Decodifica terminologia firewall sicuro (per utenti nuovi di Firepower)

Sommario

Introduzione

Questo documento descrive diversi gerghi popolari di Cisco Firewall. Nel documento viene spiegato anche come passare da una modalità CLI a un'altra.

Prerequisiti

Requisiti

Non ci sono precedenti requisiti per imparare questo argomento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Firepower Threat Defense (FTD)
- Cisco Firepower Device Management (FDM)
- Firepower eXtensible Operating System (FXOS)
- Firepower Chassis Manager (FCM)
- ASA (Adaptive Security Appliance)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Terminologie tecniche di uso comune

FTD: Firepower Threat Defense

FTD è un firewall di nuova generazione che offre molto di più rispetto ai firewall tradizionali. Include servizi come Intrusion Prevention System (IPS), Advanced Malware Protection (AMP), filtro URL, Security Intelligence e così via. L'FTD è molto simile all'ASA (Adaptive Security Appliance), ma con funzionalità aggiuntive. FTD funziona su 2 motori, LINA e SNORT.

LINA: architettura di rete integrata basata su Linux

Nei dispositivi FTD, l'ASA è chiamata Lina. LINA non è altro che un codice ASA su cui viene eseguito il FTD. Lina ha come obiettivo principale la sicurezza a livello di rete. Incorpora alcune funzionalità del firewall di layer 7 tramite le funzionalità di controllo e ispezione delle applicazioni.

SNORT

Motore di snort è un sistema di rilevamento e prevenzione delle intrusioni nella rete. Le caratteristiche principali di snort includono l'ispezione dei pacchetti per identificare le anomalie, il rilevamento basato su regole, gli avvisi in tempo reale, la registrazione e l'analisi e l'integrazione con altri strumenti di sicurezza. Snort ha la capacità di eseguire l'ispezione L7 (traffico a livello di applicazione), non solo sulla base di un'intestazione di pacchetto ma anche sul contenuto dei pacchetti.

È possibile scrivere regole personalizzate per definire modelli o firme specifiche a livello dell'applicazione, migliorando così le funzionalità di rilevamento. Esegue un'ispezione approfondita dei pacchetti valutando il payload dei pacchetti. In questo caso, è possibile anche eseguire la decrittografia dei pacchetti crittografati.

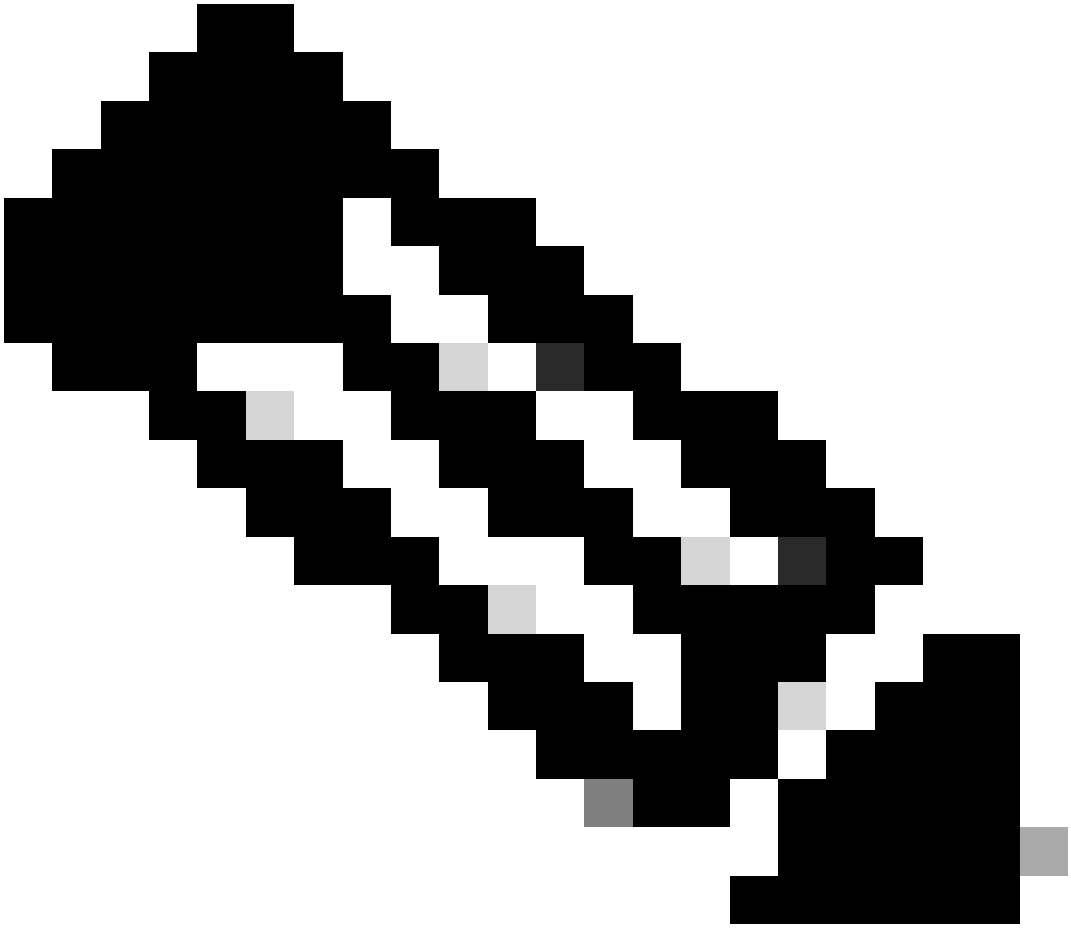
FXOS: sistema operativo estendibile Firepower

È un sistema operativo su cui viene eseguito il dispositivo FTD. A seconda delle piattaforme, FXOS viene usato per configurare le funzionalità, monitorare lo stato dello chassis e accedere alle funzionalità avanzate di risoluzione dei problemi.

FXOS su Firepower 4100/9300 e Firepower 2100 con il software Adaptive Secure Appliance in modalità piattaforma consentono modifiche alla configurazione, mentre in altre piattaforme, ad eccezione di funzionalità specifiche, è di sola lettura.

FCM: Firepower Chassis Manager

FCM è un'interfaccia grafica utilizzata per la gestione dello chassis. È disponibile solo per gli switch 9300, 4100 e 2100 con ASA in modalità piattaforma.



> Nota: potete fare un'analogia con un laptop. FXOS è un sistema operativo (sistema operativo Windows nel notebook), che funziona su chassis (laptop). Possiamo installare FTD (istanza dell'applicazione) su di esso, che viene eseguito su Lina e Snort

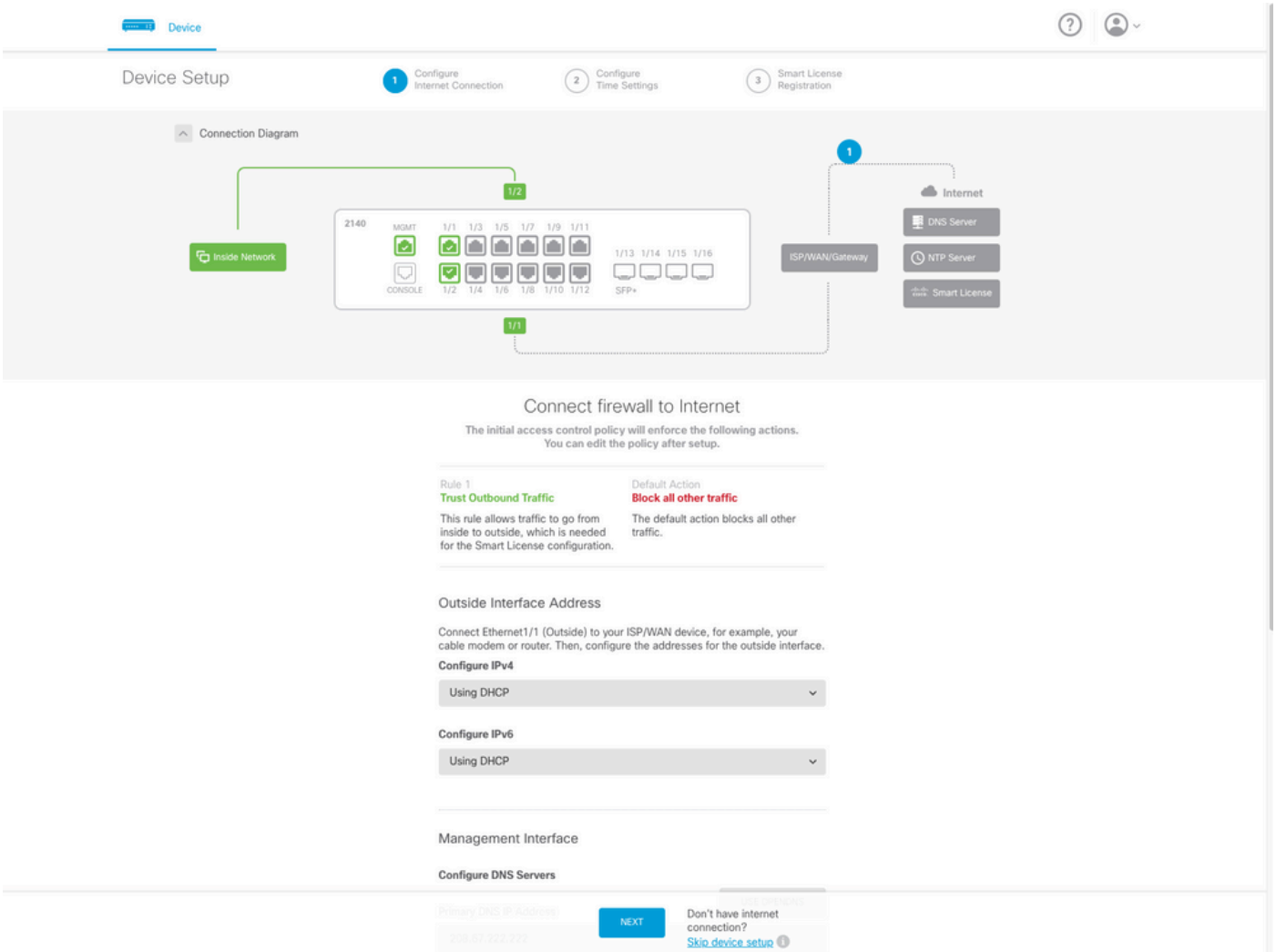
---

(componenti).

A differenza dell'ASA, non è possibile gestire l'FTD tramite la CLI. È necessaria una gestione basata su GUI separata. Esistono due tipi di servizi: FDM e FMC.

FDM: Firepower Device Management

- FDM è uno strumento di gestione integrato. Fornisce un'interfaccia basata su Web per la configurazione, la gestione e il monitoraggio dei criteri di sicurezza e delle impostazioni di sistema.
- Uno dei grandi vantaggi dell'utilizzo di FDM consiste nel fatto che non si dispone di una licenza aggiuntiva per questo prodotto.
- È possibile gestire solo 1 FTD con 1 FDM.

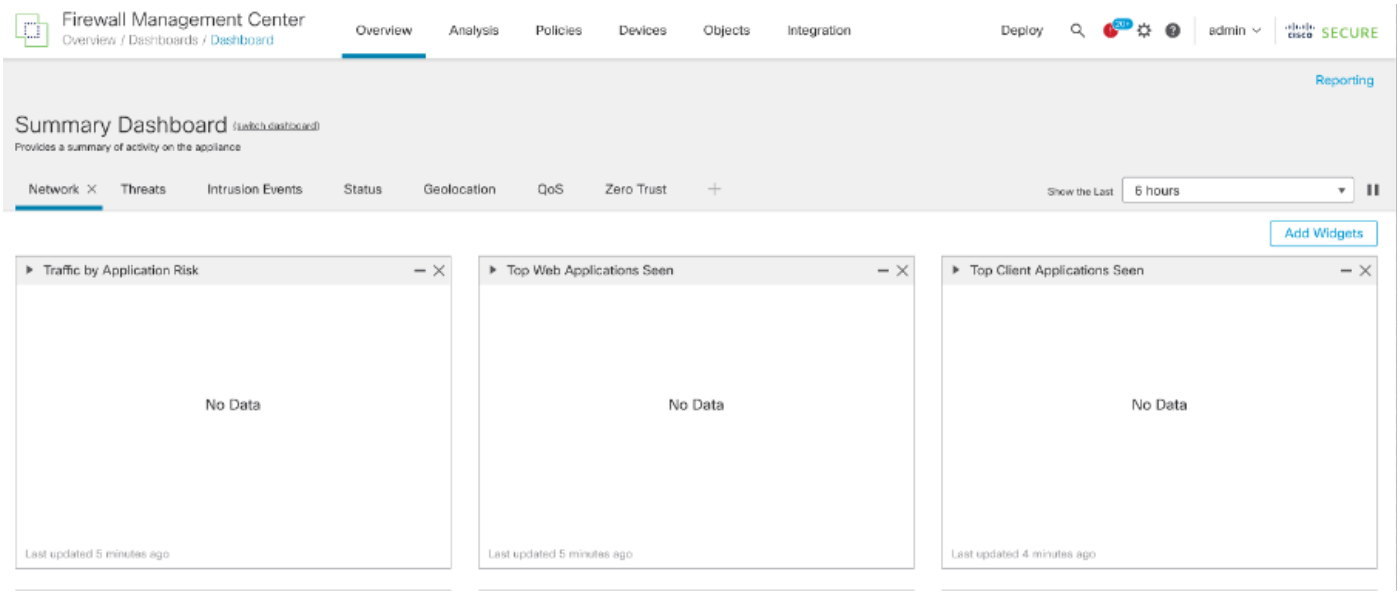


FDM

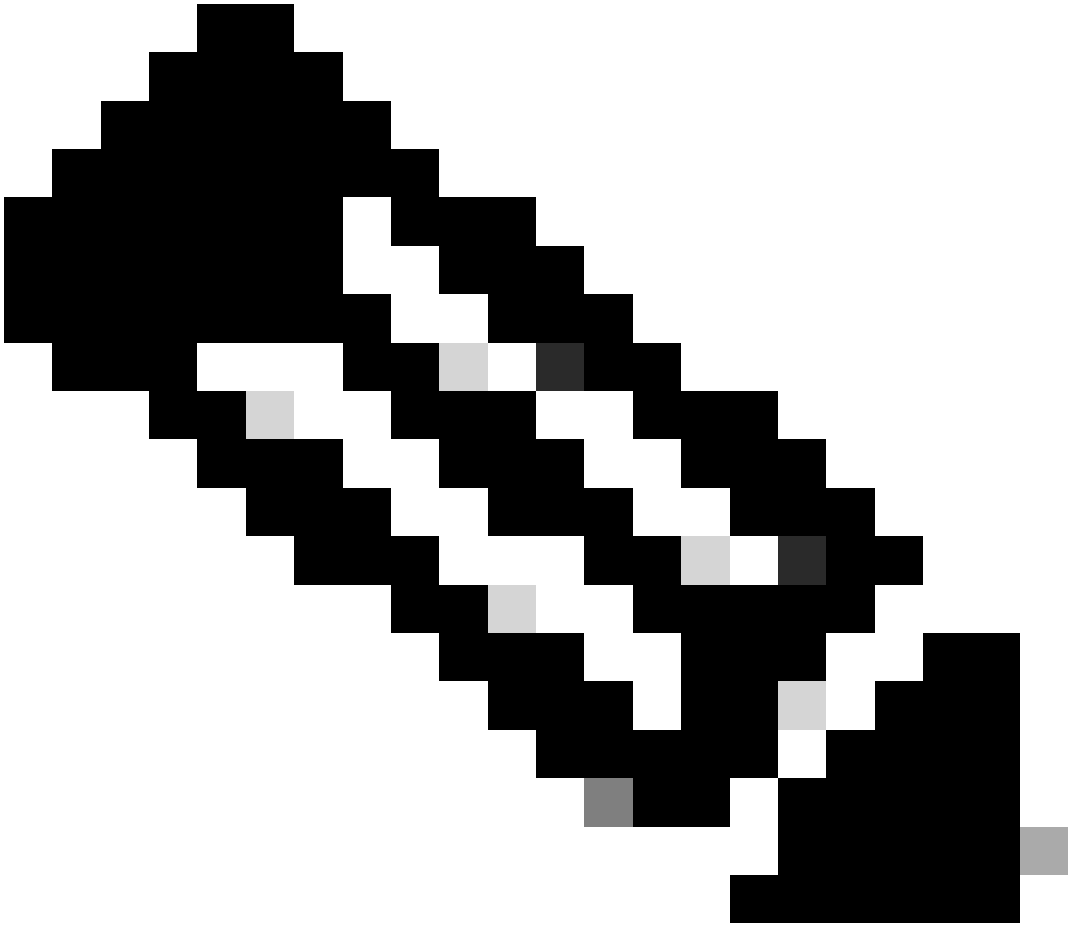
FMC: Firepower Management Center

- FMC è una soluzione di gestione centralizzata per dispositivi Cisco FTD e dispositivi Cisco ASA con servizi Firepower. Fornisce anche una GUI che può essere utilizzata per configurare, gestire e monitorare i dispositivi FTD.

- È possibile utilizzare un dispositivo FMC hardware o un dispositivo FMC virtuale.
- Per il funzionamento di questa funzionalità è necessaria una licenza separata.
- Un punto in più di FMC è che è possibile gestire più dispositivi FTD con 1 dispositivo FMC.



CCP



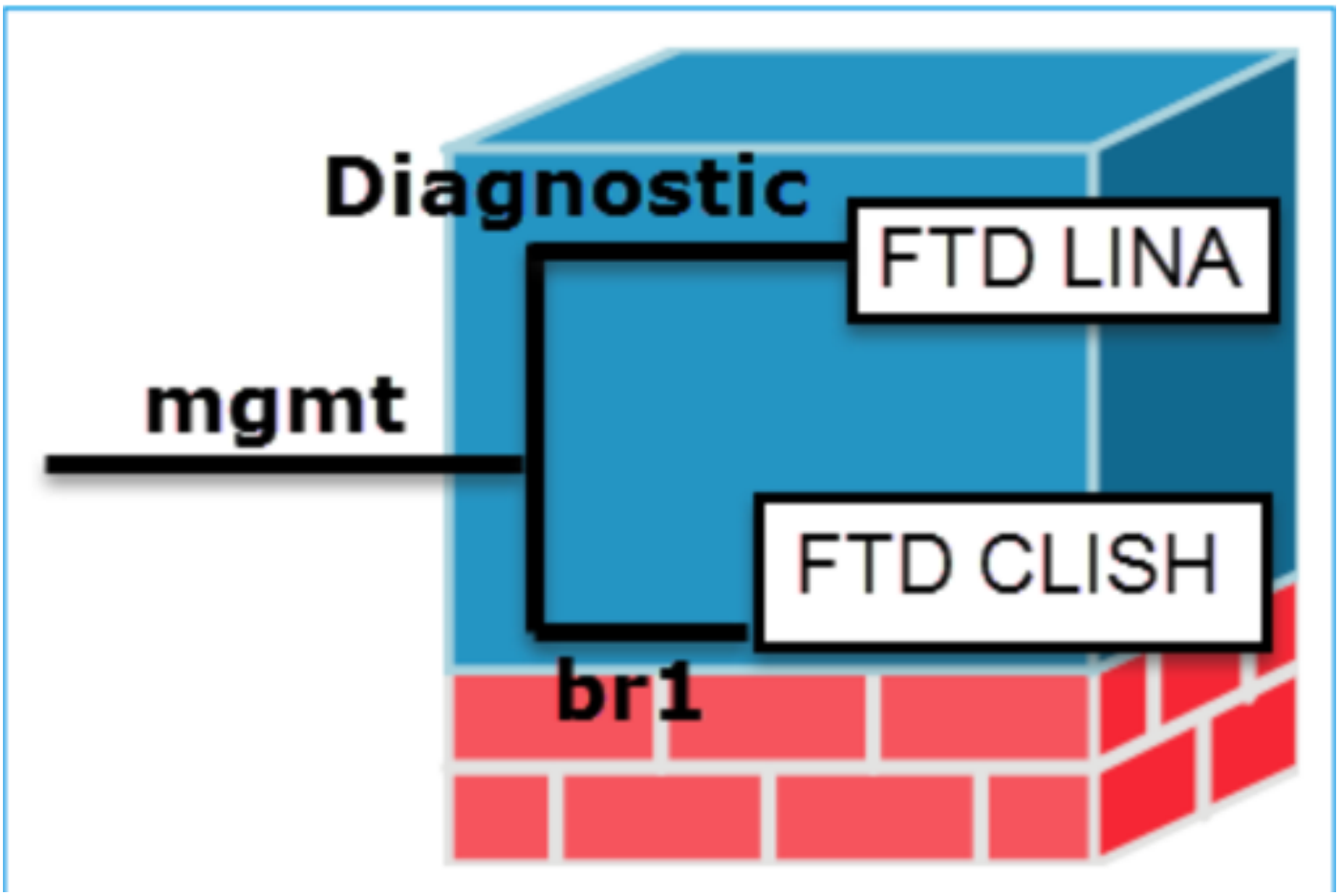
Nota: non è possibile utilizzare sia FDM che FMC per gestire un dispositivo FTD. Dopo aver attivato la gestione integrata di FDM, non è possibile utilizzare un CCP per gestire l'FTD, a meno che non si disattivi la gestione locale e non si riconfiguri la gestione per l'utilizzo di un CCP. D'altra parte, registrare l'FTD su un FMC disabilita il servizio di gestione FDM On-Box sull'FTD.

CLISH: shell interfaccia riga di comando

CLISH è un'interfaccia della riga di comando utilizzata nei dispositivi Cisco Firepower Threat Defense (FTD). Questa modalità CLISH consente di eseguire comandi su FTD.

GESTIONE DIAGNOSTICA

Abbiamo 2 interfacce di gestione nel dispositivo FTD, interfaccia di gestione diagnostica e interfaccia di gestione FTD. Se dobbiamo accedere al motore LINA, usiamo l'interfaccia di gestione diagnostica. Se dobbiamo accedere al motore SNORT, utilizziamo l'interfaccia di gestione FTD. Entrambe sono interfacce diverse e richiedono indirizzi IP di interfaccia diversi.



Interfacce di gestione

Modalità piattaforma ASA

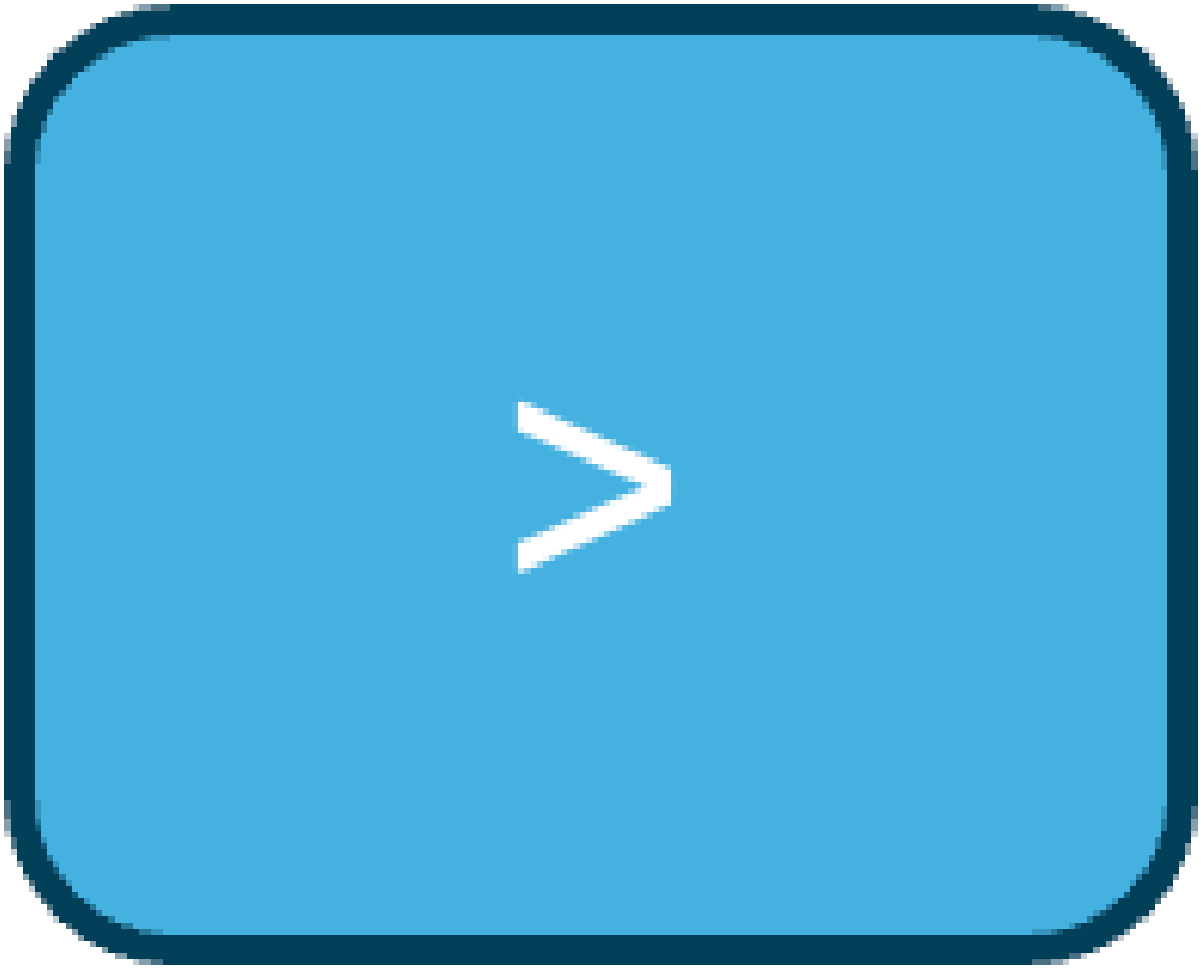
1. In modalità Piattaforma, è necessario configurare i parametri operativi di base e le impostazioni dell'interfaccia hardware in FXOS, ad esempio abilitando le interfacce, stabilendo EtherChannel, NTP, gestione delle immagini e altro ancora.
2. Tutte le altre configurazioni devono essere eseguite tramite ASA CLI / ASDM.
3. In questa cartella è disponibile l'accesso FCM.

Modalità appliance ASA

1. In Firepower 2100, l'appliance ASA in modalità appliance è stata introdotta a partire dalla versione 9.13(inclusa).
2. La modalità Appliance consente di configurare tutte le impostazioni nell'appliance ASA. Dalla CLI di FXOS sono disponibili solo comandi avanzati per la risoluzione dei problemi.
3. Nessun FCM in questa modalità.

Prompt diversi su FTD

CLISH



CLISH

Modalità principale / Modalità avanzata

Modalità Expert

Modalità Lina

Modalità Lina

Modalità FXOS

Modalità FXOS

Come spostarsi tra prompt diversi

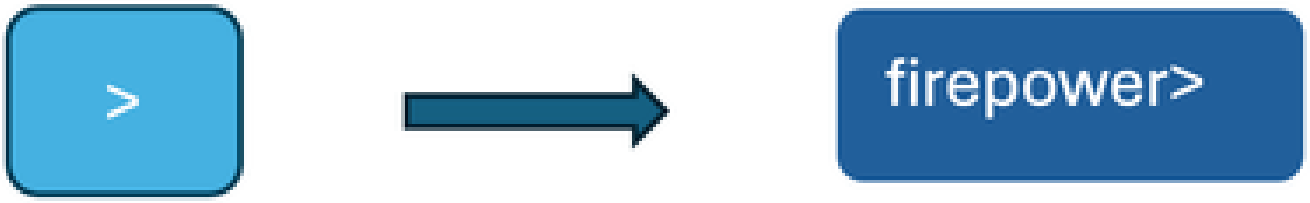
Da modalità CLISH a modalità radice FTD

Chiusura della modalità da Modalità avanzata a Modalità avanzata

```
> expert
```

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

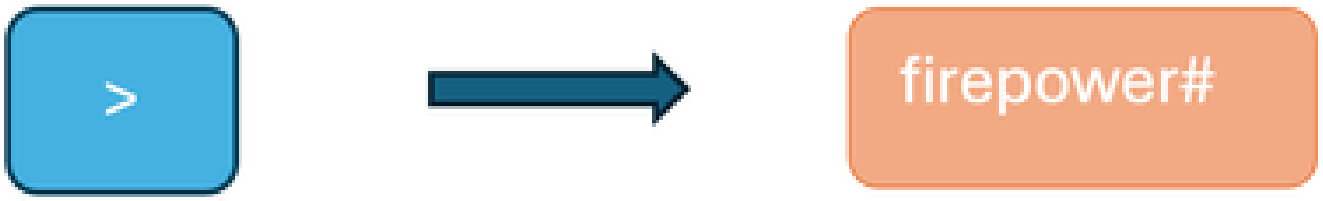
Da modalità CLISH a modalità Lina



Clish Mode (Modalità chiusura) su Lina Mode (Modalità linea)

```
> 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#
```

Da modalità CLISH a modalità FXOS



Clish Mode to FXOS mode (Chiudi modalità a FXOS)

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

Da modalità principale a modalità LINA

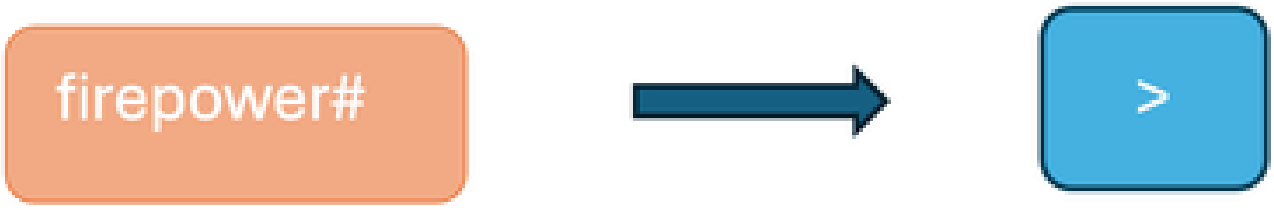
Modalità Lina avanzata

```
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#
```

o

```
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#
```

Modalità FXOS to FTD CLISH (dispositivo serie 1000/2100/3100)



Modalità FXOS to Clish

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

Modalità FXOS to FTD CLISH (dispositivo serie 4100/390)

L'esempio mostra come connettersi alla CLI di difesa dalle minacce sul modulo 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
>
```

Uscire dalla console:

Immettere ~, quindi uscire dall'applicazione Telnet.

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

Documenti correlati

Per ulteriori informazioni sui vari comandi che è possibile eseguire sui dispositivi firepower, consultare la guida di riferimento dei comandi FXOS e la guida di riferimento dei comandi FTD.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).