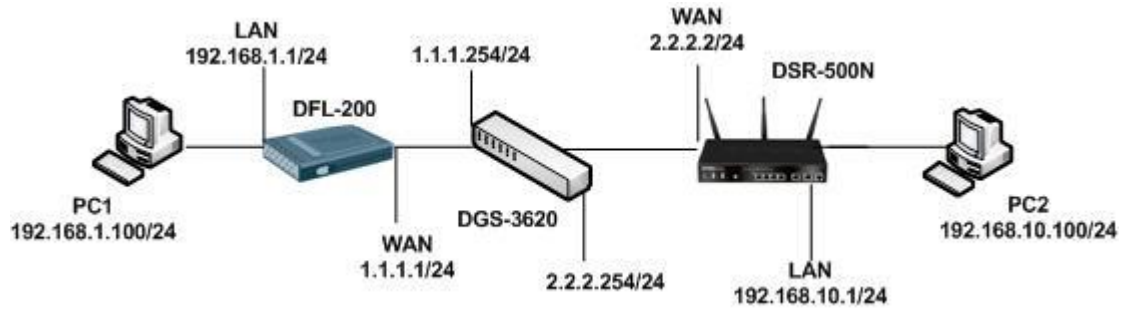


How to set up IPsec Site to Site VPN with DFL-200 and DSR series

[Topology]



[DFL-200 Setup]

VPN > Firewall > Add new

System **Firewall** Servers Tools Status Help

VPN Tunnels

Pick a VPN tunnel to edit from the below list:

[Help](#)

IPsec Tunnels

Name	Local Net	Remote Net	Remote Gateway
for-dsr500	192.168.1.0/24	192.168.10.0/24	2.2.2.2

[\[Add new\]](#) [\[Edit\]](#)

L2TP / PPTP Client

Name	Type	Remote Gateway	User	IPsec
[Add new PPTP client]				
[Add new L2TP client]				

L2TP / PPTP Server

Name	Type	Outer IP	Inner IP	IPsec
[Add new PPTP server]				
[Add new L2TP server]				

- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN
- Certificates
- Content Filtering

VPN Tunnels

Edit IPsec tunnel for-dsr500:

Name: for-dsr500

Local Net: 192.168.1.0/24

Authentication:

PSK - Pre-Shared Key

PSK: ●●●●●●●●

Retype PSK: ●●●●●●●●

Certificate-based

Local Identity: Admin - CN=000F3D6937BC

Certificates:

Use ctrl/shift click to select multiple certificates.
To use ID lists below, you must select a CA certificate.

Identity List: (no list)

Tunnel type:

Roaming Users - single-host IPsec clients

IKE XAuth: Require user authentication via IKE XAuth to open tunnel.

LAN-to-LAN tunnel

Remote Net: 192.168.10.0/24

Remote Gateway: 2.2.2.2

The gateway can be a numerical IP address, DNS name, or range of IP addresses for roaming / NATed gateways.

Route: Automatically add a route for the remote network.

Proxy ARP: Publish remote network on all interfaces via Proxy ARP.

IKE XAuth client: Pass username and password to peer via IKE XAuth, if the remote gateway requires it.

XAuth Username:

XAuth Password:

Delete this VPN tunnel





- Policy
- Port Mapping
- Users
- Schedules
- Services
- VPN**
- Certificates
- Content Filtering

VPN Tunnels

Edit advanced settings of IPsec tunnel for **-dsr500-**:

Limit MTU:

IKE Mode: Main mode IKE
 Aggressive mode IKE

IKE DH Group:

PFS: Enable Perfect Forward Secrecy

PFS DH Group:

NAT Traversal: Disabled.
 On if supported and needed (NAT detected between gateways)
 On if supported

Keepalives: No keepalives.
 Automatic keepalives (works with other DFL-200/700/1100 units)
 Manually configured keepalives:

Source IP:

Destination IP:

IKE Proposal List

	Cipher	Hash	Life KB	Life Sec
#1:	<input type="text" value="3DES"/>	<input type="text" value="MD5"/>	<input type="text" value="0"/>	<input type="text" value="28800"/>
#2:	<input type="text" value="-"/>	<input type="text" value="MD5"/>	<input type="text" value="0"/>	<input type="text" value="28800"/>
#3:	<input type="text" value="-"/>	<input type="text" value="SHA-1"/>	<input type="text" value="0"/>	<input type="text" value="28800"/>
#4:	<input type="text" value="-"/>	<input type="text" value="MD5"/>	<input type="text" value="0"/>	<input type="text" value="28800"/>
#5:	<input type="text" value="-"/>	<input type="text" value="SHA-1"/>	<input type="text" value="0"/>	<input type="text" value="28800"/>
#6:	<input type="text" value="-"/>	<input type="text" value="MD5"/>	<input type="text" value="0"/>	<input type="text" value="28800"/>
#7:	<input type="text" value="-"/>	<input type="text" value="MD5"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
#8:	<input type="text" value="-"/>	<input type="text" value="MD5"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

IPsec Proposal List

	Cipher	HMAC	Life KB	Life Sec
#1:	<input type="text" value="3DES"/>	<input type="text" value="MD5"/>	<input type="text" value="0"/>	<input type="text" value="3600"/>
#2:	<input type="text" value="-"/>	<input type="text" value="MD5"/>	<input type="text" value="0"/>	<input type="text" value="3600"/>
#3:	<input type="text" value="-"/>	<input type="text" value="SHA-1"/>	<input type="text" value="0"/>	<input type="text" value="3600"/>
#4:	<input type="text" value="-"/>	<input type="text" value="MD5"/>	<input type="text" value="0"/>	<input type="text" value="3600"/>
#5:	<input type="text" value="-"/>	<input type="text" value="SHA-1"/>	<input type="text" value="0"/>	<input type="text" value="3600"/>
#6:	<input type="text" value="-"/>	<input type="text" value="MD5"/>	<input type="text" value="0"/>	<input type="text" value="3600"/>

[DSR-500N Setup]

1. Setup > VPN Settings > IPsec > IPsec Policies.

IPSEC CONFIGURATION LOGOUT	
<p>This page allows user to add/edit VPN (IPsec) policies which includes Auto and Manual policies.</p> <p> <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/> </p>	
General	
Policy Name:	to-dfi-200
Policy Type:	Auto Policy
IKE Version:	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
IKE Version:	<input checked="" type="radio"/> IKEv1 <input type="radio"/> IKEv2
IPsec Mode:	Tunnel Mode
Select Local Gateway:	Dedicated WAN
Remote Endpoint:	IP Address
	1.1.1.1
Enable Mode Config:	<input type="checkbox"/>
Enable NetBIOS:	<input type="checkbox"/>
Enable RollOver:	<input type="checkbox"/>
Protocol:	ESP
Enable DHCP:	<input type="checkbox"/>
Local IP:	Subnet
Local Start IP Address:	192.168.10.0
Local End IP Address:	
Local Subnet Mask:	255.255.255.0
Local Prefix Length:	
Remote IP:	Subnet
Remote Start IP Address:	192.168.1.0
Remote Subnet Mask:	255.255.255.0
Remote Prefix Length:	
Enable Keepalive:	<input type="checkbox"/>
Source IP Address:	
Destination IP Address:	
Detection Period:	10
Reconnect after failure count:	3
CAST128:	<input type="checkbox"/>
Authentication Algorithm:	
MD5:	<input checked="" type="checkbox"/>
SHA-1:	<input type="checkbox"/>
SHA2-256:	<input type="checkbox"/>
SHA2-384:	<input type="checkbox"/>
SHA2-512:	<input type="checkbox"/>
Authentication Method:	Pre-shared key
Pre-shared key:	123456789
Diffie-Hellman (DH) Group:	Group 2 (1024 bit)
SA-Lifetime (sec):	28800
Enable Dead Peer Detection:	<input type="checkbox"/>
Detection Period:	10
Reconnect after failure count:	3
Extended Authentication:	None
Authentication Type:	User Database
User Name:	
Password:	

Phase1(IKE SA Parameters)

Exchange Mode:

Direction / Type:

Nat Traversal:

On:

Off:

NAT Keep Alive Frequency (in seconds):

Local Identifier Type:

Local Identifier:

Remote Identifier Type:

Remote Identifier:

Encryption Algorithm:

DES:

3DES:

AES-128:

AES-192:

AES-256:

BLOWFISH:

Phase2-(Auto Policy Parameters)

SA Lifetime:

Encryption Algorithm:

DES:

NONE:

3DES:

AES-128:

AES-192:

AES-256:

TWOFISH (128):

TWOFISH (192):

TWOFISH (256):

BLOWFISH:

CAST128:

Integrity Algorithm:

MD5:

SHA-1:

SHA2-224:

SHA2-256:

SHA2-384:

SHA2-512:

PFS Key Group:

Redundant VPN Gateway Parameters

Enable Redundant Gateway:

Select Back- up Policy:

Failback time to switch from back-up to primary: (Seconds)

[Result]

PC1 can ping to PC2 after VPN tunnel established.

END