

Configurare Gestione periferiche firewall protette in Alta disponibilità

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Attività 1. Verifica condizioni](#)

[Attività 2. Configurare Gestione periferiche firewall protette in Alta disponibilità](#)

[Esempio di rete](#)

[Abilita alta disponibilità su Gestione periferiche firewall protette nell'unità primaria](#)

[Abilita alta disponibilità su Gestione periferiche firewall protette nell'unità secondaria](#)

[Completamento Della Configurazione Delle Interfacce](#)

[Attività 3. Verifica dell'elevata disponibilità di FDM](#)

[Attività 4. Cambia ruoli di failover](#)

[Attività 5. Sospensione o ripresa della disponibilità elevata](#)

[Attività 6. Massima disponibilità](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare e verificare Secure Firewall Device Manager (FDM) High Availability (HA) su dispositivi Secure Firewall.

Prerequisiti

Requisiti

Componenti usati

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

- 2 appliance di sicurezza Cisco Secure Firewall 2100
- Eseguire FDM versione 7.0.5 (build 72)

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.

Attività 1. Verifica condizioni

Attività richiesta:

Verificare che entrambi gli accessori FDM soddisfino i requisiti della nota e possano essere configurati come unità HA.

Soluzione:

Passaggio 1. Collegarsi all'indirizzo IP di gestione dell'accessorio tramite SSH e verificare l'hardware del modulo.

Verificare con il comando `show version` la versione hardware e software del dispositivo principale:

```
> show version
-----[ FPR2130-1 ]-----
Model : Cisco Firepower 2130 Threat Defense (77) Version 7.0.5 (Build 72)
UUID : 6197946e-2747-11ee-9b20-ead7c72f2631
VDB version : 338
-----
```

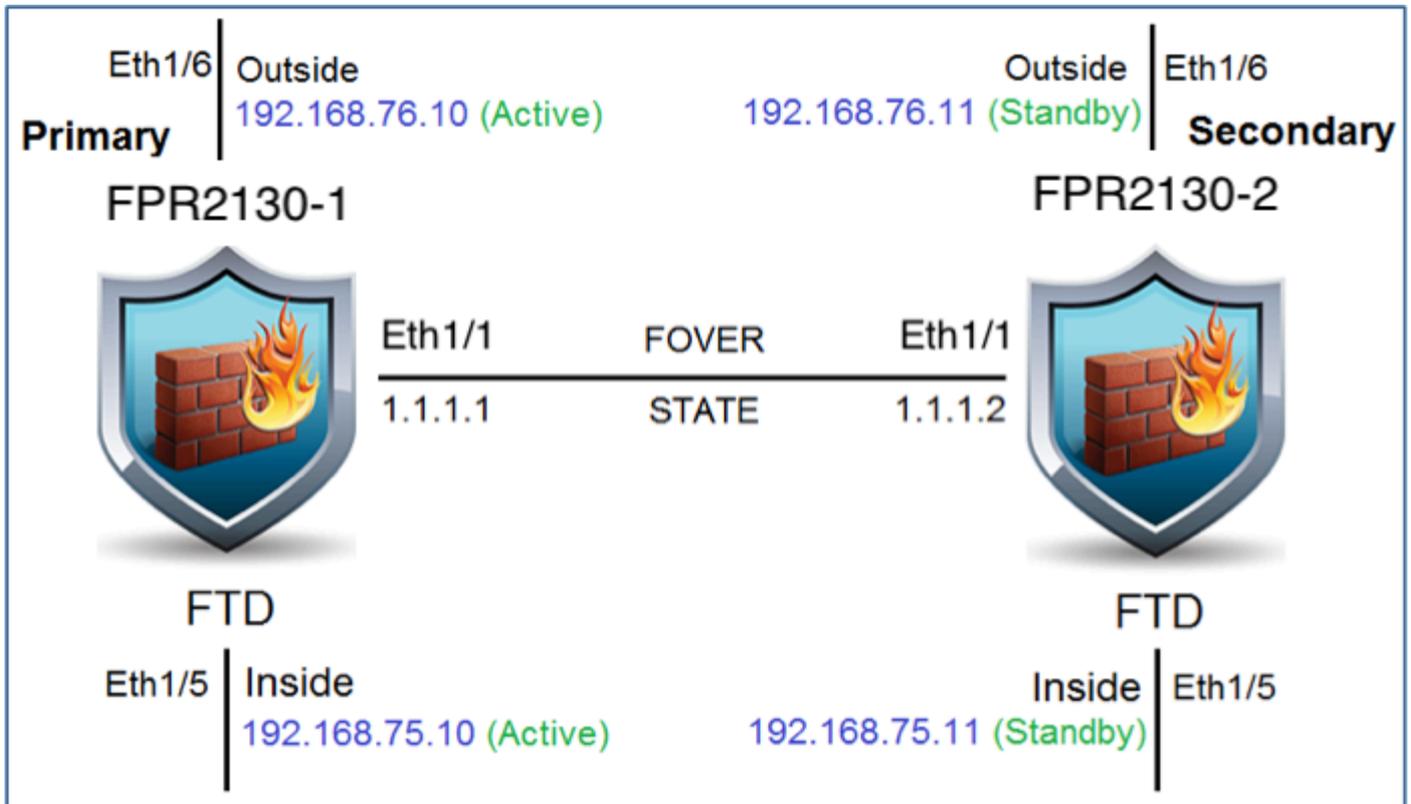
Verificare la versione hardware e software del dispositivo secondario:

```
> show version
-----[ FPR2130-2 ]-----
Model : Cisco Firepower 2130 Threat Defense (77) Version 7.0.5 (Build 72)
UUID : 6ba86648-2749-11ee-b7c9-c9e434a6c9ab
VDB version : 338
-----
```

Attività 2. Configurare Gestione periferiche firewall protette in Alta disponibilità

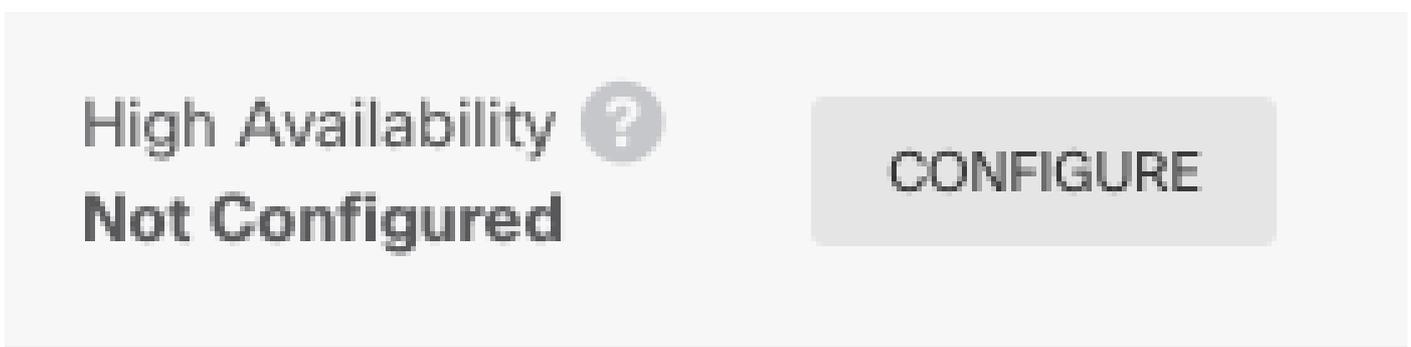
Esempio di rete

Configurare l'alta disponibilità (HA, Active/Standby High Availability) come indicato nel diagramma seguente:

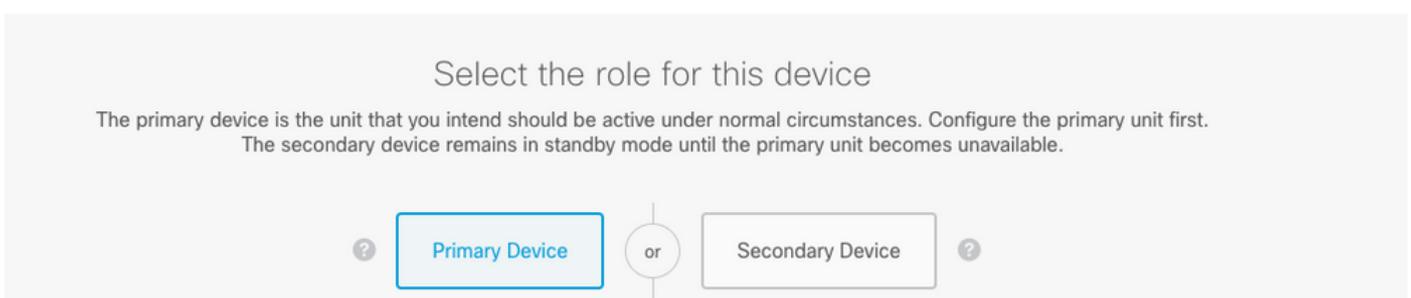


Abilita alta disponibilità su Gestione periferiche firewall protette nell'unità primaria

Passaggio 1. Per configurare il failover di FDM, passare a Dispositivo e fare clic su Configura accanto al gruppo High Availability:



Passaggio 2. Nella pagina Alta disponibilità fare clic sulla casella Periferica principale:



Avvertenza: assicurarsi di selezionare l'unità corretta come unità principale. Tutte le configurazioni sull'unità primaria selezionata vengono replicate sull'unità FTD secondaria

selezionata. A seguito della replica, la configurazione corrente sull'unità secondaria può essere sostituita.

Passaggio 3. Configurare le impostazioni del collegamento di failover e del collegamento allo stato:

In questo esempio, il collegamento di stato ha le stesse impostazioni del collegamento di failover.

FAILOVER LINK	STATEFUL FAILOVER LINK <input checked="" type="checkbox"/> Use the same interface as the Failover Link
Interface unnamed (Ethernet1/1) ▾	Interface unnamed (Ethernet1/1) ▾
Type <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6	Type <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Primary IP 1.1.1.1 <small>e.g. 192.168.10.1</small>	Primary IP 1.1.1.1 <small>e.g. 192.168.11.1</small>
Secondary IP 1.1.1.2 <small>e.g. 192.168.10.2</small>	Secondary IP 1.1.1.2 <small>e.g. 192.168.11.2</small>
Netmask 255.255.255.252 <small>e.g. 255.255.255.0 or 24</small>	Netmask 255.255.255.252 <small>e.g. 255.255.255.0 or 24</small>
IPSec Encryption Key (optional) <small>For security purposes, the encryption key will not be included in the configuration copied to the clipboard when you activate HA. You will need to manually enter the key when you configure HA on the peer device.</small>	IMPORTANT <small>If you configure an IPsec encryption key with inconsistent settings for export controlled features, both devices will become active after you activate HA. Learn More</small>

Passaggio 4. Fare clic su Attiva HA

Passaggio 5. Copiare la configurazione HA negli Appunti del messaggio di conferma, per incollarla sull'unità secondaria.

✕

You have successfully deployed
the HA configuration on the primary device.

What's next?

I need to configure Peer Device

I configured both devices

- 1

Copy the HA configuration to the clipboard.

✓ Copied [Click here to copy again](#)

- 2

Paste it on the secondary device.

Log into the secondary device and open the HA configuration page.

- ✓

You are done!

The devices should communicate and establish a high availability pair automatically.

GOT IT

La configurazione viene distribuita immediatamente nel dispositivo. Non è necessario avviare un processo di distribuzione. Se non viene visualizzato un messaggio che indica che la configurazione è stata salvata e che la distribuzione è in corso, scorrere fino alla parte superiore della pagina per visualizzare i messaggi di errore.

La configurazione viene copiata anche negli Appunti. È possibile utilizzare la copia per configurare rapidamente l'unità secondaria. Per una maggiore protezione, la chiave di crittografia non è inclusa nella copia negli Appunti.

A questo punto, è necessario essere nella pagina Alta disponibilità e lo stato del dispositivo deve essere "Negoziazione". Lo stato deve passare ad Attivo anche prima di configurare il peer, che deve essere visualizzato come Non riuscito fino a quando non viene configurato.

High Availability

Primary Device: **Active**



Peer: **Failed**

Abilita alta disponibilità su Gestione periferiche firewall protette nell'unità secondaria

Dopo aver configurato il dispositivo principale per la disponibilità elevata in modalità attiva/standby, è necessario configurare il dispositivo secondario. Accedere a FDM su tale dispositivo ed eseguire questa procedura.

Passaggio 1. Per configurare il failover di FDM, passare a Dispositivo e fare clic su Configura accanto al gruppo High Availability:

High Availability 
Not Configured

CONFIGURE

Passaggio 2. Nella pagina Alta disponibilità fare clic sulla casella Periferica secondaria:

Device Summary
High Availability

How High Availability Works 

Select the role for this device

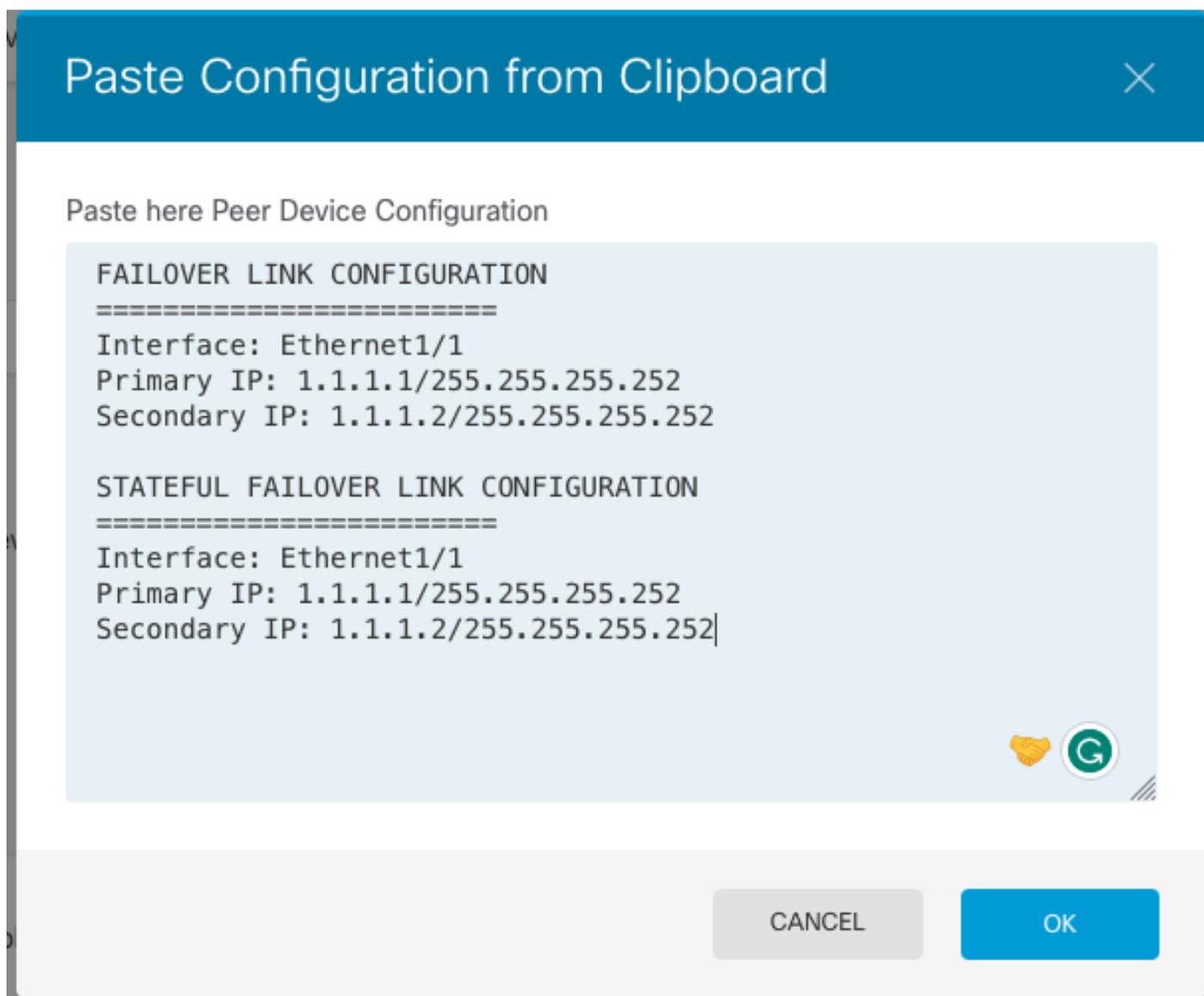
The primary device is the unit that you intend should be active under normal circumstances. Configure the primary unit first.
The secondary device remains in standby mode until the primary unit becomes unavailable.

 Primary Device  Secondary Device 

Passaggio 3. Scegliere una delle opzioni seguenti:

- Metodo Easy: fare clic sul pulsante Incolla dagli Appunti, incollare nella configurazione e fare clic su OK. In questo modo i campi vengono aggiornati con i valori appropriati che è possibile verificare.
- Metodo manuale: configurare direttamente i collegamenti di failover e failover stateful. Immettere esattamente le stesse impostazioni della periferica secondaria immesse nella

periferica principale.



Passaggio 4. Fare clic su Attiva HA

La configurazione viene distribuita immediatamente nel dispositivo. Non è necessario avviare un processo di distribuzione. Se non viene visualizzato un messaggio che indica che la configurazione è stata salvata e che la distribuzione è in corso, scorrere fino alla parte superiore della pagina per visualizzare i messaggi di errore.

Al termine della configurazione, viene visualizzato un messaggio che indica che è stata configurata la disponibilità elevata. Fare clic su Scarica per chiudere il messaggio.

A questo punto, è necessario essere nella pagina Alta disponibilità e lo stato del dispositivo deve indicare che si tratta del dispositivo secondario. Se l'unione con il dispositivo primario ha esito positivo, il dispositivo viene sincronizzato con il dispositivo primario ed eventualmente la modalità deve essere Standby e il peer deve essere Attivo.

High Availability

Secondary Device: **Standby** ↔ Peer: **Active**

Completamento Della Configurazione Delle Interfacce

Passaggio 1. Per configurare le interfacce FDM, passare a Dispositivo e fare clic su Visualizza tutte le interfacce:

Interfaces

Connected

Enabled 2 of 17

View All Interfaces



Passaggio 2. Selezionare e modificare le impostazioni Interfacce come mostrato nelle immagini:

Interfaccia Ethernet 1/5:

Ethernet1/5

Edit Physical Interface



Interface Name

inside

Mode

Routed

Status



Most features work with named interfaces only, although some require unnamed interfaces.

Description

IPv4 Address

IPv6 Address

Advanced

Type

Static

IP Address and Subnet Mask

192.168.75.10

/

255.255.255.0

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask

192.168.75.11

/

255.255.255.0

e.g. 192.168.5.16

CANCEL

OK

Interfaccia Ethernet 1/6

Ethernet1/6 Edit Physical Interface



Interface Name

outside

Mode

Routed

Status



Most features work with named interfaces only, although some require unnamed interfaces.

Description

IPv4 Address

IPv6 Address

Advanced

Type

Static

IP Address and Subnet Mask

192.168.76.10

/

255.255.255.0

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask

192.168.76.11

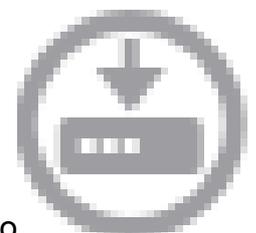
/

255.255.255.0

e.g. 192.168.5.16

CANCEL

OK



Passaggio 3. Dopo aver configurato le modifiche, fare clic su Modifiche in sospeso e Installazione immediata.

Attività 3. Verifica dell'elevata disponibilità di FDM

Attività richiesta:

Verificare le impostazioni di alta disponibilità dalla GUI di FDM e dalla CLI di FDM.

Soluzione:

Passaggio 1. Passare a Periferica e controllare le impostazioni Alta disponibilità:

Device Summary
High Availability

Primary Device
Current Device Mode: **Active** ⇌ Peer: **Standby** Failover History Deployment History

High Availability Configuration

Select and configure the peer device based on the following characteristics.

GENERAL DEVICE INFORMATION

Model	Cisco Firepower 2130 Threat Defense
Software	7.0.5-72
VDB	338.0
Intrusion Rule Update	20210503-2107

FAILOVER LINK

Interface	Ethernet1/1
Type	IPv4
Primary IP/Netmask	1.1.1.1/255.255.255.252
Secondary IP/Netmask	1.1.1.2/255.255.255.252

STATEFUL FAILOVER LINK

The same as the Failover Link.

IPSEC ENCRYPTION KEY: NOT CONFIGURED

Failover Criteria

INTERFACE FAILURE THRESHOLD

Failure Criteria	Number
Number of failed interfaces exceeds	1

1-211

INTERFACE TIMING CONFIGURATION

Poll Time	Hold Time	
5000	25000	seconds milliseconds
500-15000 milliseconds	5000-75000 milliseconds	

PEER TIMING CONFIGURATION

Poll Time	Hold Time	
1000	15000	seconds milliseconds
200-15000 milliseconds	800-45000 milliseconds	

SAVE

Passaggio 2. Connettersi alla CLI del dispositivo primario FDM utilizzando SSH e convalidare con il comando show high-availability config:

```
> show high-availability config
Failover On
Failover unit Primary
Failover LAN Interface: failover-link Ethernet1/1 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 1293 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.16(4)200, Mate 9.16(4)200
Serial Number: Ours JAD231510ZT, Mate JAD2315110V
Last Failover at: 00:01:29 UTC Jul 25 2023
  This host: Primary - Active
    Active time: 4927 (sec)
    slot 0: FPR-2130 hw/sw rev (1.3/9.16(4)200) status (Up Sys)
      Interface diagnostic (0.0.0.0): Normal (Waiting)
      Interface eth2 (0.0.0.0): Link Down (Shutdown)
```

```

    Interface inside (192.168.75.10): No Link (Waiting)
    Interface outside (192.168.76.10): No Link (Waiting)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)
Other host: Secondary - Standby Ready
Active time: 0 (sec)
slot 0: FPR-2130 hw/sw rev (1.3/9.16(4)200) status (Up Sys)
    Interface diagnostic (0.0.0.0): Normal (Waiting)
    Interface eth2 (0.0.0.0): Link Down (Shutdown)
    Interface inside (192.168.75.11): No Link (Waiting)
    Interface outside (192.168.76.11): No Link (Waiting)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)

```

Stateful Failover Logical Update Statistics

```

Link : failover-link Ethernet1/1 (up)
Stateful Obj   xmit      xerr      rcv       rerr
General        189        0         188       0
sys cmd        188        0         188       0
up time        0          0          0         0
RPC services   0          0          0         0
TCP conn       0          0          0         0
UDP conn       0          0          0         0
ARP tbl       0          0          0         0
Xlate_Timeout  0          0          0         0
IPv6 ND tbl    0          0          0         0
VPN IKEv1 SA   0          0          0         0
VPN IKEv1 P2   0          0          0         0
VPN IKEv2 SA   0          0          0         0
VPN IKEv2 P2   0          0          0         0
VPN CTCP upd   0          0          0         0
VPN SDI upd    0          0          0         0
VPN DHCP upd   0          0          0         0
SIP Session    0          0          0         0
SIP Tx 0       0          0          0         0
SIP Pinhole    0          0          0         0
Route Session  0          0          0         0
Router ID      0          0          0         0
User-Identity  1          0          0         0
CTS SGTNAME    0          0          0         0
CTS PAC        0          0          0         0
TrustSec-SXP   0          0          0         0
IPv6 Route     0          0          0         0
STS Table      0          0          0         0
Rule DB B-Sync 0          0          0         0
Rule DB P-Sync 0          0          0         0
Rule DB Delete 0          0          0         0

```

Logical Update Queue Information

```

          Cur      Max      Total
Recv Q:    0       10       188
Xmit Q:    0       11       957

```

Passaggio 3. Eseguire la stessa operazione sul dispositivo secondario.

Passaggio 4. Convalidare lo stato corrente con il comando show failover state:

```
> show failover state
```

	State	Last Failure Reason	Date/Time
This host -	Primary Active	None	
Other host -	Secondary Standby Ready	Comm Failure	00:01:45 UTC Jul 25 2023

```
====Configuration State====
```

```
Sync Done
```

```
====Communication State====
```

```
Mac set
```

Passaggio 5. Verificare la configurazione dall'unità primaria con il failover show running-config e l'interfaccia show running-config:

```
> show running-config failover
```

```
failover
failover lan unit primary
failover lan interface failover-link Ethernet1/1
failover replication http
failover link failover-link Ethernet1/1
failover interface ip failover-link 1.1.1.1 255.255.255.252 standby 1.1.1.2
```

```
> show running-config interface
```

```
!
interface Ethernet1/1
  description LAN/STATE Failover Interface
  ipv6 enable
!
interface Ethernet1/2
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Ethernet1/3
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Ethernet1/4
  shutdown
  no nameif
  no security-level
  no ip address
!
interface Ethernet1/5
  nameif inside
  security-level 0
  ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11
!
interface Ethernet1/6
  nameif outside
  security-level 0
  ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11
```

```
!  
interface Ethernet1/7  
  shutdown  
  no nameif  
  no security-level  
  no ip address  
!  
interface Management1/1  
  management-only  
  nameif diagnostic  
  cts manual  
  propagate sgt preserve-untag  
  policy static sgt disabled trusted  
  security-level 0  
  no ip address
```

Attività 4. Cambia ruoli di failover

Attività richiesta:

Dall'interfaccia grafica di Secure Firewall Device Manager, passare ai ruoli di failover da Principale/Attivo, Secondario/Standby a Principale/Standby, Secondario/Attivo

Soluzione:

Passaggio 1. Fare clic sulla periferica



Device: FPR2130-1

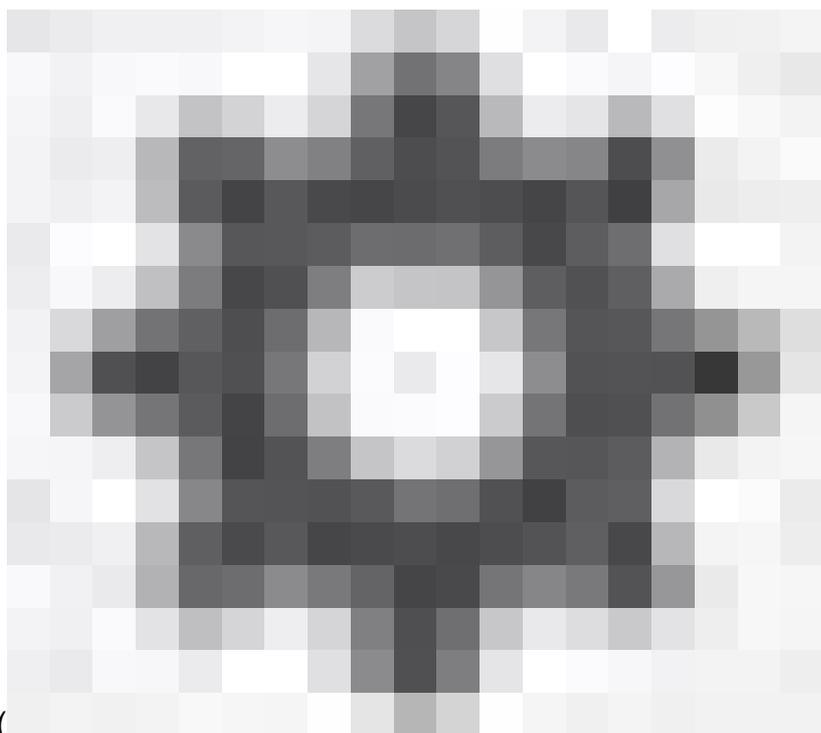
Passaggio 2. Fare clic sul collegamento Alta disponibilità sul lato destro del riepilogo del dispositivo.

High Availability

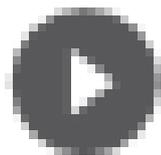
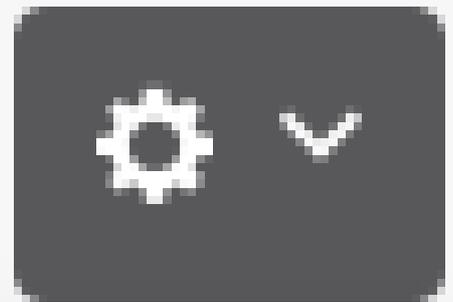
Primary Device: **Active**



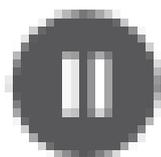
Peer: **Standby**



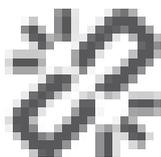
Passaggio 3. Dall'icona dell'ingranaggio (), scegliere Modalità interruttore.



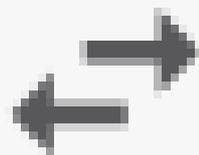
Resume HA



Suspend HA



Break HA



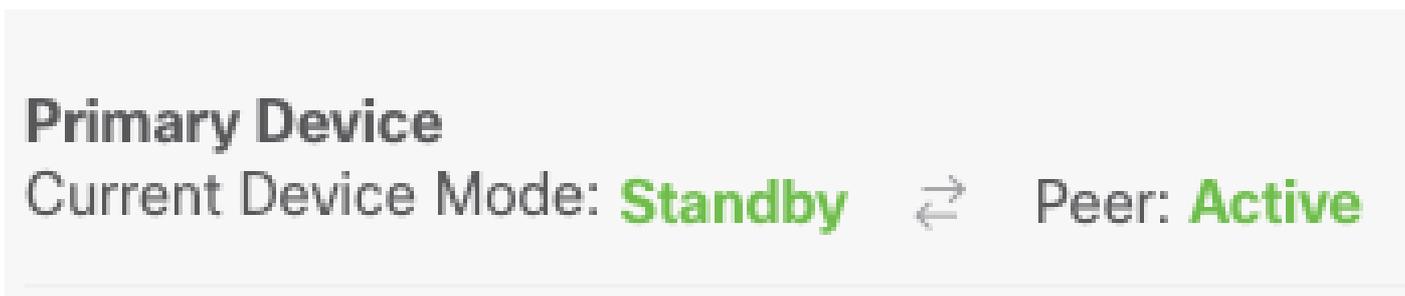
Switch Mode

Passaggio 4. Leggere il messaggio di conferma e fare clic su OK.



Il sistema forza il failover in modo che l'unità attiva diventi di standby e l'unità di standby diventi la nuova unità attiva.

Passaggio 5. Verificate il risultato come mostrato nell'immagine:



Passaggio 6. È inoltre possibile eseguire la verifica utilizzando il collegamento Cronologia di failover e la schermata popup della console CLI deve mostrare i risultati:

From State	To State	Reason
21:55:37 UTC Jul 20 2023 Not Detected	Disabled	No Error
00:00:43 UTC Jul 25 2023 Disabled	Negotiation	Set by the config command
00:01:28 UTC Jul 25 2023 Negotiation	Just Active	No Active unit found
00:01:29 UTC Jul 25 2023 Just Active	Active Drain	No Active unit found
00:01:29 UTC Jul 25 2023 Active Drain	Active Applying Config	No Active unit found
00:01:29 UTC Jul 25 2023 Active Applying Config	Active Config Applied	No Active unit found

```

00:01:29 UTC Jul 25 2023
Active Config Applied      Active      No Active unit found

18:51:40 UTC Jul 25 2023
Active                    Standby Ready      Set by the config command

```

```

=====
PEER History Collected at 18:55:08 UTC Jul 25 2023
=====

```

```

=====PEER-HISTORY=====
From State      To State      Reason
=====PEER-HISTORY=====

```

```

22:00:18 UTC Jul 24 2023
Not Detected      Disabled      No Error

00:52:08 UTC Jul 25 2023
Disabled          Negotiation   Set by the config command

00:52:10 UTC Jul 25 2023
Negotiation      Cold Standby  Detected an Active mate

00:52:11 UTC Jul 25 2023
Cold Standby     App Sync      Detected an Active mate

00:53:26 UTC Jul 25 2023
App Sync         Sync Config   Detected an Active mate

01:00:12 UTC Jul 25 2023
Sync Config      Sync File System  Detected an Active mate

01:00:12 UTC Jul 25 2023
Sync File System Bulk Sync      Detected an Active mate

01:00:23 UTC Jul 25 2023
Bulk Sync        Standby Ready  Detected an Active mate

18:45:01 UTC Jul 25 2023
Standby Ready    Just Active    Other unit wants me Active

18:45:02 UTC Jul 25 2023
Just Active      Active Drain   Other unit wants me Active

18:45:02 UTC Jul 25 2023
Active Drain     Active Applying Config  Other unit wants me Active

18:45:02 UTC Jul 25 2023
Active Applying Config  Active Config Applied  Other unit wants me Active

18:45:02 UTC Jul 25 2023
Active Config Applied  Active          Other unit wants me Active

```

```

=====PEER-HISTORY=====

```

Passaggio 7. Dopo la verifica, riattivare l'unità principale.

Attività 5. Sospensione o ripresa della disponibilità elevata

È possibile sospendere un'unità in una coppia ad alta disponibilità. Ciò è utile quando:

- Entrambe le unità si trovano in una situazione di attività-attività e la correzione della comunicazione sul collegamento di failover non consente di risolvere il problema.
- Si desidera risolvere i problemi relativi a un'unità attiva o di standby e non si desidera che le unità vengano sottoposte a failover durante tale periodo.
- Si desidera impedire il failover durante l'installazione di un aggiornamento software sul dispositivo di standby.

La differenza chiave tra sospendere HA e interrompere HA consiste nel fatto che su un dispositivo HA sospeso viene mantenuta la configurazione a elevata disponibilità. Quando si interrompe HA, la configurazione viene cancellata. Pertanto, è possibile riprendere HA su un sistema sospeso, il che consente la configurazione esistente e rende i due dispositivi nuovamente funzionanti come coppia di failover.

Attività richiesta:

Dall'interfaccia grafica di Gestione periferiche Secure Firewall, sospendere l'unità principale e riprendere l'alta disponibilità sulla stessa unità.

Soluzione:

Passaggio 1. Fare clic su Periferica.



Device: FPR2130-1

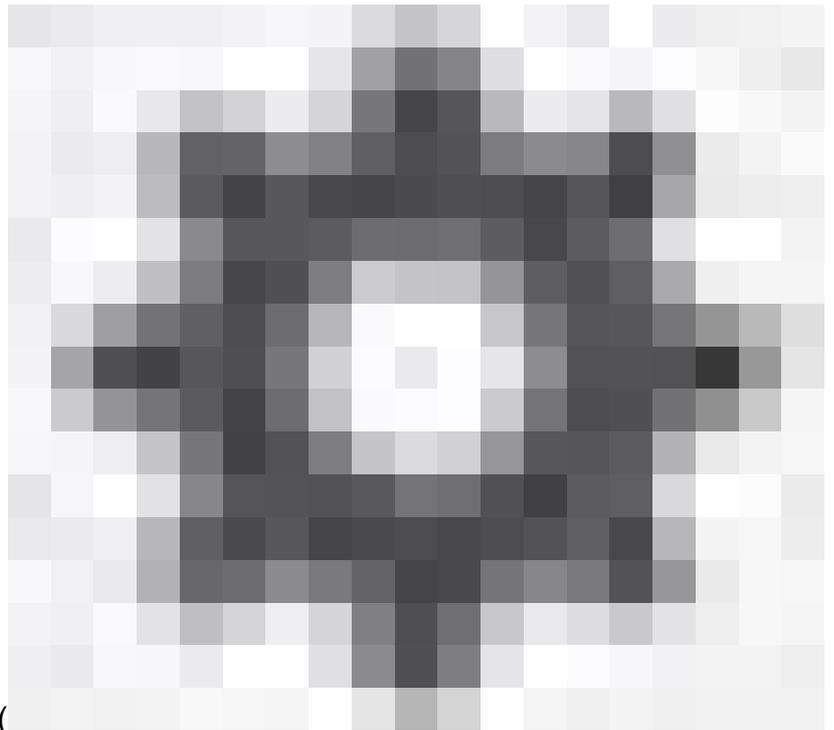
Passaggio 2. Fare clic sul collegamento Alta disponibilità sul lato destro del riepilogo del dispositivo.

High Availability

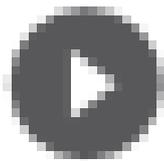
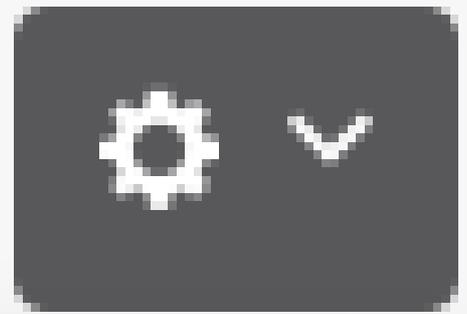
Primary Device: **Active**



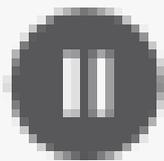
Peer: **Standby**



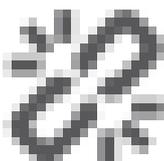
Passaggio 3. Dall'icona dell'ingranaggio (), scegliere Sospendi HA.



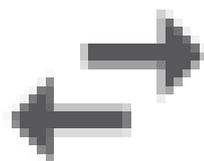
Resume HA



Suspend HA



Break HA



Switch Mode

Passaggio 4. Leggere il messaggio di conferma e fare clic su OK.

Suspend HA Configuration



Suspending high availability on the active unit suspends HA on both the active and standby unit. The active unit will continue to handle user traffic as a stand-alone device, whereas the standby unit will remain inactive. The HA configuration will not be erased.

Do you want to suspend high availability on both the active and standby unit?

CANCEL

OK

Passaggio 5. Verificate il risultato come mostrato nell'immagine:

Primary Device

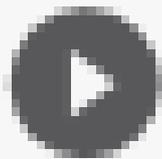
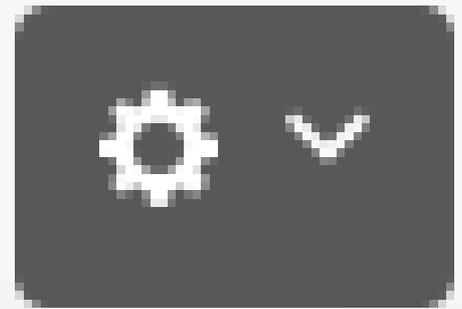
Current Device Mode: **Suspended**  Peer: **Unknown**



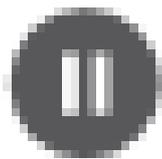
Time of event: 25 Jul 2023, 01:08:01 PM

Event description: Set by the config command

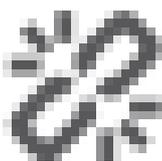
Passaggio 6. Per riprendere l'HA, dall'icona dell'ingranaggio (), scegliere Riprendi HA.



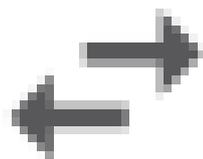
Resume HA



Suspend HA

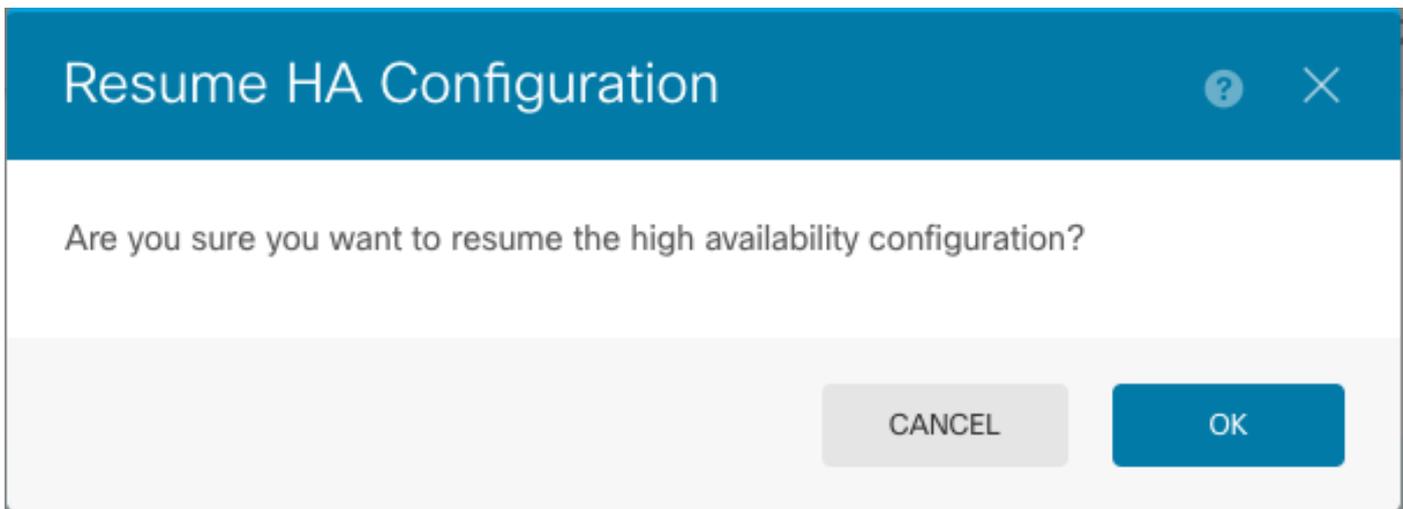


Break HA



Switch Mode

Passaggio 7. Leggere il messaggio di conferma e fare clic su OK.



Passaggio 5. Verificate il risultato come mostrato nell'immagine:



Attività 6. Massima disponibilità

Se non si desidera più che i due dispositivi funzionino come una coppia ad alta disponibilità, è possibile interrompere la configurazione HA. Quando si interrompe HA, ogni dispositivo diventa un dispositivo autonomo. Le relative configurazioni devono essere modificate come segue:

- Il dispositivo attivo conserva la configurazione completa così com'è prima dell'interruzione, con la configurazione HA rimossa.
- Il dispositivo di standby ha tutte le configurazioni di interfaccia rimosse oltre alla configurazione HA. Tutte le interfacce fisiche sono disabilitate, anche se le sottointerfacce non sono disabilitate. L'interfaccia di gestione rimane attiva, quindi è possibile accedere al dispositivo e riconfigurarlo.

Attività richiesta:

Dall'interfaccia grafica di Gestione periferiche Secure Firewall, interrompere la coppia Alta disponibilità.

Soluzione:

Passaggio 1. Fare clic su Periferica.

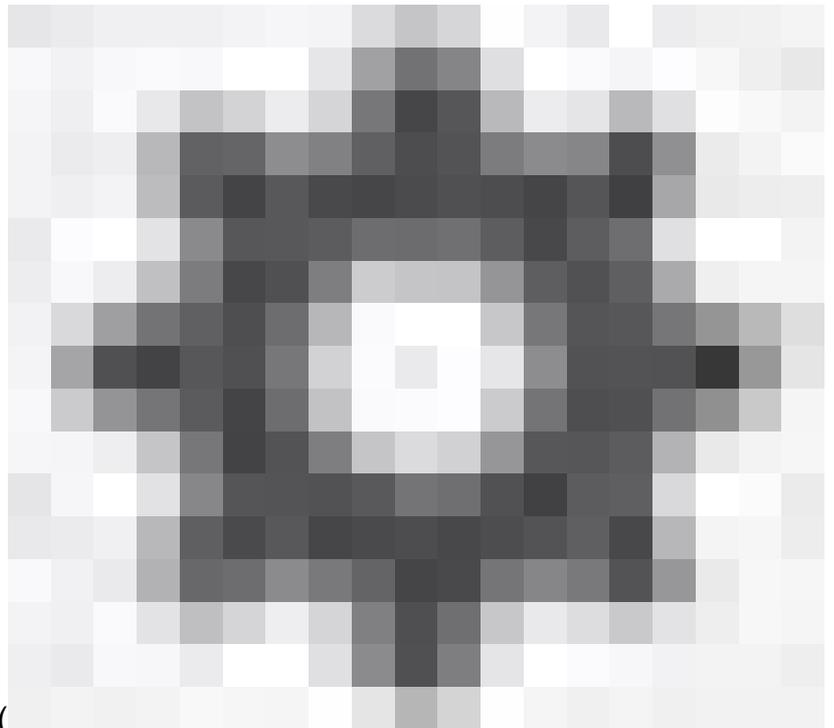


Device: FPR2130-1

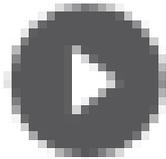
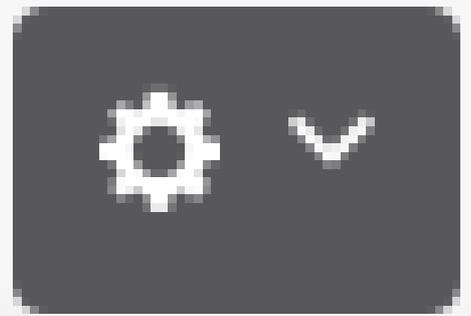
Passaggio 2. Fare clic sul collegamento Alta disponibilità sul lato destro del riepilogo del dispositivo.

High Availability

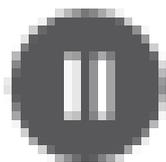
Primary Device: **Active** ↔ Peer: **Standby**



Passaggio 3. Dall'icona dell'ingranaggio (), scegliere Break HA.



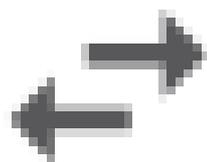
Resume HA



Suspend HA



Break HA



Switch Mode

Passaggio 4. Leggere il messaggio di conferma, scegliere se disabilitare le interfacce e fare clic su Interrompi.

È necessario selezionare l'opzione per disabilitare le interfacce se si interrompe HA dall'unità di

standby.

Il sistema distribuisce immediatamente le modifiche sia su questo dispositivo che sul dispositivo peer (se possibile). Il completamento dell'installazione su ciascun dispositivo e l'indipendenza di ciascun dispositivo può richiedere alcuni minuti.

Confirm Break HA

⚠️ Deployment might require the restart of inspection engines, which will result in a momentary traffic loss.

Are you sure you want to break the HA configuration?

When you break HA from the active unit, the HA configuration is cleared on both the active and standby unit, and the interfaces on the standby unit are disabled. When you break HA from the standby unit (which must be in the suspended state), the HA configuration is removed from that unit and interfaces must be disabled.

Disable interfaces on this unit.

CANCEL BREAK

Passaggio 5. Verificare il risultato mostrato nell'immagine:

High Availability 

Not Configured

CONFIGURE

Informazioni correlate

- Tutte le versioni della guida alla configurazione di Cisco Secure Firewall Device Manager sono disponibili qui

<https://www.cisco.com/c/en/us/support/security/firepower-ngfw/products-installation-and-configuration-guides-list.html>

- Cisco Global Technical Assistance Center (TAC) consiglia vivamente questa guida visiva per una conoscenza pratica e approfondita delle tecnologie di sicurezza di nuova generazione di Cisco Firepower:

<https://www.ciscopress.com/store/cisco-firepower-threat-defense-ftd-configuration-and-9781587144806>

- Note tecniche relative alle tecnologie Firepower per la configurazione e la risoluzione dei problemi

<https://www.cisco.com/c/en/us/support/security/defense-center/series.html>

- [Documentazione e supporto tecnico – Cisco Systems](#)

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).