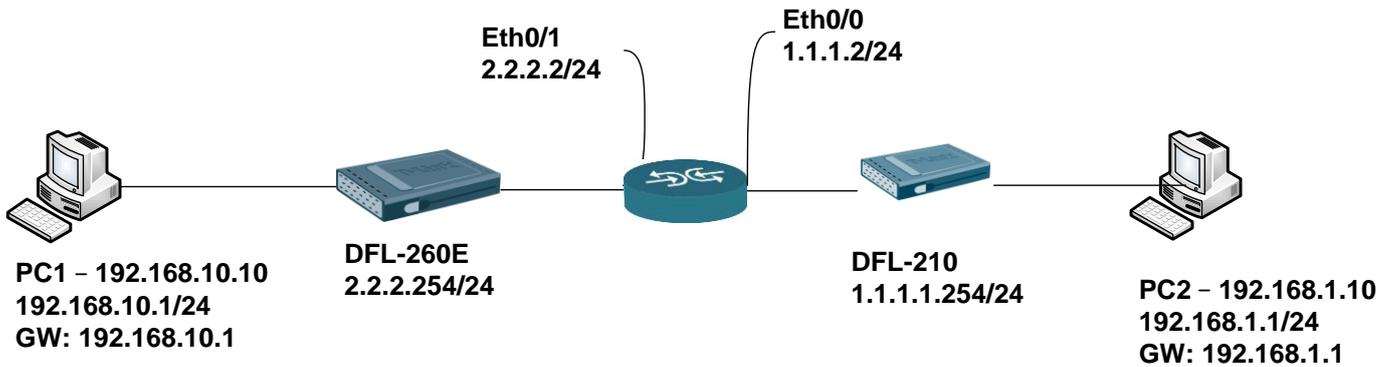


How to set up IPsec Site to Site VPN



DFL-260E Step SOP

1. Create Authentication Objects

Add > Pre-Shared Key

key
PSK (Pre-Shared Key) authentication is based on a shared secret that is known only by the parties involved.

General

General

Name: key

Shared Secret

Passphrase

Shared Secret: ●●●●●●●●

Confirm Secret: ●●●●●●●●

Note! Existing secret will always be shown with 8 characters to hide the actual length.

A PSK containing non-ASCII characters might be encoded differently on other systems and cause a mismatch, e.g. Windows uses UTF-16 while CorePlus uses UTF-8.

2. Create IPsec

Interface > IPsec > Add > IPsec Tunnel

General

site_to_site_vpn
An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

General Authentication XAuth Routing IKE Settings Keep-alive Advanced

General

Name: site_to_site_vpn

Local Network: lanet

Remote Network: 192.168.1.0/24

Remote Endpoint: 1.1.1.254

Encapsulation mode: Tunnel

IKE Config Mode Pool: (None)

Algorithms

IKE Algorithms: Medium

IKE Lifetime: 28800 seconds

IPsec Algorithms: Medium

IPsec Lifetime: 3600 seconds

IPsec Lifetime: 0 kilobytes

Notice: Both sides must have setting same IKE Algorithms.

Authentication

site_to_site_vpn
An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

General **Authentication** XAuth Routing IKE Settings Keep-alive Advanced

Authentication

X.509 Certificate

Root Certificate(s)

Available	Selected
HTTPSAdminCert	

>> <<

Gateway certificate: (None) ▾
Identification list: (None) ▾

Pre-shared Key

Pre-shared key: key ▾

Selects the Pre-shared key to use with this IPsec Tunnel.

3. Create IP Rules

Site_To_Site_Outgoing

Site_To_Site_outgoing
An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General Log Settings NAT SAT Multiplex SAT

General

Name: Site_To_Site_outgoing
Action: Allow ▾
Service: all_services ▾
Schedule: (None) ▾

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

Source	Interface	Network	Destination	Interface	Network
	lan	lannet		site_to_site_vpn	192.168.1.0/24

Site_To_Site_Incoming

Site_To_Site_Incoming
An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General Log Settings NAT SAT Multiplex SAT

General

Name: Site_To_Site_Incoming
Action: Allow ▾
Service: all_services ▾
Schedule: (None) ▾

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

Source	Interface	Network	Destination	Interface	Network
	site_to_site_vpn	192.168.1.0/24		lan	lannet

DFL-210 step SOP as follow DFL-260E.

1. Pre-Shared Key must same as DFL-260E name & password. It must use the same create setting.
2. Create IPsec

Interface > IPsec > Add > IPsec Tunnel

General

The screenshot shows the configuration page for a site-to-site IPsec tunnel. The title is 'site_to_site' with a sub-note: 'An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.' The 'General' tab is selected and highlighted with a red box. Below the tabs, the 'General' section contains several fields: Name (site_to_site), Local Network (lanet), Remote Network (192.168.10.0/24), Remote Endpoint (2.2.2.254), Encapsulation mode (Tunnel), and IKE Config Mode Pool (None). The 'Algorithms' section below contains: IKE Algorithms (Medium), IKE Lifetime (28800 seconds), IPsec Algorithms (Medium), IPsec Lifetime (3600 seconds), and another IPsec Lifetime (0 kilobytes). A red box highlights the 'General' tab and the 'General' and 'Algorithms' sections.

Authentication

The screenshot shows the 'Authentication' tab of the 'site_to_site' IPsec tunnel configuration. The 'Authentication' tab is selected and highlighted with a red box. The page shows two radio buttons for authentication: 'X.509 Certificate' (unselected) and 'Pre-shared Key' (selected). Under 'X.509 Certificate', there are two boxes: 'Available' (containing 'HTTPSAdminCert') and 'Selected' (empty), with '>>' and '<<' buttons between them. Below are dropdown menus for 'Gateway certificate' (None) and 'Identification list' (None). The 'Pre-shared Key' section has a dropdown menu for 'Pre-shared key' (key) and a note: 'Selects the Pre-shared key to use with this IPsec Tunnel.' A red box highlights the 'Pre-shared Key' section.

3. Create IP Rules

Site_To_Site_Outgoing

Site_To_Site_outgoing
An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General | Log Settings | NAT | SAT | Multiplex SAT

General

Name: Site_To_Site_outgoing
Action: Allow
Service: all_services
Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

Source: Interface: lan, Network: lannet
Destination: site_to_site, 192.168.10.0/24

Site_To_Site_Incoming

Site_To_Site_incoming
An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General | Log Settings | NAT | SAT | Multiplex SAT

General

Name: Site_To_Site_incoming
Action: Allow
Service: all_services
Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters have to match for the rule to match.

Source: site_to_site, 192.168.10.0/24
Destination: lan, lannet

Test

Use ping command ping PC2 in PC1, if ICMP has response.

The Site-to-Site VPN is working.

```
Administrator: 命令提示字元
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>
C:\Windows\system32>
C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Bluetooth ????:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Ethernet adapter Lan:

    Connection-specific DNS Suffix . :
    Link-local IPv6 Address . . . . . : fe80::3ceb:8de4:bb64:c440%11
    IPv4 Address. . . . . : 192.168.10.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1

Tunnel adapter isatap.<BDP7F960-3C5A-464A-AECL-3E6F26EF3C86>:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Windows\system32>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:
Reply from 192.168.1.10: bytes=32 time=2ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126
Reply from 192.168.1.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

END