Terminologie voor beveiligde firewall decoderen (voor mensen die nieuw zijn in FirePOWER)

Inhoud

Inleiding

Dit document beschrijft verschillende populaire Cisco-firewalljargons. Dit document beschrijft ook hoe u van de ene CLI-modus naar de andere kunt overgaan.

Voorwaarden

Vereisten

Er zijn geen vereisten vooraf om dit onderwerp te leren.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Firepower Threat Defence (FTD)
- Cisco Firepower Device Management (FDM)
- Firepower eXtensible Operating System (FXOS)
- Firepower Chassis Manager (FCM)
- Adaptieve security applicatie (ASA)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Algemeen gebruikte technische terminologie

FTD: bescherming tegen vuurkracht

FTD is een next-generation firewall die meer biedt dan traditionele firewalls. Het omvat services zoals Inbraakpreventiesysteem (IPS), Advanced Malware Protection (AMP), URL-filtering, security intelligentie enzovoort. FTD lijkt sterk op ASA (Adaptieve security applicatie), maar heeft extra functionaliteit. FTD draait op 2 motoren, LINA en SNORT.

LINA: Linux-gebaseerde geïntegreerde netwerkarchitectuur

We noemen ASA Lina in FTD-apparaten. LINA is niets anders dan een ASA code waar FTD op draait. Lina heeft zijn primaire focus op de veiligheid van de netwerklaag. Het neemt sommige Layer 7 firewallmogelijkheden door zijn toepassingsinspectie en controleeigenschappen op.

SNORT

Snortmotor is een inbraakdetectiesysteem voor het netwerk. De belangrijkste functies van snort omvatten Packet Inspection om afwijkingen daarin te identificeren, op regels gebaseerde detectie, realtime meldingen, vastlegging en analyse en integratie met andere security tools. Snort heeft de mogelijkheid om L7-inspectie uit te voeren (Application Layer Traffic), niet alleen op basis van een pakketheader maar ook op basis van de inhoud van de pakketten.

U krijgt de flexibiliteit om uw eigen douaneregels te schrijven om specifieke patronen of handtekeningen op toepassingslaag te bepalen, die de opsporingsmogelijkheden verbetert. Het doet diepe pakketinspectie door de payload van de pakketten te evalueren. U kunt hier zelfs de decryptie van de versleutelde pakketten uitvoeren.

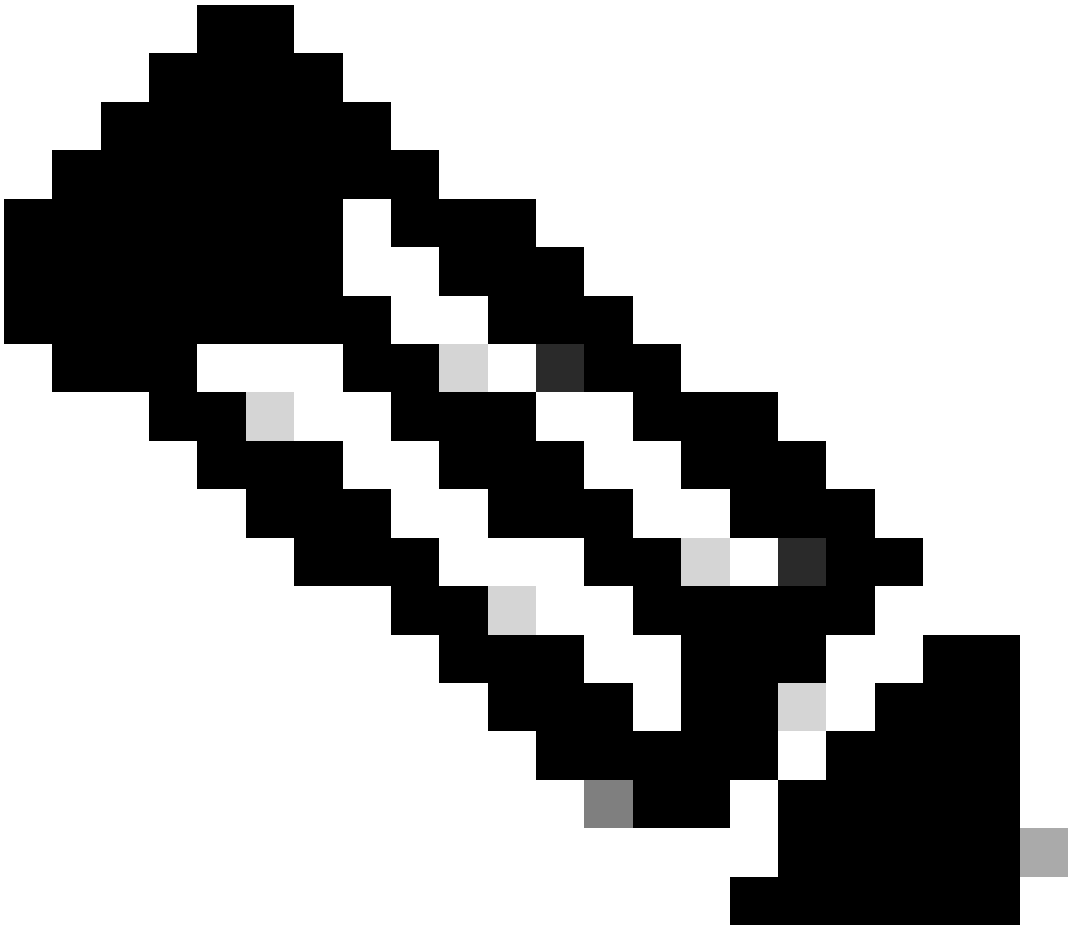
FXOS: uitbreidbaar besturingssysteem met FirePOWER

Het is een besturingssysteem waarop het FTD-apparaat draait. Afhankelijk van de platforms wordt FXOS gebruikt om functies te configureren, de status van het chassis te bewaken en toegang te krijgen tot geavanceerde functies voor probleemoplossing.

FXOS op Firepower 4100/9300 en Firepower 2100 met de Adaptive Secure Appliance software in platformmodus staan wijzigingen in de configuratie toe, terwijl in andere platforms met uitzondering van specifieke functies het alleen wordt gelezen.

FCM: Firepower Chassis Manager

FCM is een GUI die wordt gebruikt om Chassis te beheren. Het is alleen beschikbaar voor de 9300, 4100, 2100 actieve ASA in de platformmodus.

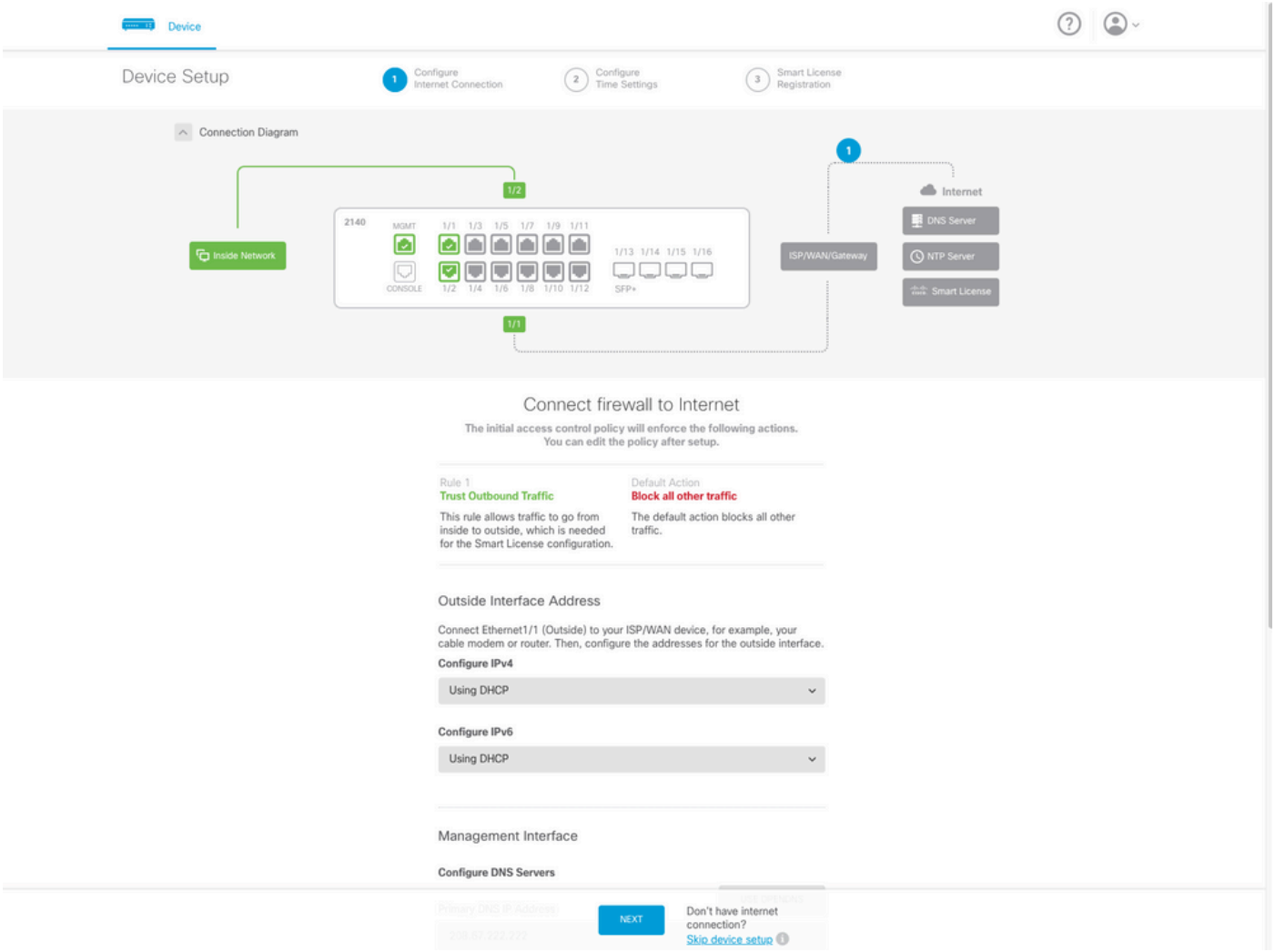


> Opmerking: je kan een analogie nemen van een laptop. FXOS is Besturingssysteem (Windows OS in laptop), dat draait op chassis (laptop). We kunnen FTD (applicatie instantie) op het installeren, die draait op Lina en Snort (componenten).

In tegenstelling tot ASA, kunt u FTD niet via CLI beheren. U hebt een afzonderlijk op GUI gebaseerd beheer nodig. Er bestaan 2 soorten van dergelijke diensten: FDM en FMC.

FDM: beheer van FirePOWER-apparaten

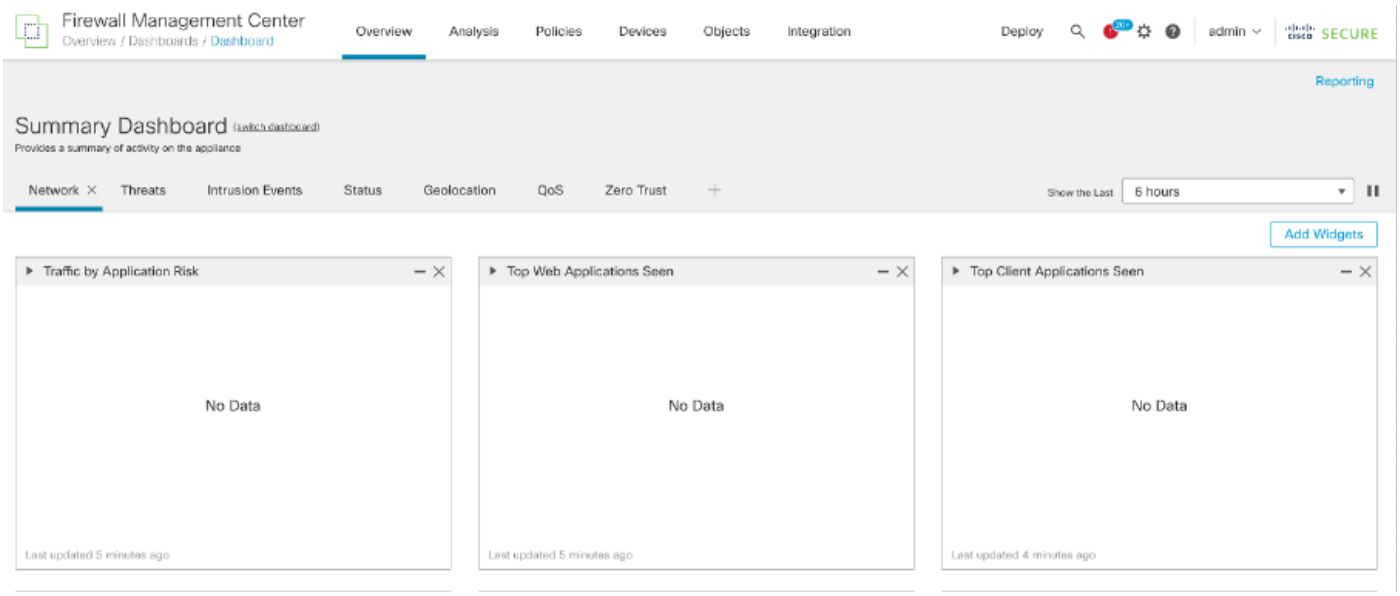
- FDM is een on-box beheerprogramma. Het biedt een webgebaseerde interface voor het configureren, beheren en bewaken van beveiligingsbeleid en systeeminstellingen.
- Een groot voordeel van het gebruik van FDM is dat je hiervoor geen extra licentie hebt.
- U kunt slechts 1 FTD beheren met 1 FDM.



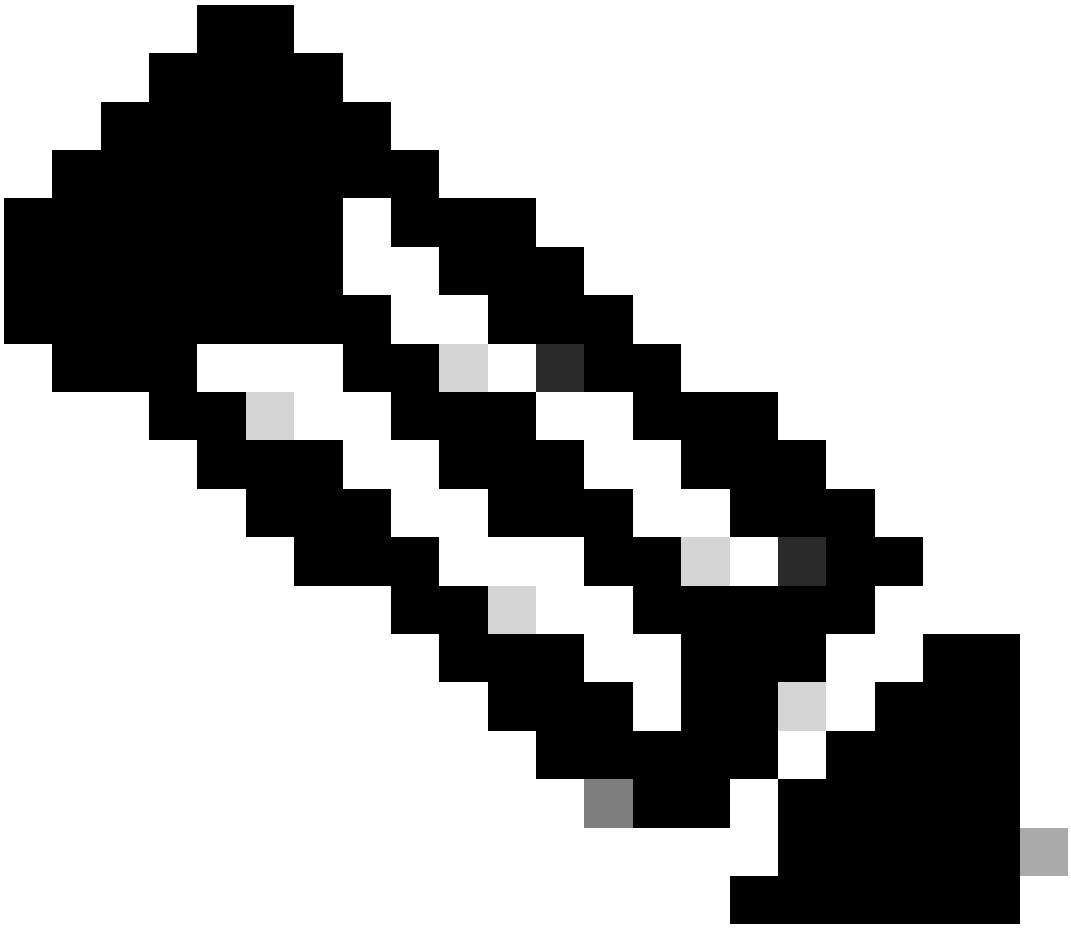
FDM

FMC: Firepower Management Center

- FMC is een gecentraliseerde beheeroplossing voor Cisco FTD-apparaten, Cisco ASA-apparaten met FirePOWER Services. Het biedt u ook GUI die u kunt gebruiken om FTD-apparaten te configureren, beheren en bewaken.
- U kunt een hardware-FMC-apparaat of een virtueel FMC-apparaat gebruiken.
- Hiervoor is een afzonderlijke licentie vereist.
- Een pluspunt van FMC is dat u meerdere FTD-apparaten kunt beheren met 1 FMC-apparaat.



VCC



Opmerking: u kunt het FDM en FMC niet gebruiken om een FTD-apparaat te beheren. Zodra het FDM On-Box-beheer is ingeschakeld, is het niet mogelijk een FMC te gebruiken

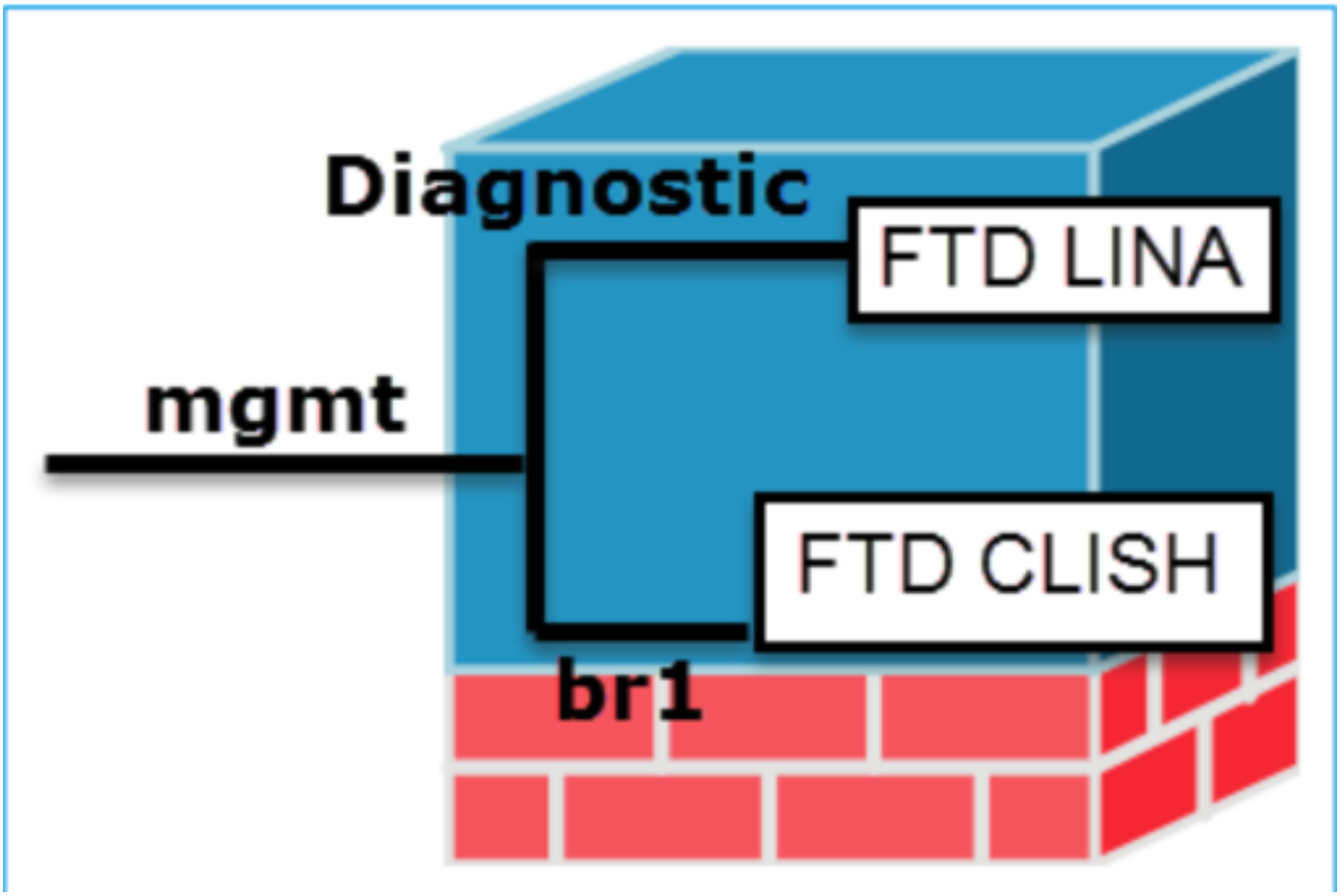
om het FTD te beheren, tenzij u het lokale beheer uitschakelt en het beheer herconfigureert om een FMC te gebruiken. Aan de andere kant schakelt registratie van het FTD bij een FMC de FDM On-Box-managementservice op het FTD uit.

CLISH: Opdrachtlijn-interfacekaart

CLISH is een opdrachtregelinterface die wordt gebruikt in Cisco Firepower Threat Defence (FTD)-apparaten. U kunt opdrachten op FTD uitvoeren in deze CLISH-modus.

DIAGNOSTISCH BEHEER

We hebben 2 managementinterfaces in FTD-apparaat, Diagnostic management interface en FTD management interface. Als we toegang moeten krijgen tot de LINA-motor, gebruiken we een diagnostische managementinterface. Als we toegang moeten krijgen tot SNORT engine, gebruiken we FTD management interface. Beiden zijn verschillende interfaces en hebben verschillende interface-IP-adressen nodig.



Beheerinterfaces

ASA platform modus

1. Wanneer op de wijze van het Platform, moet u fundamentele werkende parameters en hardware interfaceinstellingen in FXOS als het toelaten van interfaces, het vestigen van

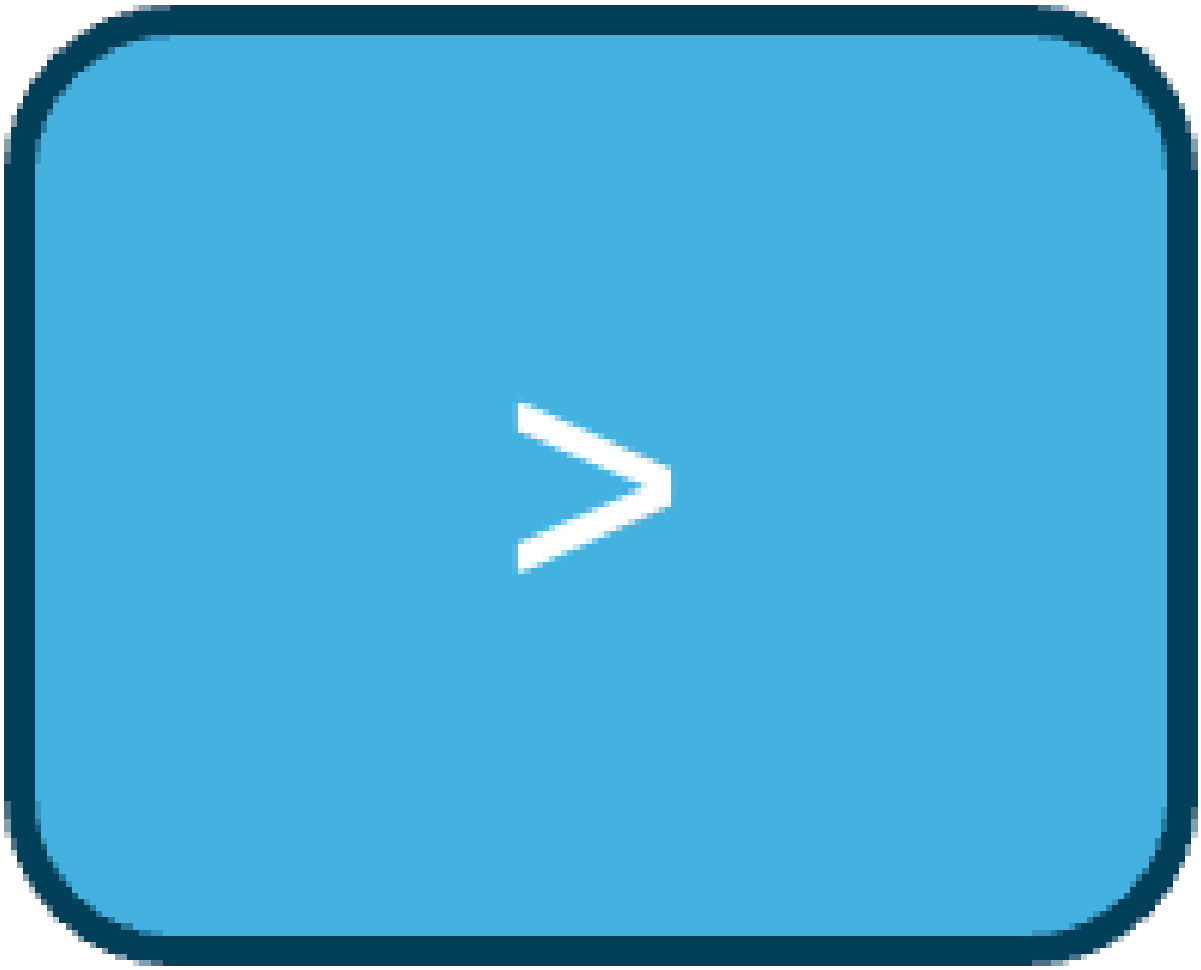
EtherChannel, NTP, beeldbeheer, en meer configureren.
2. Alle andere configuraties moeten worden uitgevoerd via ASA CLI/ASDM.
3. Je hebt FCM toegang in deze.

ASA applicatie Mode

1. In FirePOWER 2100 werd ASA in apparaatmodus vanaf 9.13(inclusief) geïntroduceerd.
2. In de applicatiemodus kunt u alle instellingen in de ASA configureren. Er zijn alleen geavanceerde opdrachten voor probleemoplossing beschikbaar in de FXOS CLI.
3. Er is geen FCM in deze modus.

Verschillende aanwijzingen voor FTD

KLIMMEN



KLIMMEN

Root Mode / Expert Mode

Expert-modus

Lina Mode

Lina Mode

FXOS-modus

FXOS-modus

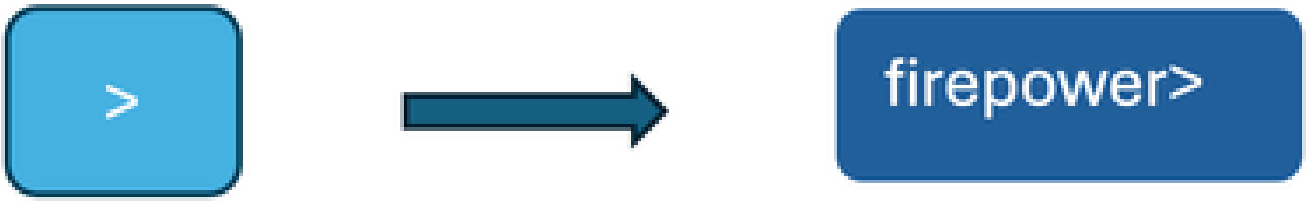
Hoe te tussen verschillende herinneringen te bewegen

CLISH-modus naar FTD Root Mode

Modus voor taal naar expertmodus

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

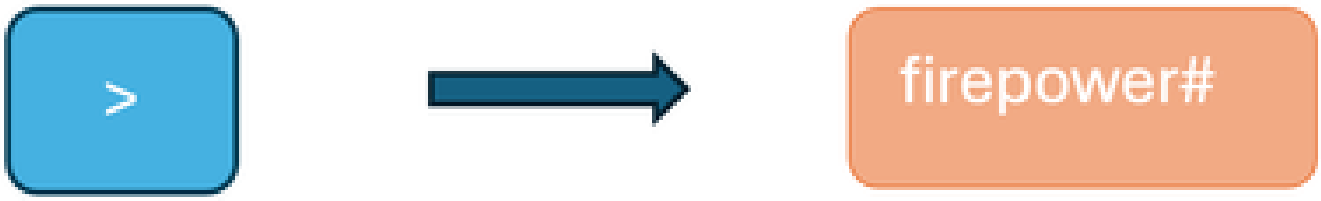
CLISH-modus naar Lina-modus



Klinkmodus naar lijnmodus

```
> 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-modus naar FXOS-modus



Modus voor taal naar FXOS-modus

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

Root Mode in op LINA Mode

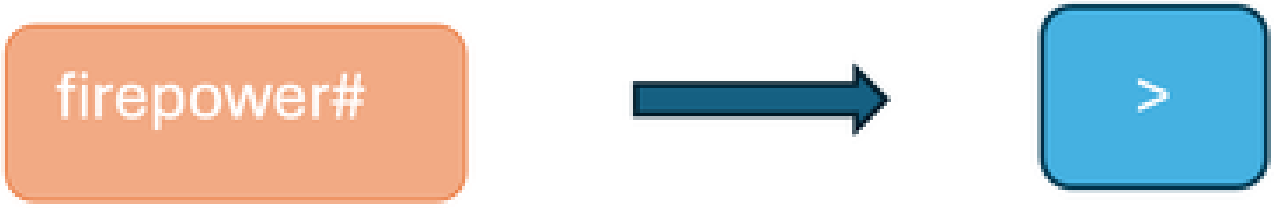
Expert naar Lina Mode

```
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#
```

of

```
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#
```

FXOS naar FTD CLISH-modus (1000/2100/3100 Series apparaat)



FXOS naar Clish-modus

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

FXOS naar FTD CLISH-modus (4100/9300 Series apparaat)

Dit voorbeeld laat zien hoe u verbinding kunt maken met de bedreigingsverdediging CLI op 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
>
```

Sluit de console:

Voer ~in en stop vervolgens om de Telnet-toepassing te beëindigen.

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

Verwante documenten

Voor meer informatie over verschillende opdrachten die u kunt uitvoeren op FirePOWER devices, raadpleegt u FXOS Command Reference , FTD Command Reference .

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.