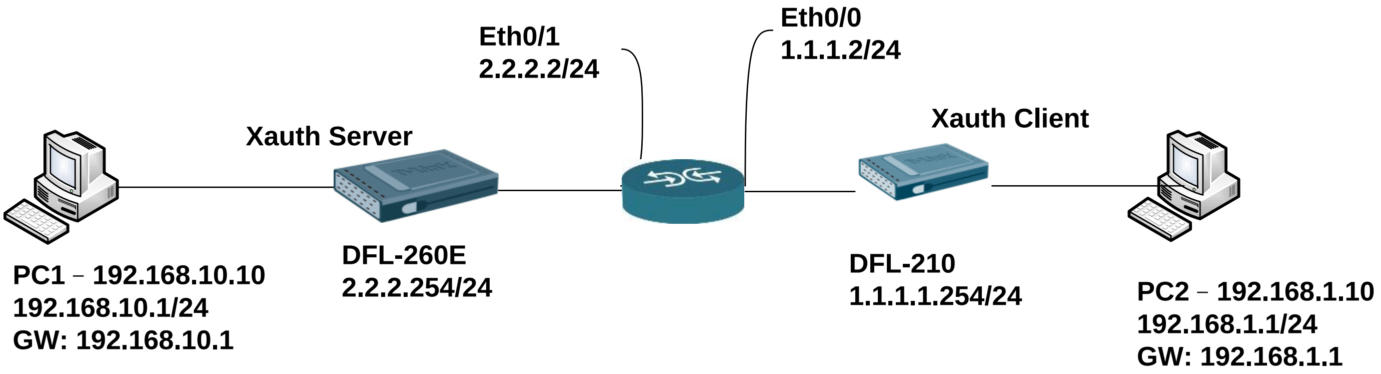
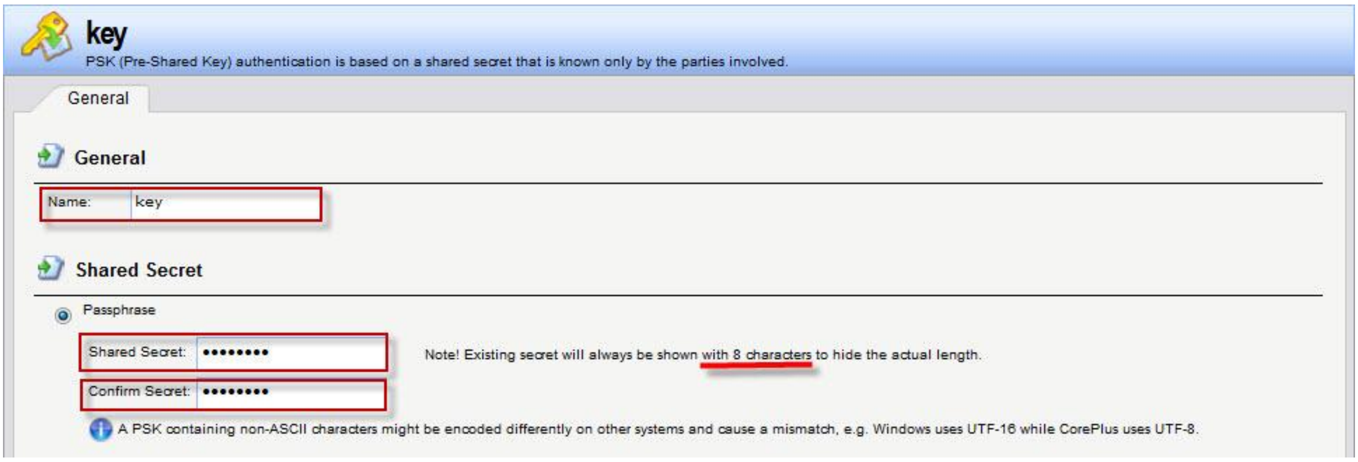
How to set up IPSec Site to Site VPN with Xauth



DFL-260E set up SOP (XAuth Server)

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: ••••••••

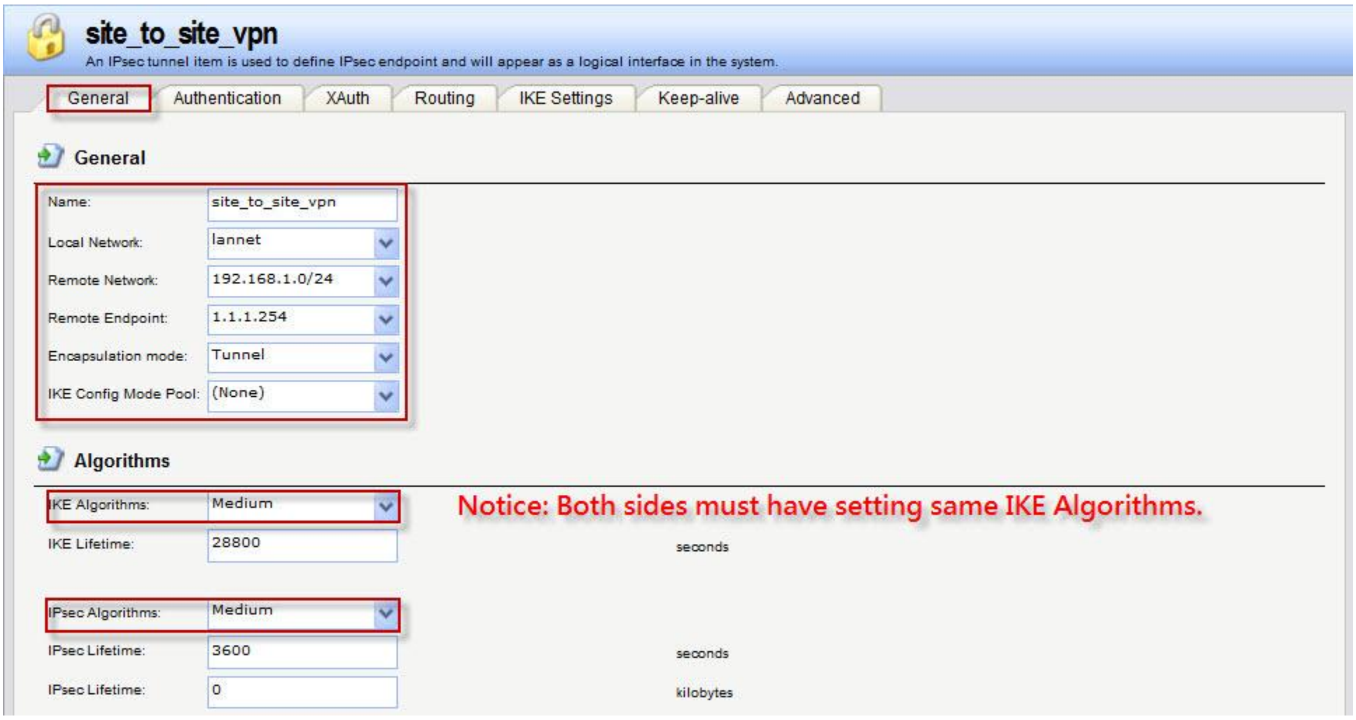
Note! Existing secret will always be shown with 8 characters to hide the actual length.

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

Name: site_to_site_vpn

Local Network: lannet

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

Notice: Both sides must have setting same IKE Algorithms.

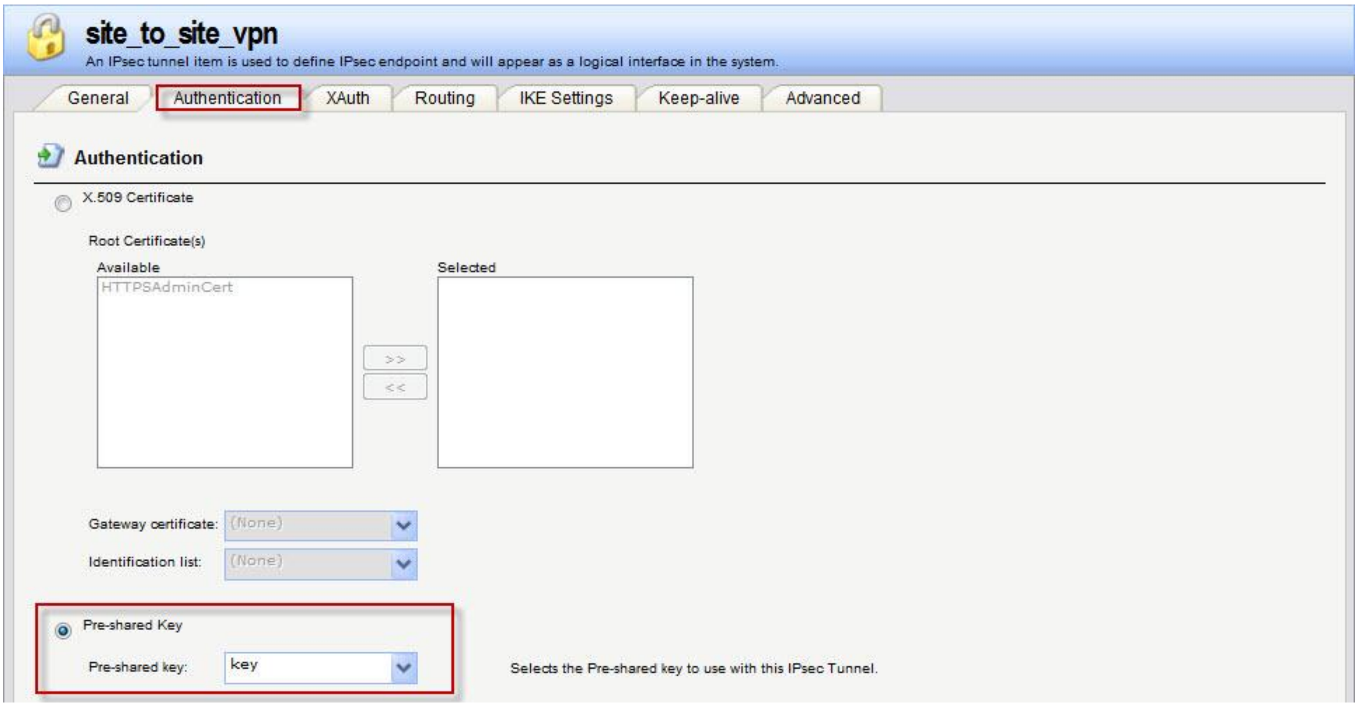
IKE Lifetime: 28800 seconds

IPsec Algorithms: Medium

IPsec Lifetime: 3600 seconds

IPsec Lifetime: 0 kilobytes

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.

Authentication

○ X.509 Certificate

Root Certificate(s)

Available: HTTPSAdminCert

Selected:

Gateway certificate: (None)

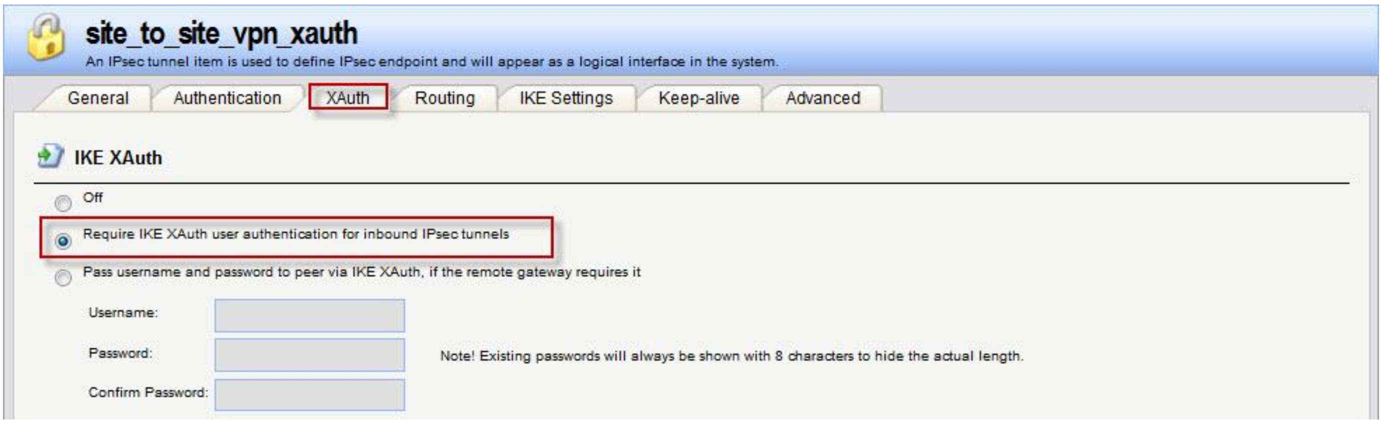
Identification list: (None)

● Pre-shared Key

Pre-shared key: key

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

XAuth



site_to_site_vpn_xauth

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:

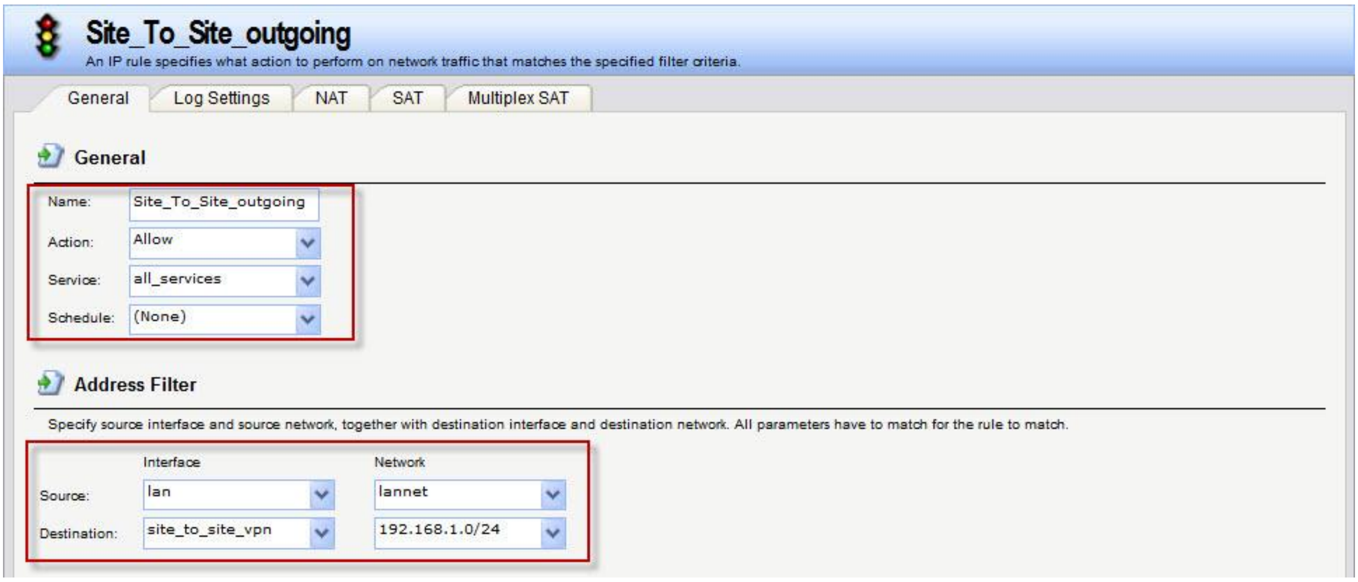
Password:

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

Confirm Password:

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

Name: Site_To_Site_outgoing

Action: Allow

Service: all_services

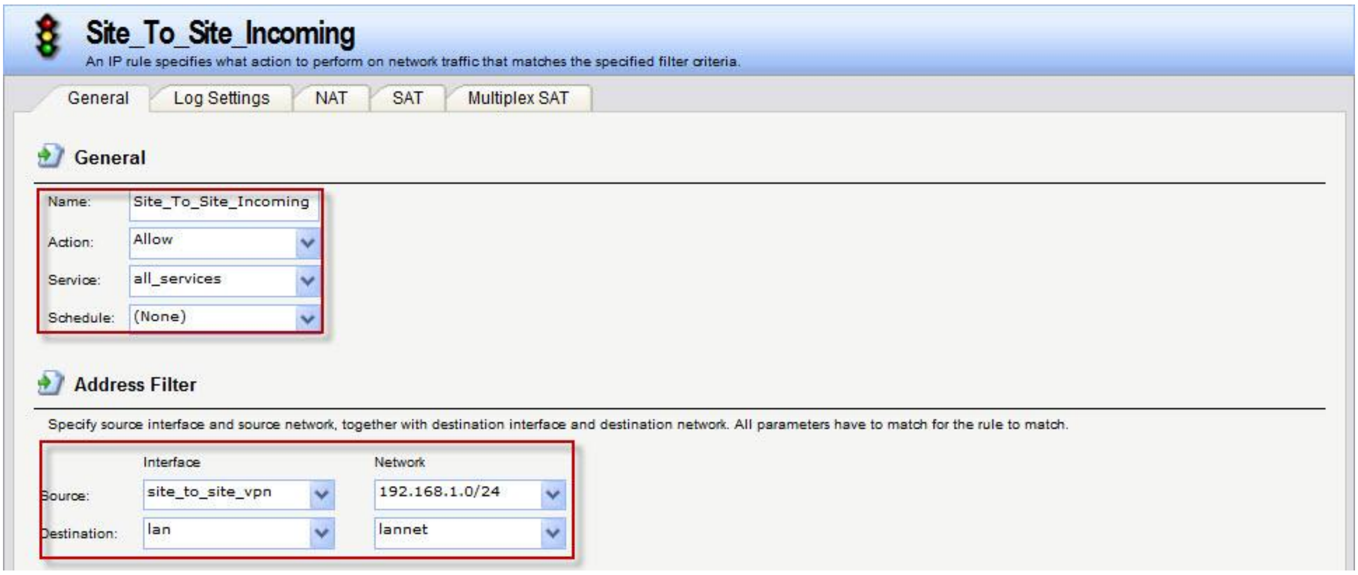
Schedule: (None)

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.

	Interface	Network
Source:	lan	lannet
Destination:	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

Name: Site_To_Site_Incoming

Action: Allow

Service: all_services

Schedule: (None)

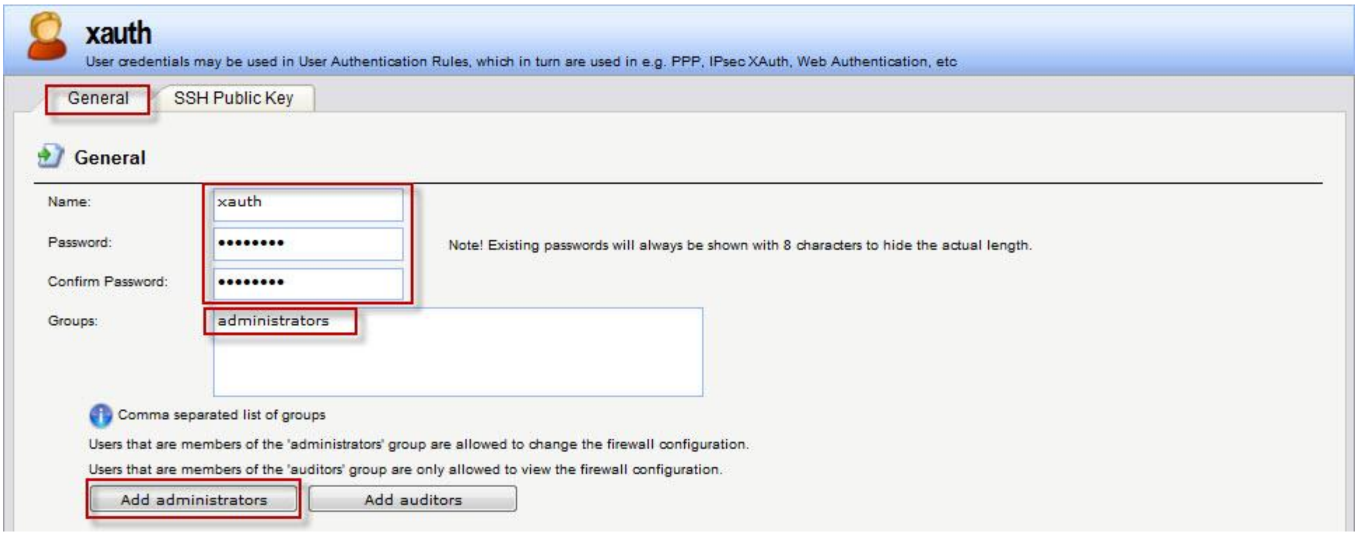
Address Filter

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

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

4. Create administrators groups account

User Authentication > Local User Databases > AdminUsers > Users > Add



xauth

User credentials may be used in User Authentication Rules, which in turn are used in e.g. PPP, IPsec XAuth, Web Authentication, etc

General

Name: xauth

Password: ••••••••

Confirm Password: ••••••••

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

Groups: administrators

Comma separated list of groups

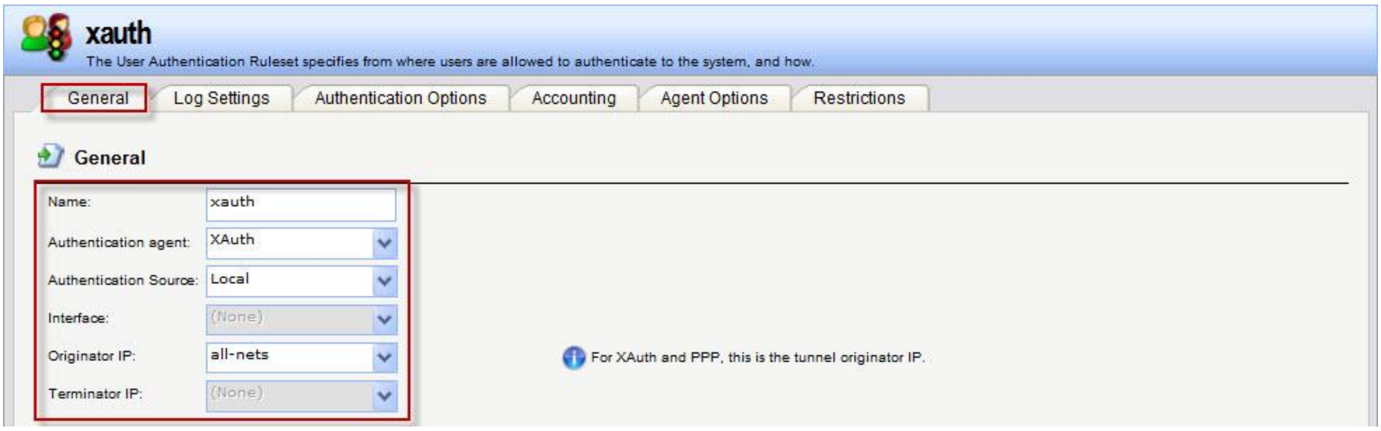
Users that are members of the 'administrators' group are allowed to change the firewall configuration.

Users that are members of the 'auditors' group are only allowed to view the firewall configuration.

5. Create Authentication Rules

User Authentication > User Authentication Rules \ Add

General



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

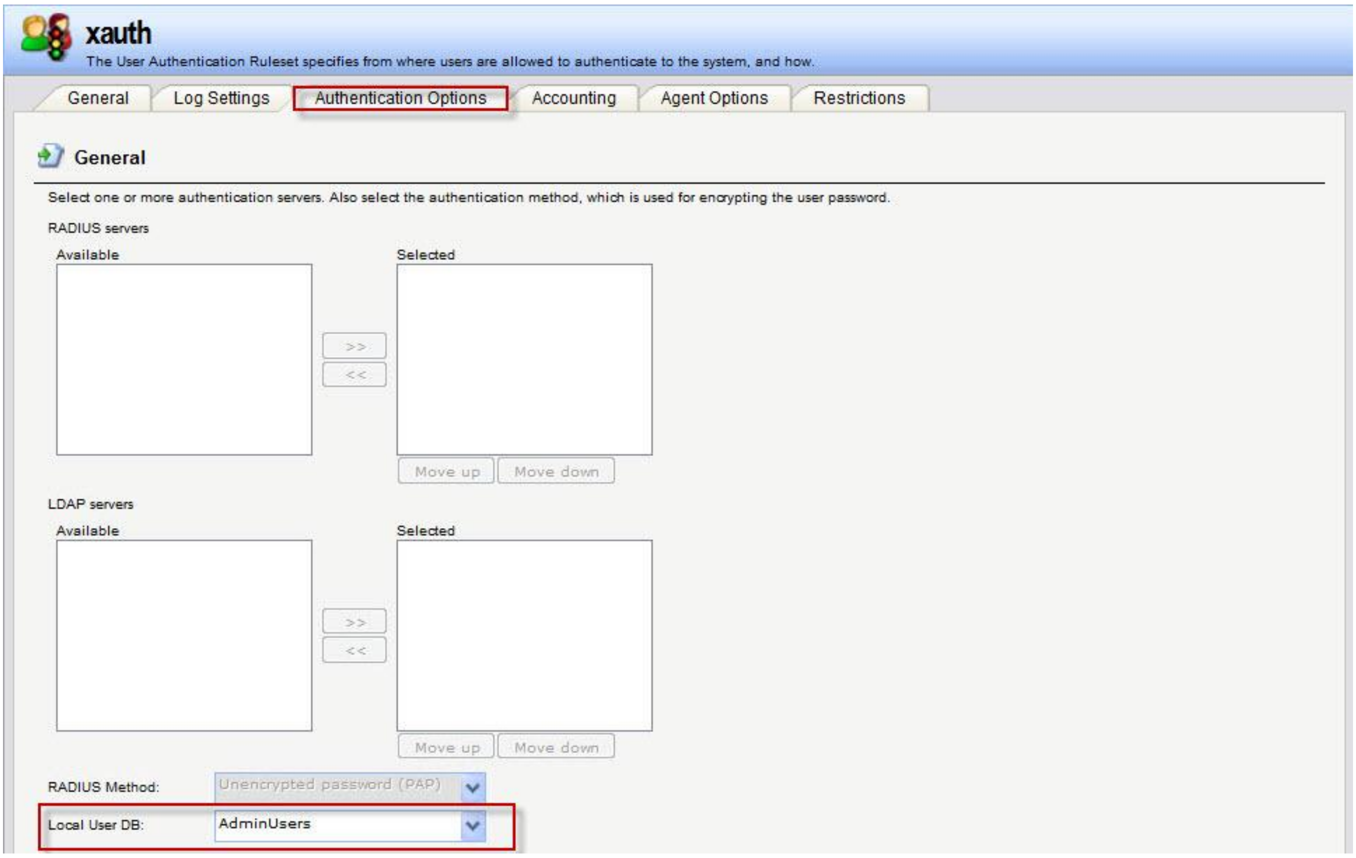
Interface: (None)

Originator IP: all-nets

Terminator IP: (None)

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

Authentication Options


xauth
The User Authentication Ruleset specifies from where users are allowed to authenticate to the system, and how.
General
Log Settings
Authentication Options
Accounting
Agent Options
Restrictions
General
Select one or more authentication servers. Also select the authentication method, which is used for encrypting the user password.
RADIUS servers
Available
Selected
>>
<<
Move up
Move down
LDAP servers
Available
Selected
>>
<<
Move up
Move down

RADIUS Method: Unencrypted password (PAP)

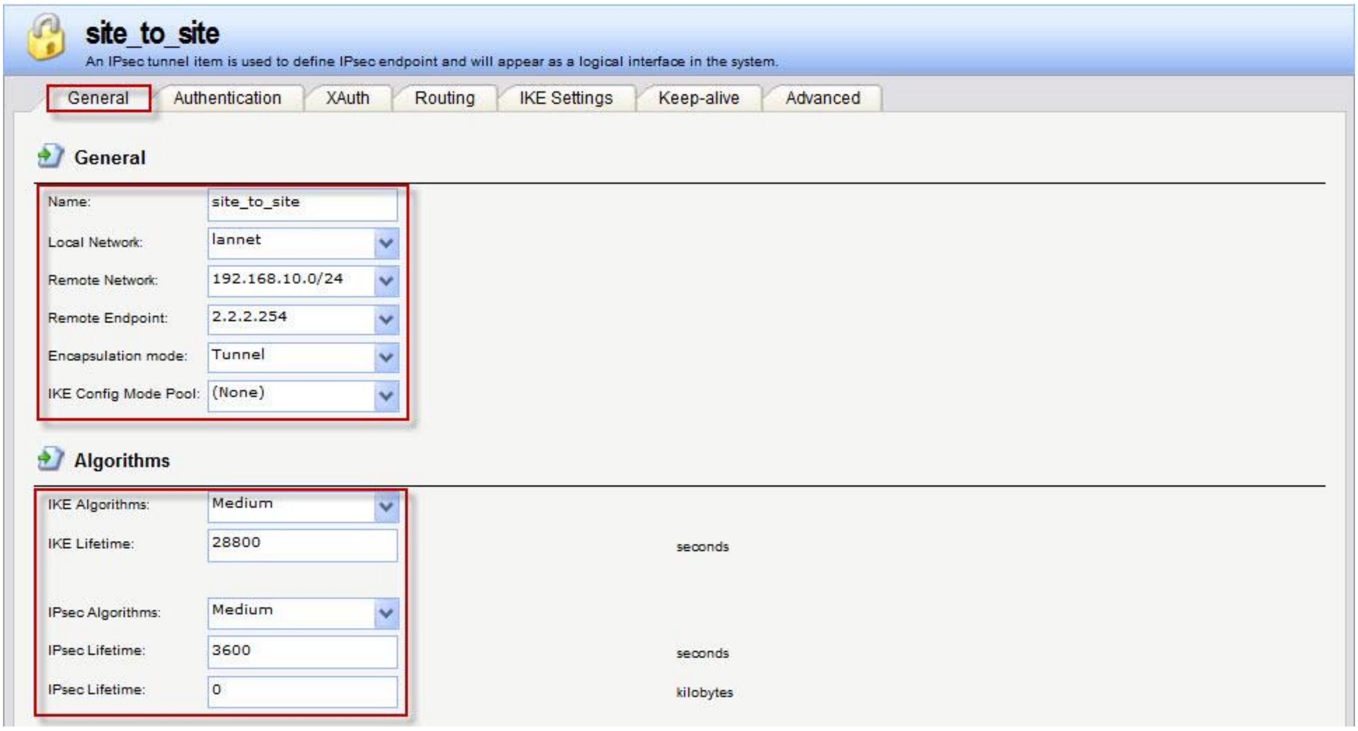
Local User DB: AdminUsers

DFL-210 set up 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


site_to_site
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
Algorithms

Name: site_to_site

Local Network: lannet

Remote Network: 192.168.10.0/24

Remote Endpoint: 2.2.2.254

Encapsulation mode: Tunnel

IKE Config Mode Pool: (None)

IKE Algorithms: Medium

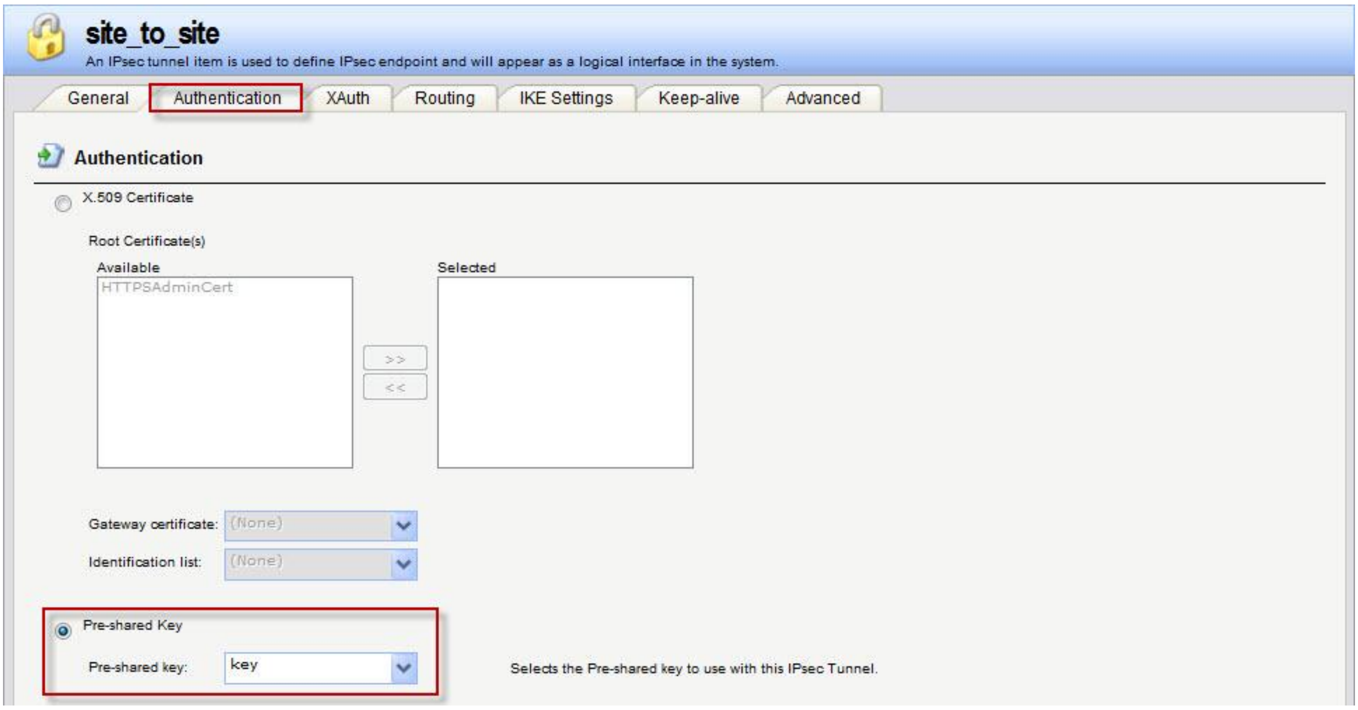
IKE Lifetime: 28800 seconds

IPsec Algorithms: Medium

IPsec Lifetime: 3600 seconds

IPsec Lifetime: 0 kilobytes

Authentication



site_to_site

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)

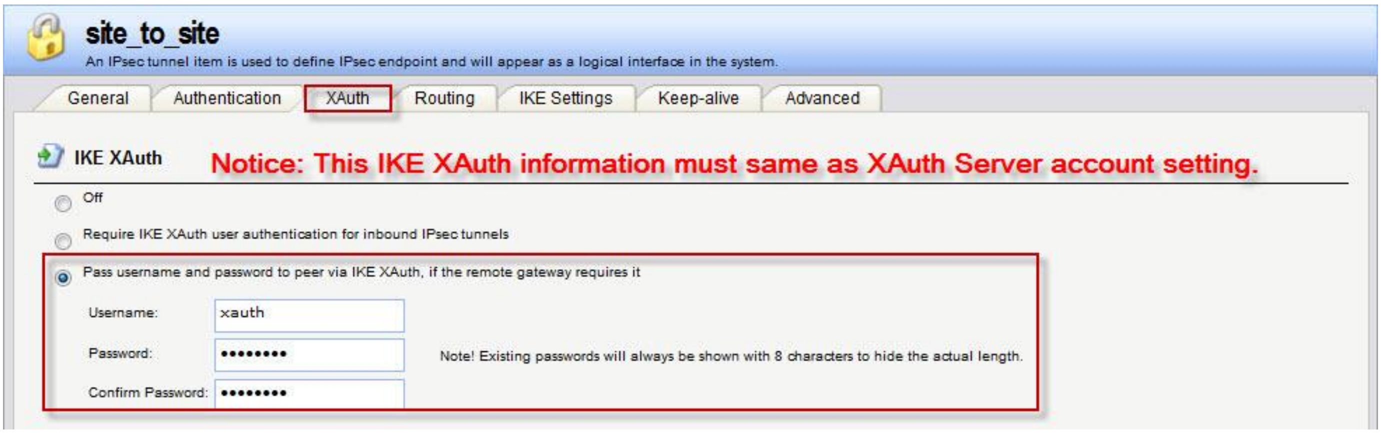
Identification list: (None)

● Pre-shared Key

Pre-shared key: key

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

XAuth



site_to_site

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

IKE XAuth

Notice: This IKE XAuth information must same as XAuth Server account setting.

○ 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

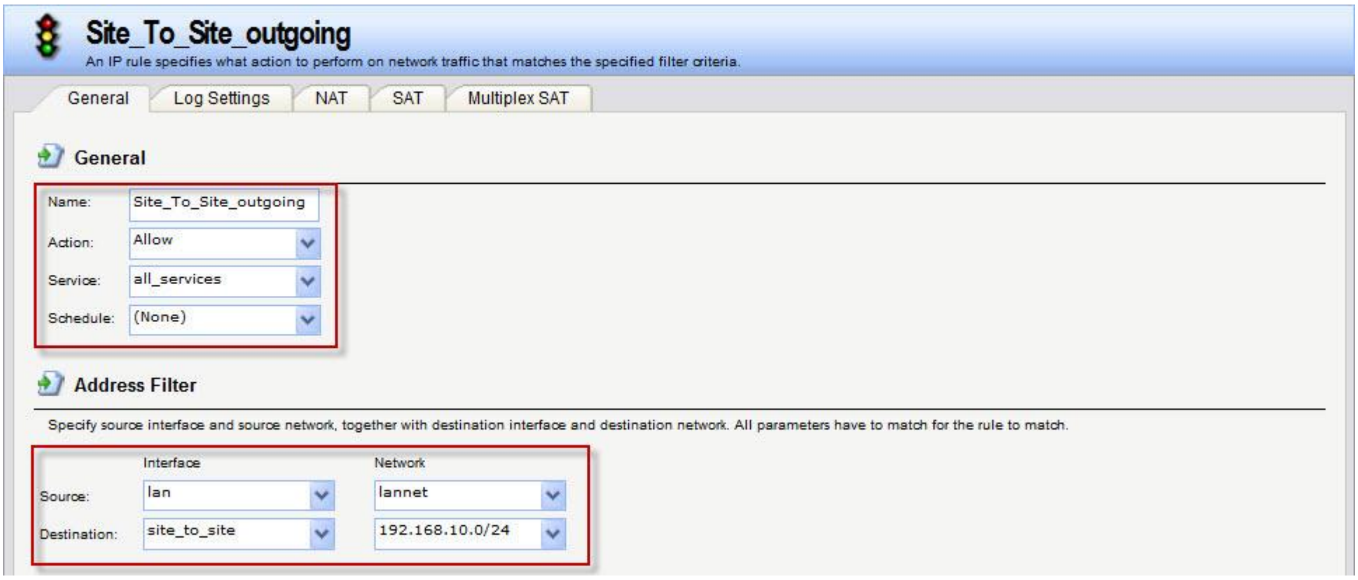
Password: ••••••••

Confirm Password: ••••••••

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

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

Name: Site_To_Site_outgoing

Action: Allow

Service: all_services

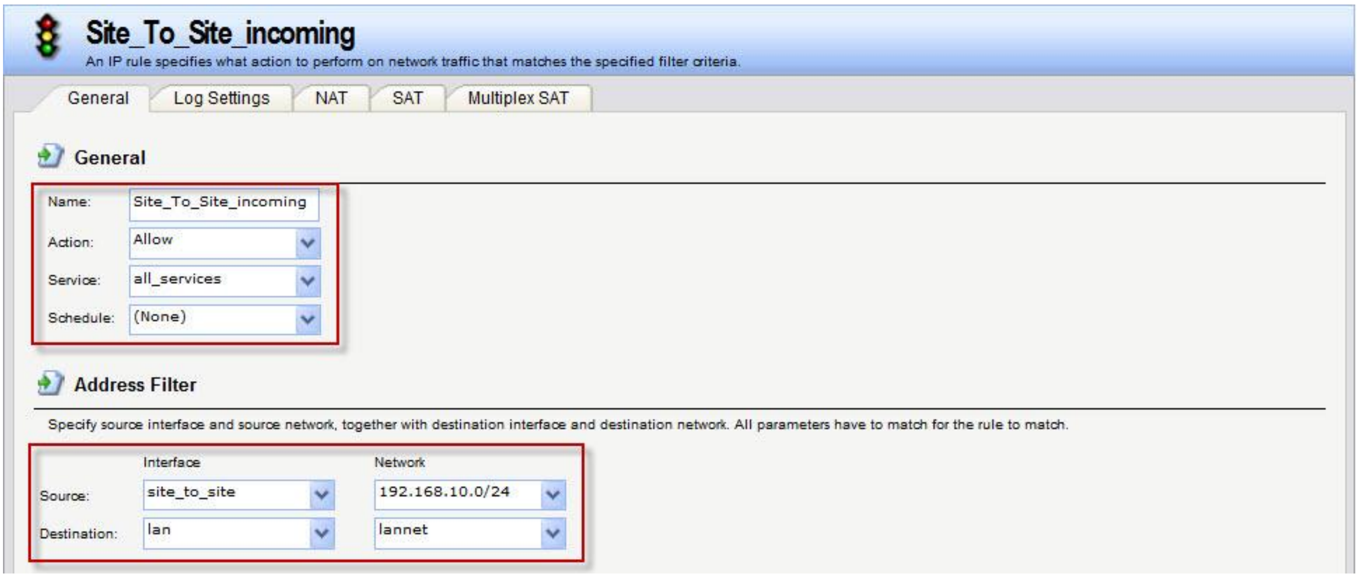
Schedule: (None)

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.

	Interface	Network
Source:	lan	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

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

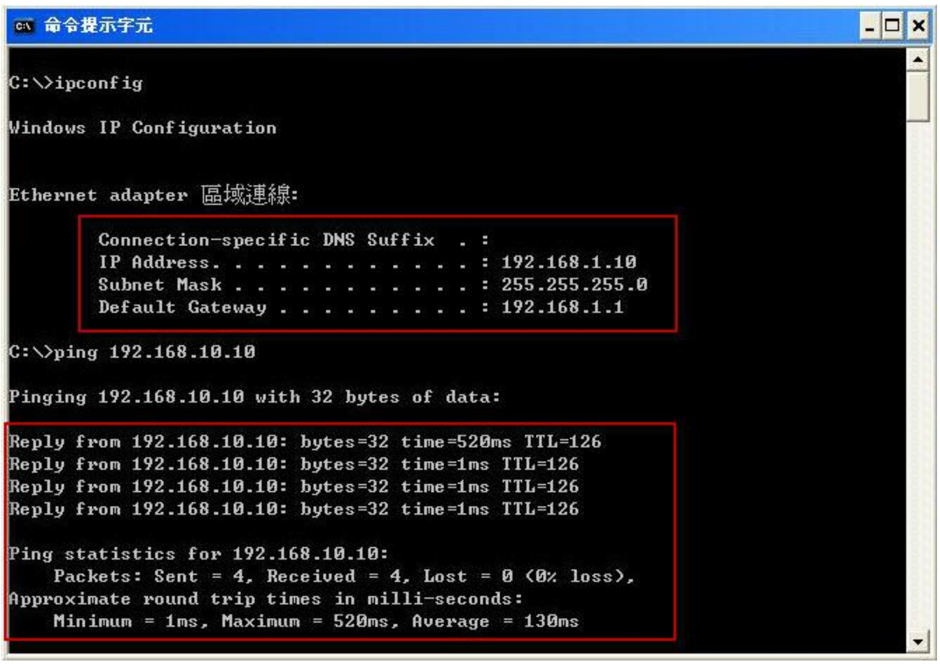
Address Filter

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

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

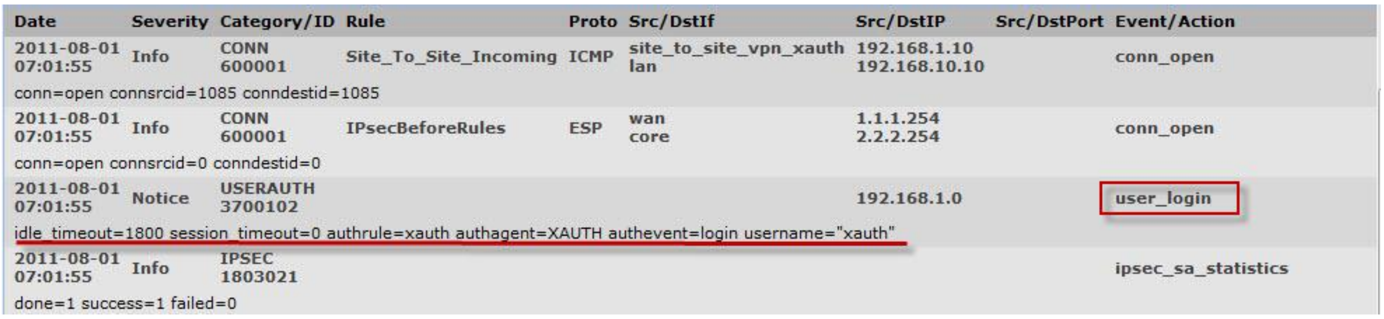
Test:

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



```
C:\>ipconfig

Windows IP Configuration


Ethernet adapter 區域連線:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.10
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

C:\>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:

Reply from 192.168.10.10: bytes=32 time=520ms TTL=126
Reply from 192.168.10.10: bytes=32 time=1ms TTL=126
Reply from 192.168.10.10: bytes=32 time=1ms TTL=126
Reply from 192.168.10.10: bytes=32 time=1ms TTL=126

Ping statistics for 192.168.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 520ms, Average = 130ms
```

You can check firewall log in XAuth Server (DFL-260E) this firewall.



Date	Severity	Category/ID	Rule	Proto	Src/DstIf	Src/DstIP	Src/DstPort	Event/Action
2011-08-01 07:01:55	Info	CONN 600001	Site_To_Site_Incoming	ICMP	site_to_site_vpn_xauth lan	192.168.1.10 192.168.10.10		conn_open
conn=open connsrcid=1085 conndestid=1085								
2011-08-01 07:01:55	Info	CONN 600001	IPsecBeforeRules	ESP	wan core	1.1.1.254 2.2.2.254		conn_open
conn=open connsrcid=0 conndestid=0								
2011-08-01 07:01:55	Notice	USERAUTH 3700102				192.168.1.0		user_login
idle_timeout=1800 session_timeout=0 authrule=xauth authagent=XAUTH authevent=login username="xauth"								
2011-08-01 07:01:55	Info	IPSEC 1803021						ipsec_sa_statistics
done=1 success=1 failed=0								

END