

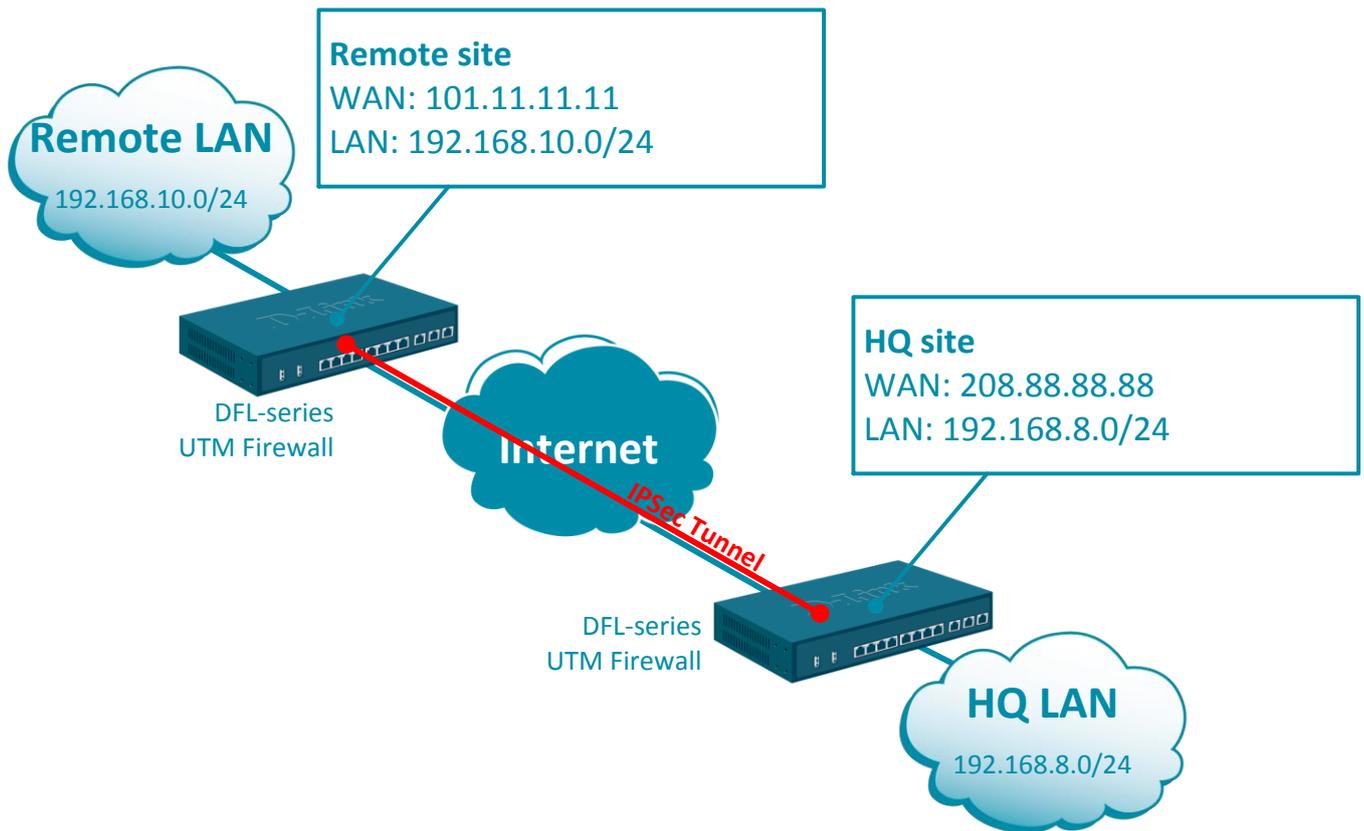
NETDEFEND

Configuration examples for the D-Link NetDefend Firewall series



Setting up IPsec VPN tunnel for site-to-site connection

This configuration example is based on the following setup:



HQ site Firewall Configuration

Step 1. Log into the firewall. The default access to LAN is via <https://192.168.10.1>. Default username is “admin” and password is “admin”.

Step 2. Set your firewall’s WAN settings as per Internet provider requirements. In our example WAN is set with a static IP address.

Step 3. Go to Objects > Key Ring. Create a new Pre-Shared Key. The same key must be used on the remote VPN Firewall.

Status System **Objects** Network Policies

▼ General
Address Book
Services
ALG
Key Ring
▼ Address Pool
IP Pools
NAT Pools
▼ VPN Objects
LDAP
IKE Config Mode Pool

Pre-Shared Key

PSK (Pre-Shared Key) authentication is based on a shared secret that is known only

Name:

Shared Secret

Passphrase

Shared Secret:

Confirm Secret:

Note! Existing secret will always be

Hexadecimal key

Passphrase:

i A PSK containing non-ASCII characters might be encoded differently on other OS uses UTF-8.

Step 4. Go to Objects > Address Book. Add two new objects for the remote network addresses: WAN IP of the remote VPN firewall (e.g. public IP) and the remote private LAN.

The screenshot shows the 'Objects' tab in the configuration interface. The left sidebar has 'Address Book' selected under the 'General' section. The main area is titled 'Address Book' and contains a '+ Add' button with a dropdown menu. The dropdown menu is open, showing options: Address Folder, Ethernet Address, Ethernet Address Group, IP4 Address (highlighted), IP4 Group, IP6 Group, and IP6 Address. Two configuration windows are overlaid on the main area. The first window is for 'VPN-remote-IP' and has the following fields: Name: VPN-remote-IP, Address: 101.11.11.11. The second window is for 'VPN-remote-net' and has the following fields: Name: VPN-remote-net, Address: 192.168.10.0/24. Both windows have tabs for 'General' and 'User Authentication', with 'General' selected.

If you have multiple remote sites – create objects for all of them (remote public IP and remote network). Each of the remote sites needs to have a different network, e.g. 192.168.5.0/24, 192.168.6.0/24, etc. If the public IP address on the remote site is dynamic you can utilize one of the Dynamic IP services. In this case your HQ firewall needs to use URL instead of IP address, following this format:
dns:myremotesite.dyndns.com

Step 5. Go to Network > IPsec. Create a new tunnel and specify the remote network settings.

The screenshot shows the 'IPsec Tunnel' configuration page in the 'Network' tab. The 'General' tab is active. The configuration fields are as follows:

Name:	IPSec-tunnel
Local Network:	lanet
Remote Network:	VPN-remote-net
Remote Endpoint:	VPN-remote-IP
Encapsulation mode:	Tunnel
Local Gateway:	(None)
IKE Config Mode Pool:	(None)

Click on Authentication tab and select the Pre-Shared Key you created on Step 3.

The screenshot shows the 'IPsec Tunnel' configuration page in the 'Authentication' tab. The 'Pre-shared Key' radio button is selected, and the 'Pre-shared key' field is set to 'IPSec-Key'.

<input type="radio"/> X.509 Certificate Root Certificate(s)
<input checked="" type="radio"/> Pre-shared Key Pre-shared key: IPSec-Key

Note: If WAN port of the firewall is set with PPPoE authentication (default metric is 90), select the Advanced tab and change the Route Metric for the IPsec Tunnel to 80.

IPsec Tunnel

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

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

Automatic Route Creation

Automatically add route for remote network.

Add route for remote network

Route metric:

Create separate VPN tunnels for each of the remote sites you have (this is needed only on the firewall at HQ site).

Step 6. Go to Interfaces > Interface Groups. Create a new group and add the IPsec Tunnel and the LAN into the group (this is just to make it easier to apply rules to both interfaces in one go).

Status System Objects **Network** Policies

Interfaces and VPN Routing Network Services

Interface Group

Use an interface group to combine several interfaces for a simplified security policy.

Name:

Security/Transport Equivalent

Interfaces

Available	Selected
core	IPSec-tunnel
dmz	lan
PPTP_Server	
SSL_Server	
wan1	
WAN1_and_WAN2	
wan2	

If you have multiple remote sites – add them all into this group.

Step 7. Go to Policies > Main IP Rules. Create a new rule to allow communication between LAN and the IPsec tunnel. Because we created the interface group “LAN-IPSec”, this one rule will cover both IPsec Tunnel – to – LAN and LAN – to – IPsec Tunnel communication.

The screenshot shows the D-Link web interface for configuring an IP Rule. The top navigation bar includes Status, System, Objects, Network, and Policies. The Policies section is active, with sub-tabs for Firewalling, User Authentication, Intrusion Prevention, and Traffic Management. The left sidebar shows a tree view with Rules, Main IP Rules, Application Rule Sets, Profiles, Schedules, Anti-virus, Web Content Filtering, URL Filter, and File Control. The main content area is titled 'IP Rule' and includes a description: 'An IP rule specifies what action to perform on network traffic that r'. Below this is a tabbed interface with 'General', 'Log Settings', 'NAT', 'SAT', and 'Multi'. The 'General' tab is active, showing the following configuration:

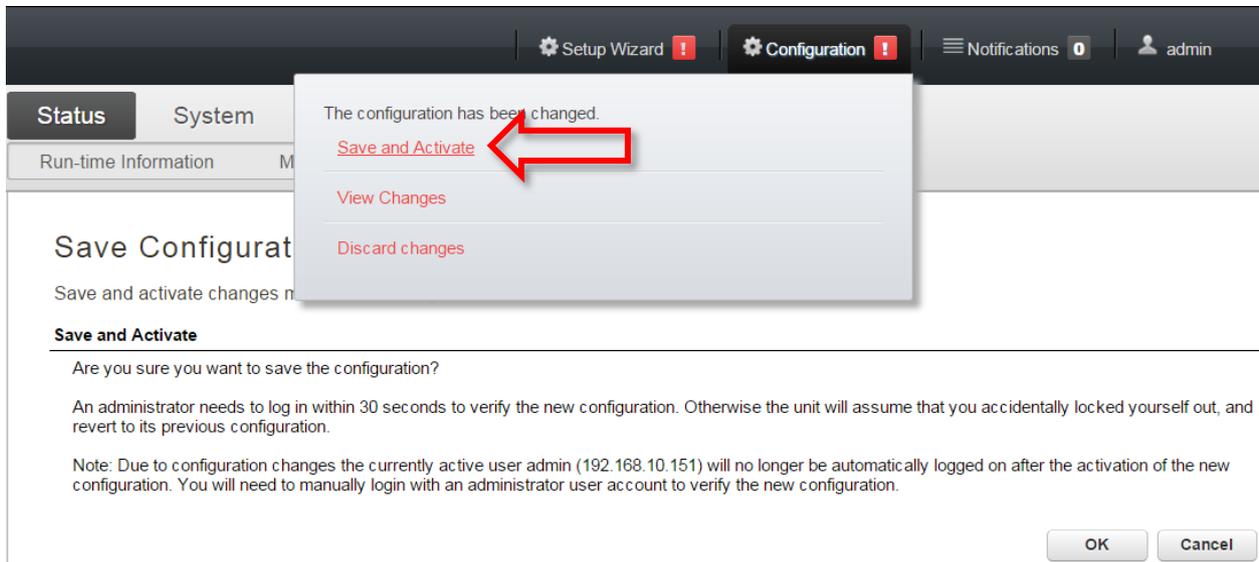
- Name: IPsec-allow
- Action: Allow
- Service: all_services
- Schedule: (None)

To the right of the Service field, there is an information icon and the text: 'NAT, SAT, SLB SAT ar'. Below the General tab is the 'Address Filter' section, which includes the instruction: 'Specify source interface and source network, together with destir'. The configuration for the Address Filter is as follows:

	Interface	Network
Source:	LAN-IPSec	all-nets
Destination:	LAN-IPSec	all-nets

Step 8. After the configuration is done, click “Configuration” in main bar and select “Save and Activate”. Then click OK to confirm. Wait for 15 sec. You will be automatically redirected to the firewall’s LAN IP address.

NOTE: If you do not re-login into the firewall within 30 sec, the configuration is reverted to its previous state. The validation timeout can be adjusted under System > Remote Management > Advanced Settings.



Remote site Firewall Configuration

Repeat the steps above on the firewall at the remote sites. The only difference will be the IP addresses in “VPN-remote-IP” (in our example it is 208.88.88.88) and “VPN-remote-net” (in our example it is 192.168.8.0/24).