Template:Networking rutxxx manual vpn dmvpn

DMVPN

Dynamic Multipoint VPN (**DMVPN**) is a method of building scalable IPsec VPNs. DMVPN is configured as a hub-and-spoke network, where tunnels between spokes are built dynamically; therefore, no change in configuration is required on the hub in order to connect new spokes.

DMVPN configuration

To create a new DMVPN instance, go to the *Services → VPN → DMVPN* section, enter a custom name and click the 'Add' button. A DMVPN instance with the given name will appear in the "DMVPN Configuration" list.

To begin configuration, click the 'Edit' button located next to the instance. Refer to the figures and tables below for information on the DMVPN instance configuration:

[[File:{{{file_dmvpn_config}}}]]

Field	Value	Description
Enabled	yes | no; default: **no**	Turns the DMVPN instance on or off.
Working mode	Spoke | Hub; default: **Spoke**	Selects the role of this instance • **Hub** - the central instance of DMVPN that connects other peers (spokes) into single network. There is no need to reconfigure the hub when connecting new spokes to it. • **Spoke** - an instance that connects to the hub.
Hub address	ip | host; default: **off**	IP address or hostname of a DMVPN hub.

[[File:{{{file_dmvpn_gre_config}}}]]

Field	Value	Description
Tunnel source	network interface; default: **none**	Network interface used to establish the GRE Tunnel.
Local GRE interface IP address	ip; default: **none**	IP address of the local GRE Tunnel network interface.
Spoke: Remote GRE interface IP address	ip; default: **none**	IP address of the remote GRE Tunnel instance.
Hub: Local GRE interface netmask	netmask; default: **none**	Subnet mask of the local GRE Tunnel network interface.

GRE MTU	integer; default: **1476**	Sets the maximum transmission unit (MTU) size. It is the largest size of a protocol data unit (PDU) that can be transmitted in a single network layer transaction.
GRE keys	integer [0..65535]; default: **none**	A key used to identify incoming and outgoing GRE packets.

[[File:{{{file_dmvpn_ipsec_config}}}]]

Field	Value	Description
Negotiation mode	Main | Aggressive; default: **Main**	Internet Security and Key Management Protocol (ISAKMP) phase 1 exchange mode. • **Main** - performs three two-way exchanges between the initiator and the receiver (a total of 9 messages). • **Aggressive** - performs fewer exchanges than main mode (a total of 6 messages) by storing most data into the first exchange. In aggressive mode, the information is exchanged before there is a secure channel, making it less secure but faster than main mode.
My identifier type	FQDN | User FQDN | Address; default: **FQDN**	Defines the type of identity used in user (IPsec instance) authentication. • **FQDN** - identity defined by fully qualified domain name. It is the complete domain name for a host (for example, *something.somedomain.com*). Only supported with IKEv2. • **User FQDN** - identity defined by fully qualified username string (for example, *username@something.somedomain.com*). Only supported with IKEv2. • **Address** - identity by IP address.
My identifier	ip | string; default: **none**	Defines how the user (IPsec instance) will be identified during authentication.
Encryption algorithm	DES | 3DES | AES128 | AES192 | AES256; default: **3DES**	Algorithm used for data encryption.
Authentication/Hash algorithm	MD5 | SHA1 | SHA256 | SHA384 | SHA512; default: **SHA1**	Algorithm used for exchanging authentication and hash information.
DH group/PFS group	MODP768 | MODP1024 | MODP1536 | MODP2048 | MODP3072 | MODP4096; default: **MODP1536**	
Lifetime	integer; default: **8 hours**	Defines a time period after which the phase will re-initiate its exchange of information.

Pre shared key	string; default: **none**	A shared password used for authentication between IPsec peers.
Secret's ID selector	string; default: **none**	Each secret can be preceded by a list of optional ID selectors. A selector is an IP address, a Fully Qualified Domain Name, user@FQDN or %any. **NOTE**: IKEv1 only supports IP address ID selector.

[[File:{{{file_dmvpn_nhrp_config}}}]]

Field	Value	Description
NHRP network ID	integer; default: **1**	An identifier used to define the NHRP domain. This is a local parameter and its value does not need to match the values specified on other domains. However, the NHRP ID is added to packets which arrive on the GRE interface; therefore, it may be helpful to use the same ID for troubleshooting purposes.
NHRP hold time	integer; default: **7200**	Specifies the holding time for NHRP Registration Requests and Resolution Replies sent from this interface or shortcut-target. The hold time is specified in seconds and defaults to two hours.