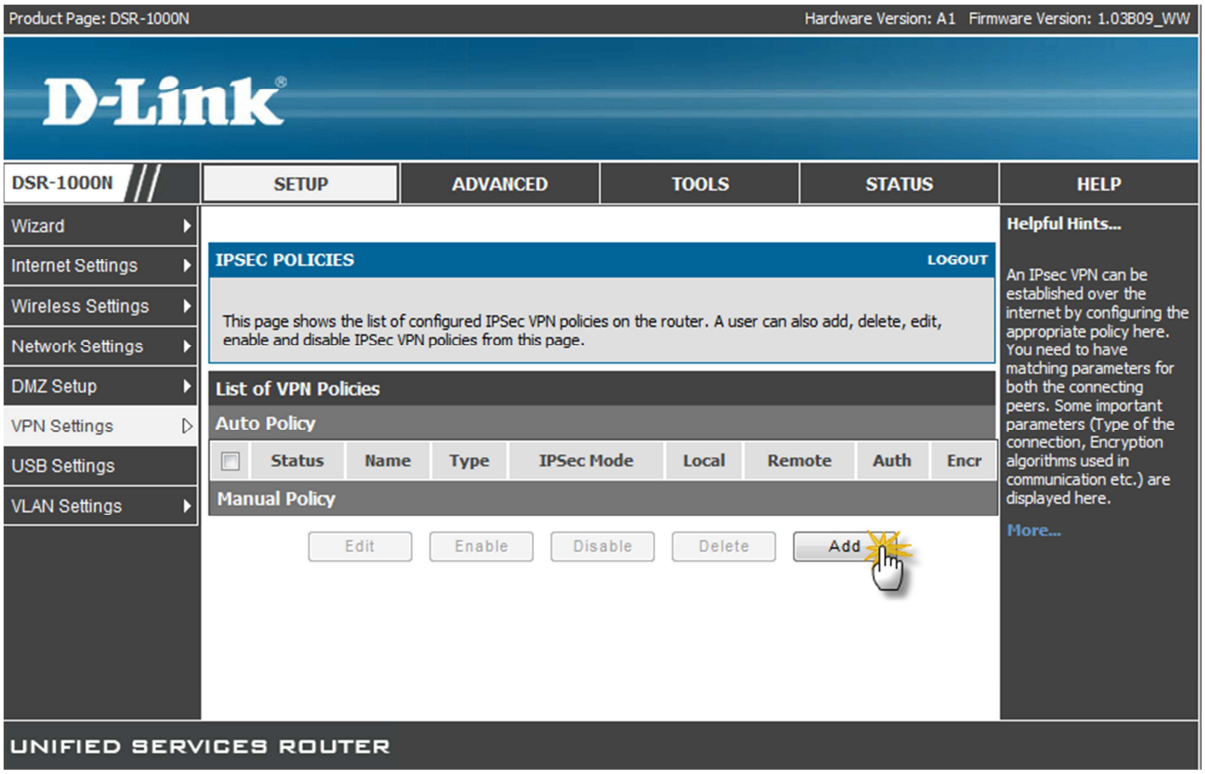
[Scenario]
The DSR is in charge of all the VPN routing and centralizes managment the VPN traffic to-and-from DFLs in the current scenario.

[Topology]

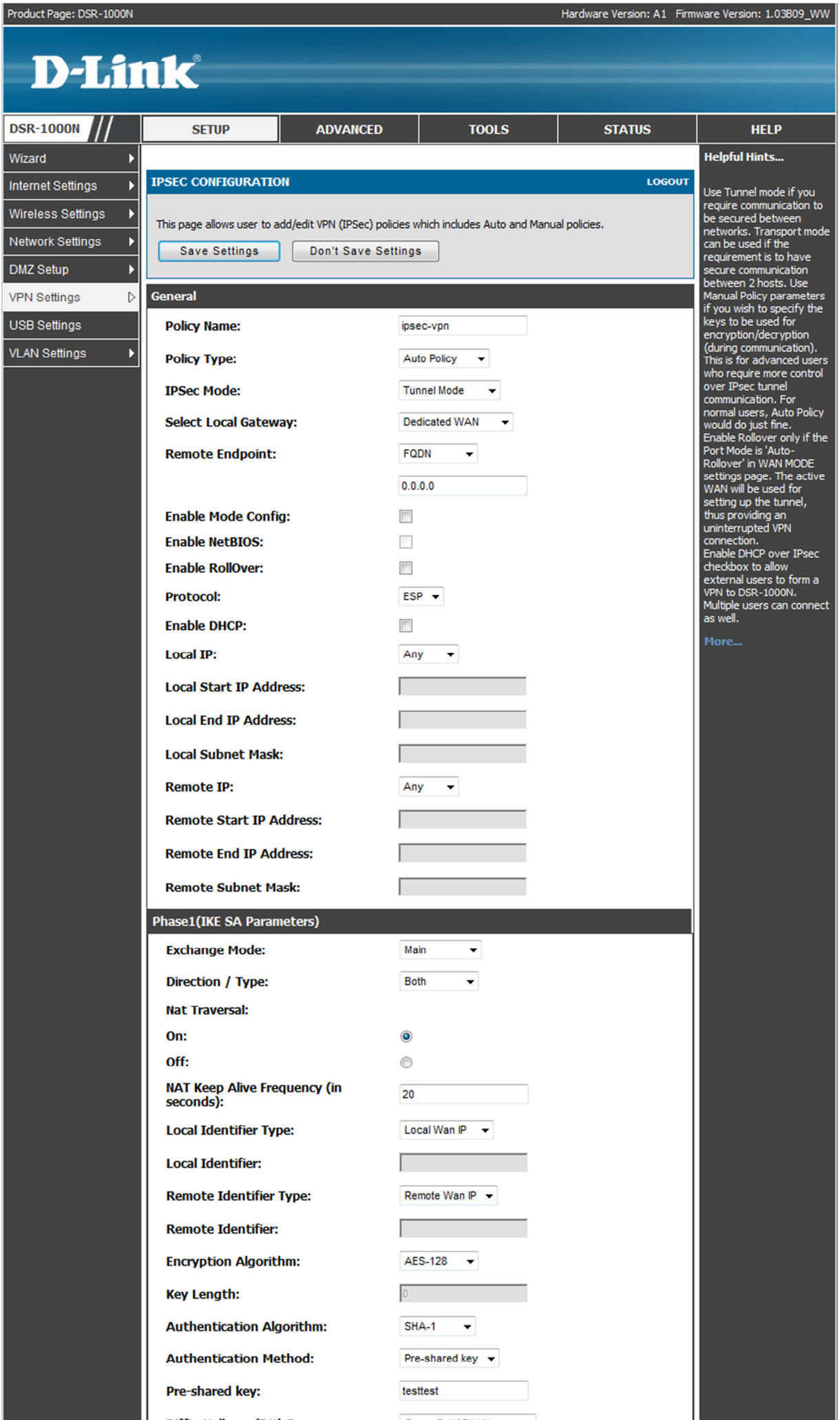


[Configuration]
The settings of DSR-1000N
##
1. In the SETUP page, go to Internet Settings->WAN1 settings->WAN1 Setup, configure the necessary information as following figure shown for WAN1 interface.

2.In the SETUP page, go to VPN settings->IPSEC->IPSEC POLICIES, add a VPN policy here.



3.In the IPSEC Configuration page, fill in all the paramaters as following figure shown, and then Save Settings.


Product Page: DSR-1000N
Hardware Version: A1 Firmware Version: 1.03B09_WW
D-Link
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.
Save Settings
Don't Save Settings
General
Policy Name:
ipsec-vpn
Policy Type:
Auto Policy
IPSec Mode:
Tunnel Mode
Select Local Gateway:
Dedicated WAN
Remote Endpoint:
FQDN
0.0.0.0
Enable Mode Config:
Enable NetBIOS:
Enable RollOver:
Protocol:
ESP
Enable DHCP:
Local IP:
Any
Local Start IP Address:
Local End IP Address:
Local Subnet Mask:
Remote IP:
Any
Remote Start IP Address:
Remote End IP Address:
Remote Subnet Mask:
Phase1(IKE SA Parameters)
Exchange Mode:
Main
Direction / Type:
Both
Nat Traversal:
On:
Off:
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:
AES-128
Key Length:
0
Authentication Algorithm:
SHA-1
Authentication Method:
Pre-shared key
Pre-shared key:
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.