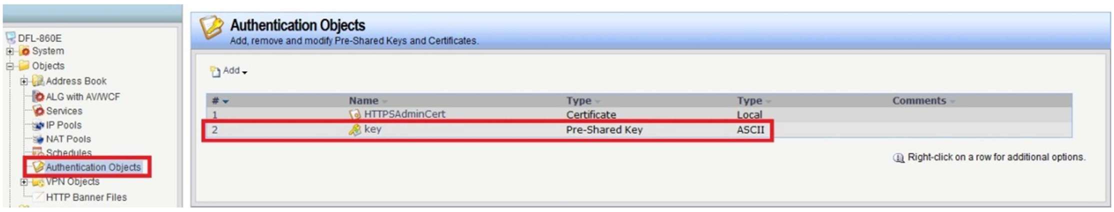
How to setup IPSec remote access on DFL-series

This example describes how to configure an IPSec tunnel at the office NetDefend firewall for roaming clients that connect to the office to gain remote access.

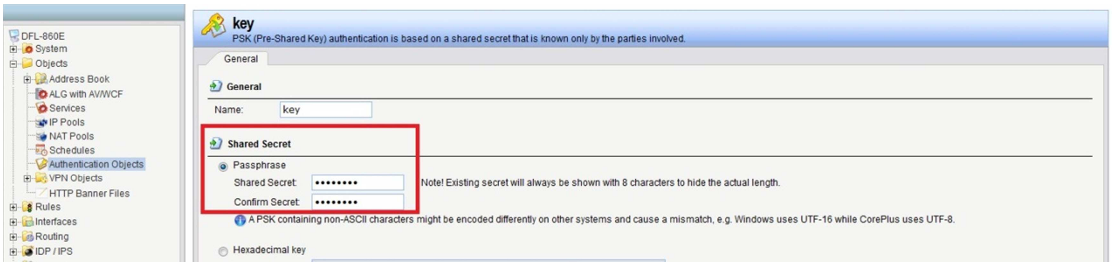
(1) Create a new pre-share key.



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

#	Name	Type	Type	Comments
1	HTTPSAdminCert	Certificate	Local	
2	key	Pre-Shared Key	ASCII	

Right-click on a row for additional options.



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

General

Name: key

Shared Secret

● Passphrase

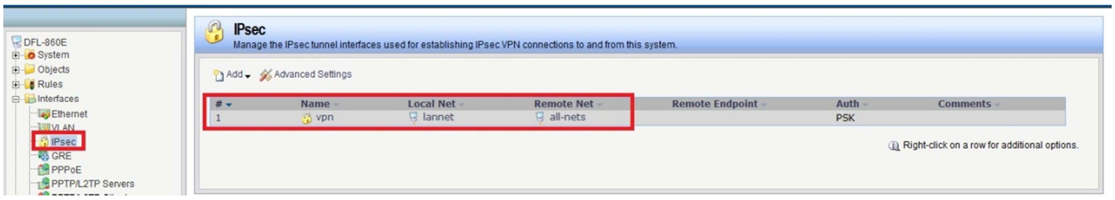
Shared Secret: •••••••• Note! Existing secret will always be shown with 8 characters to hide the actual length.

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

(2) Create a new IPSec interface.

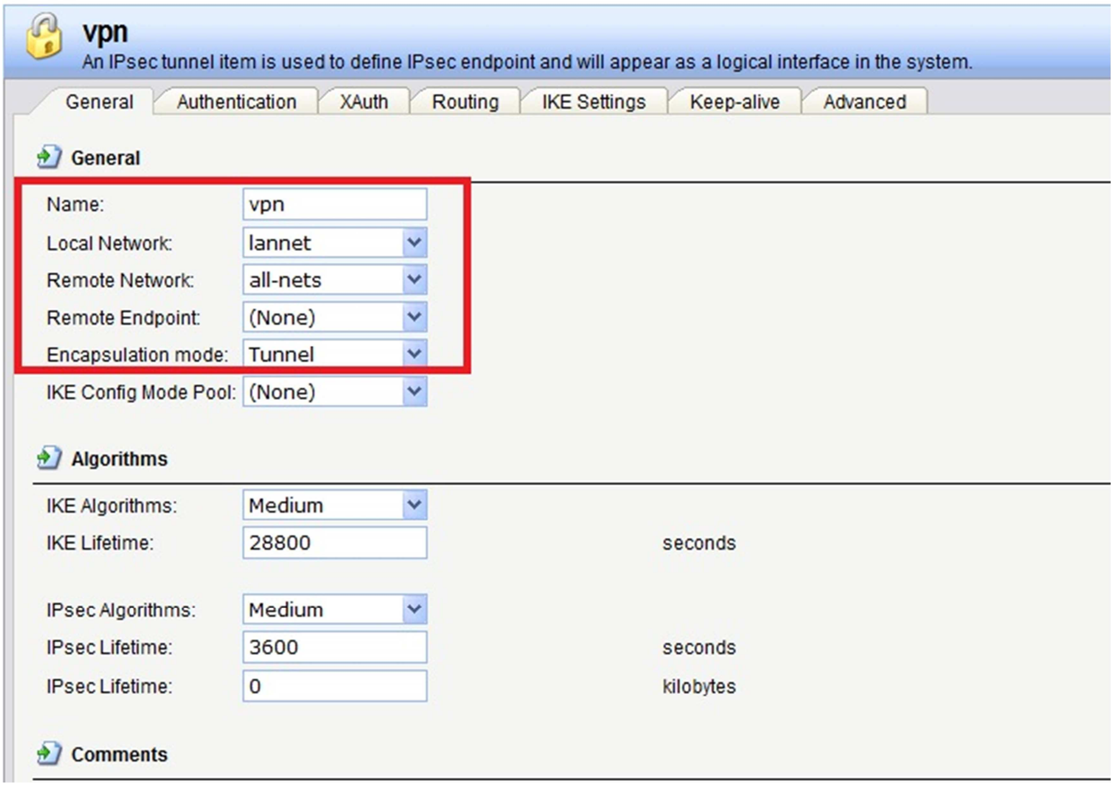


IPsec
Manage the IPsec tunnel interfaces used for establishing IPsec VPN connections to and from this system.

#	Name	Local Net	Remote Net	Remote Endpoint	Auth	Comments
1	vpn	lannet	all-nets		PSK	

Right-click on a row for additional options.

(3) Remote endpoint item choose “none”.



vpn

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

General

Name: vpn

Local Network: lannet

Remote Network: all-nets

Remote Endpoint: (None)

Encapsulation mode: Tunnel

IKE Config Mode Pool: (None)

Algorithms

IKE Algorithms: Medium

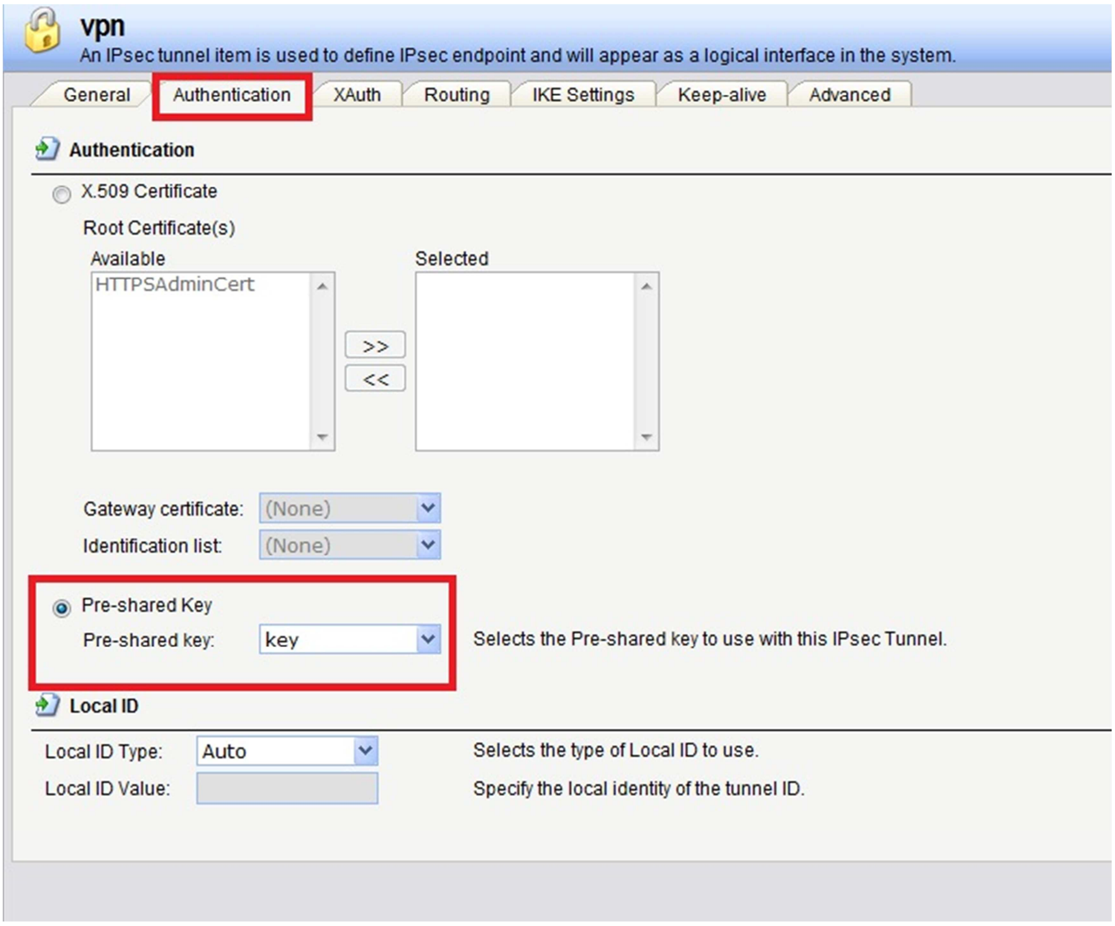
IKE Lifetime: 28800 seconds

IPsec Algorithms: Medium

IPsec Lifetime: 3600 seconds

IPsec Lifetime: 0 kilobytes

Comments



vpn

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

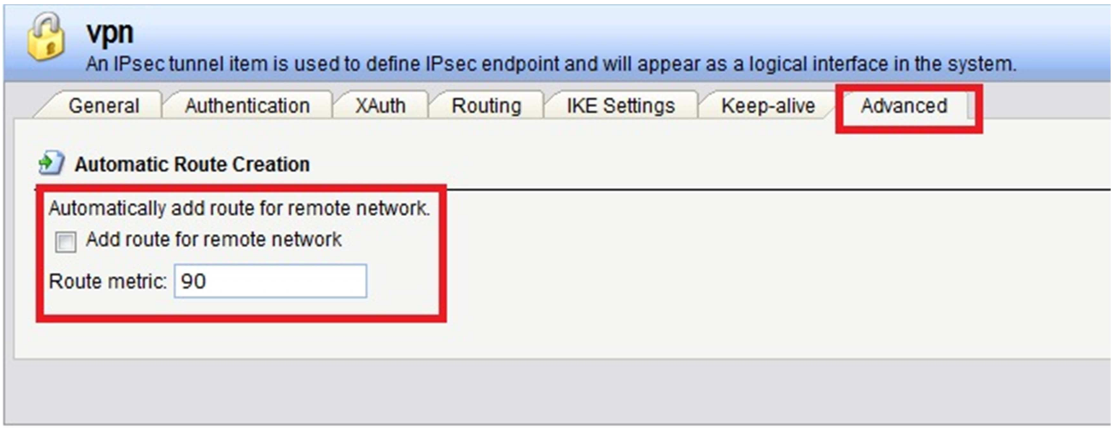
Pre-shared key: key — Selects the Pre-shared key to use with this IPsec Tunnel.

Local ID

Local ID Type: Auto — Selects the type of Local ID to use.

Local ID Value: — Specify the local identity of the tunnel ID.

(4) Don’t choose “add route for remote network” item.



vpn

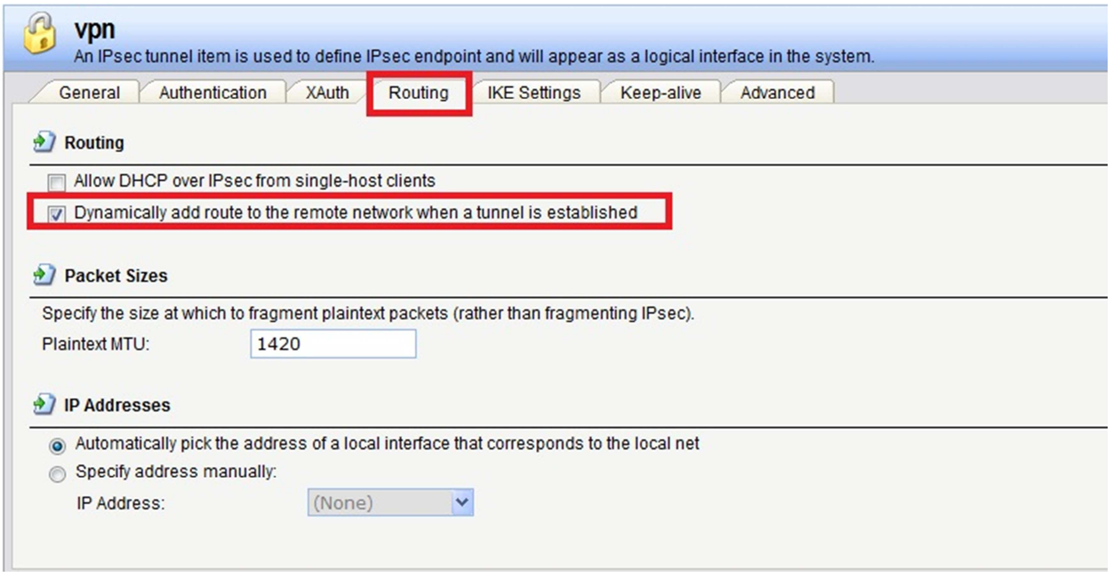
An IPsec tunnel item is used to define IPsec endpoint and will appear as a logical interface in the system.

Automatic Route Creation

Automatically add route for remote network.

□ Add route for remote network

Route metric: 90



vpn

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

Routing

□ Allow DHCP over IPsec from single-host clients

☑ Dynamically add route to the remote network when a tunnel is established

Packet Sizes

Specify the size at which to fragment plaintext packets (rather than fragmenting IPsec).

Plaintext MTU: 1420

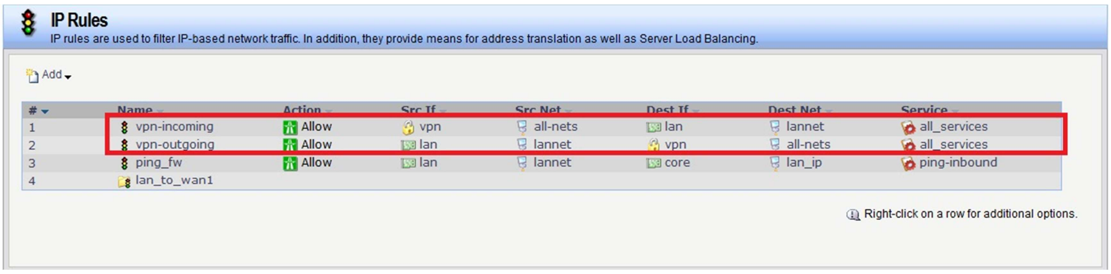
IP Addresses

● Automatically pick the address of a local interface that corresponds to the local net

○ Specify address manually:

IP Address: (None)

(5) Create two IP rules. VPN-incoming and VPN-outgoing.

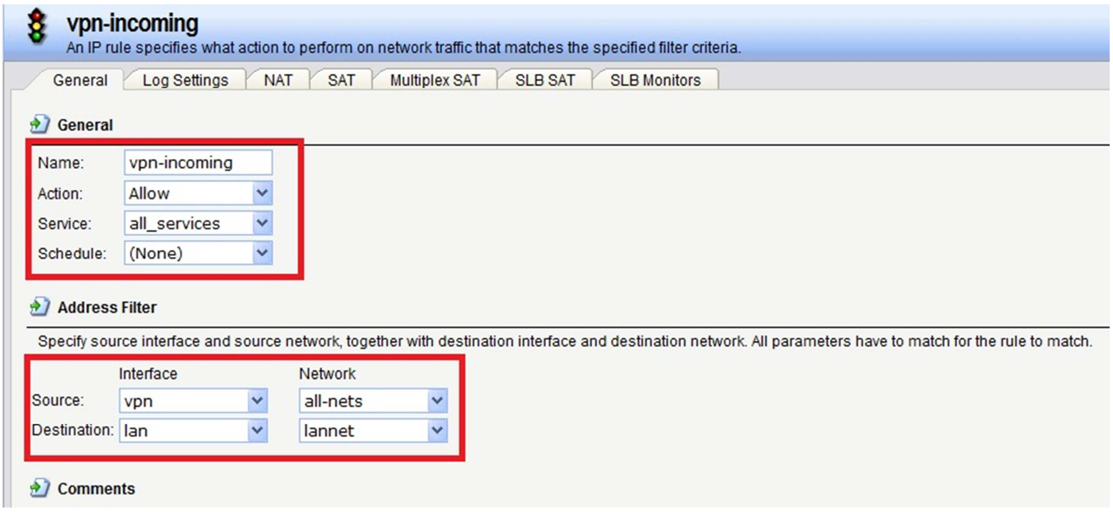


IP Rules

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	vpn-incoming	Allow	vpn	all-nets	lan	lannet	all_services
2	vpn-outgoing	Allow	lan	lannet	vpn	all-nets	all_services
3	ping_fw	Allow	lan	lannet	core	lan_ip	ping-inbound
4	lan_to_wan1						

Right-click on a row for additional options.



vpn-incoming

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

General

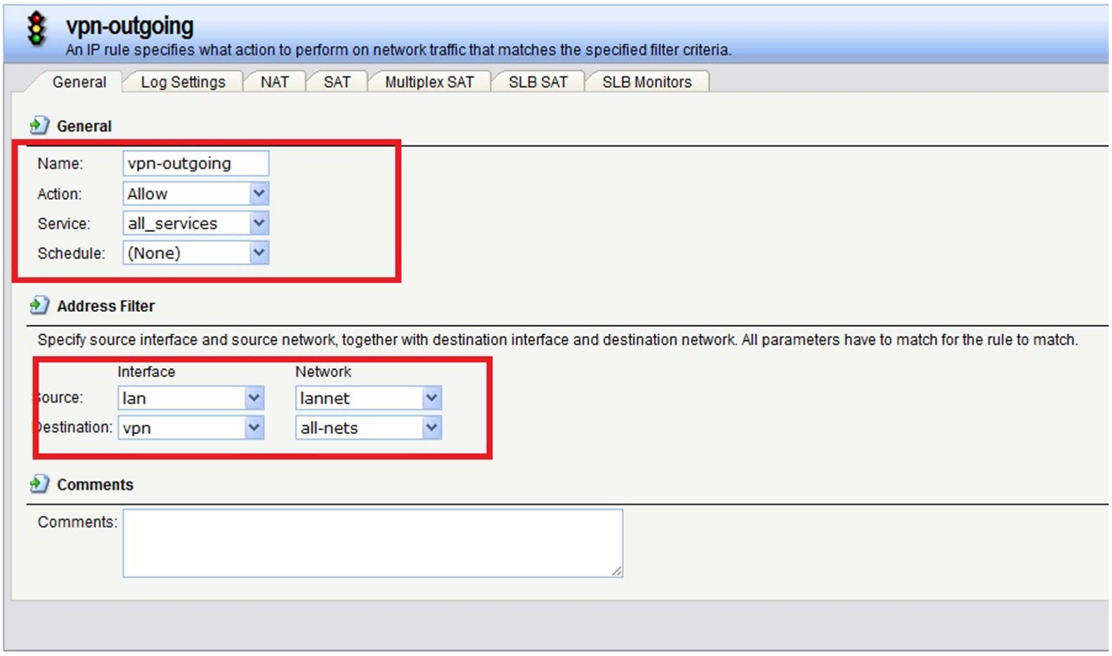
Name: vpn-incoming
Action: Allow
Service: all_services
Schedule: (None)

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.

	Interface	Network
Source:	vpn	all-nets
Destination:	lan	lannet

Comments



vpn-outgoing

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

General

Name: vpn-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.

	Interface	Network
Source:	lan	lannet
Destination:	vpn	all-nets

Comments

Comments:

END