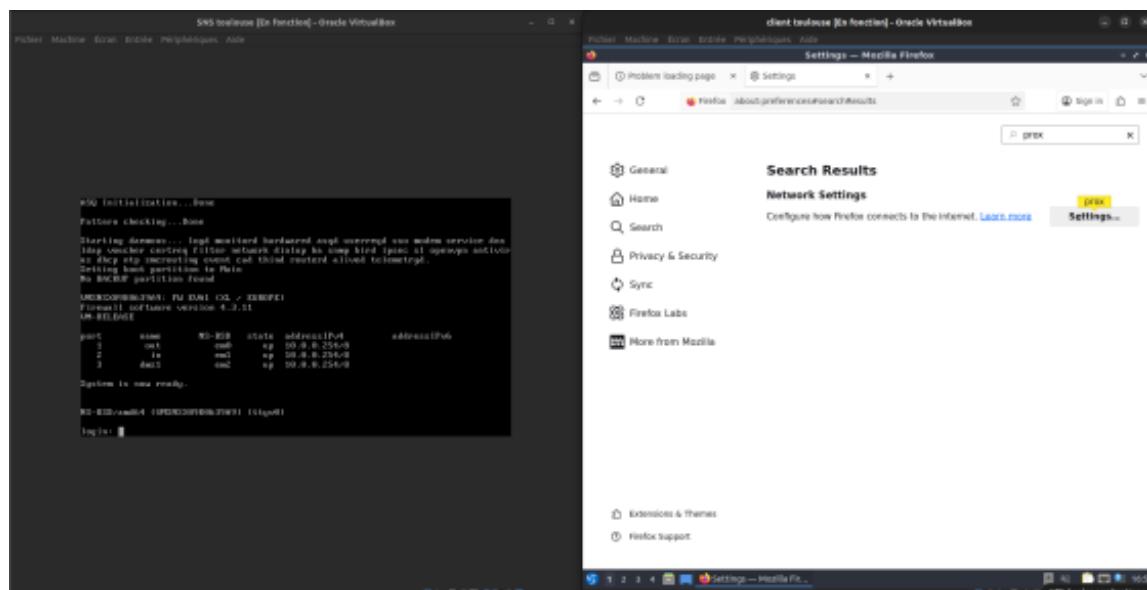
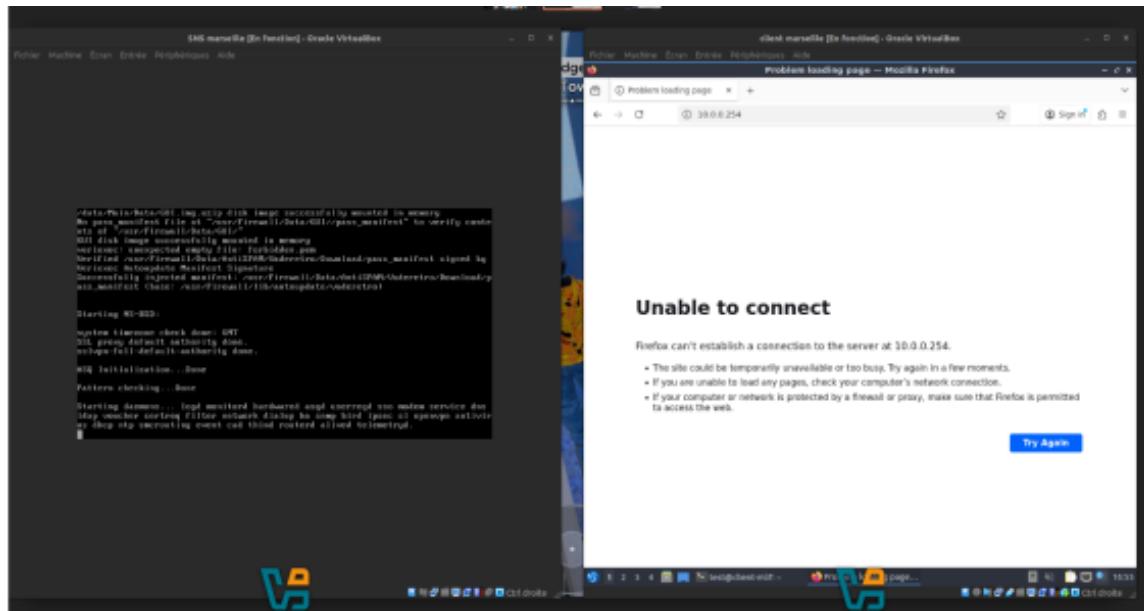


AHOUARI idriss

Mise en place des maquettes des site de Toulouse et Marseille avec leur firewall Stormshield et leur machine cliente pour préparer la connexion VPN site à site.



AHOUARI idriss

Mise en place du fuseau horaire français sur les deux firewalls afin d'assurer une bonne synchronisation du système et des certificats.

The screenshot displays two separate computer interfaces, likely representing two different Fortinet firewalls or configurations. Both interfaces are titled "EVAT" and are navigating through the "SYSTEM / CONFIGURATION" section of the FortiGate management interface. The "GENERAL CONFIGURATION" tab is active on both screens. The configuration details are as follows:

- Keyboard (language):** French
- Cryptographic settings:**
 - Enable regular retrieval of certificate revocation lists (CRL)
 - Enable "X.509/Diffusion/Rebroadcast" (OF) mode
- Password policy:**
 - Minimum password length: 8
 - Mandatory character types: None
 - Minimum entropy: 20
- Date/Time settings:** 11/01/2023 09:02:59 PM
 - Manual mode
 - Synchronizes with your machine - 11/01/2023 09:02:59 PM
 - Synchronizes fixed time (NTP)
- Timezone:** Europe/Paris

AHOUARI idriss

Mise en place de la configuration réseau des firewalls de Marseille et Toulouse afin d'assurer la communication et l'établissement du tunnel VPN site à site.

in Marseille :

Address range:

Address range inherited from the bridge
 Dynamic / Static

IPv4 address:

Dynamic IP (obtained by DHCP)
 Fixed IP (static)

+ Add X Delete

Address/ Mask	Comments
192.168.80.254/24	

Apply Cancel

out Marseille :

Address range

Address range:

Address range inherited from the bridge
 Dynamic / Static

IPv4 address:

Dynamic IP (obtained by DHCP)
 Fixed IP (static)

+ Add X Delete

Address/ Mask	Comments
82.10.20.2/30	

in Toulouse :

Address range

Address range:

Address range inherited from the bridge
 Dynamic / Static

IPv4 address:

Dynamic IP (obtained by DHCP)
 Fixed IP (static)

+ Add X Delete

Address/ Mask	Comments
192.168.50.254/24	

Apply Cancel

out Toulouse :

Address range

Address range:

Address range inherited from the bridge
 Dynamic / Static

IPv4 address:

Dynamic IP (obtained by DHCP)
 Fixed IP (static)

+ Add X Delete

Address/ Mask	Comments
82.10.20.1/30	

Apply Cancel

AHOUARI idriss

Mise en place du tunnel VPN IPsec site à site entre Toulouse et Marseille avec une authentification par clé partagée .

The screenshot shows the EVA1 software interface for configuring an IPsec tunnel. The top navigation bar has tabs for MONITORING and CONFIGURATION, with CONFIGURATION selected. The title bar says "EVA1 sns-toulouse". The main area is titled "VPN / IPSEC VPN". It shows an "ENCRYPTION POLICY - TUNNELS" section with one entry: "IPsec 01 (01)". Below this is a table for "SITE TO SITE (GATEWAY-GATEWAY)" and "MOBILE - MOBILE USERS". The table has columns for Status, Local network, Peer, Remote network, and Encryption profile. One row is listed: Status is off, Local network is "Network_in", Peer is "Site_Gw-Marseille", Remote network is "Lan-marseille", and Encryption profile is "StrongEncryption".

Configuration des réseaux et des règles de filtrage pour permettre la communication VPN entre les deux sites.

The screenshot shows the EVA1 software interface for configuring security policies. The top navigation bar has tabs for MONITORING and CONFIGURATION, with CONFIGURATION selected. The title bar says "EVA1 sns-toulouse". The main area is titled "SECURITY POLICY / FILTER - NAT". It shows a table with rules for "Remote Management" and "politique vpn". Rule 1: Action pass, Source Any, Destination firewall_all, Dest. port https, Protocol https, Security inspection none, Comments "Admin from everywhere". Rule 2: Action pass, Source Any, Destination firewall_all, Dest. port Any, Protocol icmp, Security inspection none, Comments "Allow Ping from everywhere". Rule 3: Action pass, Source Network_in, Destination Lan-marseille, Dest. port Any, Protocol Any, Security inspection none, Comments "Created on 2025-11-28 17:23:35 by admin (192.168.50.1)". Rule 4: Action pass, Source Lan-marseille, Destination Network_in, Dest. port Any, Protocol Any, Security inspection none, Comments "Created on 2025-11-28 17:22:31 by admin (192.168.50.1)". Rule 5: Action block, Source Any, Destination Any, Dest. port Any, Protocol Any, Security inspection none, Comments "Block all".

The screenshot shows the EVA1 software interface for configuring security policies. The top navigation bar has tabs for MONITORING and CONFIGURATION, with CONFIGURATION selected. The title bar says "EVA1 sns-marseille". The main area is titled "SECURITY POLICY / FILTER - NAT". It shows a table with rules for "Remote Management" and "politique vpn". Rule 1: Action pass, Source Any, Destination firewall_all, Dest. port https, Protocol https, Security inspection none, Comments "Admin from everywhere". Rule 2: Action pass, Source Any, Destination firewall_all, Dest. port Any, Protocol icmp, Security inspection none, Comments "Allow Ping from everywhere". Rule 3: Action pass, Source Network_in, Destination Lan-Toulouse, Dest. port Any, Protocol Any, Security inspection none, Comments "Created on 2025-11-28 17:30:16 by admin (192.168.80.1)". Rule 4: Action pass, Source Lan-Toulouse, Destination Network_in, Dest. port Any, Protocol Any, Security inspection none, Comments "Created on 2025-11-28 17:30:14 by admin (192.168.80.1)". Rule 5: Action block, Source Any, Destination Any, Dest. port Any, Protocol Any, Security inspection none, Comments "Block all".

AHOUARI idriss

Réalisation d'un test de connectivité (ping) entre les deux machines clientes afin de valider le fonctionnement du VPN.

The image shows two Oracle VirtualBox windows side-by-side. Both windows have a terminal session titled "test@client-milf:" and a Mozilla Firefox browser window titled "administration".

Left Window (client toulouse):

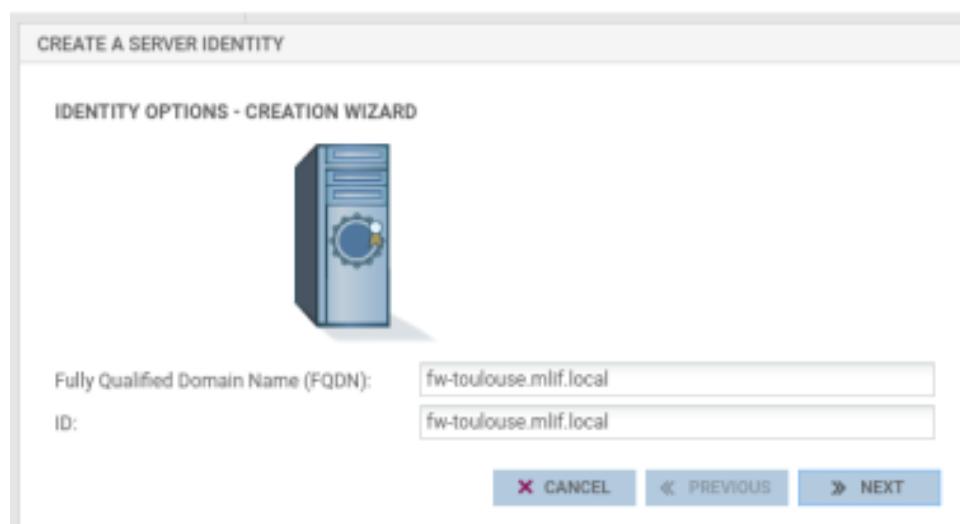
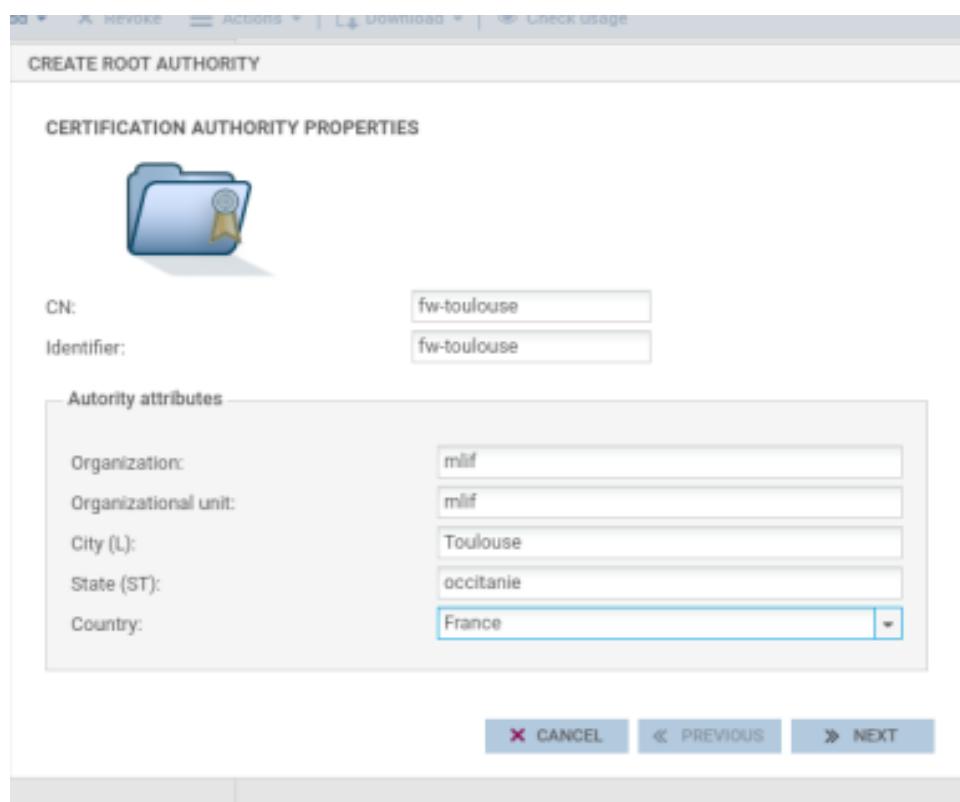
```
inet 127.0.0.1/8 scope host lo
  valid_lft forever preferred_lft forever
inet ::1/128 scope host
  valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
  link/ether 08:00:27:15:af:f6 brd ff:ff:ff:ff:ff:ff
  inet 192.168.50.1/24 brd 192.168.50.255 scope global noprefixroute enp0s3
    valid_lft forever preferred_lft forever
  inet 192.168.50.1/24 brd 192.168.50.255 scope global noprefixroute
    valid_lft forever preferred_lft forever
  inet 192.168.50.1/24 brd 192.168.50.255 scope global noprefixroute
    valid_lft forever preferred_lft forever
test@client-milf:~$ ping 192.168.80.1
PING 192.168.80.1 (192.168.80.1) 56(84) bytes of data.
64 bytes from 192.168.80.1: icmp_seq=1 ttl=64 time=2.27 ms
64 bytes from 192.168.80.1: icmp_seq=2 ttl=64 time=2.37 ms
64 bytes from 192.168.80.1: icmp_seq=3 ttl=64 time=2.58 ms
64 bytes from 192.168.80.1: icmp_seq=4 ttl=64 time=2.98 ms
64 bytes from 192.168.80.1: icmp_seq=5 ttl=64 time=3.78 ms
64 bytes from 192.168.80.1: icmp_seq=6 ttl=64 time=3.86 ms
64 bytes from 192.168.80.1: icmp_seq=7 ttl=64 time=2.27 ms
...
--- 192.168.80.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6080ms
rtt min/avg/max/mdev = 2.271/2.734/3.698/0.485 ms
test@client-milf:~$
```

Right Window (client marseille):

```
inet 127.0.0.1/8 scope host lo
  valid_lft forever preferred_lft forever
inet ::1/128 scope host
  valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
  link/ether 08:00:27:15:af:f6 brd ff:ff:ff:ff:ff:ff
  inet 192.168.50.1/24 brd 192.168.50.255 scope global noprefixroute enp0s3
    valid_lft forever preferred_lft forever
  inet 192.168.50.1/24 brd 192.168.50.255 scope global noprefixroute
    valid_lft forever preferred_lft forever
  inet 192.168.50.1/24 brd 192.168.50.255 scope global noprefixroute
    valid_lft forever preferred_lft forever
test@client-milf:~$ ping 192.168.80.1
PING 192.168.80.1 (192.168.80.1) 56(84) bytes of data.
64 bytes from 192.168.80.1: icmp_seq=1 ttl=64 time=2.74 ms
64 bytes from 192.168.80.1: icmp_seq=2 ttl=64 time=2.41 ms
64 bytes from 192.168.80.1: icmp_seq=3 ttl=64 time=3.87 ms
64 bytes from 192.168.80.1: icmp_seq=4 ttl=64 time=2.07 ms
64 bytes from 192.168.80.1: icmp_seq=5 ttl=64 time=2.91 ms
64 bytes from 192.168.80.1: icmp_seq=6 ttl=64 time=2.43 ms
64 bytes from 192.168.80.1: icmp_seq=7 ttl=64 time=2.46 ms
64 bytes from 192.168.80.1: icmp_seq=8 ttl=64 time=3.12 ms
64 bytes from 192.168.80.1: icmp_seq=9 ttl=64 time=3.00 ms
64 bytes from 192.168.80.1: icmp_seq=10 ttl=64 time=2.72 ms
64 bytes from 192.168.80.1: icmp_seq=11 ttl=64 time=3.17 ms
64 bytes from 192.168.80.1: icmp_seq=12 ttl=64 time=3.04 ms
64 bytes from 192.168.80.1: icmp_seq=13 ttl=64 time=3.70 ms
64 bytes from 192.168.80.1: icmp_seq=14 ttl=64 time=3.18 ms
64 bytes from 192.168.80.1: icmp_seq=15 ttl=64 time=3.50 ms
64 bytes from 192.168.80.1: icmp_seq=16 ttl=64 time=3.28 ms
64 bytes from 192.168.80.1: icmp_seq=17 ttl=64 time=3.34 ms
64 bytes from 192.168.80.1: icmp_seq=18 ttl=64 time=3.53 ms
64 bytes from 192.168.80.1: icmp_seq=19 ttl=64 time=2.79 ms
64 bytes from 192.168.80.1: icmp_seq=20 ttl=64 time=2.75 ms
64 bytes from 192.168.80.1: icmp_seq=21 ttl=64 time=4.07 ms
64 bytes from 192.168.80.1: icmp_seq=22 ttl=64 time=3.07 ms
64 bytes from 192.168.80.1: icmp_seq=23 ttl=64 time=2.72 ms
64 bytes from 192.168.80.1: icmp_seq=24 ttl=64 time=3.23 ms
64 bytes from 192.168.80.1: icmp_seq=25 ttl=64 time=2.64 ms
64 bytes from 192.168.80.1: icmp_seq=26 ttl=64 time=2.03 ms
64 bytes from 192.168.80.1: icmp_seq=27 ttl=64 time=2.95 ms
64 bytes from 192.168.80.1: icmp_seq=28 ttl=64 time=2.53 ms
64 bytes from 192.168.80.1: icmp_seq=29 ttl=64 time=2.68 ms
64 bytes from 192.168.80.1: icmp_seq=30 ttl=64 time=2.31 ms
64 bytes from 192.168.80.1: icmp_seq=31 ttl=64 time=2.86 ms
64 bytes from 192.168.80.1: icmp_seq=32 ttl=64 time=2.93 ms
64 bytes from 192.168.80.1: icmp_seq=33 ttl=64 time=2.39 ms
64 bytes from 192.168.80.1: icmp_seq=34 ttl=64 time=3.77 ms
...
--- 192.168.80.1 ping statistics ---
74 packets transmitted, 74 received, 0% packet loss, time 8741ms
rtt min/avg/max/mdev = 2.025/2.954/4.135/0.437 ms
test@client-milf:~$
```

AHOUARI idriss

Mise en place de la CA et du certificat du firewall de Toulouse pour l'authentification VPN.



AHOUARI idriss

CREATE A SERVER IDENTITY

SUMMARY

Finish this wizard in order to create the server identity below

Name:	fw-toulouse.mlif.local
Identifier:	fw-toulouse.mlif.local
Parent authority:	Fw-toulouse
Organization:	MLif
Organizational unit:	MLif
City (L):	France
State (ST):	Occitanie
Country:	FR
Type de clé:	RSA
Key size:	2048

Valid until: Sat Nov 28 2026 16:48:48 GMT+0100 (Central European Standard Time) (365 days)

✖ CANCEL ◀ PREVIOUS ✓ FINISH

Création et importation du certificat du firewall de Marseille pour permettre l'authentification par certificats.

CREATE A SERVER IDENTITY

IDENTITY OPTIONS - CREATION WIZARD

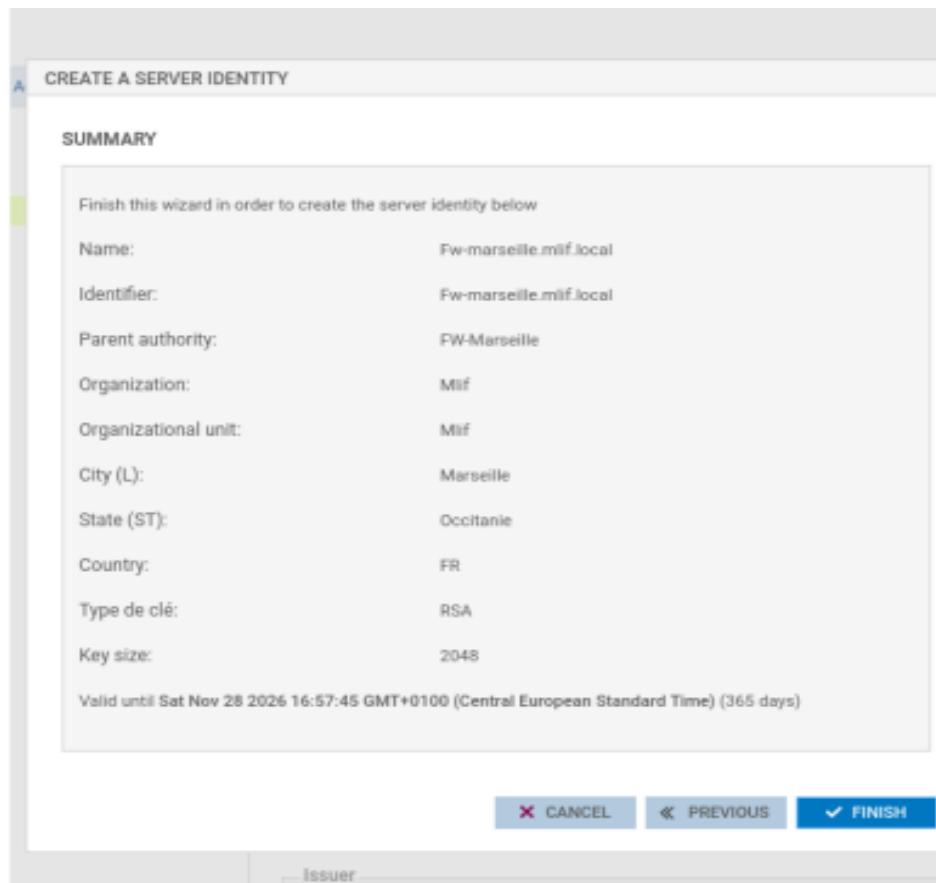


Fully Qualified Domain Name (FQDN): Fw-marseille.mlif.local
ID: Fw-marseille.mlif.local

✖ CANCEL ◀ PREVIOUS » NEXT

Country Name:	FR
Email Address:	
Subject hash:	00136e81

AHOUARI idriss



Modification de la configuration du tunnel VPN afin de remplacer l'authentification par PSK par une authentification par certificats.

The screenshot shows the 'IDENTIFICATION' tab of a VPN policy configuration. Under the 'APPROVED CERTIFICATION AUTHORITY' section, there is a list containing 'Futuose'. Below this, under 'MOBILE TUNNELS: PRE-SHARED KEYS (PSK)', there is a table with one entry: 'Identity' and 'Key'. At the bottom of the screen, there is a 'CHECKING THE POLICY' progress bar.

AHOUARI idriss

Identification

Authentication method:	Certificate
Certificate:	Fw-toulouse/fw-toulouse.mlif.local
Local ID:	Enter an ID (optional)
Peer ID:	Enter an ID (optional)
Pre-shared key (PSK):	 

Certificates					
Name	Issuer	Distinguished Name	In Use	Actions	
webConfigurator default (640991c5c0c8c) Server Certificate CA: No Server: Yes	self-signed	O=pfSense webConfigurator Self-Signed Certificate, CN=pfSense-640991c5c0c8c 		   	
Certificat-JHON-DOE User Certificate CA: No Server: No	external	ST=IDF, OU=COMMERCIAUX, O=MLIF, L=Paris, CN=b2b.mlif.local, C=FR  Valid From: Tue, 02 Dec 2025 10:17:05 +0100 Valid Until: Fri, 30 Nov 2035 10:17:05 +0100		   	
CERT-SRV-VPN User Certificate CA: No Server: No	external	ST=IDF, OU=COMMERCIAUX, O=MLIF, L=Paris, CN=srv-vpn.mlif.local, C=FR  Valid From: Wed, 03 Dec 2025 13:59:28 +0100 Valid Until: Sat, 01 Dec 2035 13:59:28 +0100		   	

 Add/Sign

The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.

- a AES-192-CFB (192 bit key, 128 bit block)
- n AES-192-CFB1 (192 bit key, 128 bit block)
- s AES-192-CFB8 (192 bit key, 128 bit block)
- AES-192-GCM (192 bit key, 128 bit block)
- AES-192-OFB (192 bit key, 128 bit block)
- AES-256-CBC (256 bit key, 128 bit block)**
- AES-256-CFB (256 bit key, 128 bit block)
- AES-256-CFB1 (256 bit key, 128 bit block)
- AES-256-CFB8 (256 bit key, 128 bit block)
- AES-256-GCM (256 bit key, 128 bit block)
- ~~AES-256-OFB (256 bit key, 128 bit block)~~

Available Data Encryption Algorithms
Click to add or remove an algorithm from the

- AES-128-CBC
- AES-128-GCM
- AES-256-CBC

Allowed Data Encryption Algorithms. Click
an algorithm name to remove it from the list