Configurazione di Secure Firewall Management Center senza Eth0 come server di gestione

Sommario

Introduzione

In questo documento viene descritto come configurare Secure Firewall Management Center (FMC) con una porta diversa anziché con l'interfaccia Eth0 predefinita.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza di Cisco Secure Firewall Management Center (in precedenza Firepower Management Center)
- Conoscenza delle reti di base

Componenti usati

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

- Cisco Secure Firewall Management Center (FMC 1000, 1600, 2500, 2600, 4500, 4600 e virtuale) con software versione 5.x e successive.

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

Informazioni su Connessione di gestione su Centro gestione firewall protetto

Dopo aver configurato il dispositivo con le informazioni FMC e dopo averlo aggiunto al FMC, il dispositivo o il FMC possono stabilire la connessione di gestione. A seconda dell'impostazione iniziale:

- Il dispositivo o il CCP può avviare.
- L'avvio può essere eseguito solo dal dispositivo.
- Solo il CCP può avviare la procedura.

L'avvio ha sempre origine con eth0 sul FMC o con l'interfaccia di gestione con il numero più basso sul dispositivo. Se la connessione non viene stabilita, vengono eseguiti tentativi di utilizzo di interfacce di gestione aggiuntive. Più interfacce di gestione nel FMC consentono di connettersi a reti discrete o di separare la gestione dal traffico degli eventi. Tuttavia, l'iniziatore non sceglie l'interfaccia migliore in base alla tabella di routing.

L'interfaccia interna etichettata come Gestione (Eth0) è una 1 Gigabit Ethernet incorporata nello chassis del dispositivo. Alcuni modelli di chassis FMC dispongono di uno slot di espansione che può trasportare una scheda di espansione del modulo di rete, che può essere in rame o in fibra e fino a 10 Gigabit. Alcune porte incorporate dello chassis possono supportare ricetrasmettitori 10 Gigabit Ethernet SFP+.

La figura mostra il pannello posteriore di FMC 1000.

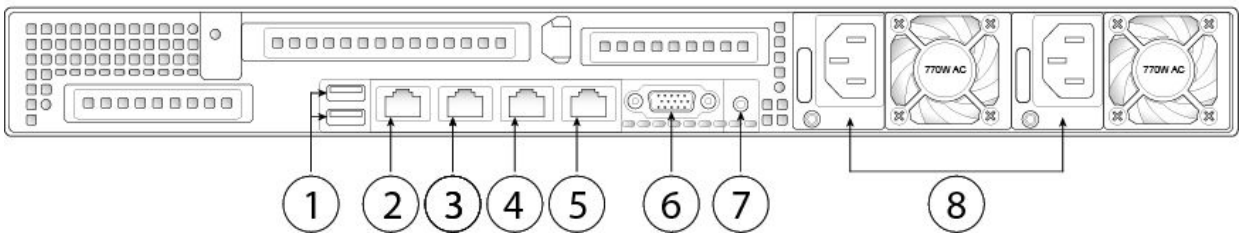

Figura 1. Pannello posteriore di FMC 1000

1	2 porte per tastiera USB	2	Interfaccia CIMC (contrassegnata con "M")

	È possibile collegare una tastiera e, insieme a un monitor sulla porta VGA, accedere alla console.		Questa interfaccia non è supportata.
3	Porta console seriale Questa porta è disabilitata per impostazione predefinita. utilizzare invece la porta VGA e la porta USB della tastiera.	4	eth0 interfaccia di gestione (con etichetta "1") Interfaccia Gigabit Ethernet 10/100/1000 Mbps, RJ-45 eth0 è l'interfaccia di gestione predefinita.
5	eth1 management interface (con etichetta "2") Interfaccia Gigabit Ethernet 10/100/1000 Mbps, RJ-45	6	Interfaccia VGA Attivato per impostazione predefinita.
7	Pulsante/LED di identificazione dell'unità	8	Due alimentatori CA da 770 W

La figura mostra il pannello posteriore dei CCP 2500 e 4500.

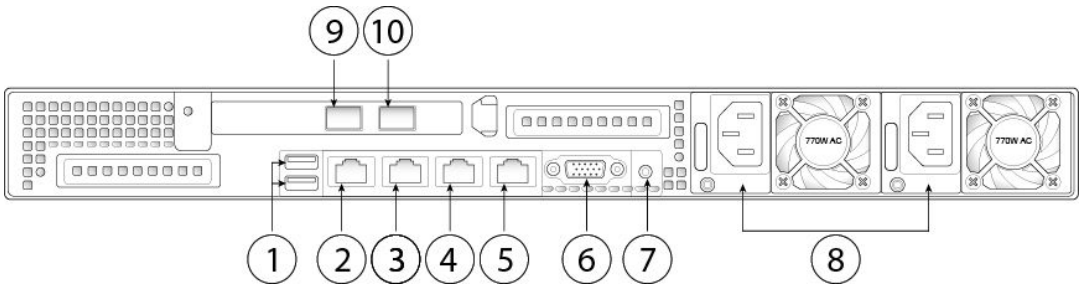

Figura 2. FMC 2500 e 4500 - Pannello posteriore

1	2 porte per tastiera USB È possibile collegare una tastiera e, insieme a un monitor sulla porta VGA, accedere alla console.	2	Interfaccia CIMC (contrassegnata con "M") Questa interfaccia non è supportata.

3	Porta console seriale Questa porta è disabilitata per impostazione predefinita. utilizzare invece la porta VGA e la porta USB della tastiera.	4	eth0 interfaccia di gestione (con etichetta "1") Interfaccia Gigabit Ethernet 10/100/1000 Mbps, RJ-45 eth0 è l'interfaccia di gestione predefinita.
5	eth1 management interface (con etichetta "2") Interfaccia Gigabit Ethernet 10/100/1000 Mbps, RJ-45	6	Interfaccia VGA Attivato per impostazione predefinita.
7	Pulsante/LED di identificazione dell'unità	8	Due alimentatori CA da 770 W
9	eth2 management interface Nota: Usare solo ricetrasmettitori SFP+ supportati da Cisco.	10	eth3 management interface Nota: Usare solo ricetrasmettitori SFP+ supportati da Cisco.

La figura mostra il pannello posteriore dei CCP 1600, 2600 e 4600.

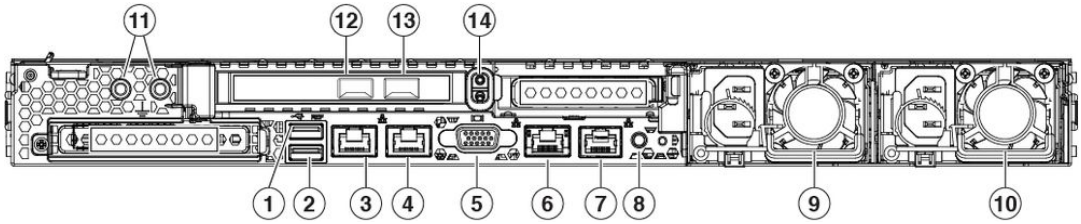

Figura 3. FMC 1600, 2600 e 4600 - Pannello posteriore

1	USB 3.0 tipo A (USB 1) È possibile collegare una tastiera e, insieme a un monitor sulla porta VGA, accedere alla console.	2	USB 3.0 tipo A (USB 2) È possibile collegare una tastiera e, insieme a un monitor sulla porta VGA,

			accedere alla console.
3	eth0 interfaccia di gestione (con etichetta 1) Supporta 100/1000/1000 Mbps in base alla capacità del partner di collegamento.	4	eth1 management interface (con etichetta 2) Gigabit Ethernet 100/1000/1000 Mbps interface, RJ-45, LAN2
5	Porta video VGA (connettore DB-15)	6	Interfaccia CIMC (con etichetta M) Nota: CIMC è supportato solo per l'accesso LOM. CIMC non è supportato su altre interfacce.
7	Porta console seriale (connettore RJ-45) Disabilitato per impostazione predefinita; utilizzare invece la porta VGA e la porta USB della tastiera. Per ulteriori informazioni sulla porta seriale, vedere l'argomento "Set up Serial Access" nella Guida introduttiva di Cisco Firepower Management Center per i modelli 1600, 2600 e 4600.	8	Pulsante identificazione unità
9	Alimentatore CA da 770 W (PSU 1)	10	Alimentatore CA da 770 W (PSU 2)
11	Fori filettati per sporgenza di messa a terra a doppio foro	12	eth2 management interface (Opzionale) Supporto 10-Gigabit Ethernet SFP+

			L'SFP-10G-SR e l'SFP-10G-LR possono essere utilizzati sul CCP.
13	eth3 management interface (Opzionale) Supporto 10-Gigabit Ethernet SFP+ L'SFP-10G-SR e l'SFP-10G-LR possono essere utilizzati sul CCP.	14	Maniglia riser Non supportata

Documentazione correlata

Per istruzioni dettagliate sull'installazione dell'hardware, vedere la Guida all'installazione dell'hardware di Cisco Firepower Management Center 1600, 2600 e 4600.

Per un elenco completo della documentazione della serie Cisco Secure Firewall e dove trovarla, vedere la roadmap della documentazione.

Preconfigurazione

Installare Secure Firewall Management Center per le versioni 6.5 e successive

Per istruzioni dettagliate sull'installazione, consultare la Guida introduttiva a Cisco Firepower Management Center 1600, 2600 e 4600 fino alla fase Connect Cables Turn On Power Verify Status for Versions 6.5 and later (Cavi di connessioneAttiva verifica alimentazione versioni 6.5 e successive). Collegare il cavo all'interfaccia richiesta in base ai diagrammi posteriori.

Configurazione iniziale di Secure Firewall Management Center tramite CLI per le versioni 6.5 e successive

Completare la configurazione iniziale di Management Center utilizzando la CLI descritta nel documento Configurazione iniziale di Management Center Utilizzo della CLI per le versioni 6.5 e successive in tutti gli 8 passaggi.

Modifica dell'interfaccia di gestione mediante la CLI della console

Procedura

1. Accedere alla console virtuale del centro di gestione utilizzando admin come nome utente e

password per l'account admin definito nella configurazione iniziale. La password fa distinzione tra maiuscole e minuscole.

2. Per accedere alla modalità shell Linux, usare il comando expert.
3. Modificare il file ims.conf utilizzando vi editor con il comando sudo vi /etc/sf/ims.conf:

Figura 4

4. Utilizzare i tasti freccia sulla tastiera e individuare la riga MANAGEMENT=eth0:

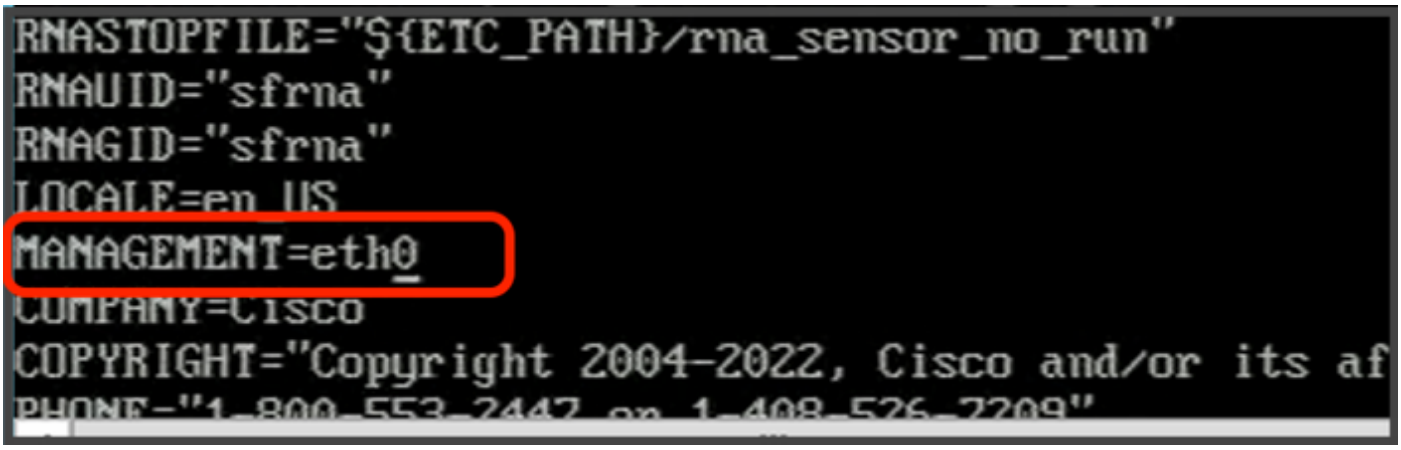

Figura 5

5. Entrare in modalità INSERT per modificare digitando il tasto "I", la riga inferiore sullo schermo può confermare con il messaggio INSERT che siamo in modalità di modifica e sostituire eth0 con l'interfaccia progettata, utilizzare le tabelle precedenti come riferimento:

Figura 6

6. Premere il tasto Esc sulla tastiera per uscire dalla modalità INSERT e usare i due punti ":" per entrare in modalità di comando, digitare "wq!" per salvare le modifiche e uscire dal file:

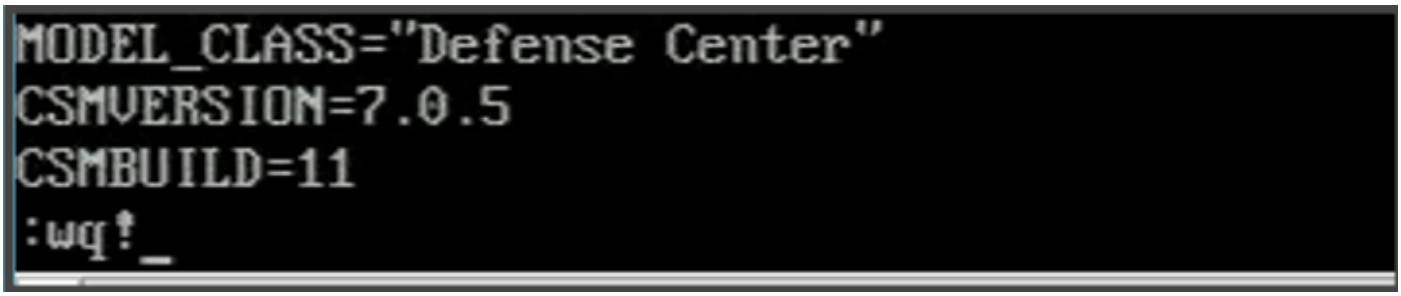

Figura 7

7. Disabilitare l'interfaccia eth0 con il comando sudo ip link set eth0:

Figura 8

8. Eseguire la Configurazione guidata rete per immettere nuovamente l'indirizzo IP, la maschera di rete e l'indirizzo del gateway con il comando sudo usr/local/sf/bin/configure-network, in modo da creare l'interfaccia e assegnare un percorso predefinito:

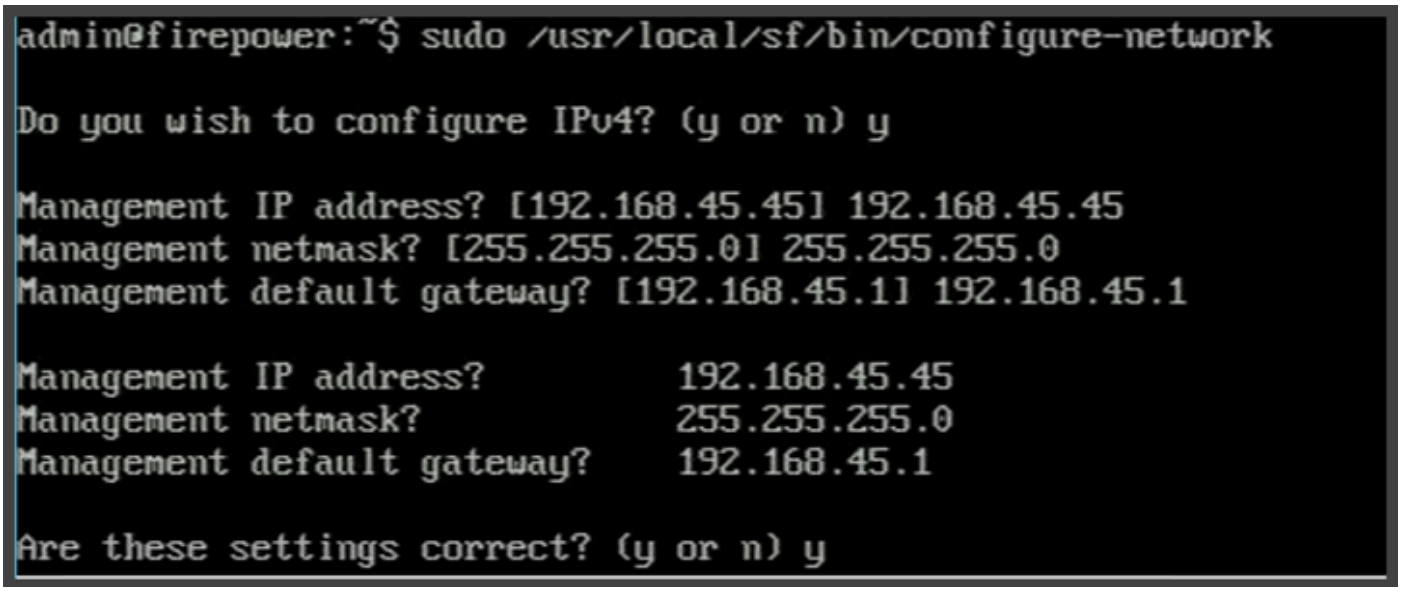

Figura 9

9. Uscire dalla modalità shell di Linux con il comando exit.

Verifica

Per verificare se l'interfaccia selezionata è abilitata, attenersi alla seguente procedura:

1. Eseguire dalla modalità Linux Shell il comando sudo route -n per confermare la tabella di route predefinita per la nuova interfaccia di gestione:

Figura 10

Risoluzione dei problemi

Se la nuova interfaccia non è compilata nella tabella di routing, verificare quanto segue:

1. Confermare di aver disattivato l'interfaccia eth0 con il comando sudo ifconfig.
2. Se l'interfaccia è ancora abilitata, eseguire di nuovo il passaggio 7.
3. Eseguire nuovamente lo script di configurazione della rete nel passaggio 8 per generare la configurazione dell'interfaccia e il percorso predefinito.

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).