# Décodage de la terminologie du pare-feu sécurisé (pour les nouveaux utilisateurs de Firepower)

## Table des matières



## Introduction

Ce document décrit les différents jargons populaires de Cisco Firewall. Ce document explique également comment passer d'un mode CLI à un autre.

## Conditions préalables

### Exigences

Il n’existe aucune condition préalable pour apprendre cette rubrique.

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Secure Firewall Management Center (FMC)
- Cisco Firepower Threat Defense (FTD)
- Gestion des périphériques Cisco Firepower (FDM)
- Firepower eXtensible Operating System (FXOS)
- Firepower Chassis Manager (FCM)
- Appareil de sécurité adaptatif (ASA)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

## Terminologies techniques couramment utilisées

### FTD : Défense contre les menaces Firepower

FTD est un pare-feu de nouvelle génération qui offre plus que les pare-feu traditionnels. Il inclut des services tels que IPS (Intrusion Prevention System), AMP (Advanced Malware Protection), le filtrage des URL, Security Intelligence, etc. FTD est très similaire à ASA (Adaptive Security Appliance), mais avec des fonctionnalités supplémentaires. FTD fonctionne sur 2 moteurs, LINA et SNORT.

### LINA : architecture réseau intégrée basée sur Linux

Nous appelons ASA Lina dans les périphériques FTD. LINA n'est rien d'autre qu'un code ASA sur lequel FTD s'exécute. Lina se concentre principalement sur la sécurité de la couche réseau. Il intègre certaines fonctionnalités de pare-feu de couche 7 grâce à ses fonctions d'inspection et de contrôle des applications.

### RENIFLEUR

Snort Engine est un système de détection et de prévention des intrusions sur le réseau. Les principales fonctionnalités de snort incluent l'inspection des paquets pour identifier les anomalies, la détection basée sur des règles, les alertes en temps réel, la journalisation et l'analyse, ainsi que l'intégration à d'autres outils de sécurité. Snort peut effectuer une inspection de couche 7 (trafic de couche application), non seulement en fonction d’un en-tête de paquet, mais également en fonction du contenu des paquets.

Vous avez la possibilité d'écrire vos propres règles personnalisées pour définir des modèles ou des signatures spécifiques au niveau de la couche application, ce qui améliore les fonctionnalités de détection. Il effectue une inspection approfondie des paquets en évaluant leur charge utile.

Vous pouvez même effectuer le déchiffrement des paquets chiffrés ici.

## FXOS : système d'exploitation extensible Firepower

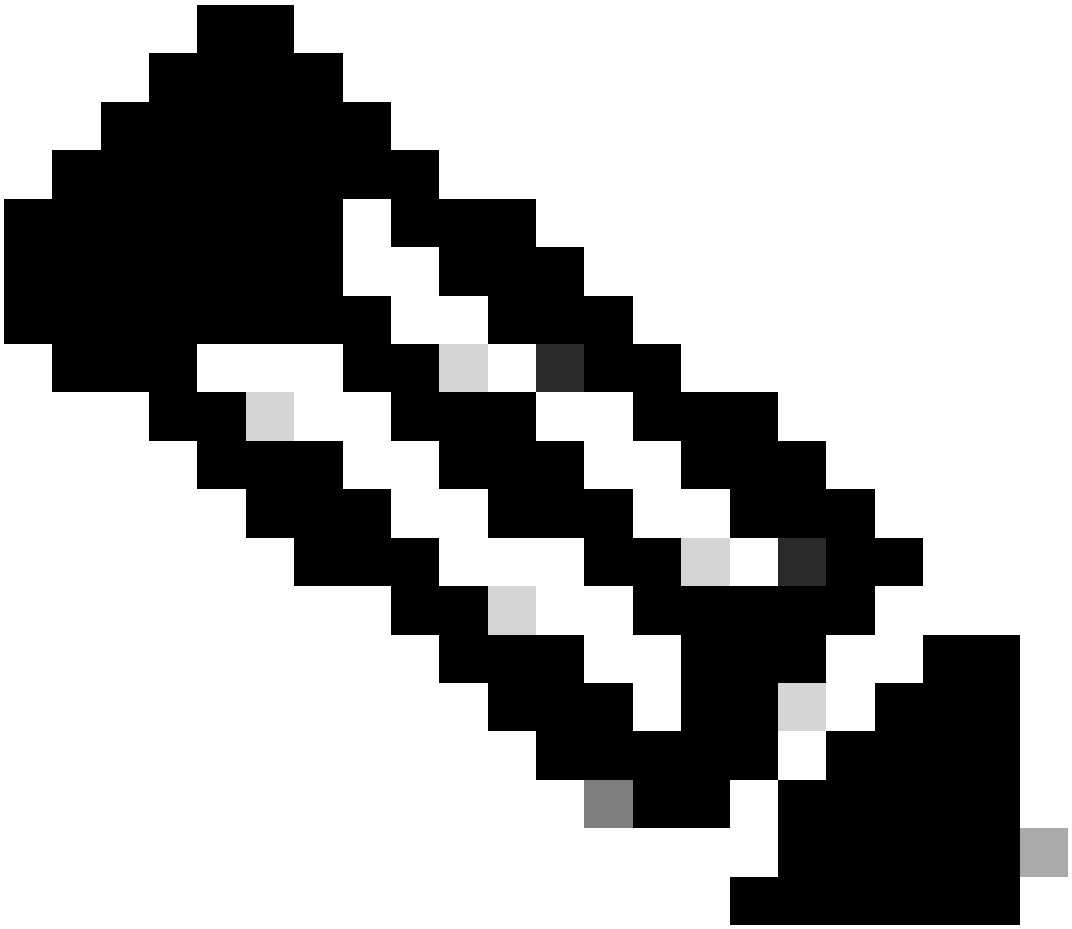
Il s'agit d'un système d'exploitation sur lequel le périphérique FTD s'exécute. En fonction des plates-formes, FXOS est utilisé pour configurer les fonctionnalités, surveiller l'état du châssis et accéder aux fonctionnalités de dépannage avancées.

FXOS sur Firepower 4100/9300 et Firepower 2100 avec le logiciel Adaptive Secure Appliance en mode plate-forme permet de modifier la configuration, alors que sur d'autres plates-formes, à l'exception de fonctionnalités spécifiques, il est en lecture seule.

## FCM : Gestionnaire de châssis Firepower

FCM est une interface utilisateur graphique utilisée pour gérer le châssis. Il est uniquement disponible pour les modèles 9300, 4100 et 2100 exécutant ASA en mode Plate-forme.

---



Remarque : vous pouvez prendre l'analogie d'un ordinateur portable. FXOS est un

---

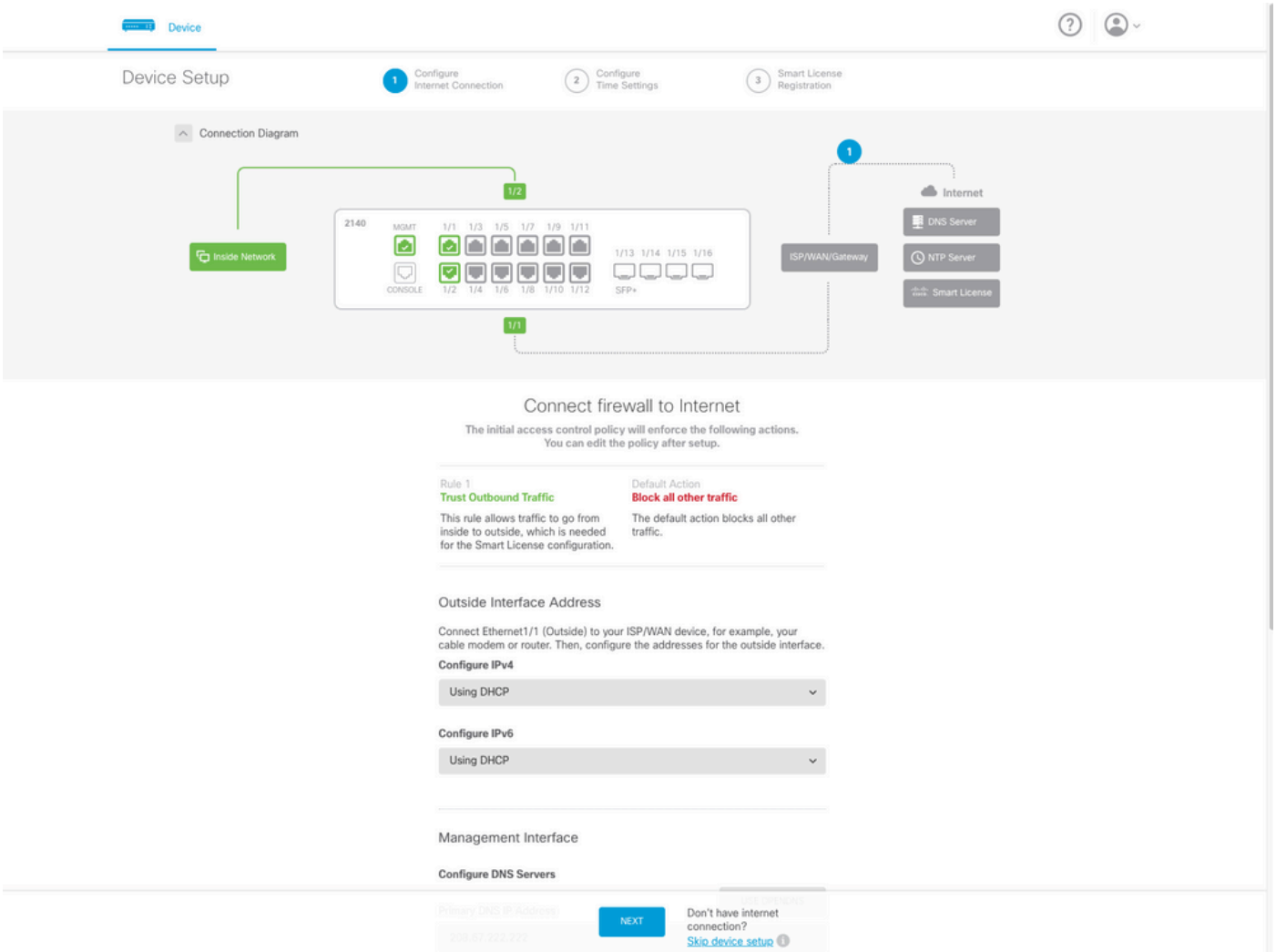
système d'exploitation (système d'exploitation Windows dans un ordinateur portable) qui fonctionne sur un châssis (ordinateur portable). Nous pouvons installer FTD (instance d'application) sur elle, qui fonctionne sur Lina et Snort (composants).

---

Contrairement à ASA, vous ne pouvez pas gérer FTD via CLI. Vous avez besoin d'une gestion séparée basée sur une interface utilisateur graphique. Il existe 2 types de services de ce type : FDM et FMC.

## FDM : gestion des périphériques Firepower

- FDM est un outil de gestion prêt à l'emploi. Il fournit une interface Web pour la configuration, la gestion et la surveillance des stratégies de sécurité et des paramètres système.
- L'un des grands avantages de l'utilisation de FDM est que vous ne disposez pas d'une licence supplémentaire pour cela.
- Vous ne pouvez gérer qu'1 FTD avec 1 FDM.



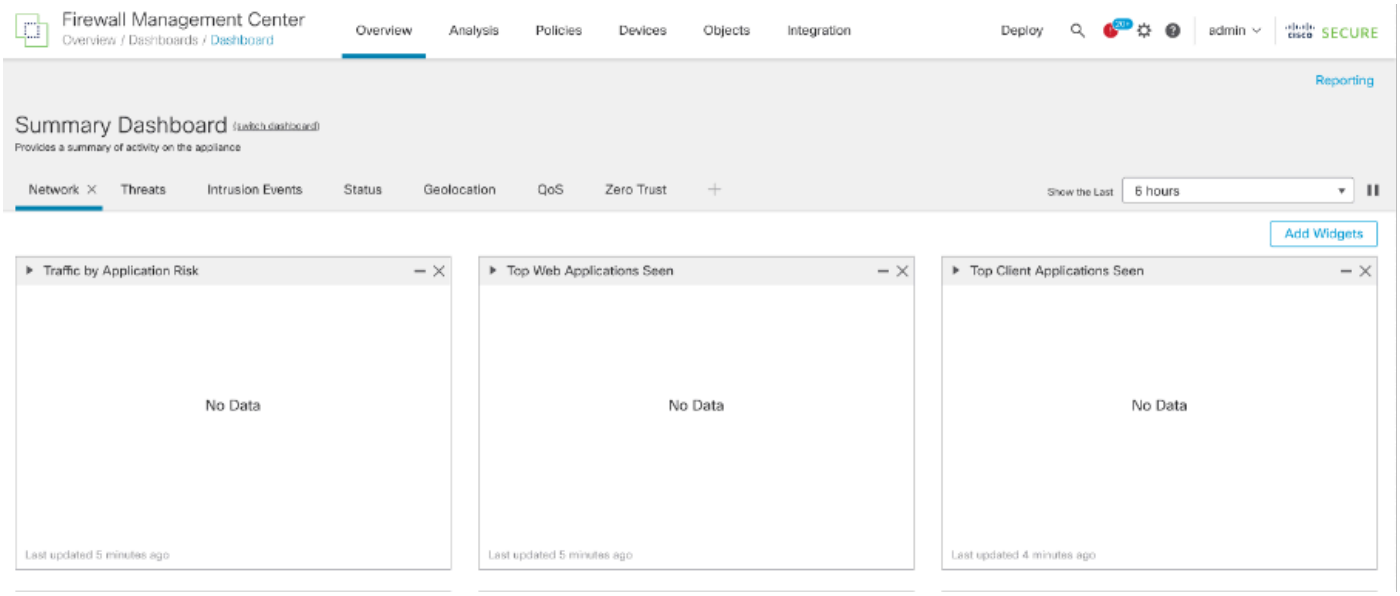

FDM

## FMC : Firepower Management Center

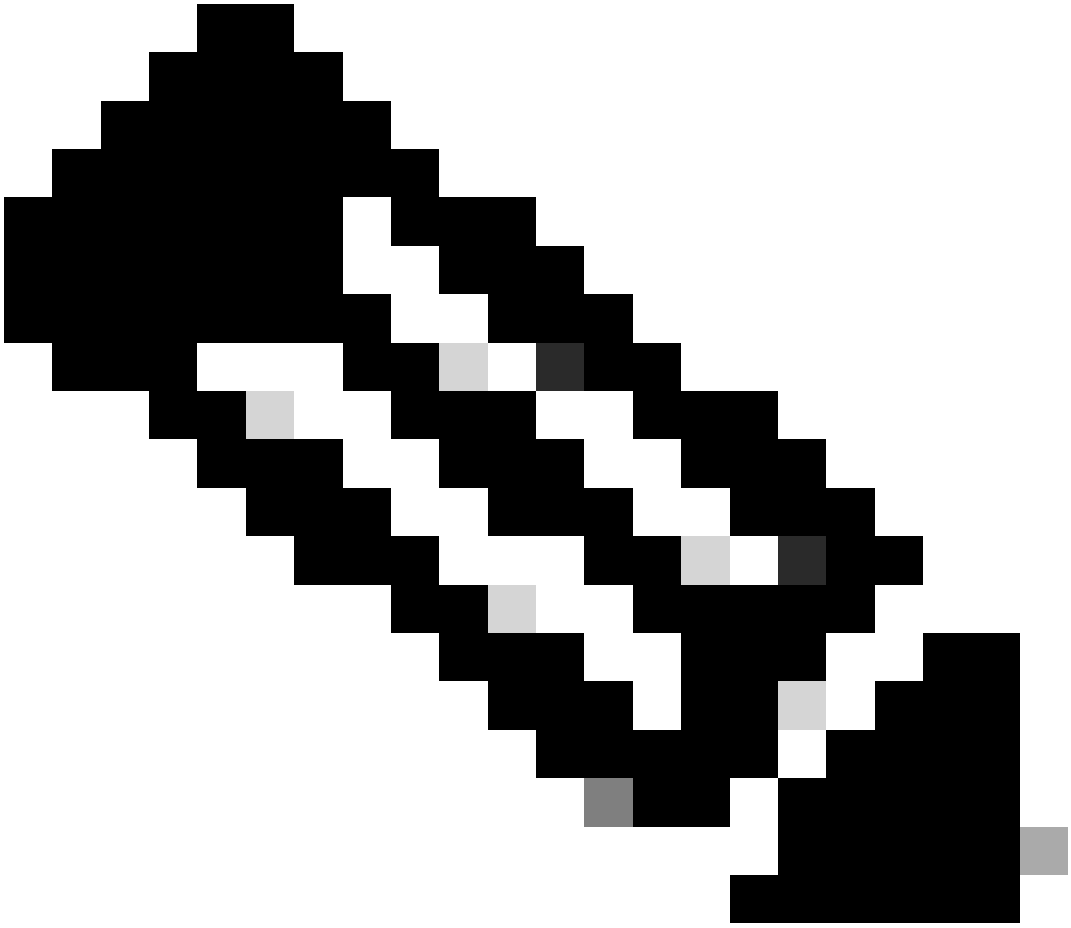
- FMC est une solution de gestion centralisée pour les périphériques Cisco FTD, les

périphériques Cisco ASA avec les services Firepower. Il vous fournit également une interface utilisateur graphique que vous pouvez utiliser pour configurer, gérer et surveiller les périphériques FTD.

- Vous pouvez utiliser un périphérique FMC matériel ou un périphérique FMC virtuel.
- Cette opération nécessite une licence distincte pour fonctionner.
- Un point positif de FMC est que vous pouvez gérer plusieurs périphériques FTD avec 1 périphérique FMC.




FMC



Remarque : vous ne pouvez pas utiliser à la fois FDM et FMC pour gérer un périphérique FTD. Une fois la gestion FDM On-Box activée, il n'est pas possible d'utiliser un FMC pour gérer le FTD, sauf si vous désactivez la gestion locale et reconfigurez la gestion pour utiliser un FMC. D'un autre côté, l'enregistrement du FTD sur un FMC désactive le service de gestion FDM On-Box sur le FTD.

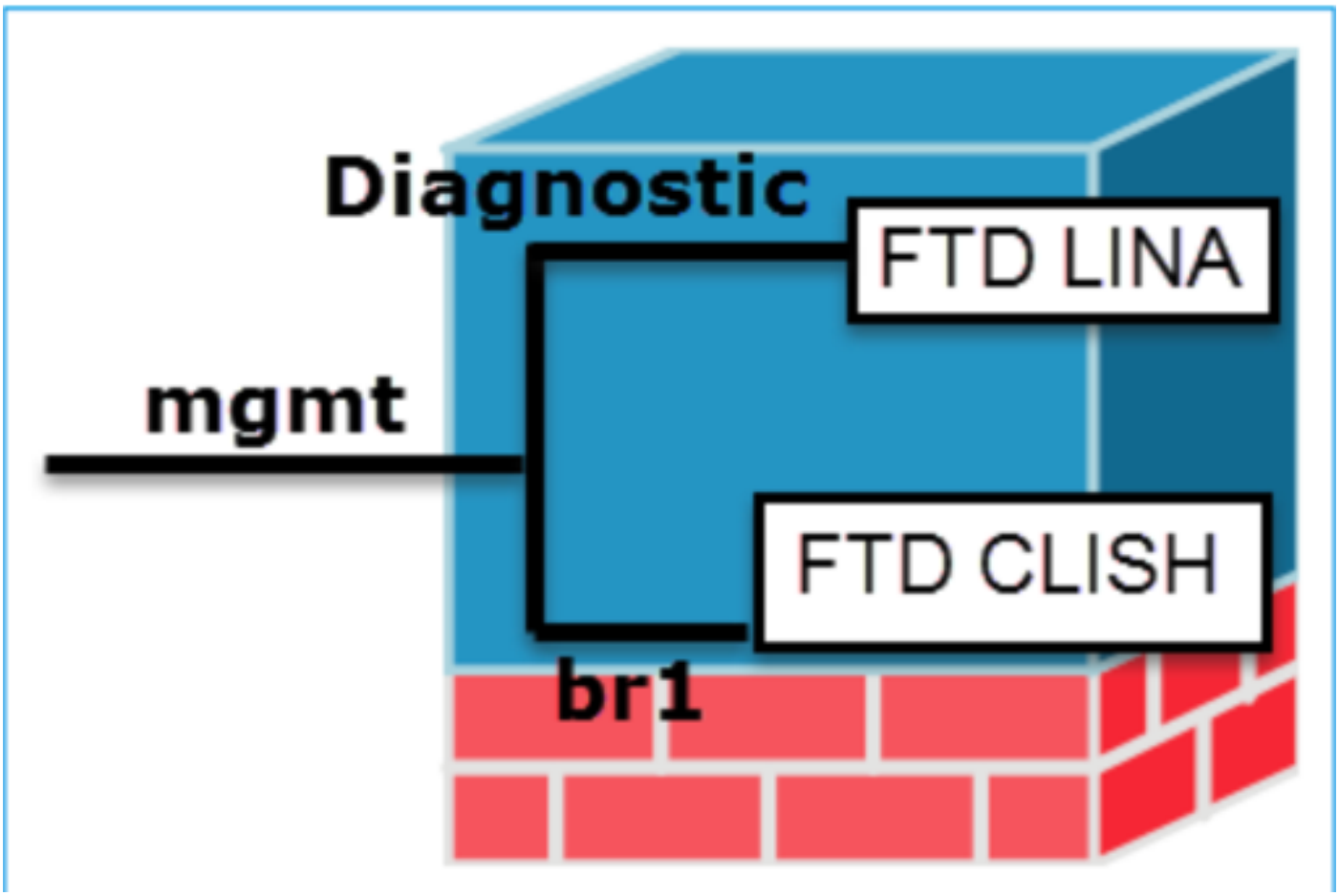
## CLISH : interface de ligne de commande Shell

CLISH est une interface de ligne de commande utilisée dans les périphériques Cisco Firepower Threat Defense (FTD). Vous pouvez exécuter des commandes sur FTD à l'aide de ce mode CLISH.

## GESTION DU DIAGNOSTIC

Nous avons 2 interfaces de gestion dans le périphérique FTD, interface de gestion de diagnostic et interface de gestion FTD. Si nous devons accéder au moteur LINA, nous utilisons une interface de gestion de diagnostic. Si nous devons accéder au moteur SNORT, nous utilisons l'interface de

gestion FTD. Les deux sont des interfaces différentes et ont besoin d'adresses IP d'interface différentes.




Interfaces de gestion

### Mode plate-forme ASA

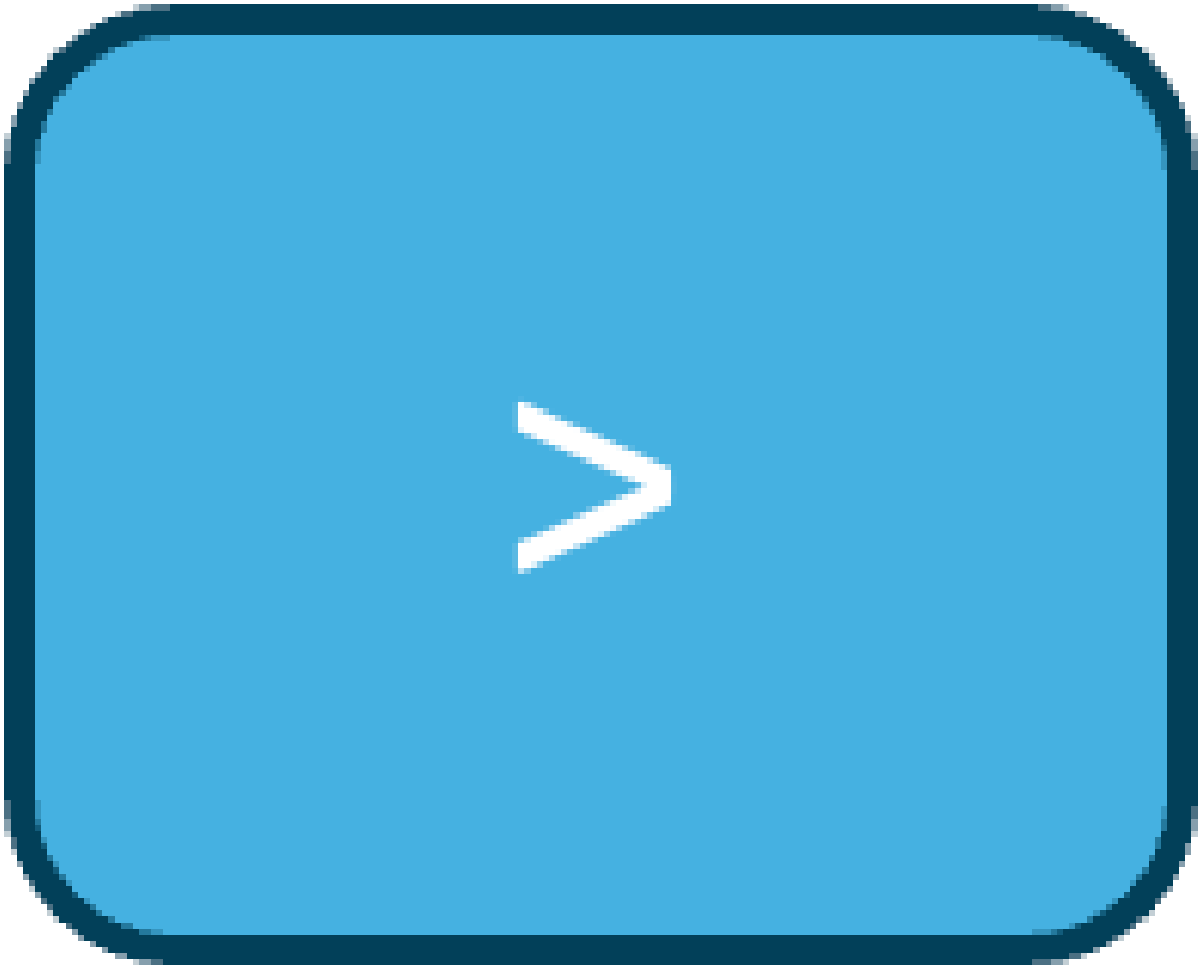
1. En mode Plate-forme, vous devez configurer les paramètres d'exploitation de base et les paramètres d'interface matérielle dans FXOS, comme l'activation des interfaces, l'établissement des EtherChannels, NTP, la gestion des images, etc.
2. Toutes les autres configurations doivent être effectuées via l'interface CLI/ASDM ASA.
3. Vous disposez d'un accès FCM dans cette section.

### Mode Appliance ASA

1. Dans Firepower 2100, ASA en mode appliance a été introduit à partir de la version 9.13 (y compris).
2. Le mode Appliance vous permet de configurer tous les paramètres de l'ASA. Seules les commandes de dépannage avancées sont disponibles à partir de l'ILC FXOS.
3. Il n'y a pas de FCM dans ce mode.

## Différentes invites sur le FTD

CONFLIT



CONFLIT

Mode racine / Mode expert

root@firepower:/home/admin#

Mode expert

Mode Lina


Mode Lina

Mode FXOS


Mode FXOS

## Comment passer d'une invite à une autre

### Mode CLISH vers mode racine FTD



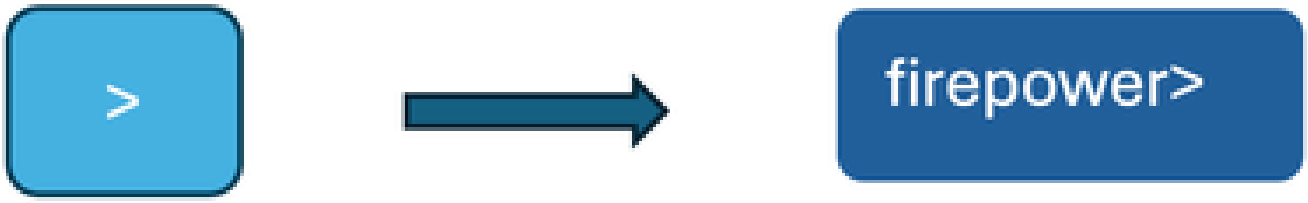


Passer du mode Écriture au mode Expert

```
> expert
```

```
admin@firepower:~$  sudo su
Password:
root@firepower:/home/admin#
```

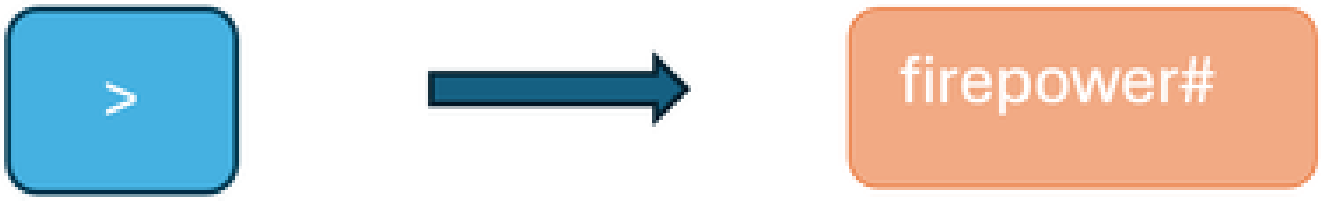
## CLISH Mode vers Lina Mode




Du mode Clish au mode Lina

```
> system support diagnostic-cli
Attaching to Diagnostic CLI . . . Press 'Ctrl+a then d' to detach .
Type help or '?' for a list of available commands .
firepower> enable
Password :
firepower#
```

## CLISH Mode vers FXOS Mode




Mode de coupure vers le mode FXOS

```
> connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.
(------ cropped output -------)
firepower#
```

## Du mode racine au mode LINA

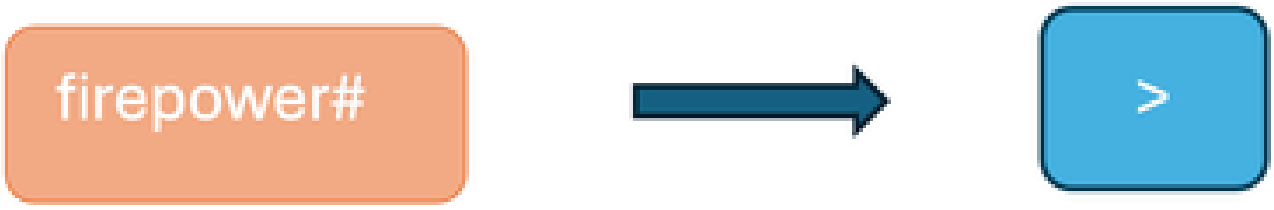

Expert en mode Lina

```
root@firepower:/home/admin#
root@firepower:/home/admin#   exit
exit
admin@firepower:~$ exit
logout
>
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower#
```

ou

```
root@firepower:/home/admin#
root@firepower:/home/admin#   sfconsole
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
firepower> en
Password:
firepower#
```

## Mode FXOS vers FTD CLISH (périphériques de la gamme 1000/2100/3100)




Mode FXOS vers Clish

```
firepower# connect ftd
>
To exit the fxos console
> exit
firepower#
```

### Mode FXOS vers FTD CLISH (périphérique de la gamme 4100/9300)

Cet exemple montre comment se connecter à l'interface de ligne de commande de défense contre les menaces du module 1 :

```
firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
CISCO Serial Over LAN:
Close Network Connection to Exit
Firepower-module1> connect ftd
>
```

Quittez la console :

Entrez ~, puis quittez pour quitter l’application Telnet.

```
Example:
>exit
Firepower-module1> ~
telnet> quit
firepower#
```

## Documents associés

Pour plus d'informations sur les différentes commandes que vous pouvez exécuter sur les périphériques firepower, veuillez vous référer à FXOS Command Reference , FTD command reference .

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.