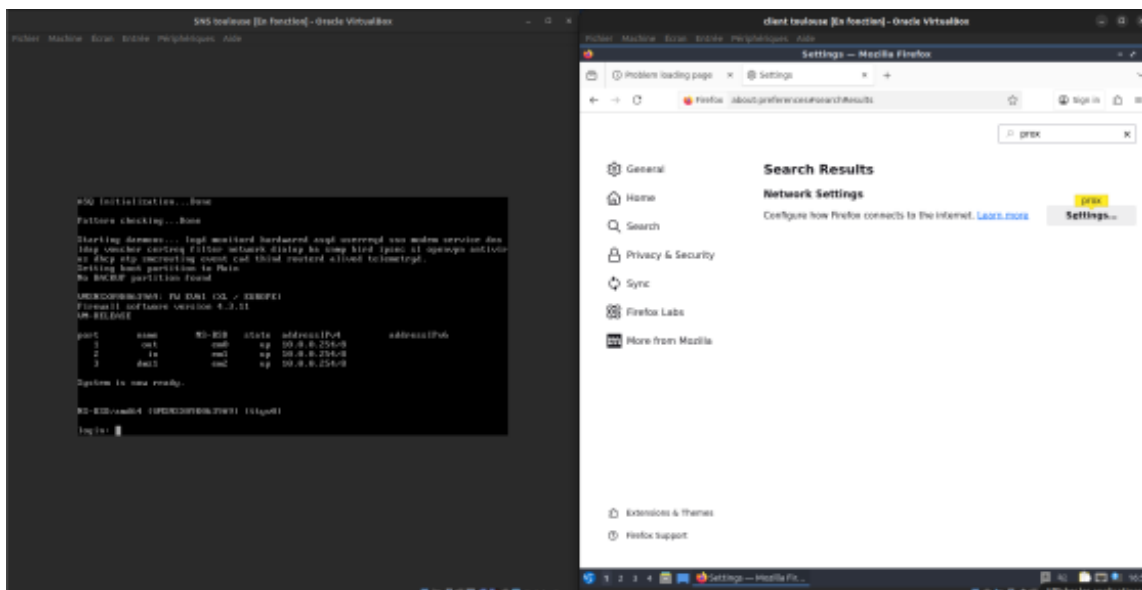
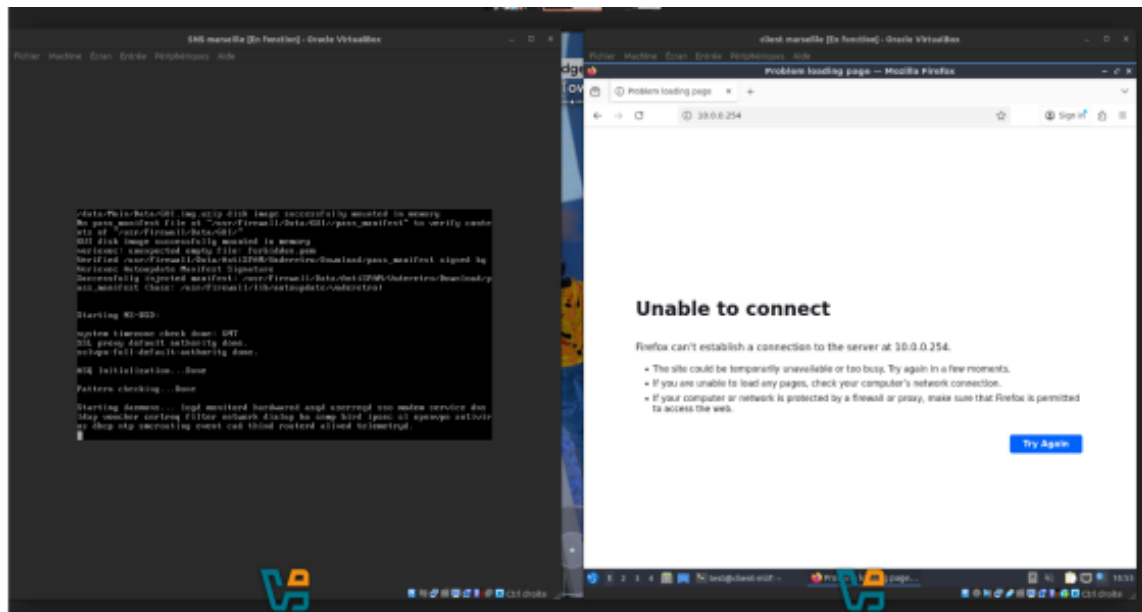
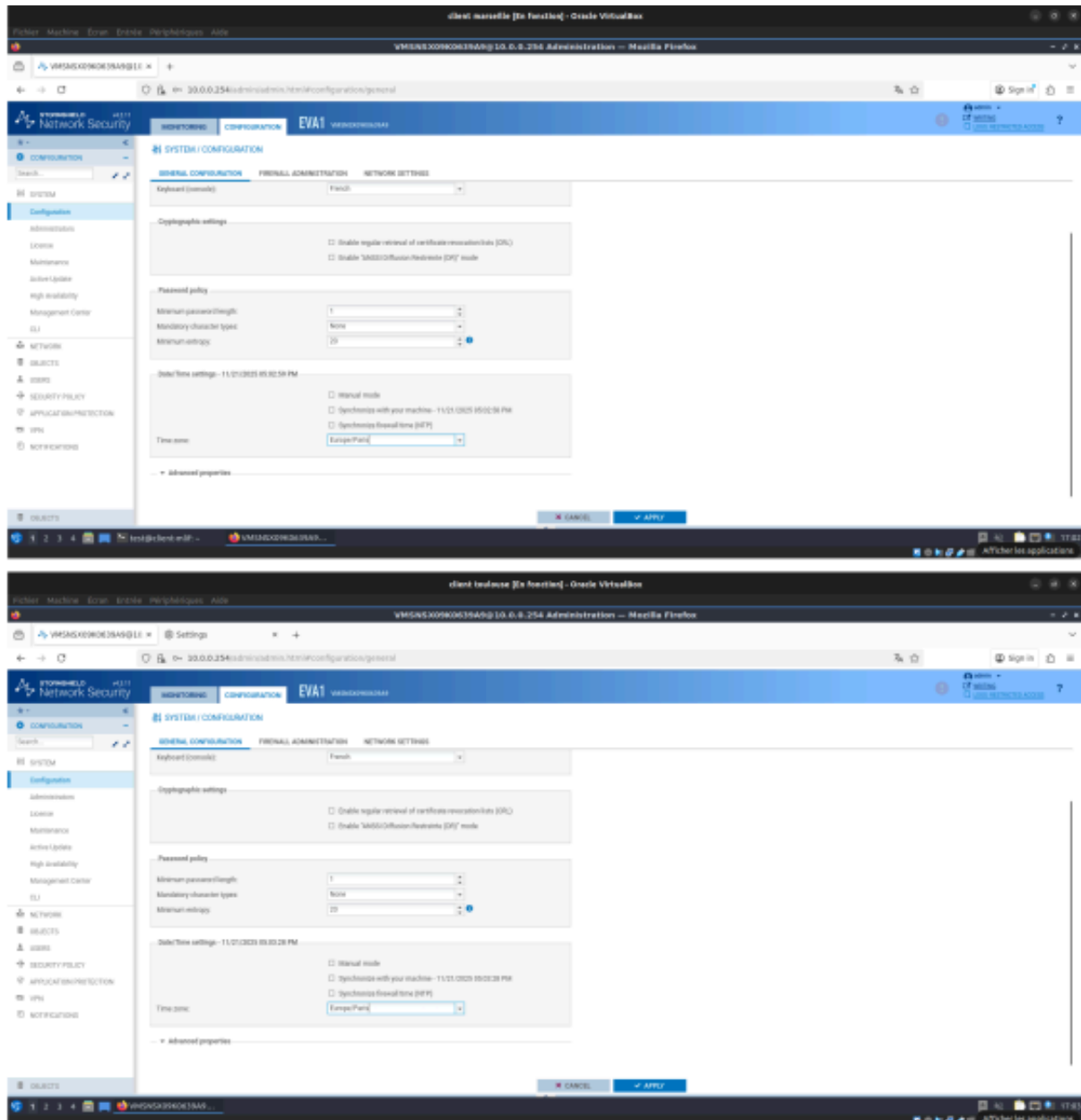


Mise en place des maquettes des site de Toulouse et Marseille avec leur firewall Stormshield et leur machine cliente pour préparer la connexion VPN site à site.



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



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: ☐ 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

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

MONITORING

CONFIGURATION

EVA1sns-toulouse

VPN / IPSEC VPN

ENCIPHERMENT POLICY - TUNNELSPEERSIDENTIFICATIONENCIPHERMENT PROFILES

IPsec 01 (01)

Actions

SITE TO SITE (GATEWAY-GATEWAY)MOBILE - MOBILE USERS

Enter a filter

+ AddX DeleteUpDownCutCopyPasteShow detailsSearch in logsSearch in monitoring

	Status	Local network	Peer	Remote network	Encryption profile
1	off	Network_in	Site_Gw-Marseille	Lan-marseille	StrongEncryption

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

MONITORING

CONFIGURATION

EVA1sns-toulouse

SECURITY POLICY / FILTER - NAT

(1) Block all

EditExport

FILTERINGNAT

Searching...

+ New ruleX DeleteUpDownCutCopyPasteSearch in logsSearch in monitoring

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
Remote Management: Go to System - Configuration to setup the web administration application access (contains 2 rules, from 1 to 2)								
1	on	pass	Any	firewall_Lan	firewall_srv https			Admin from everywhere
2	on	pass	Any	firewall_all	Any	icmp (Echo request)		Allow Ping from everywhere
politique vpn (contains 2 rules, from 3 to 4)								
3	on	pass	Network_in	Lan-marseille	Any			Created on 2025-11-28 17:23:35 by admin (192.168.50.1)
4	on	pass	Lan-marseille	Network_in	Any			Created on 2025-11-28 17:22:31 by admin (192.168.50.1)
Default policy - Updated on 2025-11-28 17:21:15 by admin (192.168.50.1) (contains 1 rules, from 5 to 5)								
5	on	block	Any	Any	Any			Block all

MONITORING

CONFIGURATION

EVA1sns-marseille

SECURITY POLICY / FILTER - NAT

(1) Block all

EditExport

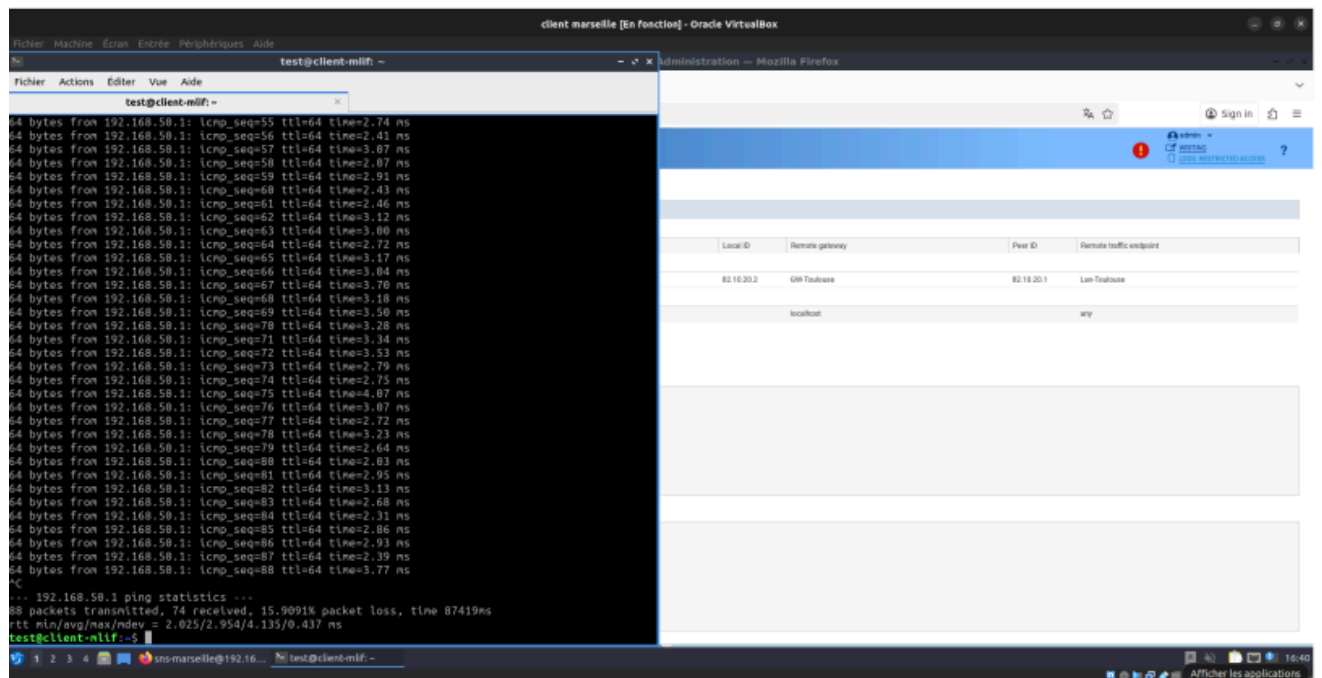
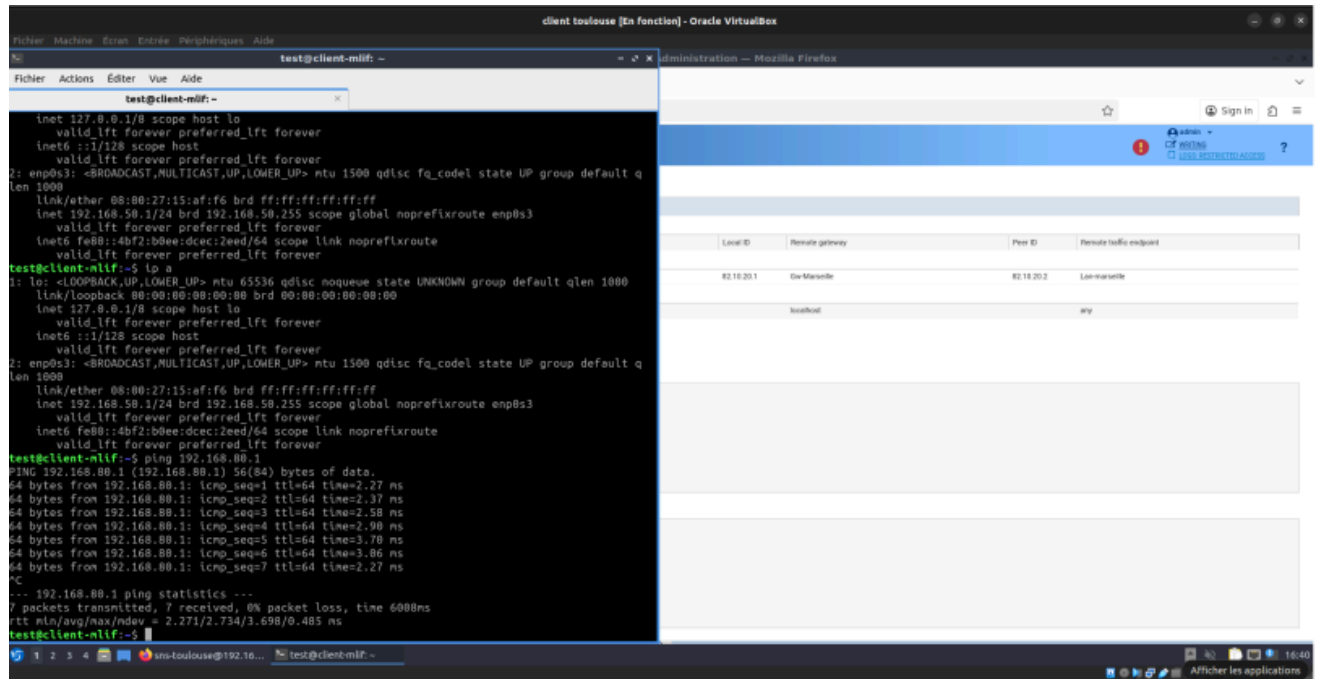
FILTERINGNAT

Searching...

+ New ruleX DeleteUpDownCutCopyPasteSearch in logsSearch in monitoring

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments
Remote Management: Go to System - Configuration to setup the web administration application access (contains 2 rules, from 1 to 2)								
1	on	pass	Any	firewall_Lan	firewall_srv https			Admin from everywhere
2	on	pass	Any	firewall_all	Any	icmp (Echo request)		Allow Ping from everywhere
politique vpn (contains 2 rules, from 3 to 4)								
3	on	pass	Network_in	Lan-Toulouse	Any			Created on 2025-11-28 17:30:16 by admin (192.168.80.1)
4	on	pass	Lan-Toulouse	Network_in	Any			Created on 2025-11-28 17:30:14 by admin (192.168.80.1)
Default policy - Updated on 2025-11-28 17:29:52 by admin (192.168.80.1) (contains 1 rules, from 5 to 5)								
5	on	block	Any	Any	Any			Block all


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



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

CREATE ROOT AUTHORITY

CERTIFICATION AUTHORITY PROPERTIES




CN: fw-toulouse
Identifier: fw-toulouse

Authority attributes

Organization: mlif
Organizational unit: mlif
City (L): Toulouse
State (ST): occitanie
Country: France

CREATE A SERVER IDENTITY

IDENTITY OPTIONS - CREATION WIZARD



Fully Qualified Domain Name (FQDN): fw-toulouse.mlif.local
ID: fw-toulouse.mlif.local

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.

DETAILS


REVOCATION (CRL)

CERTIFICATE PROFILES

Validity

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

CREATE A SERVER IDENTITY

SUMMARY

Finish this wizard in order to create the server identity below

Name:	Fw-marseille.mlif.local
Identifier:	Fw-marseille.mlif.local
Parent authority:	FW-Marseille
Organization:	Mlif
Organizational unit:	Mlif
City (L):	Marseille
State (ST):	Occitanie
Country:	FR
Type de clé:	RSA
Key size:	2048

Valid until Sat Nov 28 2026 16:57:45 GMT+0100 (Central European Standard Time) (365 days)

CANCEL

PREVIOUS

FINISH

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

MONITORING CONFIGURATION EVA1

VPN / IPSEC VPN

ENCRYPTION POLICY - TUNNELS PEERS IDENTIFICATION ENCRYPTION PROFILES

APPROVED CERTIFICATION AUTHORITY

+ Add X Delete

CA

Fortissuase

MOBILE TUNNELS: PRE-SHARED KEYS (PSK)

Find key + Add X Delete Edit selection Export the list of PSKs

Identity	Key
----------	-----

Advanced properties

CHECKING THE POLICY

CANCEL

APPLY

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):

●●●●●●●●●●●●

✕

Edit

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 Valid From: Thu, 09 Mar 2023 08:59:01 +0100 Valid Until: Wed, 10 Apr 2024 09:59:01 +0200		   
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 2025 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 2025 13:59:28 +0100		   
<div>+ Add/Sign</div>				

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

Available Data Encryption Algorithms

Click to add or remove an algorithm from the

AES-128-CFB (128 bit key, 128 bit block)

AES-192-CFB1 (192 bit key, 128 bit block)

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)

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

AES-128-CBC

AES-128-GCM

AES-256-CBC