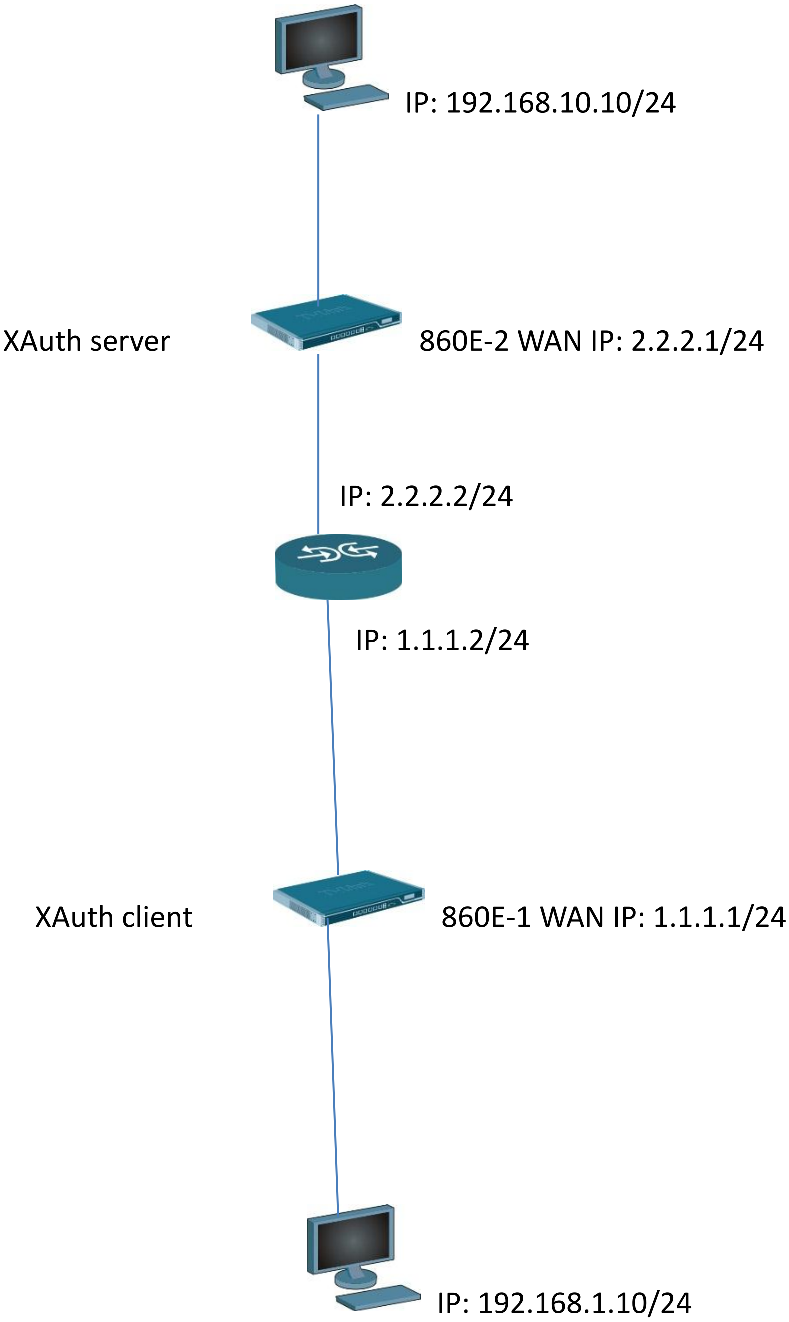
How to set up IPSec site to site with Xauth

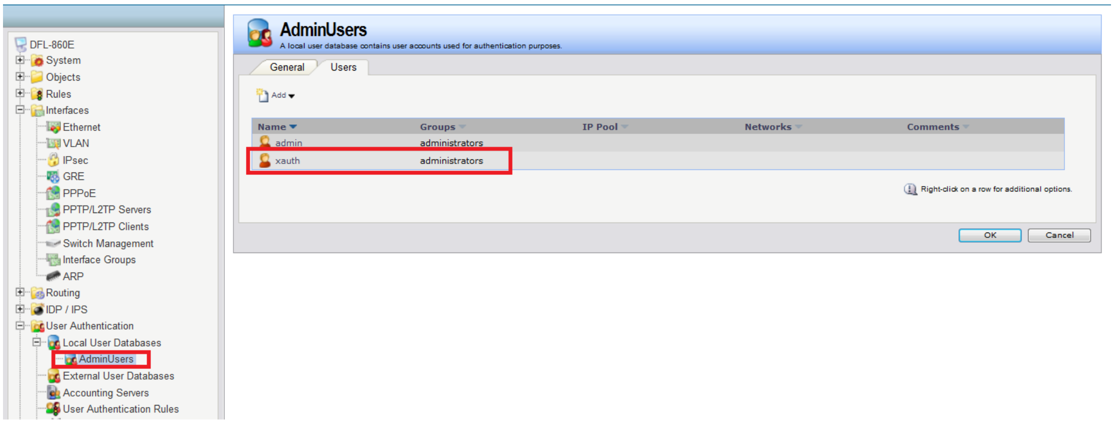
Topology:



This reference files just focus on the XAuth setup procedure. We suppose user know how to setup site-to-site IPsec VPN policy.

DFL-860E-2

Go to User authentication > AdminUsers. Add a new user account “xauth”. You have to give this user “username” and “password”.



AdminUsers

A local user database contains user accounts used for authentication purposes.

Name	Groups	IP Pool	Networks	Comments
admin	administrators			
xauth	administrators			

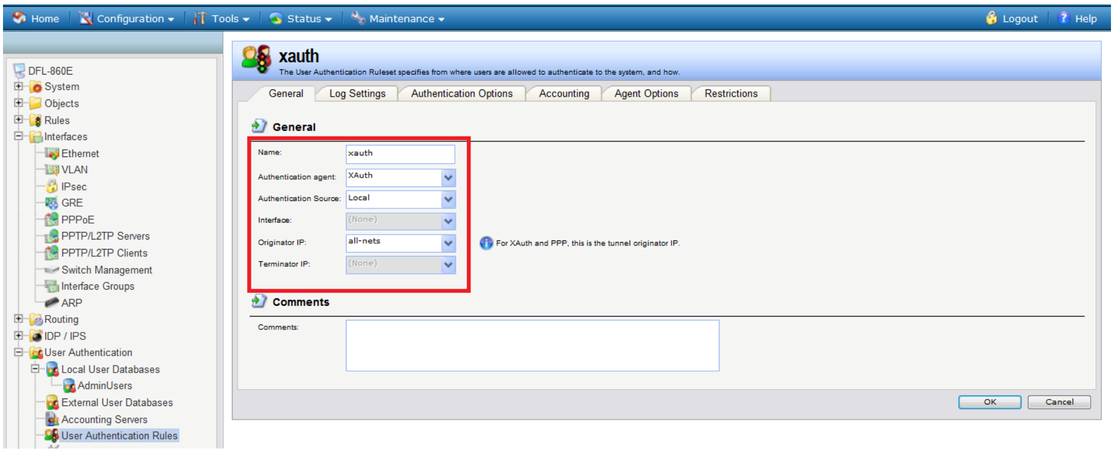
Right-click on a row for additional options.

Go to User authentication > User Authentication Rules. Create a new User Authentication Rule with the “Authentication source” set to trusted users.

Agent: xAuth

Authentication Source: Local

Originator IP: all0nets



xauth

The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.

General

Name: xauth

Authentication agent: XAuth

Authentication Source: Local

Interface: (None)

Originator IP: all-nets

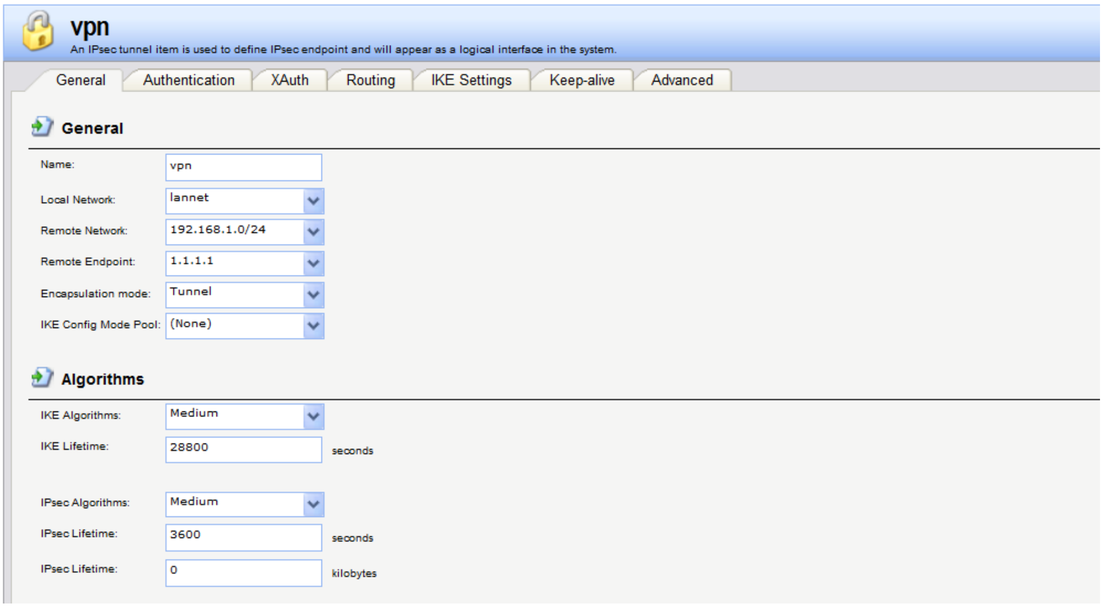
For XAuth and PPP, this is the tunnel originator IP.

Terminator IP: (None)

Comments

Comments:

Go to interface > IPSec. Add a new IPSec interface.



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: 192.168.1.0/24

Remote Endpoint: 1.1.1.1

Encapsulation mode: Tunnel

IKE Config Mode Pool: (None)

Algorithms

IKE Algorithms: Medium

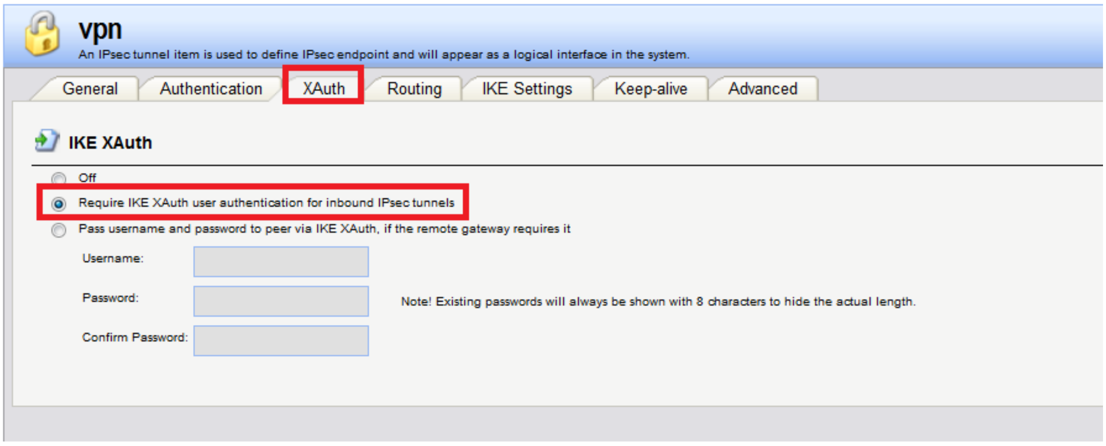
IKE Lifetime: 28800 seconds

IPsec Algorithms: Medium

IPsec Lifetime: 3600 seconds

IPsec Lifetime: 0 kilobytes

Go to XAuth then choose number 2 button.



vpn

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

IKE XAuth

○ Off

● Require IKE XAuth user authentication for inbound IPsec tunnels

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

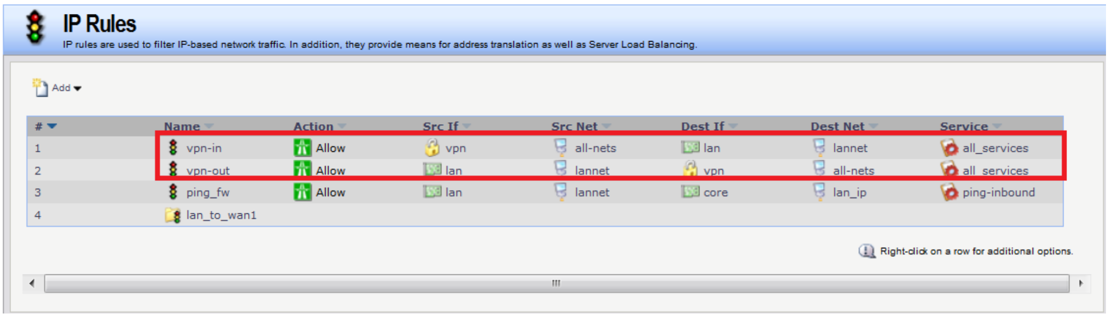
Username:

Password:

Confirm Password:

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

Go to IP rules. Add two IP rules for IPSec VPN.



IP Rules

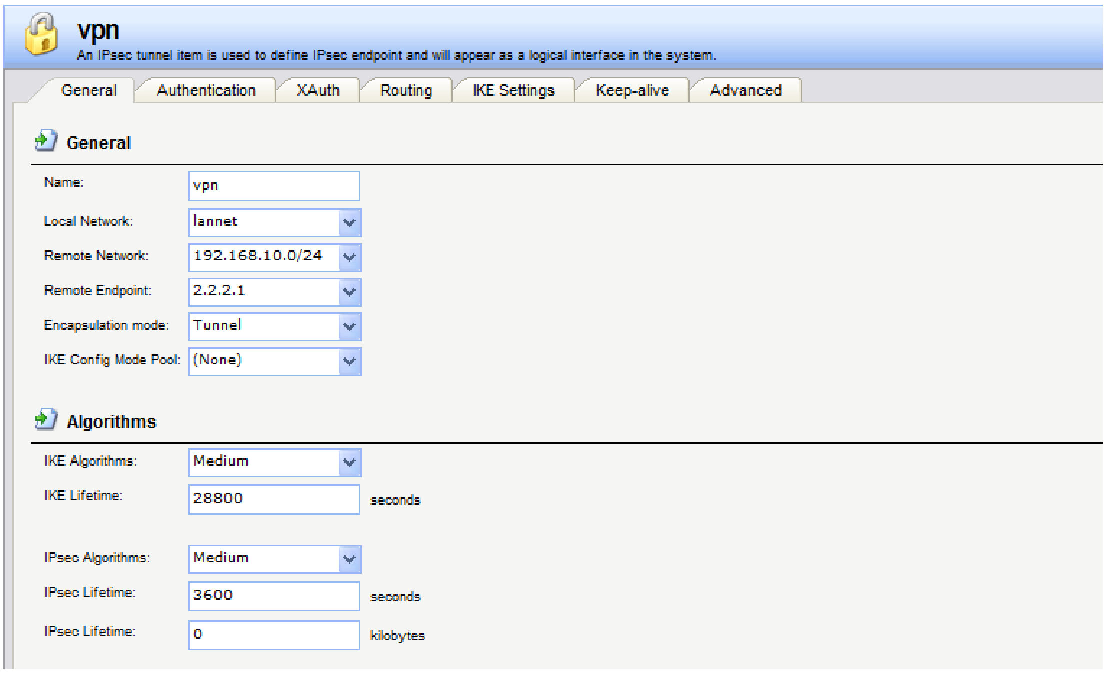
IP rules are used to filter IP-based network traffic. In addition, they provide means for address translation as well as Server Load Balancing.

#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	vpn-in	Allow	vpn	all-nets	lan	lannet	all_services
2	vpn-out	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.

DFL-860E-1

Go to interface > IPSec. Add a new IPSec interface.



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: vpn

Local Network: lannet

Remote Network: 192.168.10.0/24

Remote Endpoint: 2.2.2.1

Encapsulation mode: Tunnel

IKE Config Mode Pool: (None)

Algorithms

IKE Algorithms: Medium

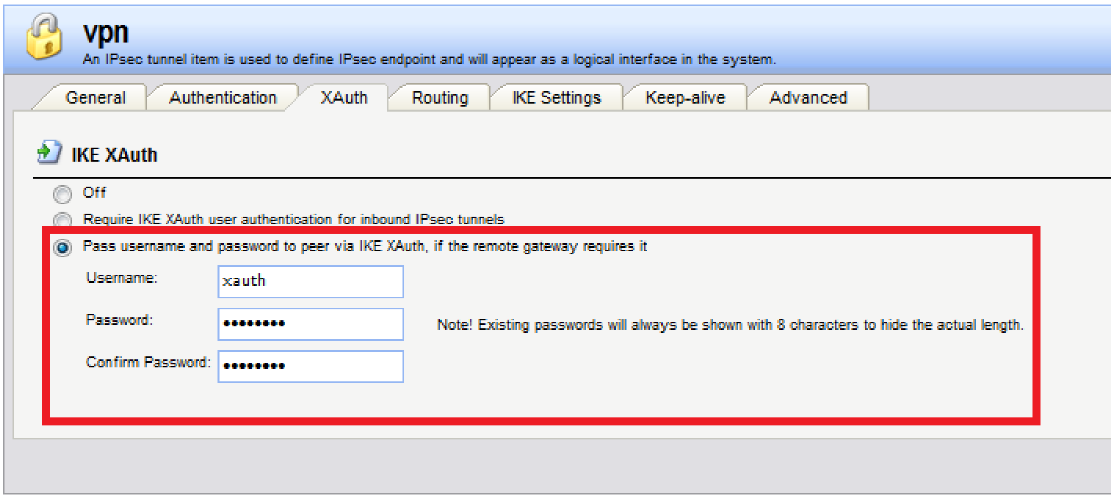
IKE Lifetime: 28800 seconds

IPsec Algorithms: Medium

IPsec Lifetime: 3600 seconds

IPsec Lifetime: 0 kilobytes

Go to XAuth then choose number 3 button. Fill out the username and password.



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

IKE XAuth

○ Off

○ Require IKE XAuth user authentication for inbound IPsec tunnels

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

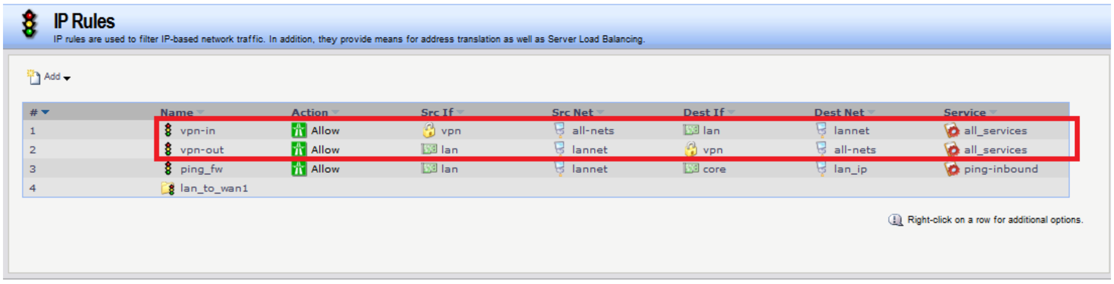
Username: xauth

Password: ••••••••

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

Confirm Password: ••••••••

Go to IP rules. Add two IP rules for IPSec VPN.



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-in	Allow	vpn	all-nets	lan	lannet	all_services
2	vpn-out	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.

END