

Configurazione del servizio di gestione integrata di FDM per Firepower 2100

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Verifica](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare il servizio On-Box di Firepower Device Management (FDM) per la serie 2100 con FTD installato.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Firepower 2100, installazione del software FTD.
- Configurazione di base e risoluzione dei problemi di Cisco FTD (Firepower Threat Defense).

Componenti usati

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

- Cisco Firepower serie 2100.
- Cisco FTD versione 6.2.3

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.

Premesse

Lo scopo principale di questo documento è di guidare l'utente attraverso i passaggi necessari per abilitare la gestione On-Box di FDM per la serie firepower 2100.

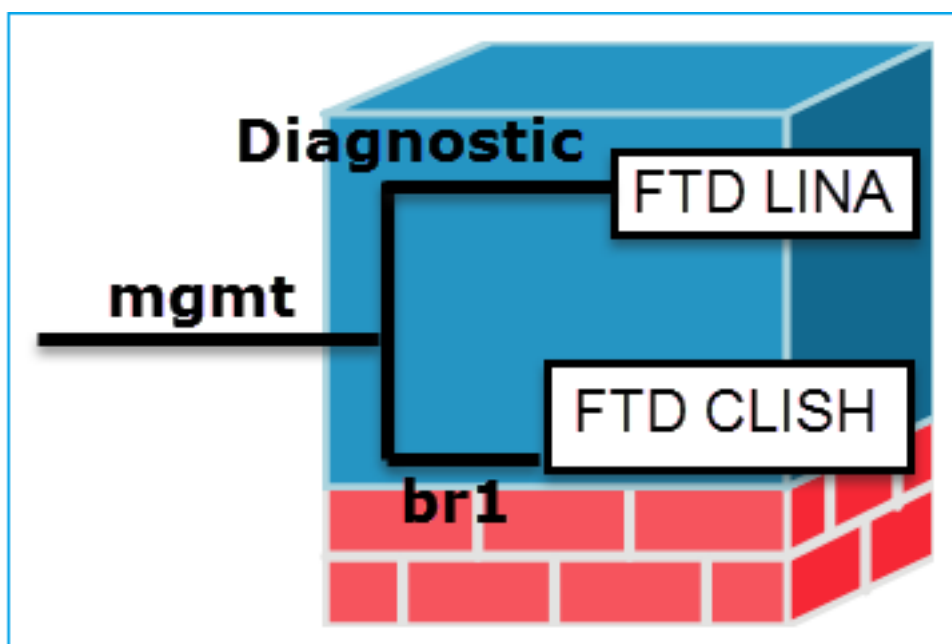
Per gestire Firepower Threat Defense (FTD) installato su un Firepower 2100 sono disponibili due opzioni:

- Gestione integrata di FDM.
- Cisco FMC (Firepower Management Center).

Nota: non è possibile utilizzare sia FDM che FMC per gestire un FTD installato in un Firepower 2100. Dopo aver attivato la gestione integrata di FDM sul FTD firepower 2100, non è possibile utilizzare un FMC per gestire l'FTD, a meno che non si disattivi la gestione locale e si riconfiguri la gestione per utilizzare un FMC. D'altra parte, registrare l'FTD su un FMC disabilita il servizio di gestione FDM On-Box sull'FTD.

Attenzione: al momento Cisco non dispone di alcuna opzione per eseguire la migrazione della configurazione di Firepower per FDM a un FMC e viceversa, tenerne conto quando si sceglie il tipo di gestione che si configura per FTD installato in Firepower 2100.

L'interfaccia di gestione è divisa in due interfacce logiche, br1 (management0 sugli accessori FPR2100/4100/9300) e diagnostica:



Gestione - br1/management0

- Questa interfaccia viene usata per assegnare l'indirizzo IP FTD usato per la comunicazione FTD/FMC.
- Termina il tunnel tra FMC/FTD.
- Utilizzato come origine per i syslog basati su regole.
- Fornisce accesso SSH e HTTPS alla casella FTD.

Scopo

Obbligatorio

Sì, in quanto viene utilizzato per la comunicazione FTD/FMC (il tunnel sftunnel termina su di esso).

Gestione -Diagnostica

- Fornisce accesso remoto (ad esempio SNMP) al motore ASA.
- Utilizzato come origine per i messaggi syslog, AAA, SNMP e così via a livello LINA.

No. Si consiglia di non configurarlo. Si consiglia di utilizzare un'interfaccia dati

(vedere la nota seguente).

Nota: il vantaggio di lasciare l'indirizzo IP fuori dall'interfaccia diagnostica è che è possibile posizionare l'interfaccia di gestione sulla stessa rete di qualsiasi altra interfaccia dati. Se si configura l'interfaccia diagnostica, il relativo indirizzo IP deve essere sulla stessa rete dell'indirizzo IP di gestione e viene conteggiata come un'interfaccia normale che non può essere sulla stessa rete di altre interfacce dati. Poiché l'interfaccia di gestione richiede l'accesso a Internet per gli aggiornamenti, posizionare l'interfaccia di gestione sulla stessa rete di un'interfaccia FTD interna significa che è possibile implementare l'FTD con un solo switch sulla LAN e puntare l'interfaccia interna come gateway predefinito per l'interfaccia di gestione (ciò vale solo quando l'FTD è distribuito in modalità di routing).

L'FTD può essere installato in un accessorio firepower 2100. Lo chassis firepower esegue il proprio sistema operativo chiamato FXOS (Firepower eXtensible Operating System) per controllare le operazioni di base del dispositivo, mentre il dispositivo logico FTD è installato su un modulo/blade.

Nota: è possibile utilizzare l'interfaccia grafica FXOS (Graphic User Interface) chiamata FCM (Firepower Chassis Manager) o la CLI di FXOS (Command Line Interface) per configurare le funzioni dello chassis firepower; tuttavia l'interfaccia grafica FCM non è disponibile quando l'FTD è installato sulla serie Firepower 2100, ma solo sulla CLI di FXOS.

Appliance Firepower 21xx:

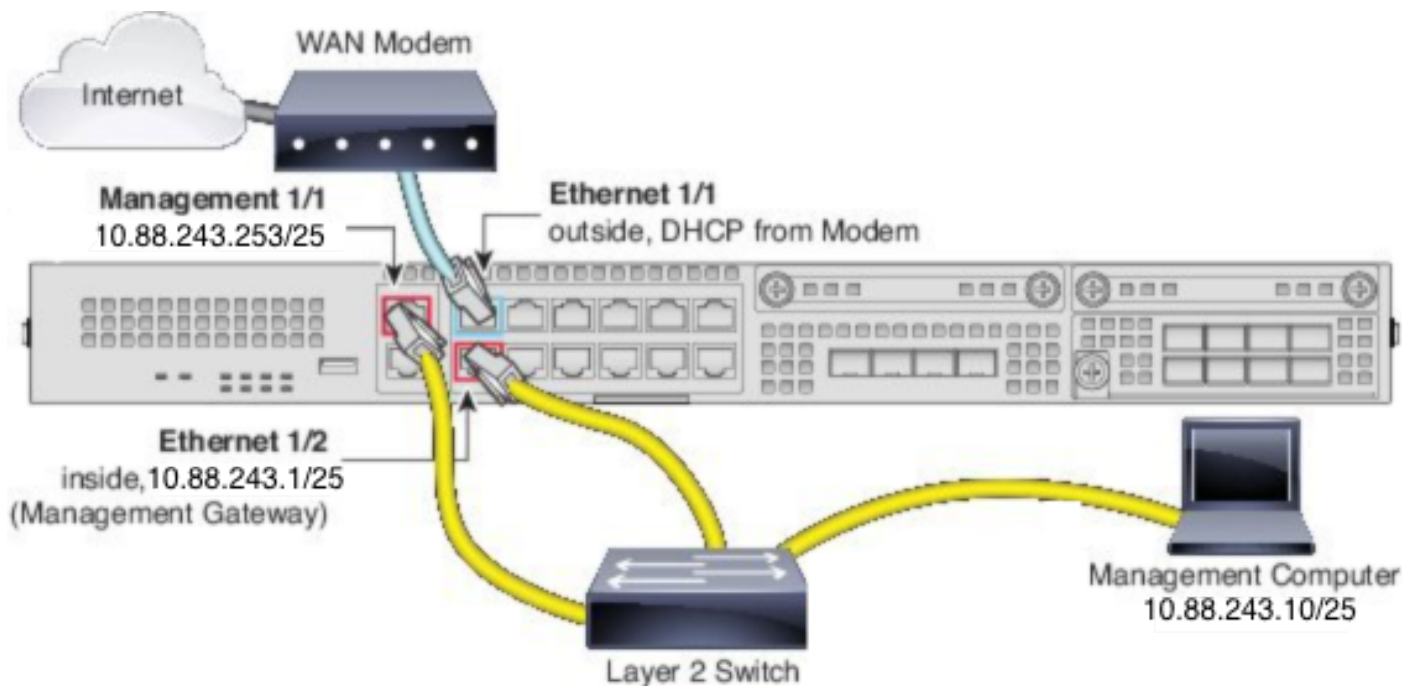


Nota: su firepower serie 2100 l'interfaccia di gestione è condivisa tra lo chassis FXOS e il dispositivo logico FTD.

Configurazione

Esempio di rete

La configurazione predefinita presuppone che alcune interfacce firepower 2100 vengano utilizzate per le reti interne ed esterne. La configurazione iniziale è più facile da completare se si collegano cavi di rete alle interfacce in base a queste aspettative. Per collegare i cavi alla serie Firepower 2100, vedere l'immagine successiva.



Nota: l'immagine mostra una topologia semplice che utilizza uno switch di layer 2. È possibile utilizzare altre topologie e l'implementazione può variare a seconda della connettività di rete logica di base, delle porte, dell'indirizzamento e dei requisiti di configurazione.

Configurazioni

Per abilitare la gestione On-Box di FDM su firepower serie 2100, procedere come segue.

1. Accesso da console allo chassis FPR2100 e collegamento all'applicazione FTD.

```
firepower# connect ftd
>
```

2. Configurare l'indirizzo IP di gestione FTD.

```
>configure network ipv4 manual 10.88.243.253 255.255.255.128 10.88.243.1
```

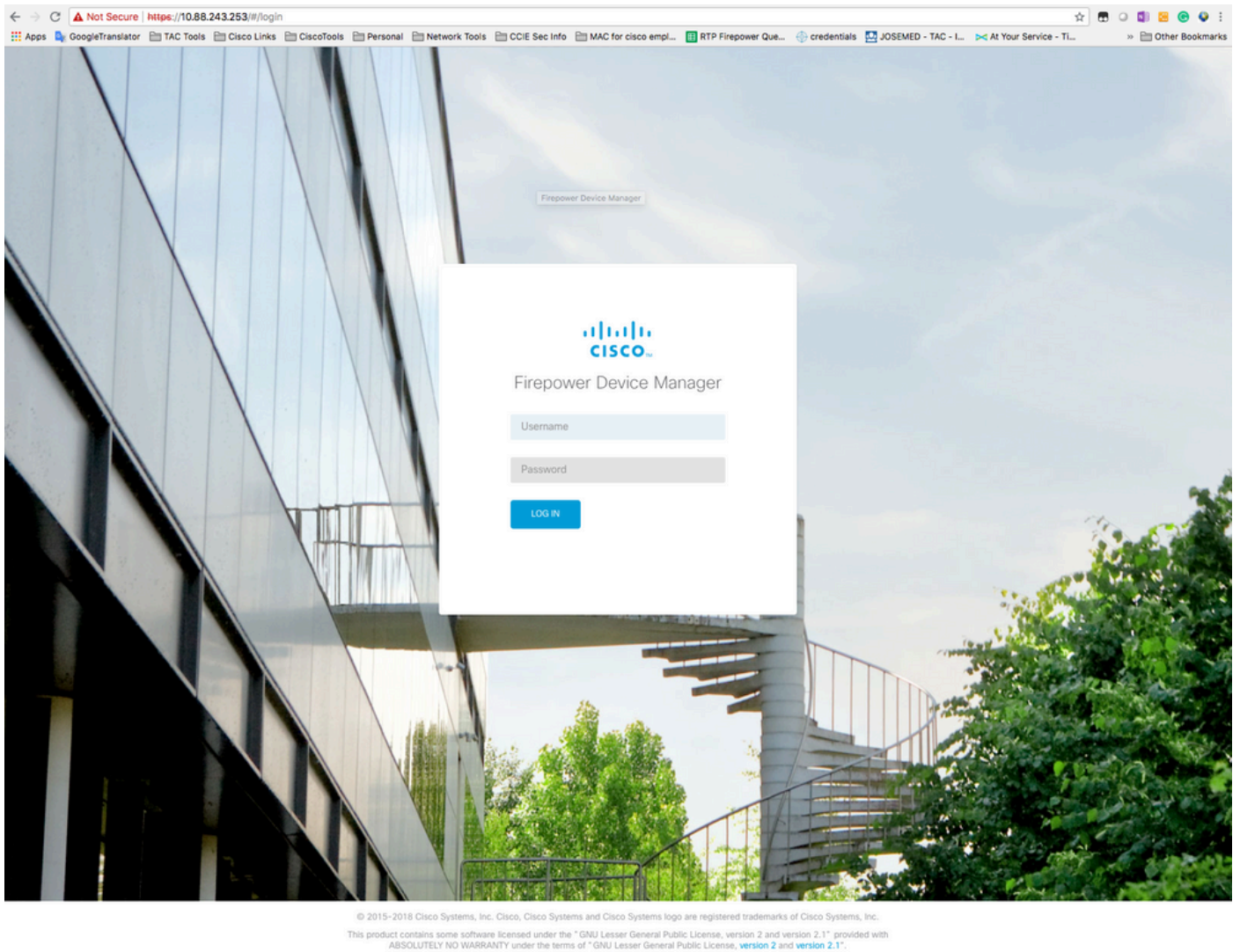
3. Configurare il tipo di gestione come locale.

```
>configure manager local
```

4. Configurare da quali indirizzi IP/subnet è possibile consentire l'accesso di gestione on-box all'FTD.

```
>configure https-access-list 0.0.0.0/0
```

5. Aprire un browser e https nell'indirizzo IP configurato per gestire l'FTD. In questo modo è possibile aprire la gestione FDM (On-Box).



6. Accedere e utilizzare le credenziali firepower predefinite, il nome utente admin e la password Admin123.

Device Setup

1 Configure Internet Connection 2 Configure Time Settings 3 Smart License Registration

Connect firewall to Internet

The initial access control policy will enforce the following actions.
You can edit the policy after setup.

Rule 1	Default Action
Trust Outbound Traffic	Block all other traffic
This rule allows traffic to go from inside to outside, which is needed for the Smart License configuration.	The default action blocks all other traffic.

Outside Interface Address

Connect Ethernet1/1 (Outside) to your ISP/WAN device, for example, your cable modem or router. Then, configure the addresses for the outside interface.

Configure IPv4

Using DHCP

Configure IPv6

Using DHCP

Management Interface

Configure DNS Servers

Primary DNS IP Address: 208.67.222.222

NEXT

Don't have internet connection? [Skip device setup](#)

Verifica

1. Verificare le impostazioni di rete configurate per l'FTD con il comando successivo.

```
> show network
===== [ System Information ] =====
Hostname                : firepower
DNS Servers             : 208.67.222.222
                        : 208.67.220.220
Management port        : 8305
IPv4 Default route     :
  Gateway               : 10.88.243.129

===== [ management0 ] =====
State                   : Enabled
Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 1500
MAC Address             : 00:2C:C8:41:09:80
----- [ IPv4 ] -----
Configuration           : Manual
Address                 : 10.88.243.253
Netmask                 : 255.255.255.128
Broadcast               : 10.88.243.255
----- [ IPv6 ] -----
Configuration           : Disabled
```

```
=====[ Proxy Information ]=====
```

```
State : Disabled
```

```
Authentication : Disabled
```

2. Verificare il tipo di gestione configurato per l'FTD con il comando successivo.

```
> show managers  
Managed locally.
```

Informazioni correlate

[Cisco Firepower Device Manager](#)

[Guida introduttiva a Cisco Firepower Threat Defense per Firepower serie 2100 Using Firepower Management Center](#)

[Configurazione dell'interfaccia di gestione Firepower Threat Defense \(FTD\)](#)

[Nuova immagine di Firepower serie 2100](#)

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).