

DMVPN

[Original file](#)

NETSHe firmware user guide

DM VPN implementation

2018 © NETSHe Lab Ltd.

DM VPN overview

DM VPN is a technology to establish secured VPN over public IP networks such as Internet.

DM VPN operates with two types of nodes:

- HUB which represent central office or cloud service and control all VPN connections;
- SPOKE which represent branch office and establish connection to central office and (may be) another branches.

DM VPN implements star (all traffic in VPN goes through HUB) or full mesh (traffic goes between branches) topologies.

It is possible to prohibit spoke-to-spoke communications by firewall or advanced routing rules in star topology. This case may be useful to meet different enterprise requirements.

I other way, mesh topology allows to unload hub channels, to reduce hub load (and hub hardware requirements), to reduce spoke-to-spoke delay.

Spokes may have static or dynamically assigned IP address, may be behind NAT (*).

Hub must have static IP address and must not be behind NAT (). **Hub may be addressed through FQDN (Full Qualified Domain Name). In case of FQDN addressing, using of dynamically assigned IP addresses is allowed with understanding and agreement about service interruption when Hub address is changing. * Some types of NAT or NAT settings may prohibit DM VPN Spoke functionality.** Hub may be behind properly configured NAT with multi-point GRE and IPSec bypassing.

Typical DM VPN application is shown below.

Hub





VPN



Spoke n



Spoke 1



Spoke 2

DMVPN Tunnels btween Spokes

Traditional Static Tunnels and DM VPN tunnels which match traditional

Static and known IP Addresses

Dynamically assigned IP Addresses

DM VPN basics

DM VPN relies on three proven technologies:

1. Next Hop Resolution Protocol (NHRP): Creates a distributed (NHRP) mapping database of all the spoke tunnels to real (public interface) addresses.
2. Multi-point GRE Tunnel Interface: Single GRE interface to support multiple GRE tunnels.
3. IPSec: Secures data through GRE tunnels.

To simplify and automate routing management, DM VPN also uses dynamic routing service like OSPF

or BGP.

DM VPN components. NHRP.

Provides registration, resolution and redirect services.

NHRP registration:

- Spoke dynamically registers its mapping with NHS
- Supports spokes with dynamic NBMA addresses or NAT

NHRP resolutions and redirects

- Supports building dynamic spoke-to-hub and spoke-to-spoke tunnels
- Creates star or full-mesh overlay network topology

DM VPN components. Multipoint GRE tunnel

Provides single tunnel interface and NHRP source.

Single tunnel interface (multi-point)

- Non-Broadcast Multi-Access (NBMA) network
- Smaller hub configuration
- Multicast and broadcast support
- Dynamic tunnel destination

Next Hop Resolution Protocol (NHRP)

- VPN IP-to-NBMA IP address mapping
- Short-cut forwarding
- Direct support for dynamic addresses and NAT

DM VPN components. IPSec

DM VPN builds out a dynamic tunnel overlay network.

IPSec is triggered through “tunnel protection” and works with NHRP together:

- NHRP triggers IPSec before installing new mappings.
- IPSec notifies NHRP when encryption is ready.
- NHRP installs mappings, and sends registration if needed.
- NHRP and IPSec notify each other when a mapping or service assurance is cleared.

DM VPN components. Dynamic routing

Dynamic routing service such as BGP or OSPF is used to establish right routing rules to Hub and every Spoke automatically.

Each available routing services have own advantages:

- OSPF requires less configuration.
- BGP provides less delay for overlay network reconfiguration and routing exchange.

Major features

1. DM VPN offers configuration reduction and no-touch deployment
2. Supports IP Unicast, IP Multicast, and dynamic routing protocols
3. Supports remote peers with dynamically assigned addresses
4. Supports spoke routers behind dynamic NAT and hub routers behind static NAT
5. Dynamic spoke-to-spoke tunnels for scaling partial- or full-mesh VPNs
6. Uses IPsec encryption to secure data

Typical use cases

Controlled corporate extra-net network

Star topology. Spoke-to-spoke communications are prohibited (or controlled) by firewall or routing rules.

Meshed corporate network

Meshed topology. Spoke-to-spoke communications are allowed to reduce latency and hub load.

DM VPN as backup for MPLS network

Meshed topology. Spoke-to-spoke communications are allowed to reduce latency and hub load. DM VPN is used only when primary MPLS network is down.

DM VPN implementation details and limitations

NETSHe firmware provides:

- Simple configuration in a few steps
- Hub and Spoke functionality out of the box.
- PSK protected IPsec tunnels
- OSPF or BGP routing over the overlay network. Routing does not require any additional configuration.
- CISCO Hub and Spoke compatibility with BGP and OSPF routing over the overlay network.

Limitations:

- Single or twoHub(s) in the network.
- One device can act as one HUB only.
- SPOKE can have no more than two configured tunnel to HUBs.
- Requires to have default-route through main WAN interface for HUB and first/single SPOKE tunnels functionality.
- Another vendor Hub and Spoke compatibility with OSPF is not tested yet. (*)

* - Work is in progress.

How to configure

Typical supported topology

Current implementation supports next DM VPN topology:

1. Single HUB and single tunnel from SPOKE through main (or single) WAN interface.
2. Single HUB and single tunnel from SPOKE through main WAN interface. Second WAN interface may be used as backup link for single tunnel.
3. Two HUBs (primary and backup) with two different concurrent tunnels through single WAN interface.
4. Two HUBs (primary and backup) with two different concurrent tunnels through main WAN interface and second WAN interface.

This topologies will be addressed below.

Spoke configuration

Spoke can be configured in two ways:

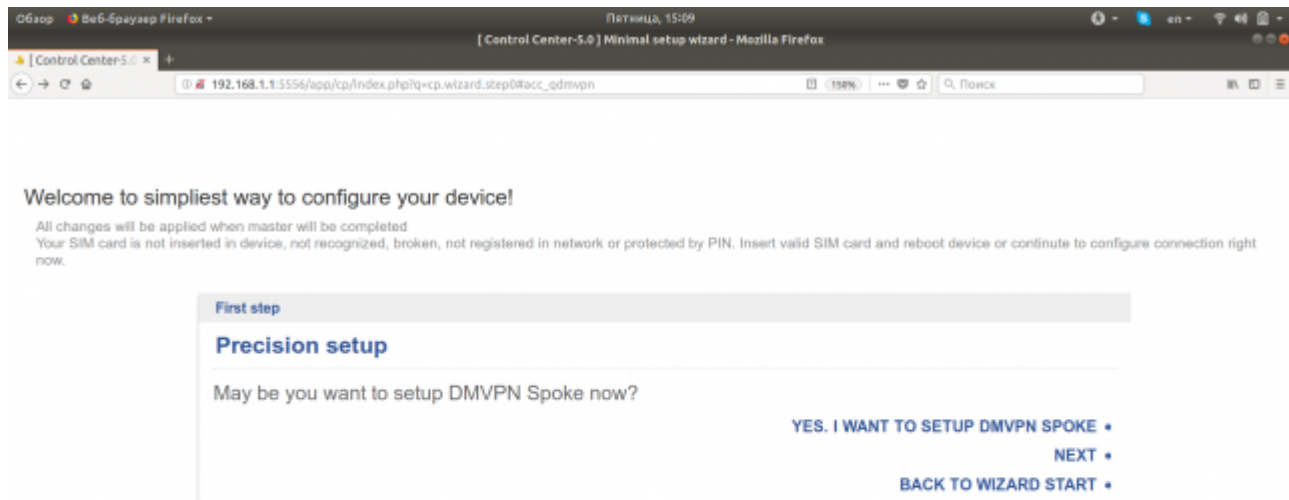
Through setup wizard or simple web-interface

This way allow to configure SPOKE with single tunnel to single HUB in the network (topology 1) or primary tunnel for SPOKE for topologies 2,3 and 4 (second tunnel configuration will require to access full web-interface).

Please keep in mind that this way allows to configure cellular connection as backup or second WAN

link for topologies 2 and 4.

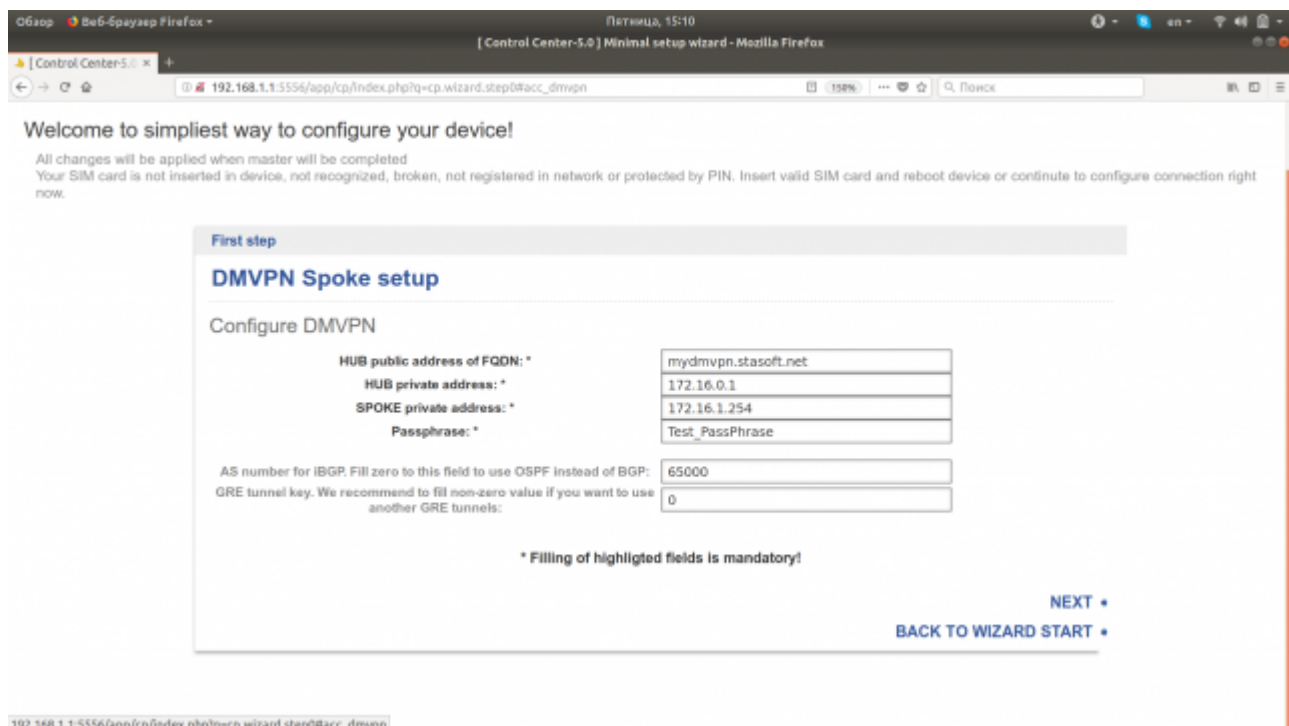
To configure spoke, go through setup wizard till DM VPN configuration question as shown below.



192.168.1.1:5556/app/cp/index.php?q=cp.wizard.step0@acc_dmvpn

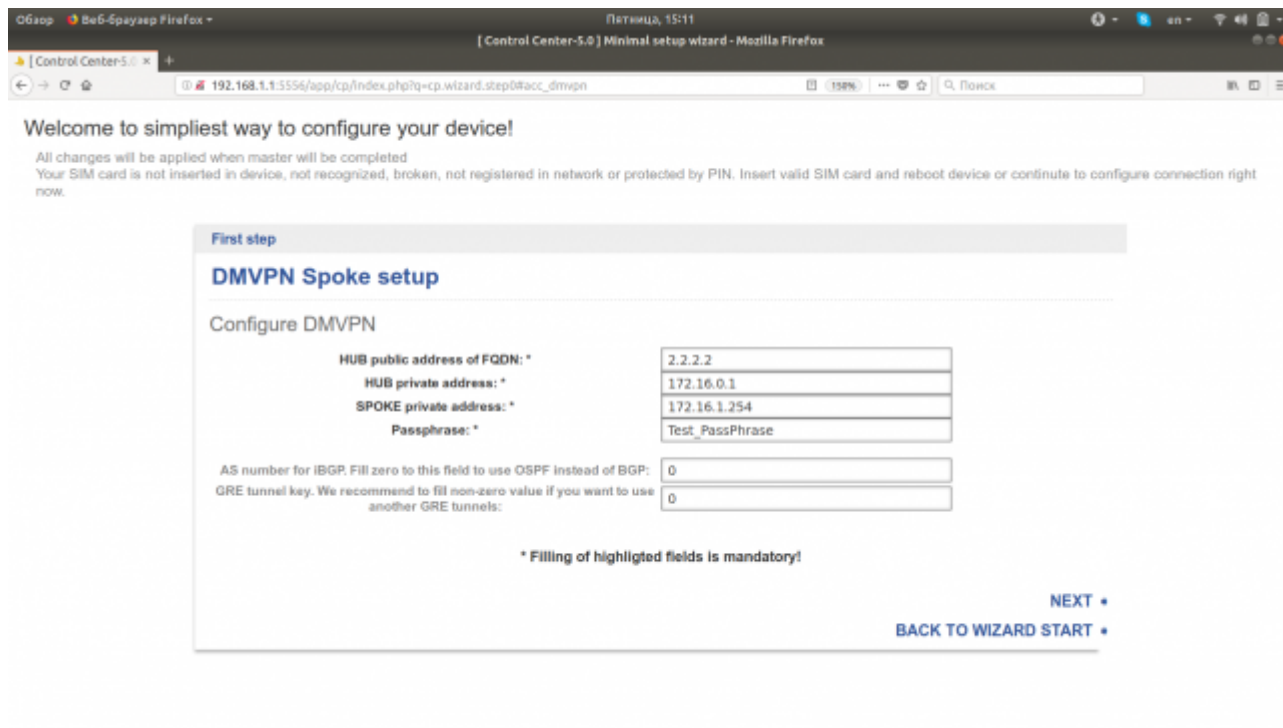
Choose „Yes. I want to setup DM VPN spoke» option then fill DM VPN Hub address, Spoke private address, passphrase for IPsec, AS number if you want to use BGP routing and mandatory tunnel key.

Please keep in mind that Hub address may be FQDN as show below or



192.168.1.1:5556/app/cp/index.php?q=cp.wizard.step0@acc_dmvpn

static IP address as shown below



The

last setup will use OSPF routing (AS number is zero).

Some optional parameters can be configured here like authentication secret and hold time for NHRP, tunnel cost, area, hello and dead time for OSPF, metric for BGP.

Complete setup wizard and reboot device. Enjoy running DM VPN spoke.

Through full web-interface

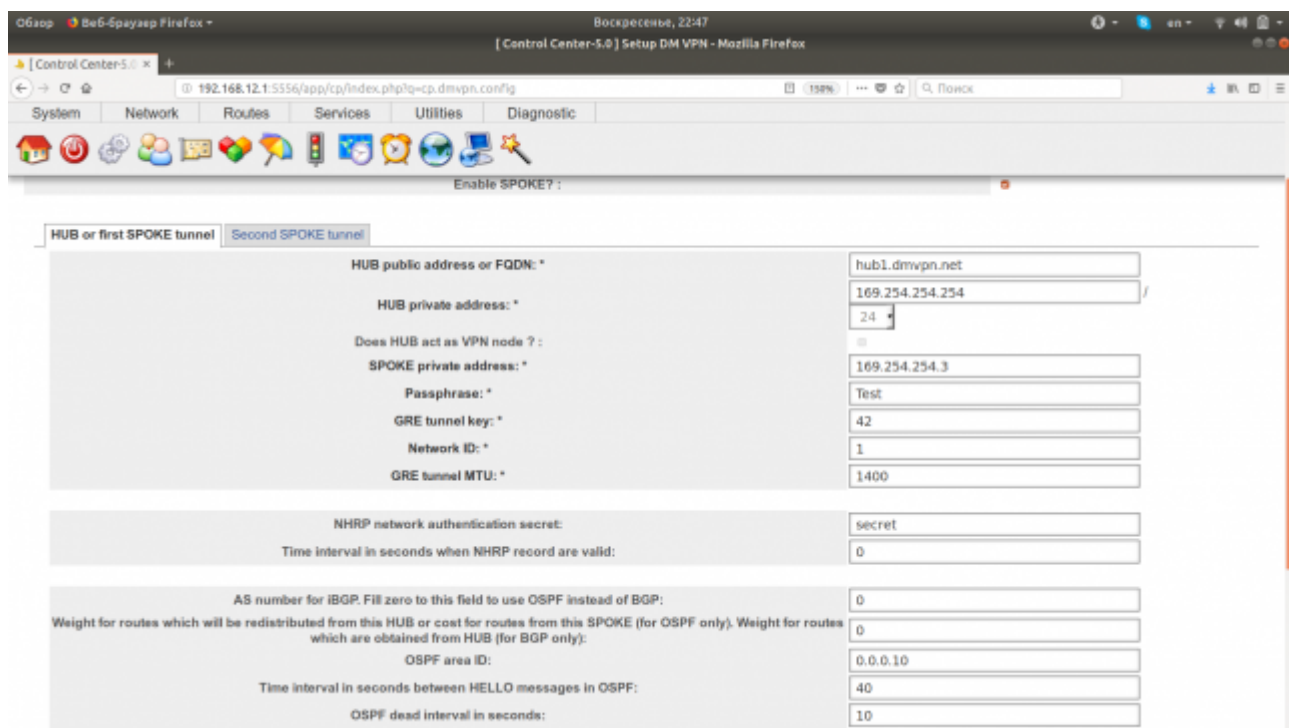
This way allows to configure SPOKE to any available topologies.

To configure DM VPN Spoke through expert web-interface, please select menu „Services→Access concentrator→DM VPN» as shown below.

Last update: 2020/12/17 05:40
настройка_dm_vpn http://docs.netshe-lab.ru/doku.php?id=%D0%BD%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B9%D0%BA%D0%B0_dm_vpn



Tick „Enable SPOKE“ checkbox and fill related fields as shown below.



To configure second tunnel to another HUB, please select second tab.

It should be noted! Second tunnel can be configured through the same WAN interface as primary tunnel or through another WAN interface.

If system does not see second WAN interface, it will not offer to select source interface for second tunnel and will use primary WAN interface automatically.

It should be noted! Configuring DM VPN SPOKE with two concurrent tunnels through two WAN

interfaces (topology 4) with concurrent default-routes will provide non predicable result.

We offer to implement topology 4 in next manner:

- Configure primary WAN interface with default route (wire or cellular)
- Configure second WAN interface without default route (wire or cellular). Use option 'Do not replace existing default route' when configure this interface.
- Configure static route to second HUB through second WAN interface.
- Configure second SPOKE tunnel to second HUB and select second WAN interface as tunnel source.

Control Center-5.0 Setup DM VPN - Mozilla Firefox

192.168.12.1:5556/app/cp/index.php?c=cp.dmvpn.config

System Network Routes Services Utilities Diagnostic

Enable SPOKE? :

HUB or first SPOKE tunnel Second SPOKE tunnel

Source interface for second connection: wwan0

HUB public address or FQDN: 100.100.100.1

HUB private address: 172.16.0.1

SPOKE private address: 172.16.100.100

GRE tunnel key: 43

Network ID: 1

GRE tunnel MTU: 1400

NHRP network authentication secret: secret2

Time interval in seconds when NHRP record are valid: 0

Weight for routes which will be redistributed from this HUB or cost for routes from this SPOKE (for OSPF only). Weight for routes which are obtained from HUB (for BGP only): 200

OSPF area ID:

Time interval in seconds between HELLO messages in OSPF: 0

OSPF dead interval in seconds: 0

Tick to restart service(s) after saving: ☐ Save

Control Center-5.0 Configure interface wwan0 - Mozilla Firefox

192.168.12.1:5556/app/cp/index.php?c=core.ifaces.cfg&fname=wwan0

System Network Routes Services Utilities Diagnostic

[Configure interface wwan0]

Enable interface :

Base settings Additional Helpful information Routes through interface

Type of connection: * QMI

Username:

Password:

Access point (APN): internet

PIN code:

Authentication type: auto

Use any possible cellular network or specified only: auto

Disable roaming: ☐

Do not replace existing default route?: ☒

Do not use peer DNS?: ☐

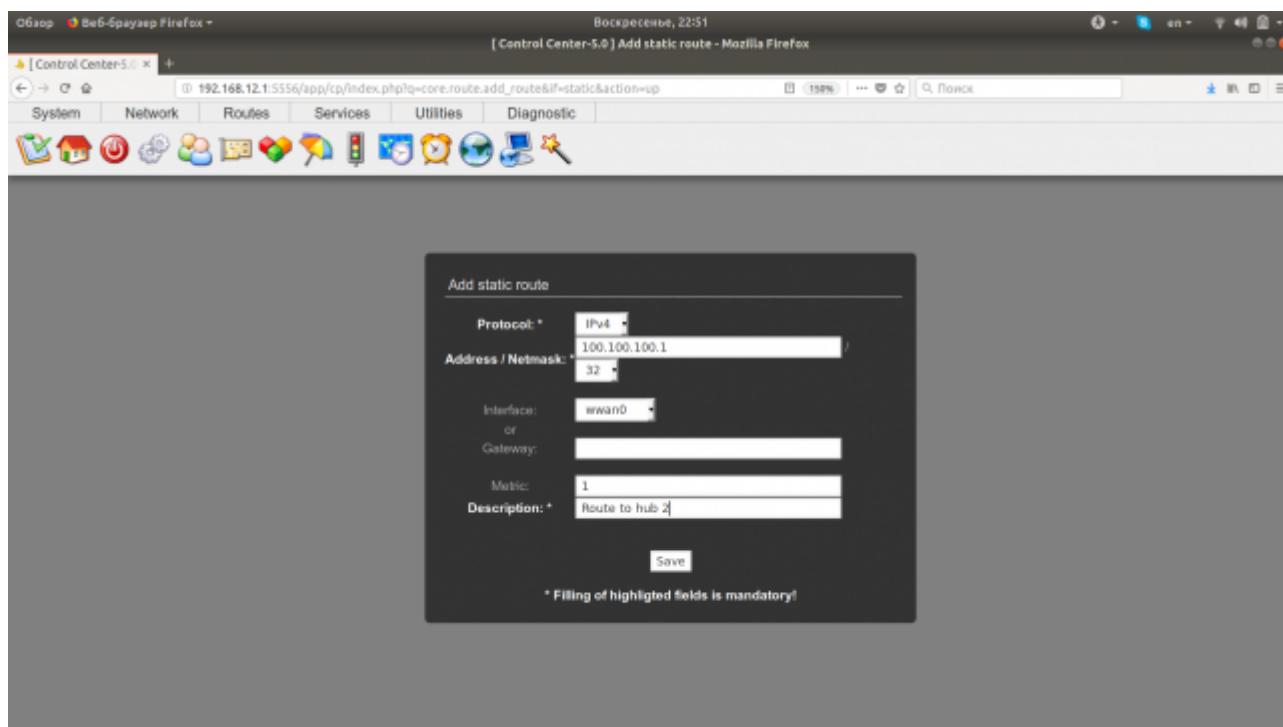
Enable IP v6 over PPP link?: ☐

Switch device in IP passthrough mode?: ☐

MTU: 1500

Static IP address for interface. Usually ISP assigns address in automatic manner. Leave blank if you are unsure:

Tick to control console(s) after enable: ☐ Save

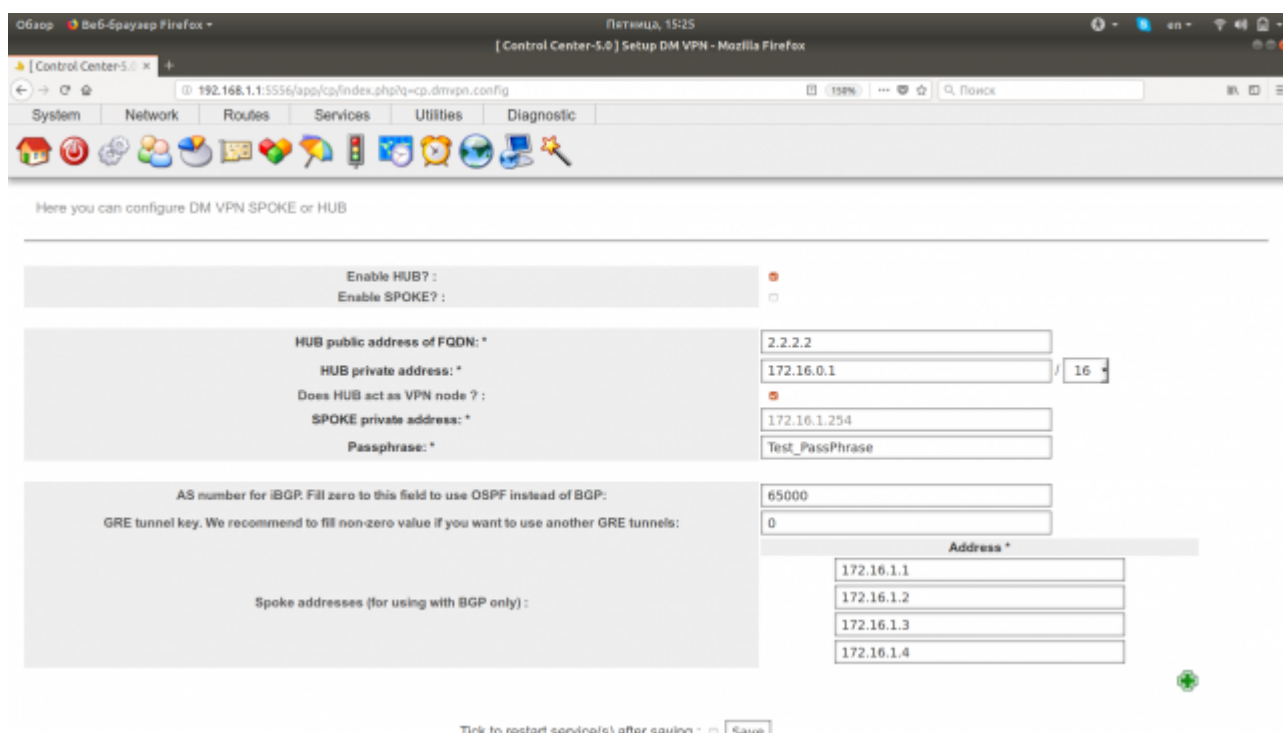


Press «Save» button. If you will tick «Restart service..» checkbox, you will be prompted to reboot device.

Hub configuration

Hub configuration is available in full web-interface only.

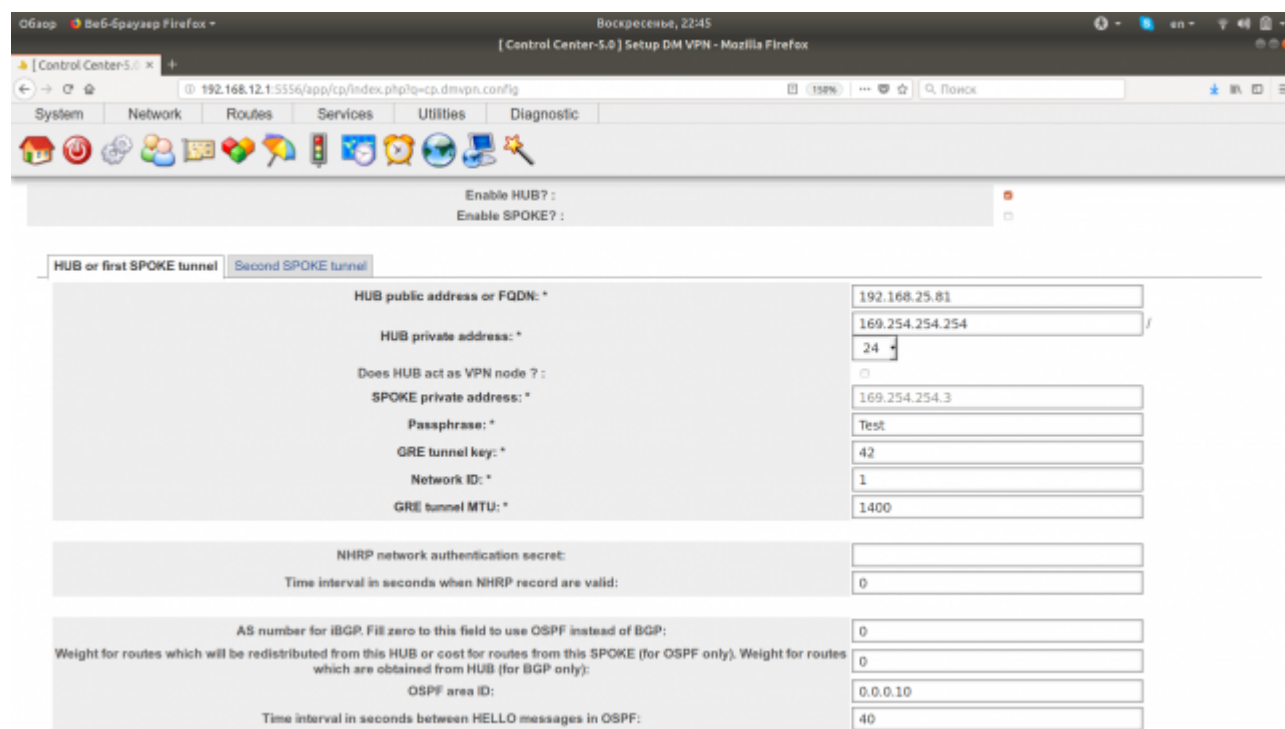
To configure DM VPN Hub, select menu «Services→Access concentrator→DM VPN». Tick «Enable HUB» checkbox and fill related fields as shown below.



Please keep in mind that when you used BGP routing (AS number is not zero), you must specify every SPOKE address. Of course, when you use OSPF routing (AS number is zero), you may not specify any SPOKE addresses.

Please keep in mind that you must specify private network netmask for HUB setup. Any SPOKE addresses must be from network which is specified by HUB private address and netmask.

Another field which is specific for HUB setup is «Does HUB act as VPN node?». When this field is ticked, networks behind HUB LAN interfaces will be introduced to overlay network.



Control Center 5.0 Setup DM VPN - Mozilla Firefox

192.168.12.1:5556/app/cp/index.php?cp=dmvpn.config

System Network Routes Services Utilities Diagnostic

Enable HUB? :
Enable SPOKE? :

HUB or first SPOKE tunnel Second SPOKE tunnel

HUB public address or FQDN: * 192.168.25.81

HUB private address: * 169.254.254.254 / 24

Does HUB act as VPN node ? : ☐

SPOKE private address: * 169.254.254.3

Passphrase: * Test

GRE tunnel key: * 42

Network ID: * 1

GRE tunnel MTU: * 1400

NHRP network authentication secret:

Time interval in seconds when NHRP record are valid: 0

AS number for iBGP. Fill zero to this field to use OSPF instead of BGP: 0

Weight for routes which will be redistributed from this HUB or cost for routes from this SPOKE (for OSPF only). Weight for routes which are obtained from HUB (for BGP only): 0

OSPF area ID: 0.0.0.10

Time interval in seconds between HELLO messages in OSPF: 40

Why so few setup options are here?

We tried to simplify DM VPN setup process as possible:

- We announce LAN side networks to the HUB by default.
- We discover external WAN interface and WAN address automatically.
- We create and setup all parts of DM VPN automatically.
- We switch mGRE tunnel to another WAN interface and back in a backup process automatically.

Conclusion

The security has never been so affordable!

Last
update:
2020/12/17 05:40 настройка_dm_vpn http://docs.netshe-lab.ru/doku.php?id=%D0%BD%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B9%D0%BA%D0%B0_dm_vpn

From:
<http://docs.netshe-lab.ru/> - Документация по NETSHe

Permanent link:
http://docs.netshe-lab.ru/doku.php?id=%D0%BD%D0%B0%D1%81%D1%82%D1%80%D0%BE%D0%B9%D0%BA%D0%B0_dm_vpn

Last update: **2020/12/17 05:40**

