Configuration Guide

How to Configure an IPSec VPN tunnel between the DSR router and DFL firewall

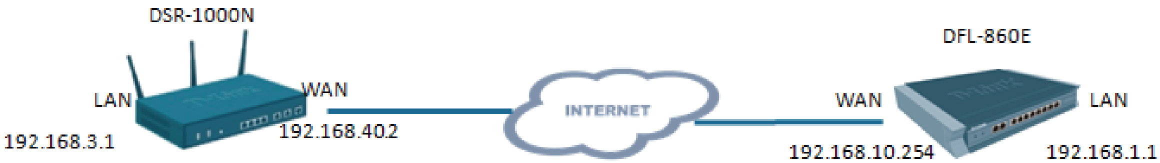
Overview

The IPSec gateway-to-gateway VPN tunnel using pre-shared keys (PSK) is the most secure method to ensure end-to-end data security across the Internet.

D-Link®

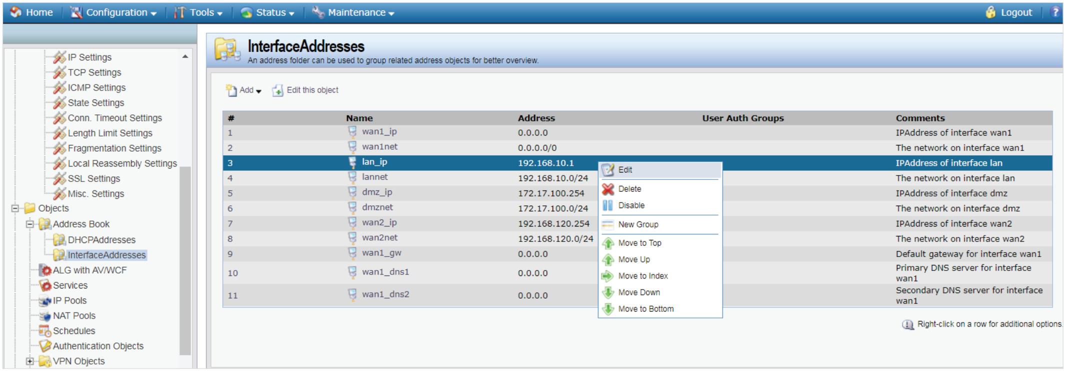
Scope

This document describes the configuration of D-Link DSR Series routers to implement an IPSec VPN tunnel secured with pre-shared keys. This use case will cover IPSec VPN tunnel configuration between a D-Link DSR-250N router and DFL-860E firewall.



Configuring the DFL-860E

Step 1. Go to Object>>InterfaceAddresses



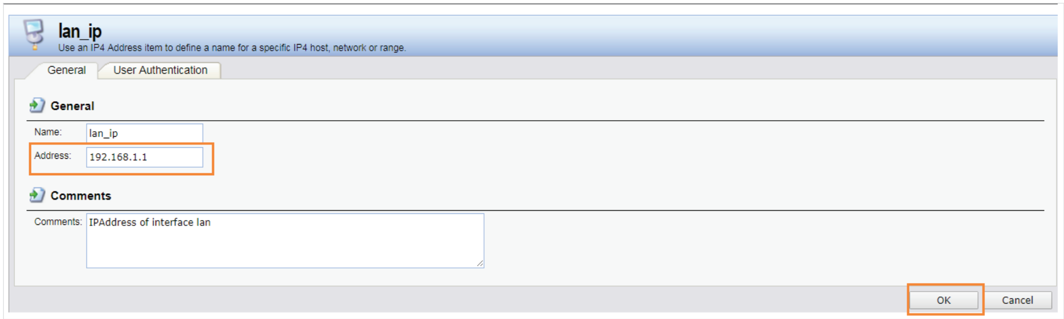
InterfaceAddresses

An address folder can be used to group related address objects for better overview.

#	Name	Address	User Auth Groups	Comments
1	wan1_ip	0.0.0.0		IPAddress of interface wan1
2	wan1net	0.0.0.0/0		The network on interface wan1
3	lan_ip	192.168.10.1		IPAddress of interface lan
4	lannet	192.168.10.0/24		The network on interface lan
5	dmz_ip	172.17.100.254		IPAddress of interface dmz
6	dmznet	172.17.100.0/24		The network on interface dmz
7	wan2_ip	192.168.120.254		IPAddress of interface wan2
8	wan2net	192.168.120.0/24		The network on interface wan2
9	wan1_gw	0.0.0.0		Default gateway for interface wan1
10	wan1_dns1	0.0.0.0		Primary DNS server for interface wan1
11	wan1_dns2	0.0.0.0		Secondary DNS server for interface wan1

Right-click on a row for additional options.

Edit lan-ip 192.168.10.1 to 192.168.1.1; Click **OK** to save the setting.



lan_ip

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General

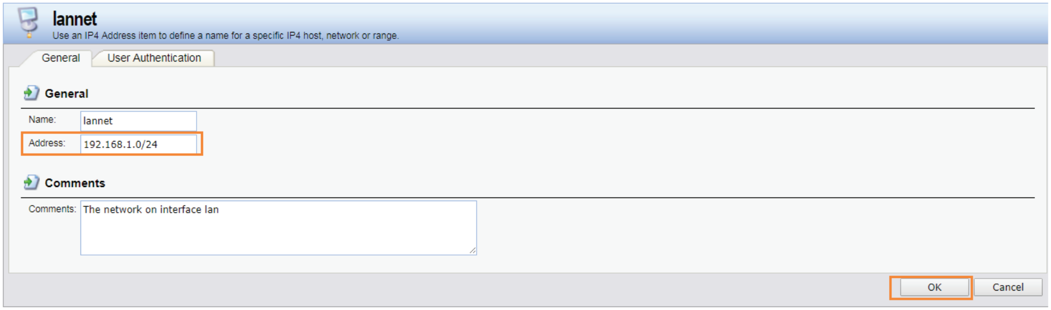
Name: lan_ip

Address: 192.168.1.1

Comments

Comments: IPAddress of interface lan

Edit lannet 192.168.10.0/24 to 192.168.1.0/24; Click **OK** to save the setting.



lannet

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General

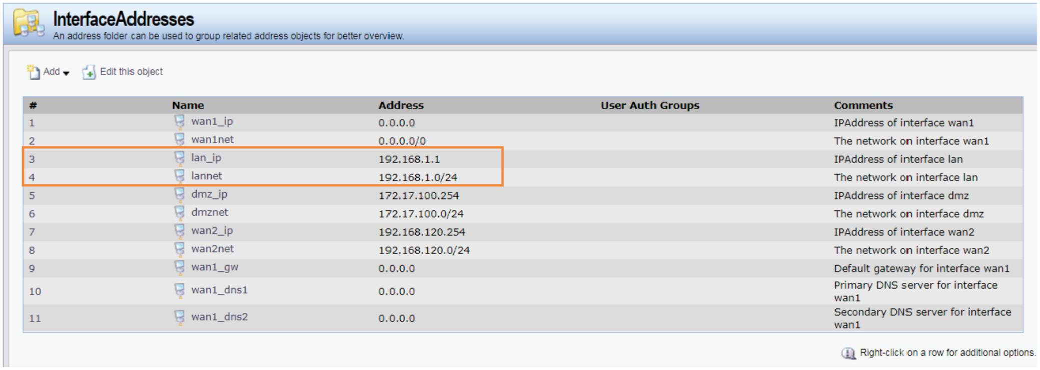
Name: lannet

Address: 192.168.1.0/24

Comments

Comments: The network on interface lan

After editing, the following page will display:



InterfaceAddresses
An address folder can be used to group related address objects for better overview.

#	Name	Address	User Auth Groups	Comments
1	wan1_ip	0.0.0.0		IPAddress of interface wan1
2	wan1net	0.0.0.0/0		The network on interface wan1
3	lan_ip	192.168.1.1		IPAddress of interface lan
4	lannet	192.168.1.0/24		The network on interface lan
5	dmz_ip	172.17.100.254		IPAddress of interface dmz
6	dmznet	172.17.100.0/24		The network on interface dmz
7	wan2_ip	192.168.120.254		IPAddress of interface wan2
8	wan2net	192.168.120.0/24		The network on interface wan2
9	wan1_gw	0.0.0.0		Default gateway for interface wan1
10	wan1_dns1	0.0.0.0		Primary DNS server for interface wan1
11	wan1_dns2	0.0.0.0		Secondary DNS server for interface wan1

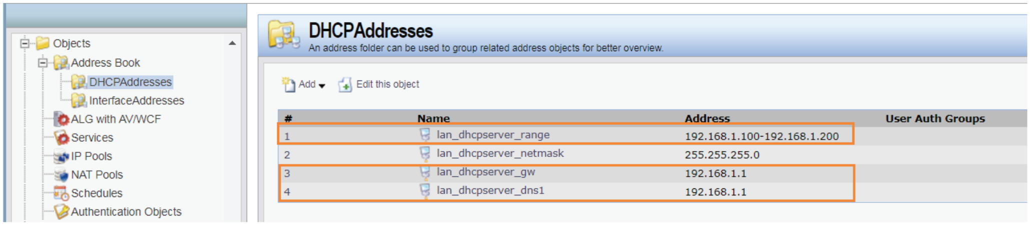
Right-click on a row for additional options.

Step 2. Go to Object>>DHCPAddresses

Edit lan_dhcpserver_range 192.168.10.100-192.168.10.200 to 192.168.1.100-192.168.1.200;

Edit lan_dhcpserver_gw 192.168.10.1 to 192.168.1.1;

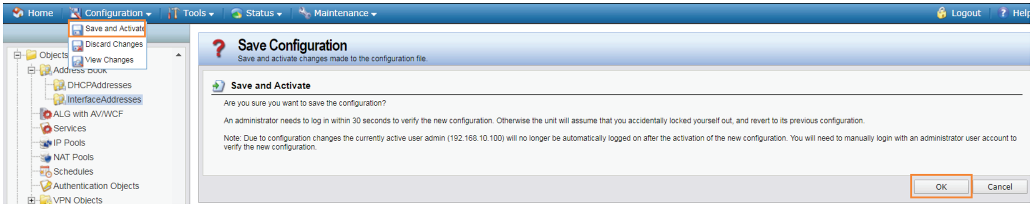
Edit lan_dhcpserver_dns1 192.168.10.1 to 192.168.1.1;



DHCPAddresses
An address folder can be used to group related address objects for better overview.

#	Name	Address	User Auth Groups
1	lan_dhcpserver_range	192.168.1.100-192.168.1.200	
2	lan_dhcpserver_netmask	255.255.255.0	
3	lan_dhcpserver_gw	192.168.1.1	
4	lan_dhcpserver_dns1	192.168.1.1	

Step 3. Go to Configuration>>Save and Activate; click **OK** to save the settings.



Save Configuration
Save and activate changes made to the configuration file.

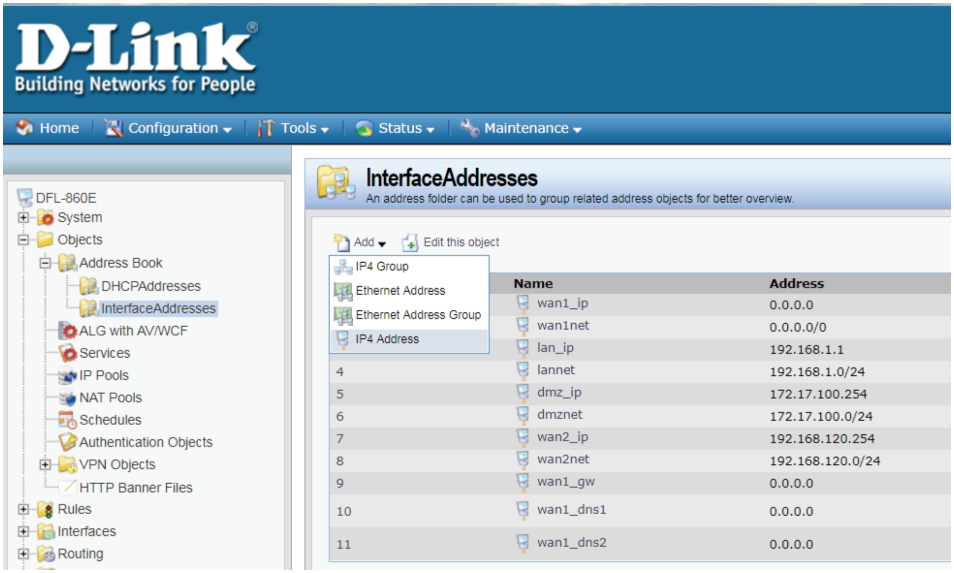
Save and Activate

Are you sure you want to save the configuration?

An administrator needs to log in within 30 seconds to verify the new configuration. Otherwise the unit will assume that you accidentally locked yourself out, and revert to its previous configuration.

Note: Due to configuration changes the currently active user admin (192.168.10.100) will no longer be automatically logged on after the activation of the new configuration. You will need to manually login with an administrator user account to verify the new configuration.

Step 4. Go to Objects > Address Book > Interface Addresses. Click on **Add** and select **IP4 address**.



InterfaceAddresses

An address folder can be used to group related address objects for better overview.

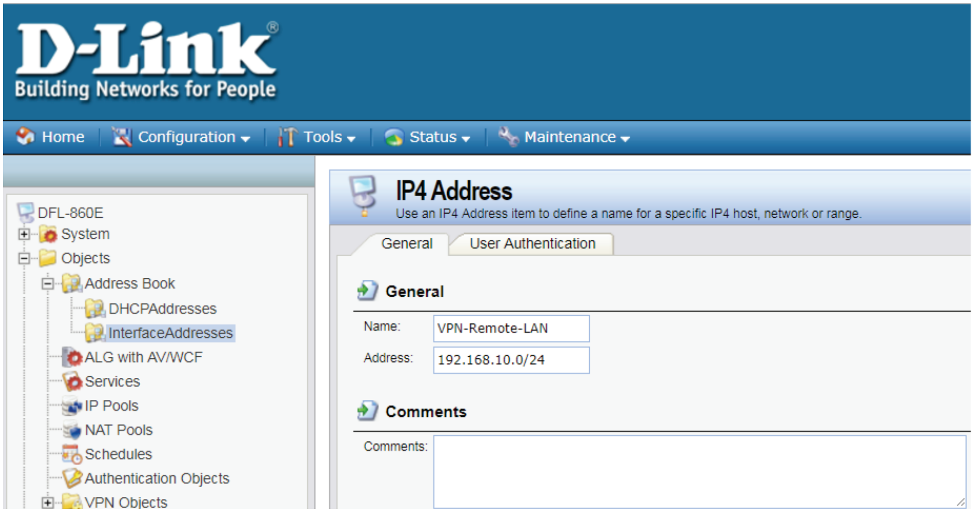
	Name	Address
	wan1_ip	0.0.0.0
	wan1net	0.0.0.0/0
	lan_ip	192.168.1.1
4	lannet	192.168.1.0/24
5	dmz_ip	172.17.100.254
6	dmznet	172.17.100.0/24
7	wan2_ip	192.168.120.254
8	wan2net	192.168.120.0/24
9	wan1_gw	0.0.0.0
10	wan1_dns1	0.0.0.0
11	wan1_dns2	0.0.0.0

Specify the settings of the remote network at the other end of the VPN tunnel.

In the Name field enter *VPN-Remote-LAN*.

In the Address field enter the Subnet ID and Mask Bits for the remote network: in our example it is 192.168.10.0/24.

Click the **OK** button.



IP4 Address

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General

Name: VPN-Remote-LAN

Address: 192.168.10.0/24

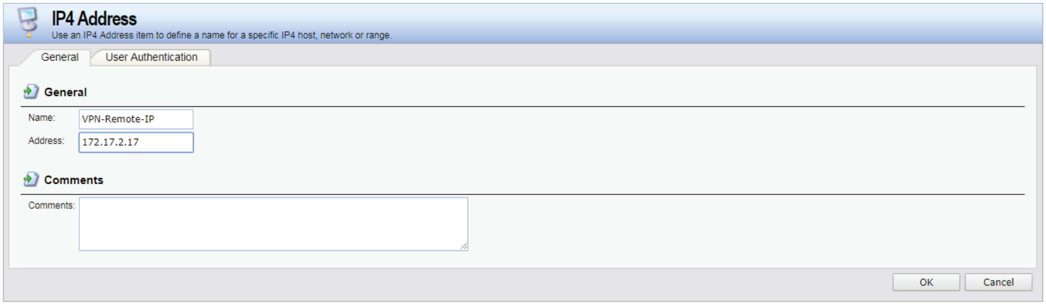
Comments

Comments:

Step 5. Add another IP Address. Enter the settings of the VPN endpoint-this is the public IP address of DSR-250N.

In the Name field enter **VPN-Remote-IP**.

In the Address field specify the public IP address of the remote network.



IP4 Address

Use an IP4 Address item to define a name for a specific IP4 host, network or range.

General

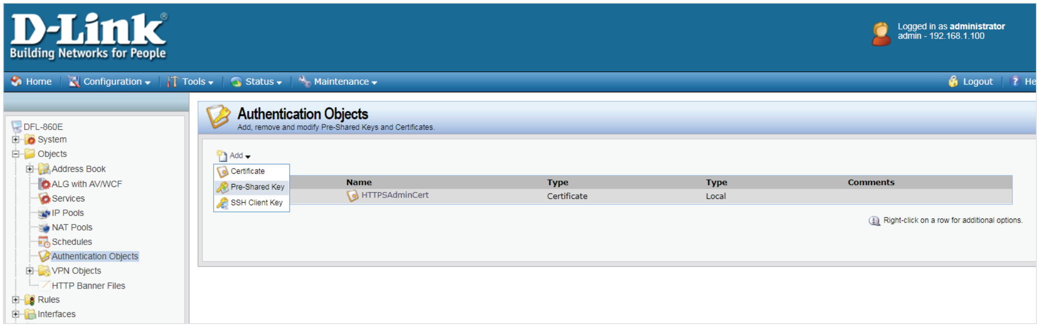
Name: VPN-Remote-IP

Address: 172.17.2.17

Comments

Comments:

Step 6. Go to Object > Authentication Objects. Click on **Add** and select **Pre-Shared Key**.



Logged in as **administrator**
admin - 192.168.1.100

Authentication Objects

Add, remove and modify Pre-Shared Keys and Certificates.

Name	Type	Type	Comments
HTTPSAdminCert	Certificate	Local	

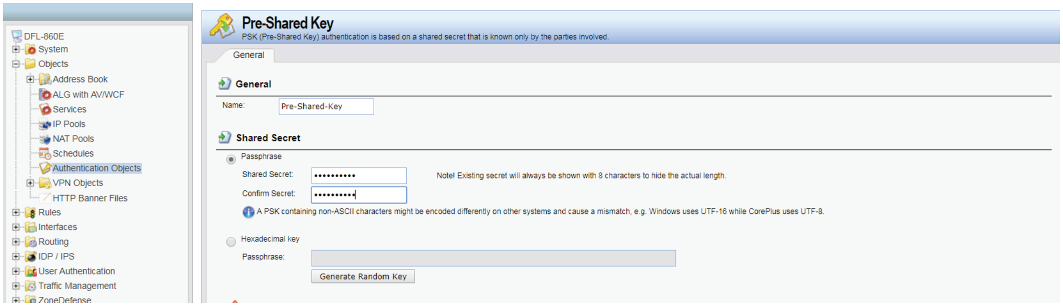
Right-click on a row for additional options.

Enter the Pre-Shared Key settings for your VPN tunnel.

In the Name field, type Pre-Shared-Key.

In the Shared Secret field, select the type of key you want to use and type in the key. In our example we are using ASCII key (passphrase). Note that you will need to use exactly the same key when setting up the firewall on the other end of the tunnel.

Click **OK** when done.



Pre-Shared Key

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

General

Name: Pre-Shared-Key

Shared Secret

● Passphrase

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

Confirm Secret: ••••••••••

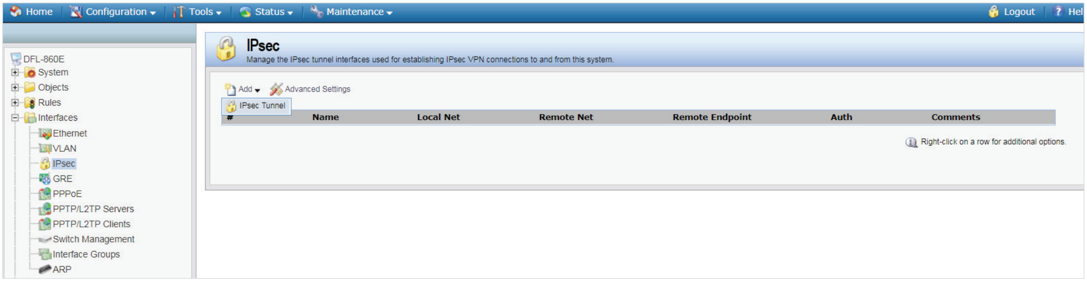
A PSK containing non-ASCII characters might be encoded differently on other systems and cause a mismatch, e.g. Windows uses UTF-16 while CorePlus uses UTF-8.

○ Hexadecimal key

Passphrase:

Generate Random Key

Step 7. Go to Interfaces > IPSec. Click on **Add** and select **IPSec Tunnel**.



IPsec

Manage the IPsec tunnel interfaces used for establishing IPsec VPN connections to and from this system.

#	Name	Local Net	Remote Net	Remote Endpoint	Auth	Comments

Right-click on a row for additional options.

Enter your IPSec tunnel settings.

In the Name field, enter *IPSec-tunnel*.

In the Local Network field, select **lannet** (this is the private network on this side of the VPN tunnel).

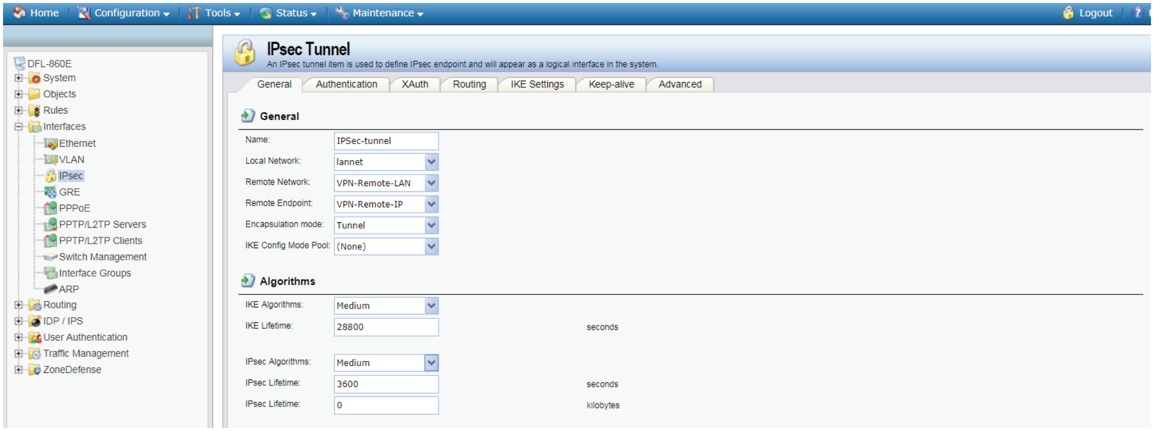
In the Remote Network field, select **VPN-Remote-LAN** (this is the private network on the other side of the VPN tunnel, see **Step 4**).

In the Remote Endpoint field, select **VPN-Remote-IP** (this is the public IP address of the remote network, see **Step 5**).

Encapsulation Mode should be set to **Tunnel**.

Under Algorithms select the desired algorithms and **IKE/IPSec Lifetime**. In our example we are using **Medium** settings.

You can modify or add your own set of security algorithms under Objects > VPN Objects > IKE Algorithms and IPSec Algorithms.



IPsec Tunnel

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

General

Name: IPSec-tunnel

Local Network: lannet

Remote Network: VPN-Remote-LAN

Remote Endpoint: VPN-Remote-IP

Encapsulation mode: Tunnel

IKE Config Mode Pool: (None)

Algorithms

IKE Algorithms: Medium

IKE Lifetime: 28800 seconds

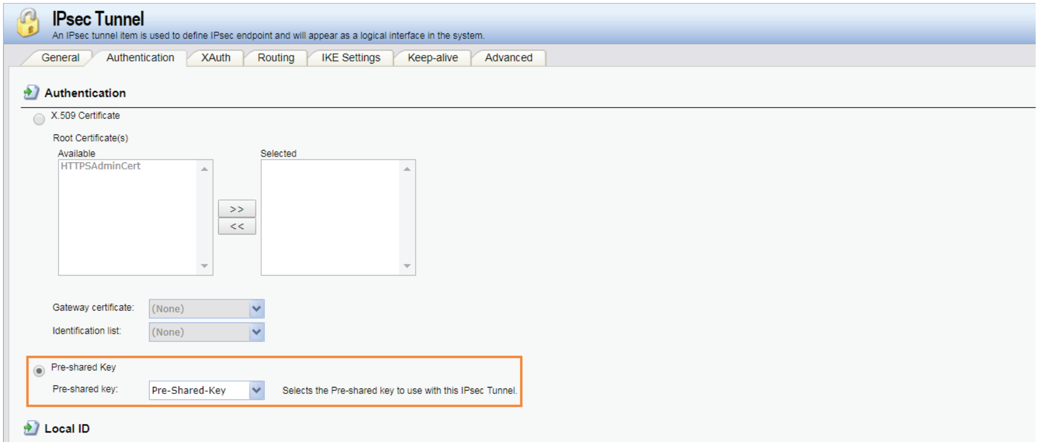
IPsec Algorithms: Medium

IPsec Lifetime: 3600 seconds

IPsec Lifetime: 0 kilobytes

Click on Authentication tab. Make sure the **Pre-Shared Key** option is enabled. Select the **Pre-Shared-Key** in the dropdown menu (see **Step 6**).

Click on the **OK** button


IPsec Tunnel

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

Authentication

○ X.509 Certificate

Root Certificate(s)

Available: HTTPSAdminCert

Selected:

Gateway certificate: (None)

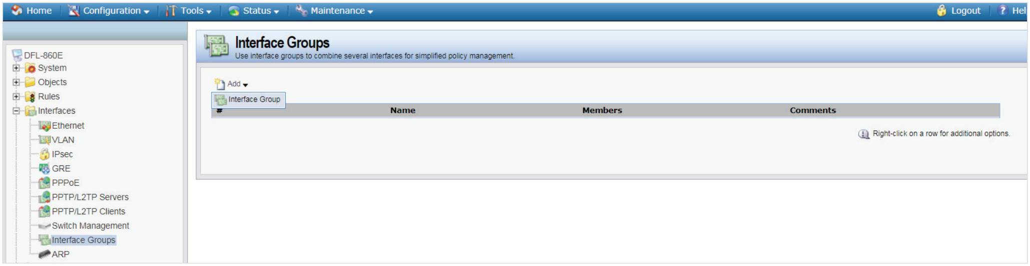
Identification list: (None)

● Pre-shared Key

Pre-shared key: Pre-Shared-Key — Selects the Pre-shared key to use with this IPsec Tunnel.

Local ID

Step 8. Go to Interfaces > Interface Groups. Click on **Add** and select **Interface Group**.



Interface Groups

Use interface groups to combine several interfaces for simplified policy management.

#	Name	Members	Comments

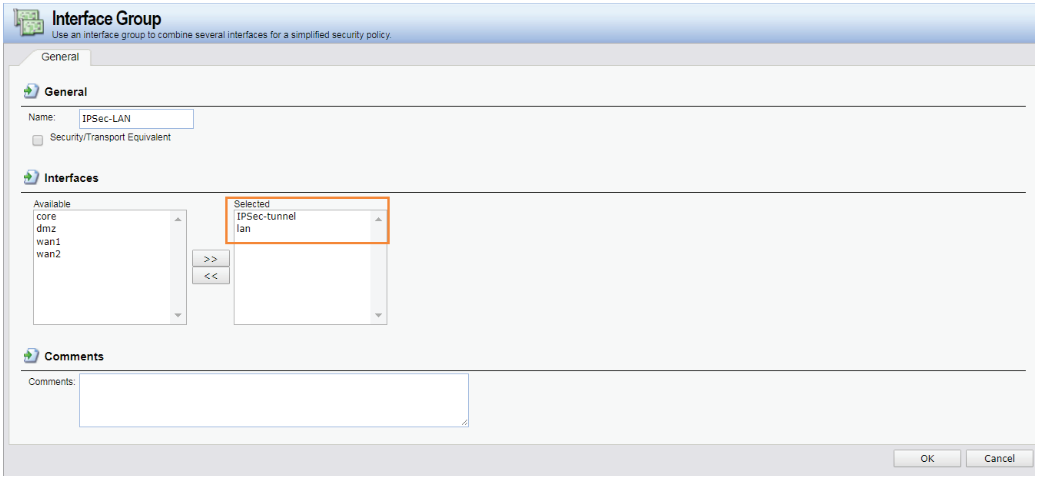
Right-click on a row for additional options.

Create a group which has your IPSec tunnel and your LAN.

In the Name field, type *IPSec-LAN*.

Under Interfaces add **IPSec-tunnel** and **lan** into the Selected field.

Click on the **OK** button.



Interface Group

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

General

Name: IPSec-LAN

□ Security/Transport Equivalent

Interfaces

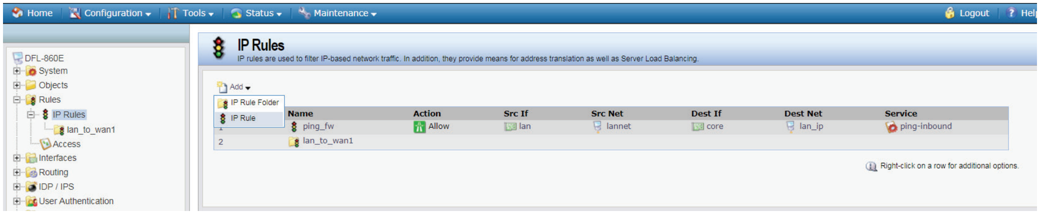
Available: core, dmz, wan1, wan2

Selected: IPSec-tunnel, lan

Comments

Comments:

Step 9. Go to Rules > IP Rules. Click on **Add** and select **IP Rule**.



IP Rules

IP rules are used to filter IP-based network traffic. In addition, they provide means for address translation as well as Server Load Balancing.

	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	ping_fw	Allow	lan	lannet	core	lan_ip	ping-inbound
2	lan_to_wan1						

Right-click on a row for additional options.

This rule will allow communication between the LAN and the IPSec tunnel.

In the Name field, type *IPSec-Allow*.

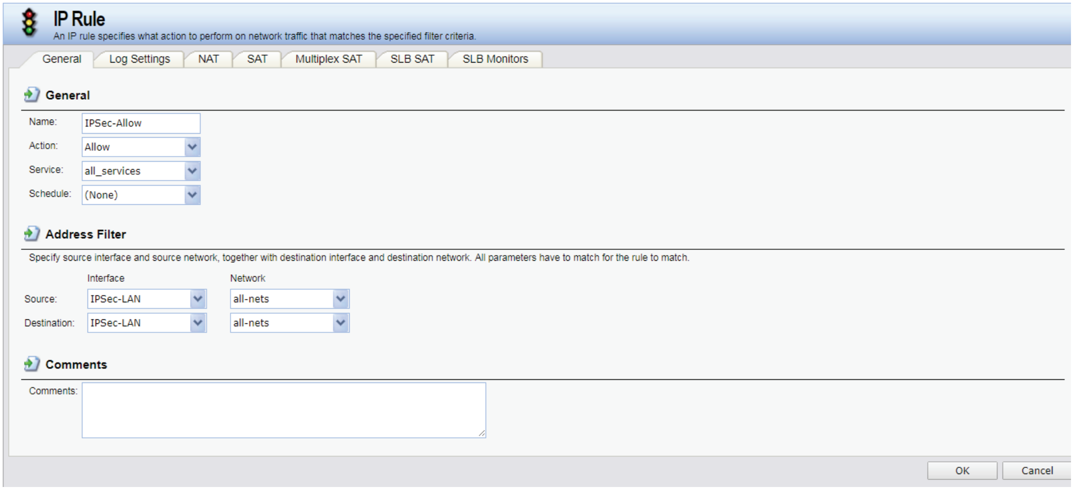
Under Action select **Allow**.

Under Service select **all_services**.

Under Address Filter specify the following:

Source and Destination Interfaces: IPSec-LAN (this is the group you created in **Step 8**).

Source and Destination Network: select **all-nets**.



IP Rule

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

General

Name: IPSec-Allow

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.

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

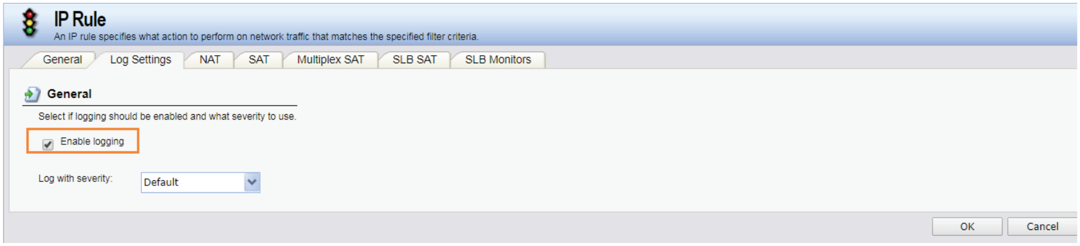
Comments

Comments:

Click on the Log Settings tab.

Select the **Enable Logging** option.

Click on the **OK** button when done.



IP Rule

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

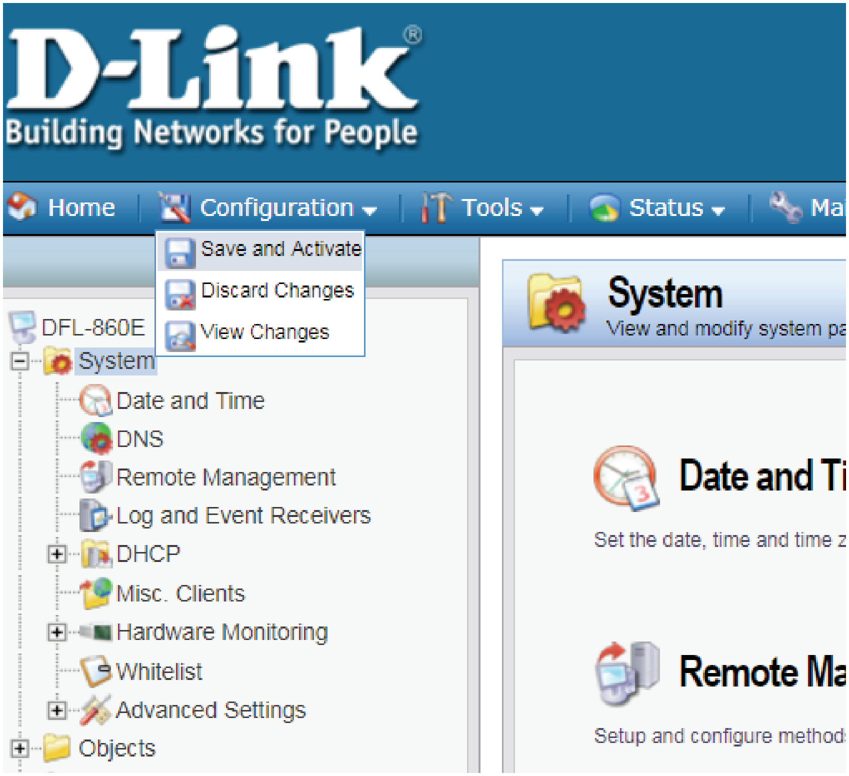
General

Select if logging should be enabled and what severity to use.

☑ Enable logging

Log with severity: Default

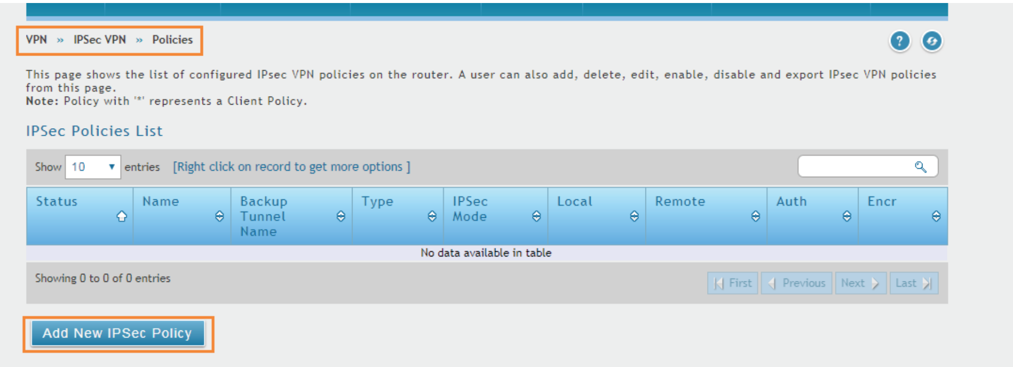
Step 10. To save the new configuration, click on **Configuration**, in the top menu bar and select **Save and Activate**.



Click **OK** to confirm the new settings.

Configuring the DSR-250N

Go to VPN>>IPsec VPN>>Policies to add an IPSec policy. Click **Add New IPSec Policy** and input the following:



This page shows the list of configured IPsec VPN policies on the router. A user can also add, delete, edit, enable, disable and export IPsec VPN policies from this page.
Note: Policy with '*' represents a Client Policy.

IPSec Policies List

Show 10 entries [Right click on record to get more options]

Status	Name	Backup Tunnel Name	Type	IPSec Mode	Local	Remote	Auth	Encr
No data available in table								

Showing 0 to 0 of 0 entries

Policy Name: **IPSec**

Policy Type: **Auto Policy**

IP Protocol Version: IPv4

IKE Version: **IKEv1**

Select Local Gateway: **Dedicated WAN**

Remote Endpoint: **IP Address**

IP Address / FQDN: The WAN IP address of your DFL-860E

Local IP: **Subnet**

Local Start IP Address: **192.168.10.0**

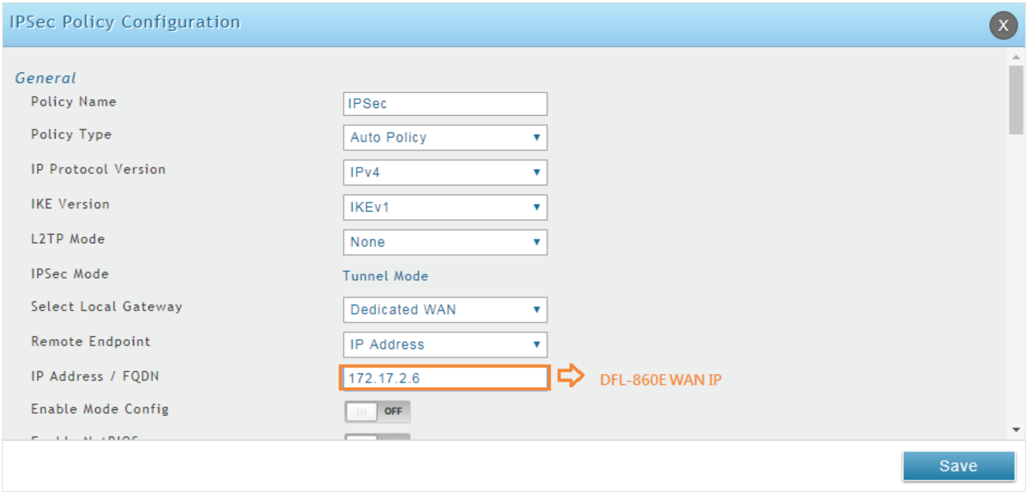
Local Subnet Mask: **255.255.255.0**

Remote IP: **Subnet**

Remote Start IP Address: **192.168.1.0**

Remote Subnet Mask: **255.255.255.0**

Pre share Key: Your DFL-860E Pre share key

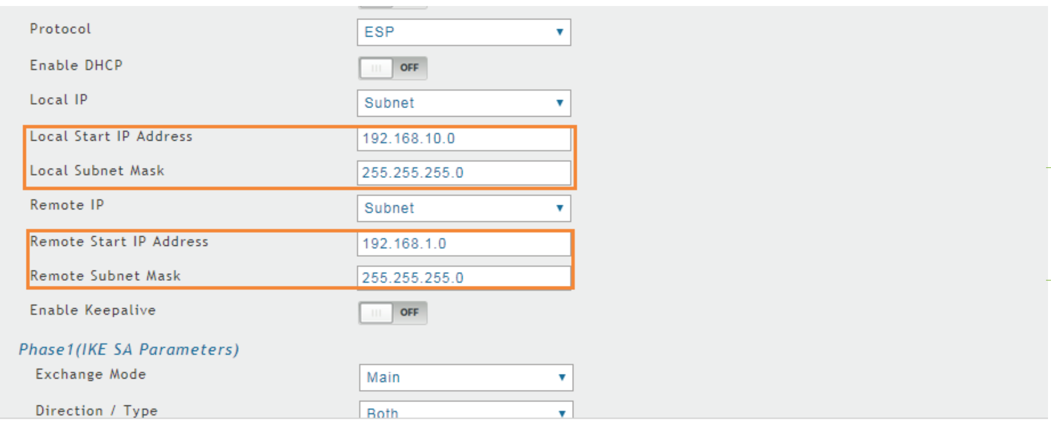


IPSec Policy Configuration

General

Policy Name	IPSec
Policy Type	Auto Policy
IP Protocol Version	IPv4
IKE Version	IKEv1
L2TP Mode	None
IPSec Mode	Tunnel Mode
Select Local Gateway	Dedicated WAN
Remote Endpoint	IP Address
IP Address / FQDN	172.17.2.6
Enable Mode Config	OFF

DFL-860E WAN IP



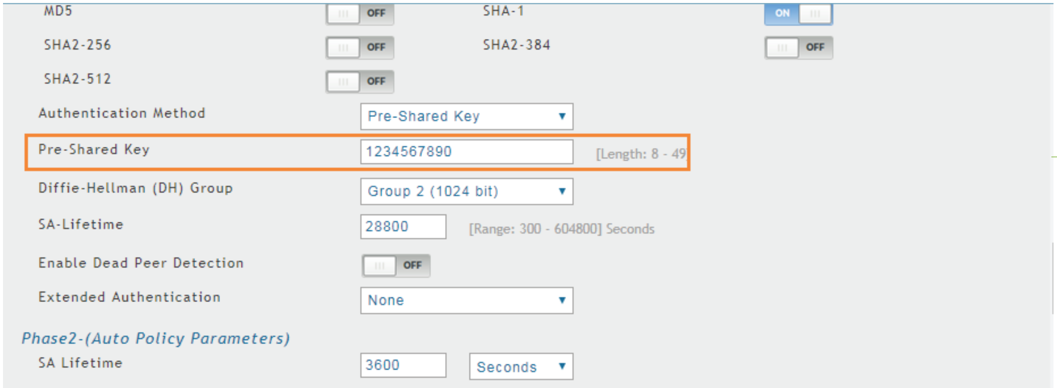
Protocol	ESP ▾
Enable DHCP	OFF
Local IP	Subnet ▾
Local Start IP Address	192.168.10.0
Local Subnet Mask	255.255.255.0
Remote IP	Subnet ▾
Remote Start IP Address	192.168.1.0
Remote Subnet Mask	255.255.255.0
Enable Keepalive	OFF

Phase1(IKE SA Parameters)

Exchange Mode	Main ▾
Direction / Type	Both ▾

This section refers to the local internal network of the DSR-250N.

This section refers to the remote internal network of the DFL-860E.



MD5	OFF	SHA-1	ON
SHA2-256	OFF	SHA2-384	OFF
SHA2-512	OFF		

Authentication Method	Pre-Shared Key ▾
Pre-Shared Key	1234567890 [Length: 8 - 49
Diffie-Hellman (DH) Group	Group 2 (1024 bit) ▾
SA-Lifetime	28800 [Range: 300 - 604800] Seconds
Enable Dead Peer Detection	OFF
Extended Authentication	None ▾

Phase2-(Auto Policy Parameters)

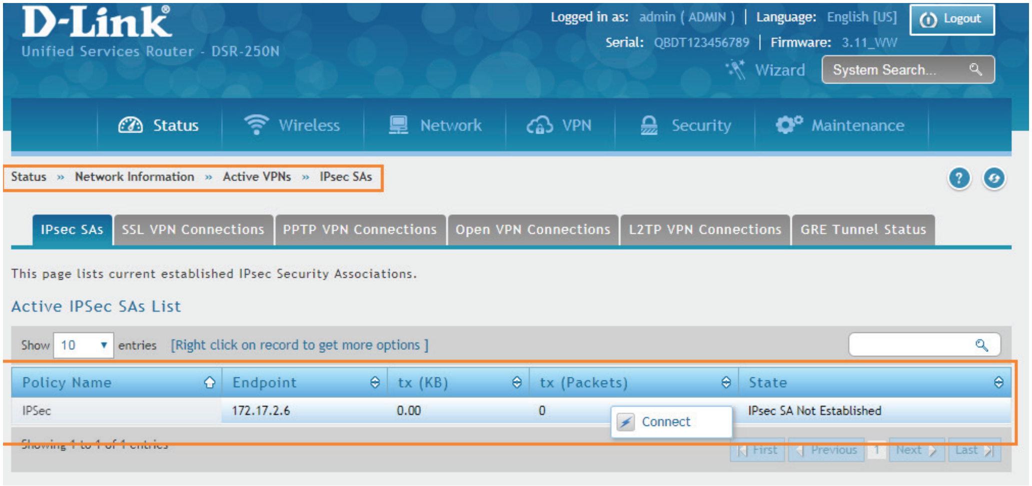
SA Lifetime	3600 Seconds ▾

Authentication Method and Pre-Shared Key settings must be identical with remote Pre-Shared Key settings on the DFL-860E.

Verifying the connection:

Go to Status>>Network Information>>Active VPNs>>IPSec SAs

Right click on **IPSec**, then select **Connect**.



Status » Network Information » Active VPNs » IPsec SAs

This page lists current established IPsec Security Associations.

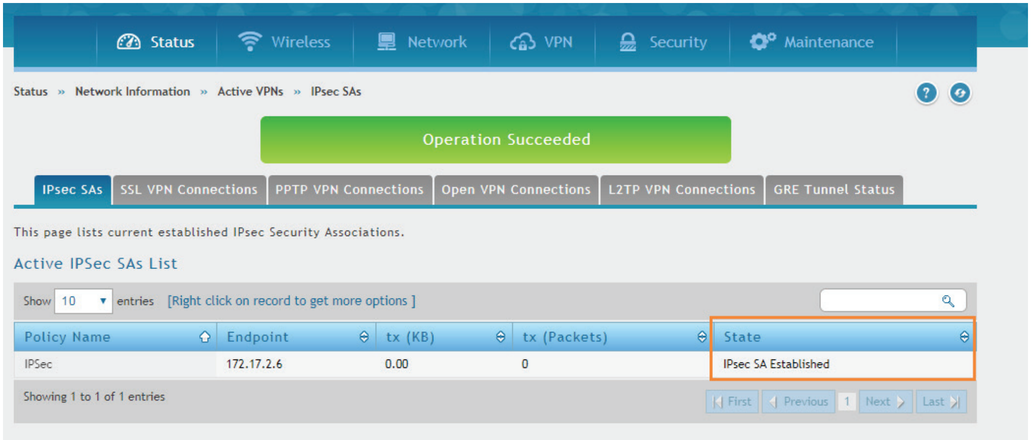
Active IPSec SAs List

Show 10 entries [Right click on record to get more options]

Policy Name	Endpoint	tx (KB)	tx (Packets)	State
IPSec	172.17.2.6	0.00	0	IPsec SA Not Established

Showing 1 to 1 of 1 entries

Connection is established.



Status » Network Information » Active VPNs » IPsec SAs

Operation Succeeded

This page lists current established IPsec Security Associations.

Active IPSec SAs List

Show 10 entries [Right click on record to get more options]

Policy Name	Endpoint	tx (KB)	tx (Packets)	State
IPSec	172.17.2.6	0.00	0	IPsec SA Established

Showing 1 to 1 of 1 entries

Visit our website for more information
www.dlink.com