Configurazione della funzionalità FTD High Availability nei dispositivi Firepower

Sommario

Introduzione

In questo documento viene descritto come configurare e verificare la coppia di Firepower Threat Defense (FTD) con funzionalità High Availability (HA) (failover Attivo/Standby) sulle appliance FPR9300.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

- 2 appliance di sicurezza Cisco Firepower 9300 - FXOS SW 2.0(1.23)
- FTD versione 10.10.1.1 (build 1023)
- Firepower Management Center (FMC) - Versione software 10.10.1.1 (build 1023)

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.

> **Nota**: su un accessorio FPR9300 con FTD, è possibile configurare solo HA tra chassis. Le due unità di una configurazione HA devono soddisfare le condizioni indicate qui.

Attività 1. Verifica condizioni

Attività richiesta:

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

Soluzione:

Passaggio 1. Connettersi all'IP di gestione FPR9300 e verificare l'hardware del modulo.

Verificare l'hardware FPR9300-1.

<#root>

```
KSEC-FPR9K-1-A#
```

```
show server inventory
```

```
Server Equipped PID Equipped VID Equipped Serial (SN) Slot Status      Ackd Memory (MB) Ackd Cores
------- ------------ ------------ -------------------- ---------------- ---------------- ----------
1/1     FPR9K-SM-36  V01          FLM19216KK6          Equipped                   262144         36
1/2     FPR9K-SM-36  V01          FLM19206H71          Equipped                   262144         36
1/3     FPR9K-SM-36  V01          FLM19206H7T          Equipped                   262144         36
KSEC-FPR9K-1-A#
```

Verificare l'hardware FPR9300-2.

<#root>

```
KSEC-FPR9K-2-A#
```

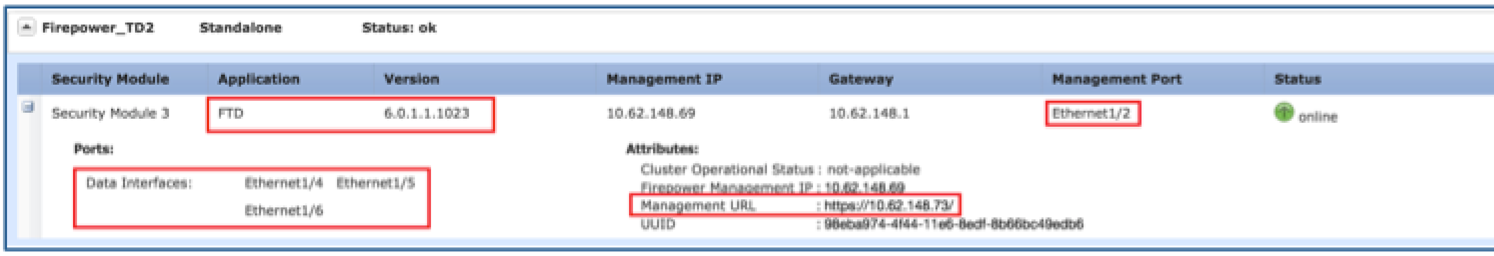
```
show server inventory
```

```
Server  Equipped PID Equipped VID Equipped Serial (SN) Slot Status      Ackd Memory (MB) Ackd Cores
------- ------------ ------------ -------------------- ---------------- ---------------- ----------
1/1     FPR9K-SM-36  V01          FLM19206H9T          Equipped                   262144         36
1/2     FPR9K-SM-36  V01          FLM19216KAX          Equipped                   262144         36
1/3     FPR9K-SM-36  V01          FLM19267A63          Equipped                   262144         36
KSEC-FPR9K-2-A#
```

Passaggio 2. Accedere a FPR9300-1 Chassis Manager e selezionare Logical Devices (Dispositivi logici).

Verificare la versione del software, il numero e il tipo di interfacce, come mostrato nelle immagini.

FPR9300-1



Firepower_TD2 Standalone Status: ok

	Security Module	Application	Version	Management IP	Gateway	Management Port	Status
	Security Module 3	FTD	6.0.1.1.1023	10.62.148.69	10.62.148.1	Ethernet1/2	online

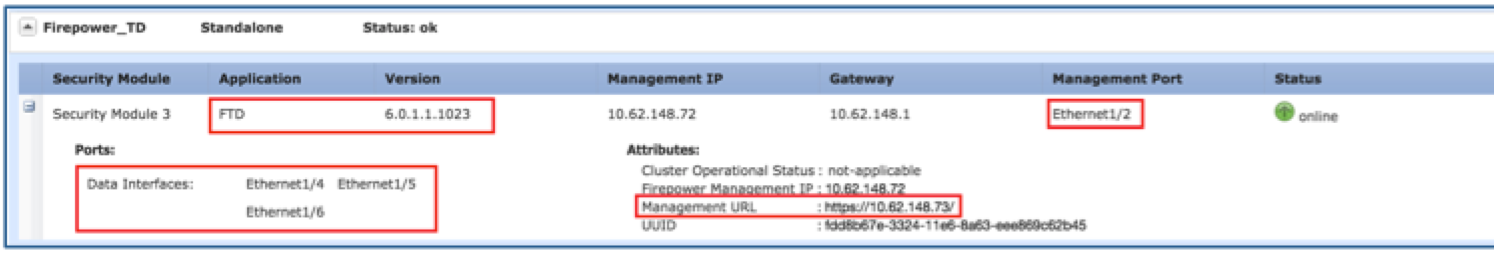
Ports:

Data Interfaces: Ethernet1/4 Ethernet1/5 Ethernet1/6

Attributes:

Cluster Operational Status : not-applicable
Firepower Management IP : 10.62.148.69
Management URL : https://10.62.148.73/
UUID : 98eba974-4f44-11e6-8edf-8b66bc49edb6

FPR9300-2



Firepower_TD Standalone Status: ok

	Security Module	Application	Version	Management IP	Gateway	Management Port	Status
	Security Module 3	FTD	6.0.1.1.1023	10.62.148.72	10.62.148.1	Ethernet1/2	online

Ports:

Data Interfaces: Ethernet1/4 Ethernet1/5 Ethernet1/6

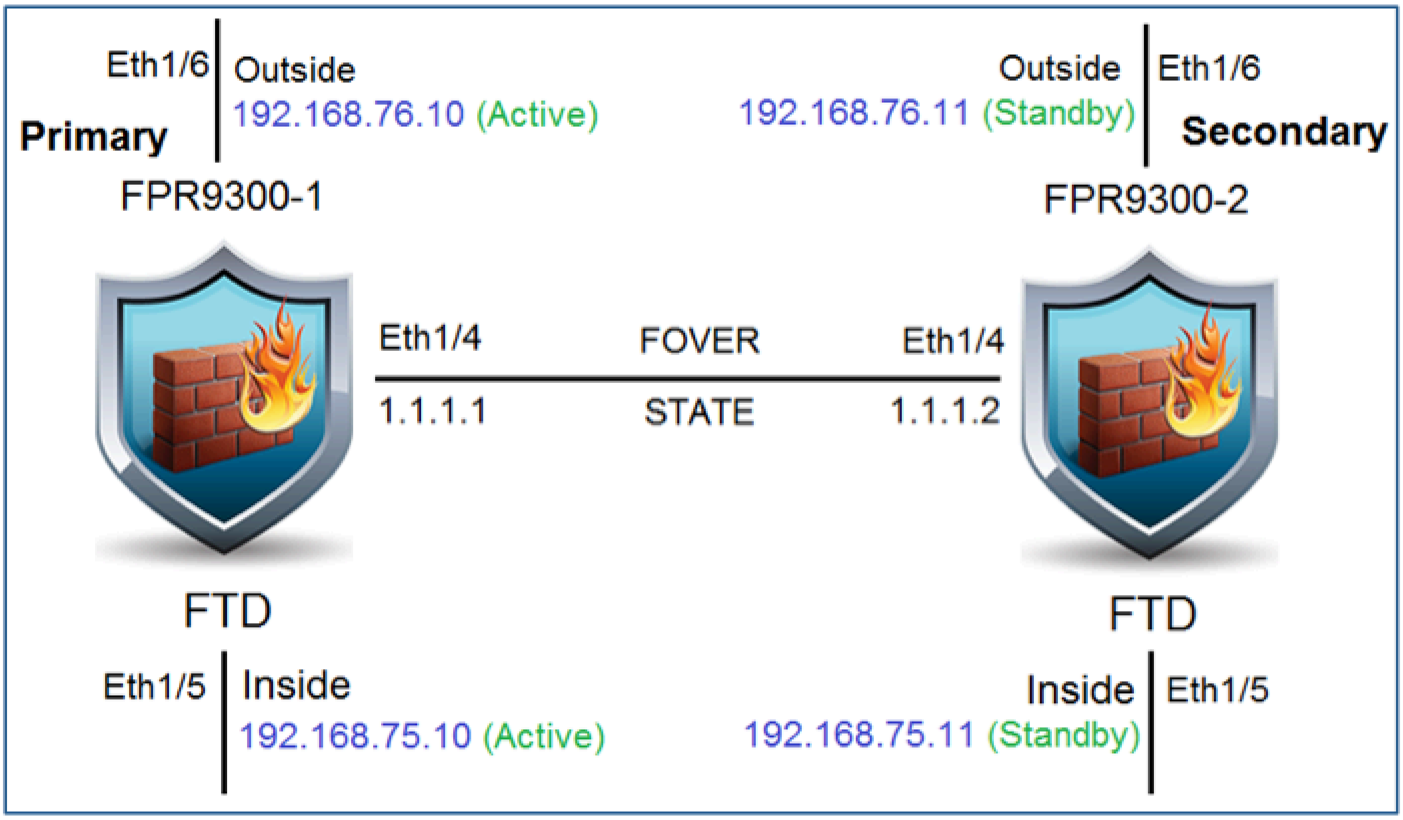
Attributes:

Cluster Operational Status : not-applicable
Firepower Management IP : 10.62.148.72
Management URL : https://10.62.148.73/
UUID : fdd8b67e-3324-11e6-8a63-eee869c62b45

Attività 2. Configurazione di FTD HA su FPR9300

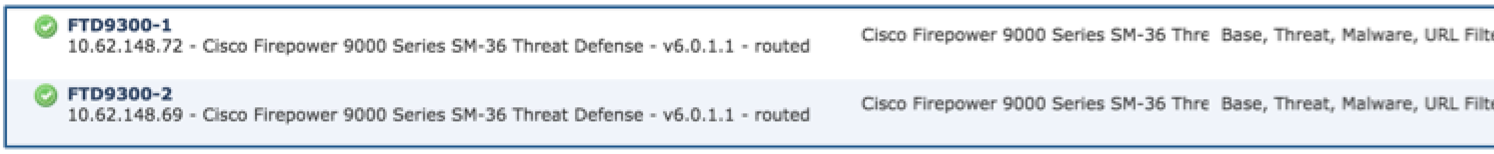
Attività richiesta:

Configurare il failover Attivo/Standby (HA) come nell'immagine seguente.



Soluzione:

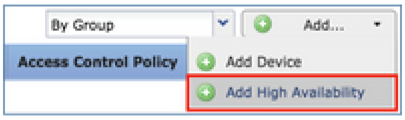
Entrambi i dispositivi FTD sono già registrati sull'FMC, come mostrato nell'immagine.



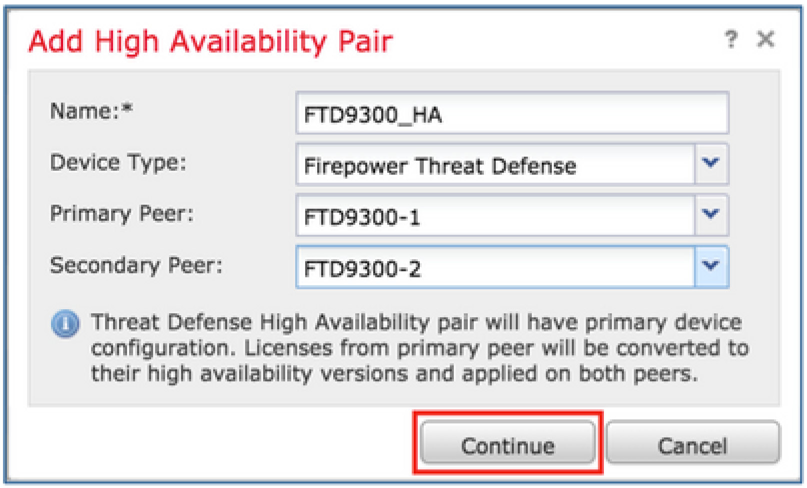
FTD9300-1
10.62.148.72 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed | Cisco Firepower 9000 Series SM-36 Thre | Base, Threat, Malware, URL Filt

FTD9300-2
10.62.148.69 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed | Cisco Firepower 9000 Series SM-36 Thre | Base, Threat, Malware, URL Filt

Passaggio 1. Per configurare il failover FTD, passare a **Dispositivi** > **Gestione dispositivi** e selezionare **Aggiungi alta disponibilità** come mostrato nell'immagine.



Passaggio 2. Immettere il **peer primario** e il **peer secondario**, quindi selezionare **Continue** (Continua) come mostrato nell'immagine.



Add High Availability Pair

Name:* FTD9300_HA
Device Type: Firepower Threat Defense
Primary Peer: FTD9300-1
Secondary Peer: FTD9300-2

Threat Defense High Availability pair will have primary device configuration. Licenses from primary peer will be converted to their high availability versions and applied on both peers.

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**.

Condizioni

Per creare una coppia HA tra 2 dispositivi FTD, è necessario soddisfare le seguenti condizioni:

- Stesso modello
- Stessa versione per FXOS e FTD - (stessa release principale (primo numero), secondaria (secondo numero) e di manutenzione (terzo numero))
- Stesso numero di interfacce
- Stesso tipo di interfacce
- Entrambe le periferiche fanno parte dello stesso gruppo/dominio in FMC
- Stessa configurazione del protocollo Network Time Protocol (NTP)
- I due dispositivi devono essere completamente implementati sull'FMC senza modifiche non confermate
- Modalità firewall uguale: instradato o trasparente.
- Controllare quanto sopra su entrambi i dispositivi FTD e sulla GUI FMC in quanto si sono verificati casi in cui gli FTD avevano lo stesso modello, ma ciò non si rifletteva sull'FMC.
- Il protocollo DHCP/Point-to-Point over Ethernet (PPPoE) non è configurato in alcuna interfaccia
- I nomi host (nome di dominio completo (FQDN)) devono essere diversi sui due chassis. Per controllare il nome host dello chassis, passare alla CLI FTD ed eseguire questo comando:

<#root>

```
firepower#

show chassis-management-url


https://

KSEC-FPR9K-1.cisco.com

:443//
```

Nota: nell'FTD successivo alla 6.3 usare il comando **'show chassis detail'**

<#root>

```
firepower#

show chassis detail

Chassis URL                 : https://KSEC-FPR4100-1:443//
Chassis IP                  : 192.0.2.1
Chassis Serial Number       : JMX12345678
Security Module             : 1
```

Se entrambi gli chassis hanno lo stesso nome, modificarne uno con questi comandi:

<#root>

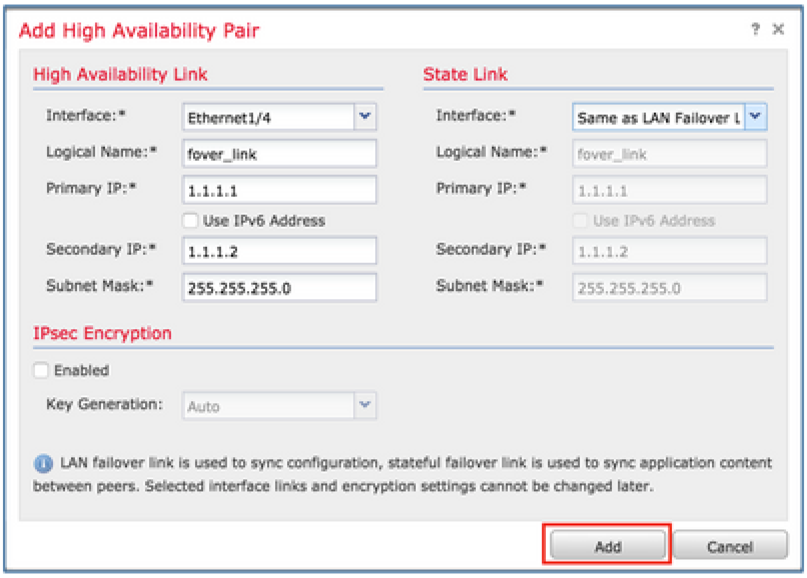
```
KSEC-FPR9K-1-A#

scope system

KSEC-FPR9K-1-A /system #

set name FPR9K-1new

Warning: System name modification changes FC zone name and redeploys them non-disruptively
KSEC-FPR9K-1-A /system* #

commit-buffer

FPR9K-1-A /system #

exit

FPR9K-1new-A

#
```

Dopo aver modificato il nome dello chassis, annullare la registrazione dell'FTD dall'FMC e registrarlo di nuovo. Quindi, procedere con la creazione della coppia HA.

Passaggio 3. Configurare HA e lo stato delle impostazioni dei collegamenti.

In questo caso, le impostazioni del collegamento dello stato sono le stesse del collegamento High Availability.

Selezionare **Add** (Aggiungi) e attendere alcuni minuti finché la coppia HA non viene implementata, come mostrato nell'immagine.



Add High Availability Pair

High Availability Link

Interface:* Ethernet1/4

Logical Name:* fover_link

Primary IP:* 1.1.1.1

□ Use IPv6 Address

Secondary IP:* 1.1.1.2

Subnet Mask:* 255.255.255.0

State Link

Interface:* Same as LAN Failover L

Logical Name:* fover_link

Primary IP:* 1.1.1.1

□ Use IPv6 Address

Secondary IP:* 1.1.1.2

Subnet Mask:* 255.255.255.0

IPsec Encryption

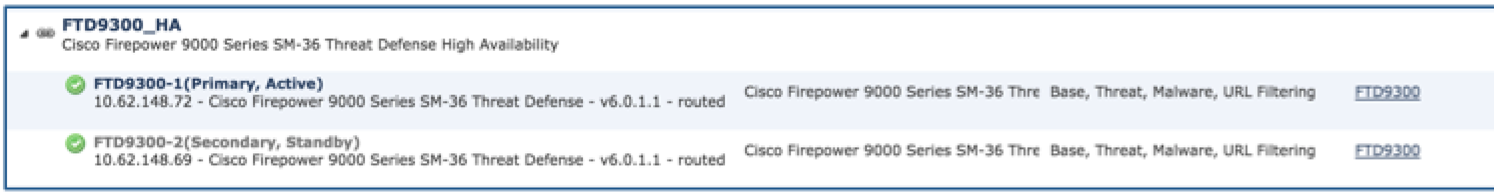
□ Enabled

Key Generation: Auto

LAN failover link is used to sync configuration, stateful failover link is used to sync application content between peers. Selected interface links and encryption settings cannot be changed later.

Passaggio 4. Configurare le interfacce dati (indirizzi IP primario e in standby)

Dalla GUI dell'FMC, selezionare sull'HA **Edit** (Modifica) come mostrato nell'immagine.

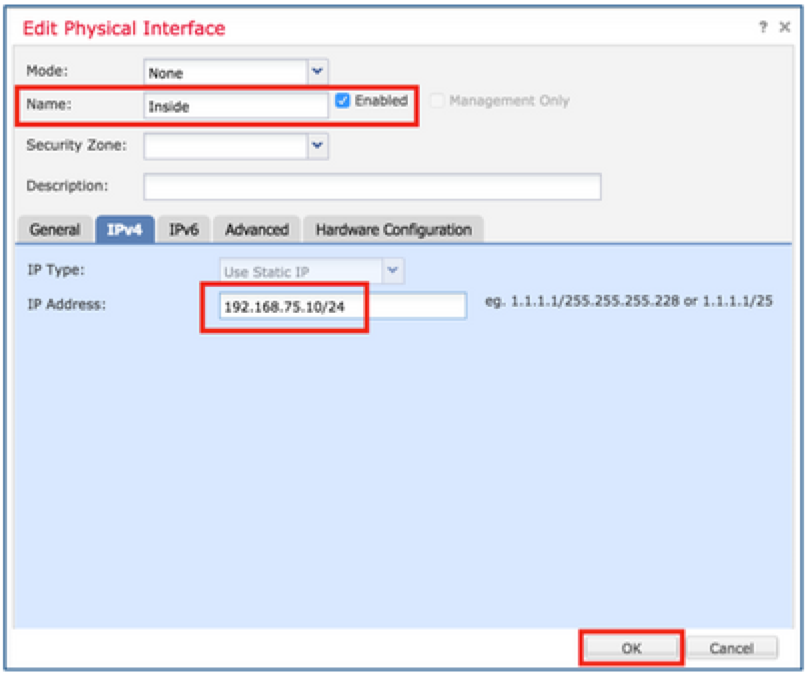


FTD9300_HA
Cisco Firepower 9000 Series SM-36 Threat Defense High Availability

FTD9300-1(Primary, Active) 10.62.148.72 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed	Cisco Firepower 9000 Series SM-36 Thre	Base, Threat, Malware, URL Filtering	FTD9300
FTD9300-2(Secondary, Standby) 10.62.148.69 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed	Cisco Firepower 9000 Series SM-36 Thre	Base, Threat, Malware, URL Filtering	FTD9300

Passaggio 5. Configurare le impostazioni dell'interfaccia come mostrato nelle immagini.

Interfaccia Ethernet 1/5.



Edit Physical Interface

Mode: None

Name: Inside ☑ Enabled □ Management Only

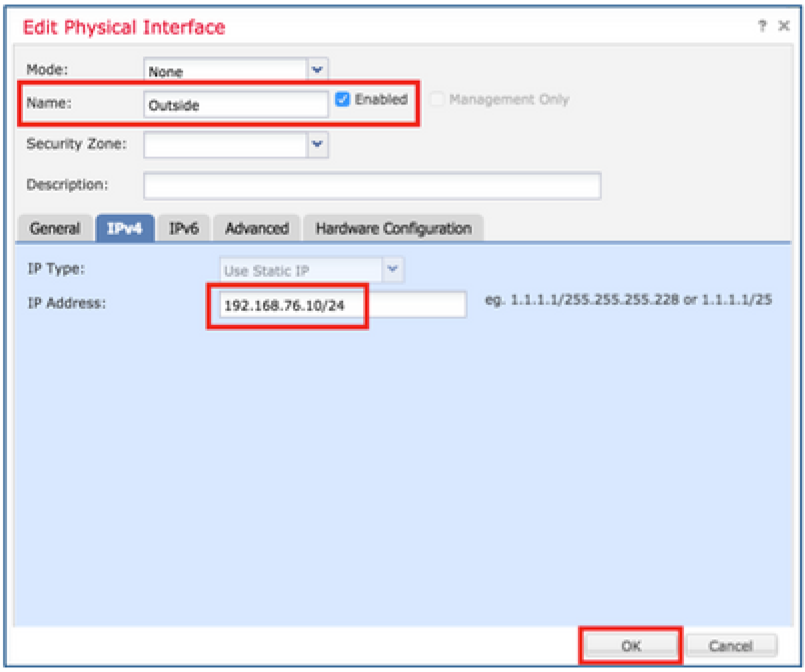
Security Zone:

Description:

IP Type: Use Static IP

IP Address: 192.168.75.10/24 eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25

Interfaccia Ethernet 1/6.



Edit Physical Interface

Mode: None

Name: Outside ☑ Enabled □ Management Only

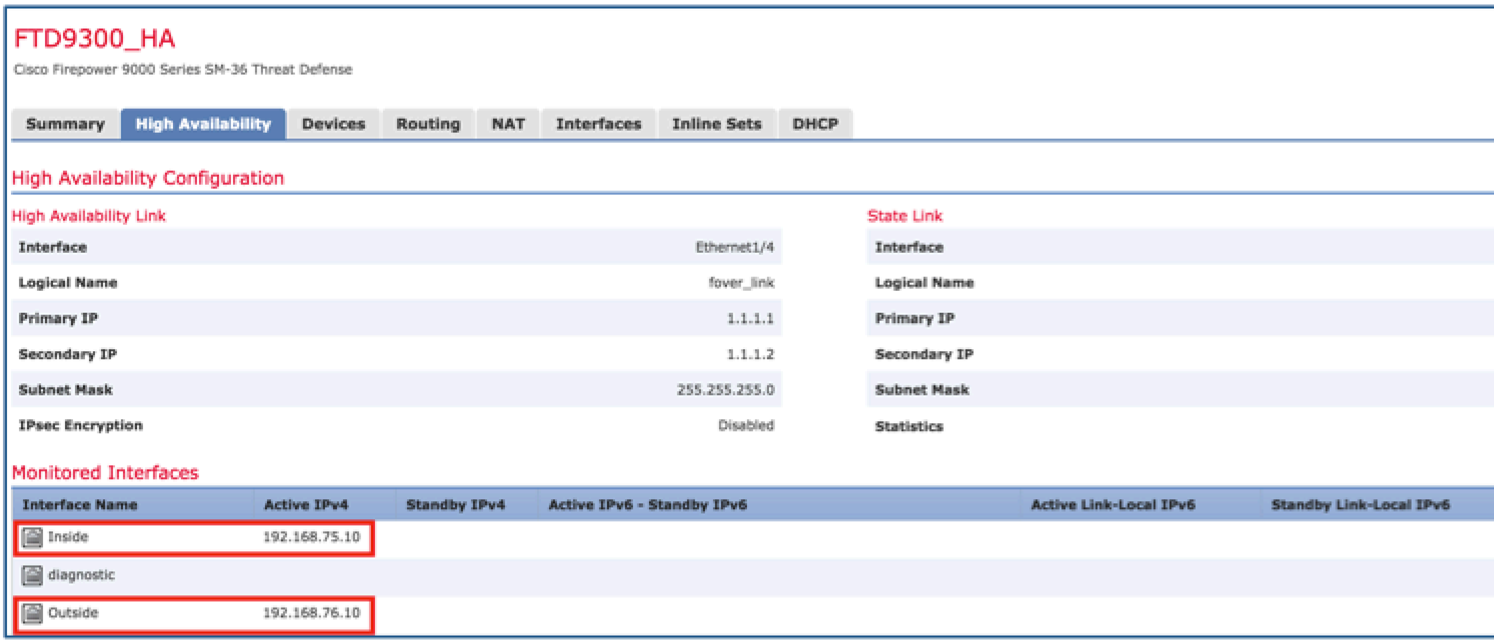
Security Zone:

Description:

IP Type: Use Static IP

IP Address: 192.168.76.10/24 eg. 1.1.1.1/255.255.255.228 or 1.1.1.1/25

Passaggio 6. Passare a **Alta disponibilità** e selezionare il nome dell'interfaccia **Modifica** per aggiungere gli indirizzi IP in standby, come mostrato nell'immagine.



FTD9300_HA

Cisco Firepower 9000 Series SM-36 Threat Defense

High Availability Configuration

High Availability Link

Interface	Ethernet1/4
Logical Name	fover_link
Primary IP	1.1.1.1
Secondary IP	1.1.1.2
Subnet Mask	255.255.255.0
IPsec Encryption	Disabled

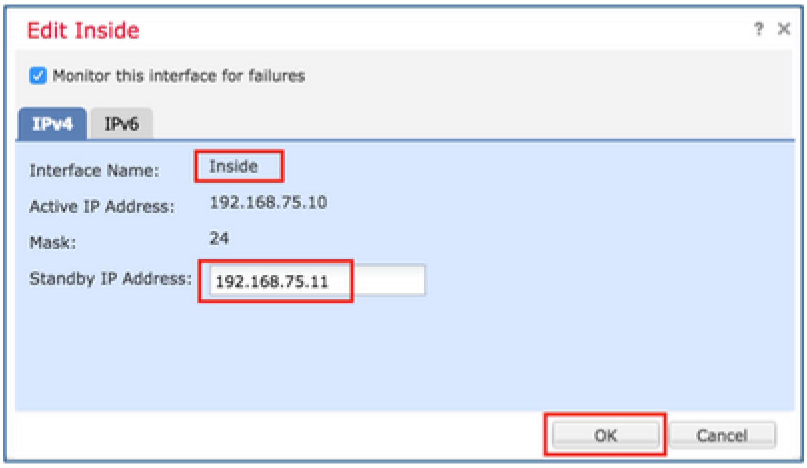
State Link

Interface
Logical Name
Primary IP
Secondary IP
Subnet Mask
Statistics

Monitored Interfaces

Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6
Inside	192.168.75.10				
diagnostic					
Outside	192.168.76.10				

Passaggio 7. Per l'interfaccia Inside come mostrato nell'immagine.



Edit Inside

☑ Monitor this interface for failures

Interface Name: Inside

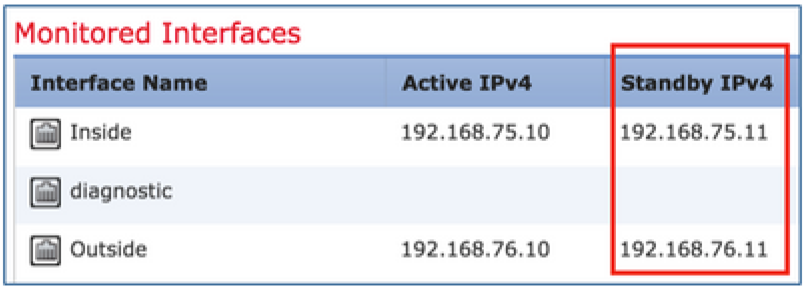
Active IP Address: 192.168.75.10

Mask: 24

Standby IP Address: 192.168.75.11

Passaggio 8. Ripetere l'operazione per l'interfaccia esterna.

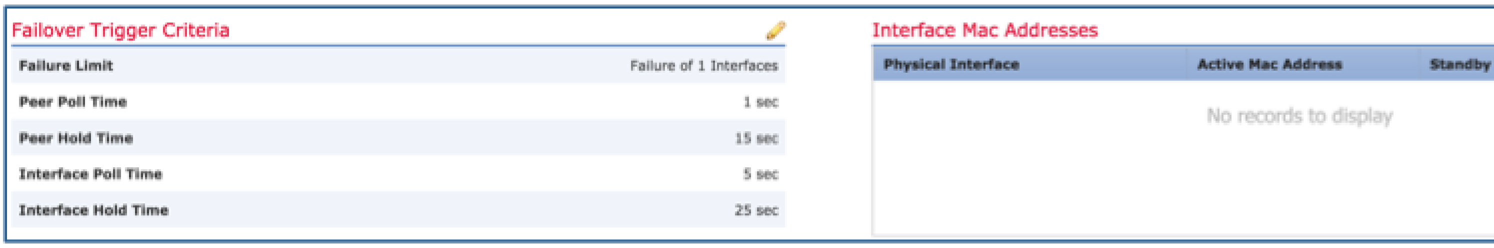
Passaggio 9. Verificare il risultato come mostrato nell'immagine.



Monitored Interfaces

Interface Name	Active IPv4	Standby IPv4
Inside	192.168.75.10	192.168.75.11
diagnostic		
Outside	192.168.76.10	192.168.76.11

Passaggio 10. Rimanere nella scheda Alta disponibilità e configurare gli indirizzi MAC virtuali come mostrato nell'immagine.



Failover Trigger Criteria

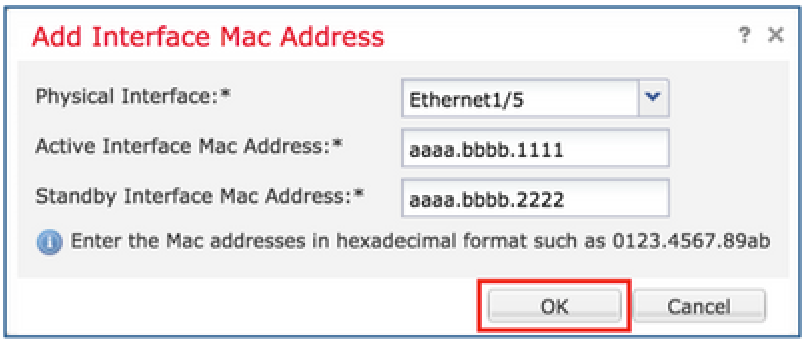
Failure Limit	Failure of 1 Interfaces
Peer Poll Time	1 sec
Peer Hold Time	15 sec
Interface Poll Time	5 sec
Interface Hold Time	25 sec

Interface Mac Addresses

Physical Interface	Active Mac Address	Standby

No records to display

Passaggio 11. Per l'interfaccia interna è come mostrato nell'immagine.



Add Interface Mac Address

Physical Interface:* Ethernet1/5

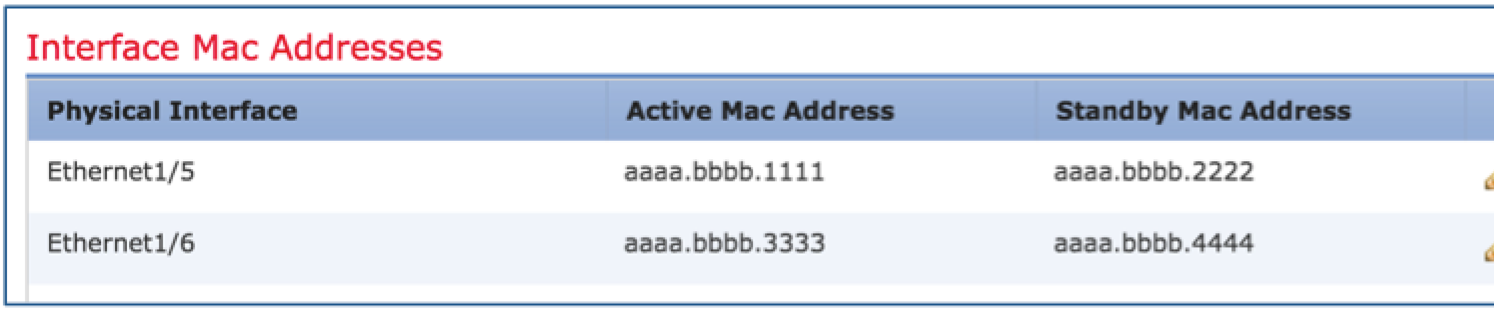
Active Interface Mac Address:* aaaa.bbbb.1111

Standby Interface Mac Address:* aaaa.bbbb.2222

Enter the Mac addresses in hexadecimal format such as 0123.4567.89ab

Passaggio 12. Ripetere l'operazione per l'interfaccia esterna.

Passaggio 13. Verificare il risultato come mostrato nell'immagine.



Interface Mac Addresses

Physical Interface	Active Mac Address	Standby Mac Address
Ethernet1/5	aaaa.bbbb.1111	aaaa.bbbb.2222
Ethernet1/6	aaaa.bbbb.3333	aaaa.bbbb.4444

Passaggio 14. Dopo aver configurato le modifiche, selezionare **Salva** e distribuisci.

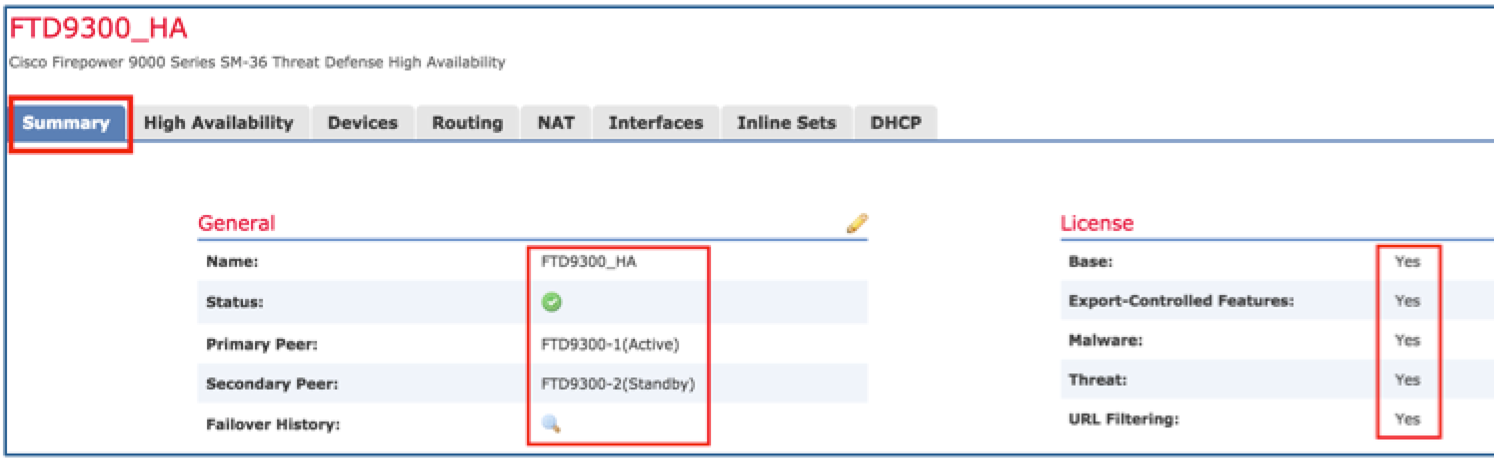
Attività 3. Verifica FTD HA e licenza

Attività richiesta:

Verificare le impostazioni HA della coppia di FTD e le licenze abilitate dalla GUI dell'FMC e dalla CLI degli FTD.

Soluzione:

Passaggio 1. Passare a **Riepilogo** e controllare le impostazioni HA e le licenze abilitate come mostrato nell'immagine.



FTD9300_HA

Cisco Firepower 9000 Series SM-36 Threat Defense High Availability

General

Name:	FTD9300_HA
Status:	✓
Primary Peer:	FTD9300-1(Active)
Secondary Peer:	FTD9300-2(Standby)
Failover History:	

License

Base:	Yes
Export-Controlled Features:	Yes
Malware:	Yes
Threat:	Yes
URL Filtering:	Yes

Passaggio 2. Dalla CLI di FTD CLISH, eseguire i seguenti comandi:

```
<#root>

>

show high-availability config

Failover

On

Failover unit

Primary

Failover LAN Interface:

fover_link Ethernet1/4 (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 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.6(1), Mate 9.6(1)
Serial Number: Ours FLM19267A63, Mate FLM19206H7T
Last Failover at: 18:32:38 EEST Jul 21 2016
    This host: Primary - Active
        Active time: 3505 (sec)
        slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(1)) status (Up Sys)
          Interface diagnostic (0.0.0.0): Normal (Waiting)
        slot 1: snort rev (1.0)  status (up)
        slot 2: diskstatus rev (1.0)  status (up)
    Other host: Secondary - Standby Ready
        Active time: 172 (sec)
        slot 0: UCSB-B200-M3-U hw/sw rev (0.0/9.6(1)) status (Up Sys)
          Interface diagnostic (0.0.0.0): Normal (Waiting)
        slot 1: snort rev (1.0)  status (up)
        slot 2: diskstatus rev (1.0)  status (up)

Stateful Failover Logical Update Statistics
    Link : fover_link Ethernet1/4 (up)
    Stateful Obj     xmit       xerr       rcv        rerr
    General        417        0          416        0
    sys cmd      416        0          416        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
    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

    Logical Update Queue Information
              Cur     Max     Total
    Recv Q:     0     10     416
    Xmit Q:     0     11     2118

>
```

Passaggio 3. Eseguire la stessa operazione sul dispositivo secondario.

Passaggio 4. Eseguire il comando **show failover state** dalla CLI di LINA:

<#root>

```
firepower#
```

```
show failover state
```

```
               State          Last Failure Reason      Date/Time
This host  -   Primary
               Active         None
Other host -   Secondary
               Standby Ready  Comm Failure             18:32:56 EEST Jul 21 2016

====Configuration State===
    Sync Done
====Communication State===
    Mac set

firepower#
```

Passaggio 5. Verificare la configurazione dall'unità principale (LINA CLI):

<#root>

```
firepower#
```

```
show running-config failover
```

```
failover
failover lan unit primary
failover lan interface fover_link Ethernet1/4
failover replication http
failover mac address Ethernet1/5
```

```
aaaa.bbbb.1111 aaaa.bbbb.2222
```

```
failover mac address Ethernet1/6
```

```
aaaa.bbbb.3333 aaaa.bbbb.4444
```

```
failover link fover_link Ethernet1/4
failover interface ip fover_link 10.10.1.1 255.255.255.0 standby 10.10.1.2
firepower#

firepower#
```

```
show running-config interface
```

```
!
interface Ethernet1/2
 management-only
 nameif diagnostic
 security-level 0
 no ip address
!
interface Ethernet1/4
```

```
 description LAN/STATE Failover Interface
!
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

firepower#
```

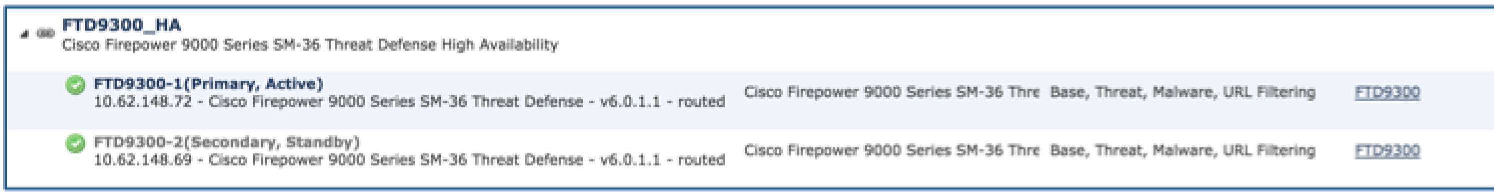
Attività 4. Cambia ruoli di failover

Attività richiesta:

Dall'FMC, invertire i ruoli di failover da Principale/Attivo, Secondario/Standby a Principale/Standby, Secondario/Attivo

Soluzione:

Passaggio 1. Selezionate l'icona come mostrato nell'immagine.

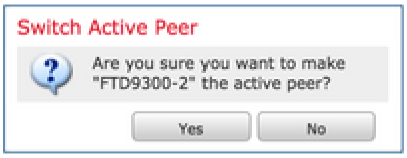


FTD9300_HA
Cisco Firepower 9000 Series SM-36 Threat Defense High Availability

FTD9300-1(Primary, Active)
10.62.148.72 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed | Cisco Firepower 9000 Series SM-36 Thre | Base, Threat, Malware, URL Filtering | FTD9300

FTD9300-2(Secondary, Standby)
10.62.148.69 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed | Cisco Firepower 9000 Series SM-36 Thre | Base, Threat, Malware, URL Filtering | FTD9300

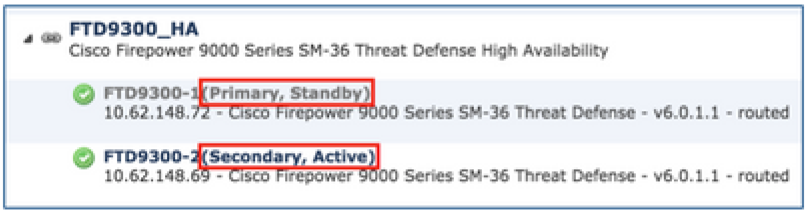
Passaggio 2. Confermare l'azione sulla finestra popup come mostrato nell'immagine.



Switch Active Peer

Are you sure you want to make "FTD9300-2" the active peer?

Passaggio 3. Verificare il risultato come mostrato nell'immagine.



FTD9300_HA
Cisco Firepower 9000 Series SM-36 Threat Defense High Availability

FTD9300-1(Primary, Standby)
10.62.148.72 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed

FTD9300-2(Secondary, Active)
10.62.148.69 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed

Dalla CLI LINA, è possibile verificare che il comando **no failover active** è stato eseguito sull'unità Principale/Attiva:

<#root>

```
Jul 22 2016 10:39:26: %ASA-5-111008: User 'enable_15' executed the '

no failover active

' command.
Jul 22 2016 10:39:26: %ASA-5-111010: User 'enable_15', running 'N/A' from IP 0.0.0.0, executed 'no failo
```

È possibile usare anche il comando **show failover history**:

<#root>

```
firepower#

show failover history

==========================================================================
From State                 To State                   Reason
10:39:26 EEST Jul 22 2016
Active                     Standby Ready              Set by the config command
```

Passaggio 4. Dopo la verifica, riattivare l'unità principale.

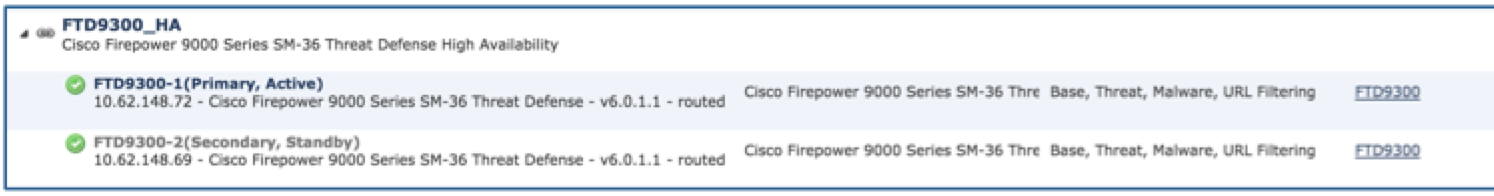
Attività 5. Interrompere la coppia HA

Attività richiesta:

Dall'FMC, separare la coppia di failover.

Soluzione:

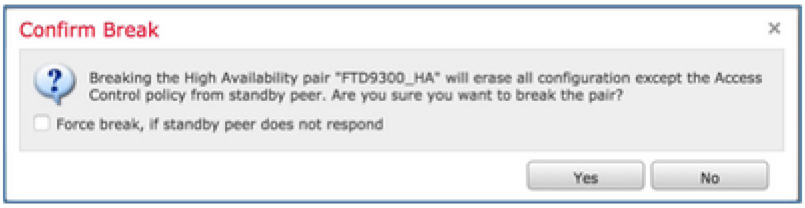
Passaggio 1. Selezionate l'icona come mostrato nell'immagine.



FTD9300_HA
Cisco Firepower 9000 Series SM-36 Threat Defense High Availability

FTD9300-1(Primary, Active) 10.62.148.72 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed	Cisco Firepower 9000 Series SM-36 Thre	Base, Threat, Malware, URL Filtering	FTD9300
FTD9300-2(Secondary, Standby) 10.62.148.69 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed	Cisco Firepower 9000 Series SM-36 Thre	Base, Threat, Malware, URL Filtering	FTD9300

Passaggio 2. Controllare la notifica come mostrato nell'immagine.

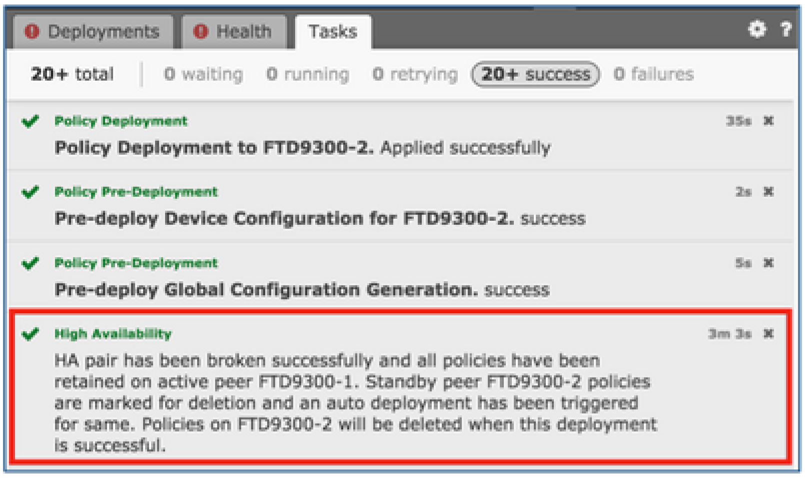


Confirm Break

Breaking the High Availability pair "FTD9300_HA" will erase all configuration except the Access Control policy from standby peer. Are you sure you want to break the pair?

□ Force break, if standby peer does not respond

Passaggio 3. Osservate il messaggio come mostrato nell'immagine.



20+ total | 0 waiting 0 running 0 retrying 20+ success 0 failures

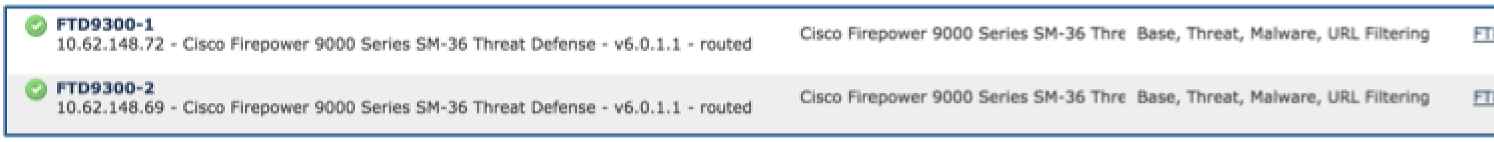
✓ **Policy Deployment** 35s ✖
Policy Deployment to FTD9300-2. Applied successfully

✓ **Policy Pre-Deployment** 2s ✖
Pre-deploy Device Configuration for FTD9300-2. success

✓ **Policy Pre-Deployment** 5s ✖
Pre-deploy Global Configuration Generation. success

✓ **High Availability** 3m 3s ✖
HA pair has been broken successfully and all policies have been retained on active peer FTD9300-1. Standby peer FTD9300-2 policies are marked for deletion and an auto deployment has been triggered for same. Policies on FTD9300-2 will be deleted when this deployment is successful.

Passaggio 4. Verificare il risultato dall'interfaccia utente di FMC, come mostrato nell'immagine.



✓ **FTD9300-1** 10.62.148.72 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed	Cisco Firepower 9000 Series SM-36 Thre	Base, Threat, Malware, URL Filtering	FT
✓ **FTD9300-2** 10.62.148.69 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed	Cisco Firepower 9000 Series SM-36 Thre	Base, Threat, Malware, URL Filtering	FT

Output del comando show running-config sull'unità Principale prima e dopo la separazione della coppia HA:

Prima della separazione della coppia HA	**Dopo la sepa**
firepower# sh run : Saved : : Serial Number: FLM19267A63 : Hardware: FPR9K-SM-36, 135839 MB RAM, CPU Xeon E5 series 2294 MHz, 2 CPUs (72 cores) :	firepower# s : Saved : : Serial Num : Hardware: :

NGFW Version 10.10.1.1	NGFW Vers
!	!
hostname firepower	hostname fir
enable password 8Ry2YjIyt7RRXU24 encrypted	enable passw
names	names
!	!
interface Ethernet1/2	interface Eth
management-only	management
nameif diagnostic	nameif diagn
security-level 0	security-leve
no ip address	no ip addres

!	!
interface Ethernet1/4	**interface Et**
description LAN/STATE Failover Interface	**no nameif**
!	**no security-**
interface Ethernet1/5	**no ip addres**
nameif Inside	!
security-level 0	interface Eth
ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11	nameif Insid
!	security-leve
interface Ethernet1/6	ip address 19
nameif Outside	!
security-level 0	interface Eth

ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11	nameif Outsi
!	security-leve
ftp mode passive	ip address 19
ngips conn-match vlan-id	!
access-list CSM_FW_ACL_ remark rule-id 268447744: ACCESS POLICY: FTD9300 - Mandatory/1	ftp mode pas
access-list CSM_FW_ACL_ remark rule-id 268447744: L4 RULE: Allow_ICMP	ngips conn-n
access-list CSM_FW_ACL_ advanced permit icmp any any rule-id 268447744 event-log both	access-list C
access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: FTD9300 - Default/1	access-list C
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: DEFAULT ACTION RULE	access-list C
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268441600	access-list C
!	access-list C

tcp-map UM_STATIC_TCP_MAP	access-list C
tcp-options range 6 7 allow	!
tcp-options range 9 255 allow	tcp-map UM
urgent-flag allow	tcp-options r
!	tcp-options r
no pager	urgent-flag a
logging enable	!
logging timestamp	no pager
logging standby	logging enab
logging buffer-size 100000	logging time
logging buffered debugging	logging stand
logging flash-minimum-free 1024	logging buffe

logging flash-maximum-allocation 3076	logging buff
mtu diagnostic 1500	logging flash
mtu Inside 1500	logging flash
mtu Outside 1500	mtu diagnost
failover	mtu Inside 1
failover lan unit primary	mtu Outside
failover lan interface fover_link Ethernet1/4	**no failover**
failover replication http	**no monitor-**
failover mac address Ethernet1/5 aaaa.bbbb.1111 aaaa.bbbb.2222	icmp unreach
failover mac address Ethernet1/6 aaaa.bbbb.3333 aaaa.bbbb.4444	no asdm hist
failover link fover_link Ethernet1/4	arp timeout 1

failover interface ip fover_link 10.10.1.1 255.255.255.0 standby 10.10.1.2	no arp permi
icmp unreachable rate-limit 1 burst-size 1	access-group
no asdm history enable	timeout xlate
arp timeout 14400	timeout pat-x
no arp permit-nonconnected	timeout conn
access-group CSM_FW_ACL_ global	timeout sunr
timeout xlate 3:00:00	timeout sip 0
timeout pat-xlate 0:00:30	timeout sip-p
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02	timeout tcp-p
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00	timeout float
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00	aaa proxy-lin
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute	no snmp-serv

timeout tcp-proxy-reassembly 0:00:30	no snmp-serv
timeout floating-conn 0:00:00	no snmp-serv
aaa proxy-limit disable	crypto ipsec
no snmp-server location	crypto ca tru
no snmp-server contact	telnet timeou
no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart	ssh stricthost
crypto ipsec security-association pmtu-aging infinite	ssh timeout 5
crypto ca trustpool policy	ssh key-exch
telnet timeout 5	console time
ssh stricthostkeycheck	dynamic-acc
ssh timeout 5	!

ssh key-exchange group dh-group1-sha1	class-map in
console timeout 0	match defaul
dynamic-access-policy-record DfltAccessPolicy	!
!	!
class-map inspection_default	policy-map t
match default-inspection-traffic	parameters
!	message-leng
!	message-leng
policy-map type inspect dns preset_dns_map	policy-map t
parameters	parameters
message-length maximum client auto	eool action a
message-length maximum 512	nop action al

policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP	router-alert a
parameters	policy-map g
eool action allow	class inspecti
nop action allow	inspect dns p
router-alert action allow	inspect ftp
policy-map global_policy	inspect h323
class inspection_default	inspect h323
inspect dns preset_dns_map	inspect rsh
inspect ftp	inspect rtsp
inspect h323 h225	inspect sqlne
inspect h323 ras	inspect skinn

inspect rsh	inspect sunrp
inspect rtsp	inspect xdmc
inspect sqlnet	inspect sip
inspect skinny	inspect netbi
inspect sunrpc	inspect tftp
inspect xdmcp	inspect icmp
inspect sip	inspect icmp
inspect netbios	inspect dcerp
inspect tftp	inspect ip-op
inspect icmp	class class-de
inspect icmp error	set connectio
inspect dcerpc	!

inspect ip-options UM_STATIC_IP_OPTIONS_MAP class class-default set connection advanced-options UM_STATIC_TCP_MAP ! service-policy global_policy global prompt hostname context call-home profile CiscoTAC-1 no active destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService destination address email callhome@cisco.com	service-polic prompt hostn call-home profile Cisco no active destination a destination a destination tr subscribe-to- subscribe-to- subscribe-to-

destination transport-method http subscribe-to-alert-group diagnostic subscribe-to-alert-group environment subscribe-to-alert-group inventory periodic monthly subscribe-to-alert-group configuration periodic monthly subscribe-to-alert-group telemetry periodic daily Cryptochecksum:933c594fc0264082edc0f24bad358031 : end firepower#	subscribe-to- subscribe-to- Cryptocheck : end firepower#

Output del comando show running-config sull'unità Secondaria prima e dopo la separazione della coppia HA mostrato nella tabella.

Prima della separazione della coppia HA	**Dopo la sepa**
firepower# sh run : Saved	firepower# s : Saved

:	:
: Serial Number: FLM19206H7T	: Serial Num
: Hardware: FPR9K-SM-36, 135841 MB RAM, CPU Xeon E5 series 2294 MHz, 2 CPUs (72 cores)	: Hardware:
:	:
NGFW Version 10.10.1.1	NGFW Vers
!	!
hostname firepower	hostname fir
enable password 8Ry2YjIyt7RRXU24 encrypted	enable passw
names	names
!	!
interface Ethernet1/2	interface Eth
management-only	management

nameif diagnostic	nameif diagn
security-level 0	security-leve
no ip address	no ip address
!	!
interface Ethernet1/4	**interface Et**
description LAN/STATE Failover Interface	**shutdown**
!	**no nameif**
interface Ethernet1/5	**no security-**
nameif Inside	**no ip addres**
security-level 0	**!**
ip address 192.168.75.10 255.255.255.0 standby 192.168.75.11	**interface Et**

!	**shutdown**
interface Ethernet1/6	**no nameif**
nameif Outside	**no security-**
security-level 0	**no ip addres**
ip address 192.168.76.10 255.255.255.0 standby 192.168.76.11	**!**
!	**interface Et**
ftp mode passive	**shutdown**
ngips conn-match vlan-id	**no nameif**
access-list CSM_FW_ACL_ remark rule-id 268447744: ACCESS POLICY: FTD9300 - Mandatory/1	**no security-**
access-list CSM_FW_ACL_ remark rule-id 268447744: L4 RULE: Allow_ICMP	**no ip addres**
access-list CSM_FW_ACL_ advanced permit icmp any any rule-id 268447744 event-log both	!
access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: FTD9300 - Default/1	ftp mode pas

access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: DEFAULT ACTION RULE	ngips conn-m
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268441600	access-list C
!	access-list C
tcp-map UM_STATIC_TCP_MAP	access-list C
tcp-options range 6 7 allow	access-list C
tcp-options range 9 255 allow	access-list C
urgent-flag allow	access-list C
!	!
no pager	tcp-map UM
logging enable	tcp-options r
logging timestamp	tcp-options r

logging standby	urgent-flag a
logging buffer-size 100000	!
logging buffered debugging	no pager
logging flash-minimum-free 1024	**no logging n**
logging flash-maximum-allocation 3076	**no logging n**
mtu diagnostic 1500	**no logging n**
mtu Inside 1500	**no logging n**
mtu Outside 1500	**no logging n**
failover	**no logging n**
failover lan unit secondary	**no logging n**
failover lan interface fover_link Ethernet1/4	**no logging n**
failover replication http	**no logging n**

failover mac address Ethernet1/5 aaaa.bbbb.1111 aaaa.bbbb.2222	**no logging n**
failover mac address Ethernet1/6 aaaa.bbbb.3333 aaaa.bbbb.4444	**no logging n**
failover link fover_link Ethernet1/4	**no logging n**
failover interface ip fover_link 10.10.1.1 255.255.255.0 standby 10.10.1.2	**no logging n**
icmp unreachable rate-limit 1 burst-size 1	**no logging n**
no asdm history enable	mtu diagnost
arp timeout 14400	**no failover**
no arp permit-nonconnected	**no monitor-**
access-group CSM_FW_ACL_ global	icmp unreach
timeout xlate 3:00:00	no asdm hist
timeout pat-xlate 0:00:30	arp timeout 1

timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02	no arp permi
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00	access-group
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00	timeout xlate
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute	timeout pat-x
timeout tcp-proxy-reassembly 0:00:30	timeout conn
timeout floating-conn 0:00:00	timeout sunr
user-identity default-domain LOCAL	timeout sip 0
aaa proxy-limit disable	timeout sip-p
no snmp-server location	timeout tcp-p
no snmp-server contact	timeout float
no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart	aaa proxy-lin
crypto ipsec security-association pmtu-aging infinite	no snmp-serv

crypto ca trustpool policy telnet timeout 5 ssh stricthostkeycheck ssh timeout 5 ssh key-exchange group dh-group1-sha1 console timeout 0 dynamic-access-policy-record DfltAccessPolicy ! class-map inspection_default match default-inspection-traffic !	no snmp-serv no snmp-serv crypto ipsec crypto ca tru telnet timeou ssh stricthost ssh timeout 5 ssh key-exch console time dynamic-acc !

!	class-map ins
policy-map type inspect dns preset_dns_map	match defaul
parameters	!
message-length maximum client auto	!
message-length maximum 512	policy-map t
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP	parameters
parameters	message-leng
eool action allow	message-leng
nop action allow	policy-map t
router-alert action allow	parameters
policy-map global_policy	eool action a
class inspection_default	nop action al

inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip	router-alert a policy-map g class inspect inspect dns p inspect ftp inspect h323 inspect h323 inspect rsh inspect rtsp inspect sqlne inspect skinn

inspect netbios	inspect sunrp
inspect tftp	inspect xdmc
inspect icmp	inspect sip
inspect icmp error	inspect netbi
inspect dcerpc	inspect tftp
inspect ip-options UM_STATIC_IP_OPTIONS_MAP	inspect icmp
class class-default	inspect icmp
set connection advanced-options UM_STATIC_TCP_MAP	inspect dcerp
!	inspect ip-op
service-policy global_policy global	class class-de
prompt hostname context	set connectio
call-home	!

profile CiscoTAC-1	service-polic
no active	prompt hostr
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService	call-home
destination address email callhome@cisco.com	profile Cisco
destination transport-method http	no active
subscribe-to-alert-group diagnostic	destination a
subscribe-to-alert-group environment	destination a
subscribe-to-alert-group inventory periodic monthly	destination tr
subscribe-to-alert-group configuration periodic monthly	subscribe-to-
subscribe-to-alert-group telemetry periodic daily	subscribe-to-
Cryptochecksum:e648f92dd7ef47ee611f2aaa5c6cbd84	subscribe-to-

: end firepower#	subscribe-to- subscribe-to- Cryptocheck : end firepower#

Considerazioni principali per la separazione della coppia HA:

Unità Principale	Unità Secondaria
Tutta la configurazione di failover è stata rimossa Gli indirizzi IP in standby rimangono	Tutta la configurazione è stata rimossa

Passaggio 5. Al termine dell'operazione, ricreare la coppia HA.

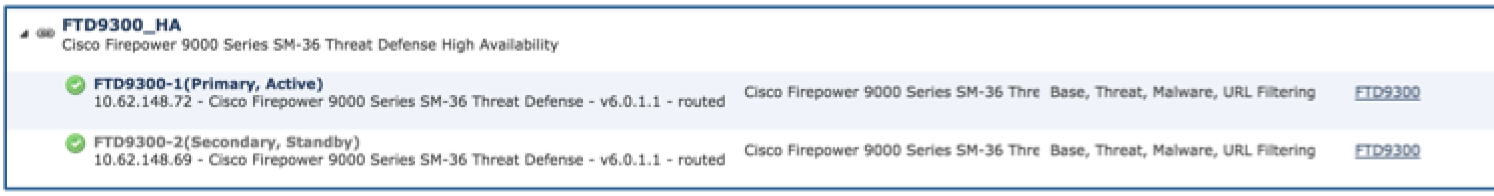
Attività 6. Disabilita coppia HA

Attività richiesta:

Dall'FMC, disabilitare la coppia di failover.

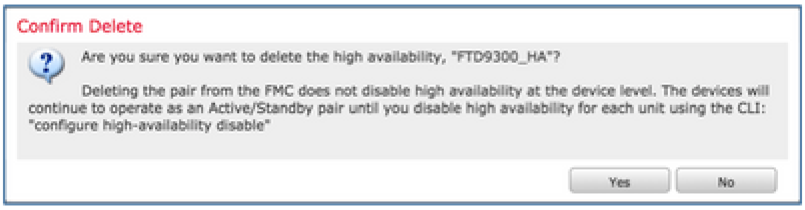
Soluzione:

Passaggio 1. Selezionate l'icona come mostrato nell'immagine.



FTD9300_HA Cisco Firepower 9000 Series SM-36 Threat Defense High Availability			
FTD9300-1(Primary, Active) 10.62.148.72 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed	Cisco Firepower 9000 Series SM-36 Thre	Base, Threat, Malware, URL Filtering	FTD9300
FTD9300-2(Secondary, Standby) 10.62.148.69 - Cisco Firepower 9000 Series SM-36 Threat Defense - v6.0.1.1 - routed	Cisco Firepower 9000 Series SM-36 Thre	Base, Threat, Malware, URL Filtering	FTD9300

Passaggio 2. Controllare la notifica e confermare come mostrato nell'immagine.



Confirm Delete

Are you sure you want to delete the high availability, "FTD9300_HA"?

Deleting the pair from the FMC does not disable high availability at the device level. The devices will continue to operate as an Active/Standby pair until you disable high availability for each unit using the CLI: "configure high-availability disable"

Passaggio 3. Dopo aver eliminato l'HA, entrambe le periferiche vengono rimosse dalla FMC.

Output del comando show running-config dalla CLI LINA:

Unità Principale	**Unità Secon**
firepower# sh run : Saved : : Serial Number: FLM19267A63 : Hardware: FPR9K-SM-36, 135839 MB RAM, CPU Xeon E5 series 2294 MHz, 2 CPUs (72 cores) : NGFW Version 10.10.1.1 ! hostname firepower	firepower# s : Saved : : Serial Num : Hardware: : NGFW Vers ! hostname fir

enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet1/2 management-only nameif diagnostic security-level 0 no ip address ! interface Ethernet1/4 description LAN/STATE Failover Interface	enable passw names ! interface Eth management nameif diagn security-leve no ip address ! interface Eth description L

! 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** ! ftp mode passive	! interface Eth nameif Insid security-leve **ip address 1** ! interface Eth nameif Outsi security-leve **ip address 1** ! ftp mode pas

ngips conn-match vlan-id access-list CSM_FW_ACL_ remark rule-id 268447744: ACCESS POLICY: FTD9300 - Mandatory/1 access-list CSM_FW_ACL_ remark rule-id 268447744: L4 RULE: Allow_ICMP access-list CSM_FW_ACL_ advanced permit icmp any any rule-id 268447744 event-log both access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: FTD9300 - Default/1 access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: DEFAULT ACTION RULE access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268441600 ! tcp-map UM_STATIC_TCP_MAP tcp-options range 6 7 allow tcp-options range 9 255 allow	ngips conn-m access-list C access-list C access-list C access-list C access-list C access-list C ! tcp-map UM tcp-options r tcp-options r

urgent-flag allow	urgent-flag a
!	!
no pager	no pager
logging enable	logging enab
logging timestamp	logging time
logging standby	logging stanc
logging buffer-size 100000	logging buffe
logging buffered debugging	logging buffe
logging flash-minimum-free 1024	logging flash
logging flash-maximum-allocation 3076	logging flash
mtu diagnostic 1500	mtu diagnost
mtu Inside 1500	mtu Inside 1

mtu Outside 1500 **failover** **failover lan unit primary** **failover lan interface fover_link Ethernet1/4** **failover replication http** **failover mac address Ethernet1/5 aaaa.bbbb.1111 aaaa.bbbb.2222** **failover mac address Ethernet1/6 aaaa.bbbb.3333 aaaa.bbbb.4444** **failover link fover_link Ethernet1/4** **failover interface ip fover_link 10.10.1.1 255.255.255.0 standby 10.10.1.2** icmp unreachable rate-limit 1 burst-size 1 no asdm history enable	mtu Outside **failover** **failover lan** **failover lan** **failover repl** **failover mac** **failover mac** **failover link** **failover inte** icmp unreach no asdm hist

arp timeout 14400	arp timeout 1
no arp permit-nonconnected	no arp permi
access-group CSM_FW_ACL_ global	access-group
timeout xlate 3:00:00	timeout xlate
timeout pat-xlate 0:00:30	timeout pat-x
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02	timeout conn
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00	timeout sunr
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00	timeout sip 0
timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute	timeout sip-p
timeout tcp-proxy-reassembly 0:00:30	timeout tcp-p
timeout floating-conn 0:00:00	timeout float
aaa proxy-limit disable	user-identity

no snmp-server location no snmp-server contact no snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart crypto ipsec security-association pmtu-aging infinite crypto ca trustpool policy telnet timeout 5 ssh stricthostkeycheck ssh timeout 5 ssh key-exchange group dh-group1-sha1 console timeout 0 dynamic-access-policy-record DfltAccessPolicy	aaa proxy-lin no snmp-serv no snmp-serv no snmp-serv crypto ipsec crypto ca tru telnet timeou ssh stricthost ssh timeout 5 ssh key-exch console time

!	dynamic-acc
class-map inspection_default	!
match default-inspection-traffic	class-map ins
!	match defaul
!	!
policy-map type inspect dns preset_dns_map	!
parameters	policy-map t
message-length maximum client auto	parameters
message-length maximum 512	message-leng
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP	message-leng
parameters	policy-map t
eool action allow	parameters

nop action allow router-alert action allow policy-map global_policy class inspection_default inspect dns preset_dns_map inspect ftp inspect h323 h225 inspect h323 ras inspect rsh inspect rtsp inspect sqlnet	eool action a nop action al router-alert a policy-map g class inspecti inspect dns p inspect ftp inspect h323 inspect h323 inspect rsh inspect rtsp

inspect skinny	inspect sqlne
inspect sunrpc	inspect skinn
inspect xdmcp	inspect sunrp
inspect sip	inspect xdmc
inspect netbios	inspect sip
inspect tftp	inspect netbi
inspect icmp	inspect tftp
inspect icmp error	inspect icmp
inspect dcerpc	inspect icmp
inspect ip-options UM_STATIC_IP_OPTIONS_MAP	inspect dcerp
class class-default	inspect ip-op
set connection advanced-options UM_STATIC_TCP_MAP	class class-de

!	set connectio
service-policy global_policy global	!
prompt hostname context	service-polic
call-home	prompt hostn
profile CiscoTAC-1	call-home
no active	profile Cisco
destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService	no active
destination address email callhome@cisco.com	destination a
destination transport-method http	destination a
subscribe-to-alert-group diagnostic	destination tr
subscribe-to-alert-group environment	subscribe-to-

subscribe-to-alert-group inventory periodic monthly subscribe-to-alert-group configuration periodic monthly subscribe-to-alert-group telemetry periodic daily Cryptochecksum:933c594fc0264082edc0f24bad358031 : end firepower#	subscribe-to- subscribe-to- subscribe-to- subscribe-to- Cryptocheck : end firepower#

Passaggio 4. La registrazione di entrambi i dispositivi FTD è stata annullata dal CCP:

```
<#root>
> show managers
No managers configured.
```

Considerazioni principali per la disabilitazione della coppia HA nell'FMC:

Unità Principale	**Unità Secondaria**
Il dispositivo viene rimosso dall'FMC. Nessuna configurazione rimossa dal dispositivo FTD	Il dispositivo viene rimosso dall'FMC. Nessuna configurazione rimossa dal dispositivo FTD

Passaggio 5. Eseguire questo comando per rimuovere la configurazione del failover dai dispositivi FTD:

```
<#root>
>
```

```
configure high-availability disable

High-availability will be disabled. Do you really want to continue?
Please enter 'YES' or 'NO':

yes

Successfully disabled high-availability.
```

Nota: è necessario eseguire il comando su entrambe le unità

Il risultato:

Unità Principale	**Unità Secondaria**
> **show failover** **Failover Off** Failover unit Secondary Failover LAN Interface: not Configured 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 2 of 1041 maximum MAC Address Move Notification Interval not set >	> **show failover** **Failover Off (pseudo-Standby)** Failover unit Secondary Failover LAN Interface: FOVER Ethernet1/3.205 (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 0 of 1041 maximum MAC Address Move Notification Interval not set failover replication http >

Primario	**Secon**
firepower# show run ! hostname firepower	firepo ! hostn

enable password 8Ry2YjIyt7RRXU24 encrypted names arp timeout 14400 no arp permit-nonconnected arp rate-limit 16384 ! interface GigabitEthernet1/1 nameif outside cts manual propagate sgt preserve-untag	enabl name arp ti no ar arp ra ! interf shutd no na no se

policy static sgt disabled trusted	no ip
security-level 0	!
ip address 10.1.1.1 255.255.255.0 <-- standby IP was removed	interf
!	shutd
interface GigabitEthernet1/2	no na
nameif inside	no se
cts manual	no ip
propagate sgt preserve-untag	!
policy static sgt disabled trusted	interf
security-level 0	descr
ip address 192.168.1.1 255.255.255.0 <-- standby IP was removed	!
!	interf

interface GigabitEthernet1/3	descr
description LAN Failover Interface	!
!	interf
interface GigabitEthernet1/4	shutd
description STATE Failover Interface	no na
!	no se
interface GigabitEthernet1/5	no ip
shutdown	!
no nameif	interf
no security-level	shutd
no ip address	no na

```
!
interface GigabitEthernet1/6
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet1/7
 shutdown
 no nameif
 no security-level
 no ip address
```

```
 no se
 no ip
!
interf
 shutd
 no na
 no se
 no ip
!
interf
 shutd
 no na
```

```
!
interface GigabitEthernet1/8
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management1/1
 management-only
 nameif diagnostic
 cts manual
```

```
 no se
 no ip
!
interf
 mana
 name
 cts m
  prop
  polic
 secur
 no ip
```

propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 no ip address ! ftp mode passive ngips conn-match vlan-id access-list CSM_FW_ACL_ remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy access-list CSM_FW_ACL_ remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE access-list CSM_FW_ACL_ advanced permit ipinip any any rule-id 9998 access-list CSM_FW_ACL_ advanced permit 41 any any rule-id 9998 access-list CSM_FW_ACL_ advanced permit gre any any rule-id 9998	! ftp m ngips acces acces acces acces acces acces acces acces acces

access-list CSM_FW_ACL_ advanced permit udp any any eq 3544 rule-id 9998	!
access-list CSM_FW_ACL_ remark rule-id 268435456: ACCESS POLICY: FTD_HA - Default/1	tcp-m
access-list CSM_FW_ACL_ remark rule-id 268435456: L4 RULE: DEFAULT ACTION RULE	tcp-
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268435456	tcp-
!	tcp-
tcp-map UM_STATIC_TCP_MAP	tcp-
tcp-options range 6 7 allow	urge
tcp-options range 9 18 allow	!
tcp-options range 20 255 allow	no pa
tcp-options md5 clear	loggi
urgent-flag allow	loggi

! no pager logging enable logging timestamp logging buffered debugging logging flash-minimum-free 1024 logging flash-maximum-allocation 3076 no logging message 106015 no logging message 313001 no logging message 313008 no logging message 106023 no logging message 710005	loggi loggi loggi no log no log no log no log no log no log no log no log no log

no logging message 710003	no log
no logging message 106100	no log
no logging message 302015	no log
no logging message 302014	no log
no logging message 302013	no log
no logging message 302018	no log
no logging message 302017	mtu o
no logging message 302016	mtu i
no logging message 302021	mtu d
no logging message 302020	**no fa**
mtu outside 1500	**failov**

mtu inside 1500 mtu diagnostic 1500 **no failover** icmp unreachable rate-limit 1 burst-size 1 no asdm history enable access-group CSM_FW_ACL_ global timeout xlate 3:00:00 timeout pat-xlate 0:00:30 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 sctp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00 timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute	**failov** **failov** **failov** **failov** **failov** icmp no as acces timeo timeo timeo timeo

timeout tcp-proxy-reassembly 0:00:30	timeo
timeout floating-conn 0:00:00	timeo
timeout conn-holddown 0:00:15	timeo
aaa proxy-limit disable	timeo
snmp-server host outside 192.168.1.100 community ***** version 2c	timeo
no snmp-server location	user-i
no snmp-server contact	aaa p
snmp-server community *****	snmp
service sw-reset-button	no sn
crypto ipsec security-association pmtu-aging infinite	no sn
crypto ca trustpool policy	snmp

```
telnet timeout 5
console timeout 0

dynamic-access-policy-record DfltAccessPolicy
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
```

```
servic
crypt
crypt
telnet
conso

dynam
!
class-
 matc
!
!
```

message-length maximum 512	polic
no tcp-inspection	para
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP	mes
parameters	mes
eool action allow	no t
nop action allow	polic
router-alert action allow	para
policy-map global_policy	eool
class inspection_default	nop
inspect dns preset_dns_map	rout
inspect ftp	polic

inspect h323 h225	class
inspect h323 ras	insp
inspect rsh	insp
inspect rtsp	insp
inspect esmtp	insp
inspect sqlnet	insp
inspect skinny	insp
inspect sunrpc	insp
inspect xdmcp	insp
inspect sip	insp
inspect netbios	insp
inspect tftp	insp

inspect icmp inspect icmp error inspect dcerpc inspect ip-options UM_STATIC_IP_OPTIONS_MAP class class-default set connection advanced-options UM_STATIC_TCP_MAP ! service-policy global_policy global prompt hostname context call-home profile CiscoTAC-1	insp insp insp insp insp insp insp class set c ! servic

no active destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService destination address email callhome@cisco.com destination transport-method http subscribe-to-alert-group diagnostic subscribe-to-alert-group environment subscribe-to-alert-group inventory periodic monthly subscribe-to-alert-group configuration periodic monthly subscribe-to-alert-group telemetry periodic daily Cryptochecksum:768a03e90b9d3539773b9d7af66b3452	prom call-h profi no a dest dest dest subs subs subs subs subs

	Crypt

Considerazioni principali per la disabilitazione della coppia HA dalla CLI dell'FTD:

Unità Principale	**Unità Secondaria**
La configurazione di failover e gli IP di standby sono stati rimossi	• Le configurazioni delle interfacce sono state rimosse • Il dispositivo passa alla modalità Pseudo-Standby

Passaggio 6. Al termine dell'operazione, registrare i dispositivi nel FMC e abilitare la coppia HA.

Attività 7. Sospendi HA

Attività richiesta:

Sospendere la coppia HA dalla CLI CLISH dell'FTD

Soluzione:

Passaggio 1. Nell'FTD principale eseguire il comando e confermare (digitare **YES**).

<#root>

```
> configure high-availability suspend

Please ensure that no deployment operation is in progress before suspending high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you wish to a

YES

Successfully suspended high-availability.
```

Passaggio 2. Verificare le modifiche sull'unità principale:

<#root>

```
>

show high-availability config

Failover Off

Failover unit Primary
Failover LAN Interface: fover_link Ethernet1/4 (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 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
```

Passaggio 3. Risultato sull'unità secondaria:

<#root>

```
>

show high-availability config
Failover Off (pseudo-Standby)

Failover unit Secondary
Failover LAN Interface: fover_link Ethernet1/4 (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 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
```

Passaggio 4. Riprendere HA sull'unità primaria:

<#root>

```
>

configure high-availability resume

Successfully resumed high-availablity.

> .

    No Active mate detected
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Beginning configuration replication: Sending to mate.
End Configuration Replication to mate

>
```

<#root>

```
>

show high-availability config

Failover On

Failover unit Primary
Failover LAN Interface: fover_link Ethernet1/4 (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 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
```

Passaggio 5. Il risultato sull'unità secondaria dopo la ripresa di HA:

<#root>

```
> ..



Detected an Active mate

Beginning configuration replication from mate.


WARNING: Failover is enabled but standby IP address is not configured for this interface.
WARNING: Failover is enabled but standby IP address is not configured for this interface.
End configuration replication from mate.

>
```

<#root>

```
>

show high-availability config

Failover On

Failover unit Secondary
Failover LAN Interface: fover_link Ethernet1/4 (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 1 of 1041 maximum
MAC Address Move Notification Interval not set
failover replication http
>
```

Domande frequenti (FAQ)

Quando la configurazione viene replicata, viene salvata immediatamente (riga per riga) o alla fine della replica?

Alla fine della replica. Fare riferimento alla fine dell'output del comando debug fover sync che mostra la replica della configurazione/del comando:

<#root>

```
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1506 remark rule-id 268442578: L7 RULE
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1507 advanced permit tcp object-group
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1508 remark rule-id 268442078: ACCESS
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ line 1509 remark rule-id 268442078: L4 RULE
...
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_2
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: ACCE
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268442077: L7 R
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ advanced permit tcp object-group group_6
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: ACCE
cli_xml_server: frep_write_cmd: Cmd: no access-list CSM_FW_ACL_ line 1510 remark rule-id 268440577: L4 R
cli_xml_server: frep_write_cmd: Cmd: access-list CSM_FW_ACL_ advanced deny ip any any rule-id 268442078
cli_xml_server: frep_write_cmd: Cmd: crypto isakmp nat-traversal
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_311
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_433
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_6
cli_xml_server: frep_write_cmd: Cmd: no object-group network group_2
cli_xml_server: frep_write_cmd: Cmd:

write memory <--
```

Cosa succede se un'unità si trova in uno stato di pseudo-standby (failover disabilitato) e viene ricaricata mentre l'altra unità ha il failover abilitato ed è attiva?

Si crea uno scenario **Attivo/Attivo** (sebbene tecnicamente sia Attivo/Failover-off). In particolare, dopo aver attivato l'unità, il failover viene disabilitato, ma l'unità utilizza gli stessi IP dell'unità Attiva. In realtà, si ha quindi:

- Unità-1: attiva
- Unità 2: failover disattivato. L'unità utilizza gli stessi IP dati dell'unità 1, ma indirizzi MAC diversi.

Che cosa succede alla configurazione di failover se si disabilita manualmente il failover (configure high-availability suspend) e si ricarica il dispositivo?

La disabilitazione del failover non è una modifica permanente (non viene salvata nella configurazione di avvio a meno che non si decida di farlo esplicitamente). Tenere presente che è possibile riavviare/ricaricare l'unità in 2 modi diversi. La seconda modalità richiede qualche attenzione in più.

Caso 1. Riavvio da CLISH

Il riavvio dalla CLISH non richiede conferma. Pertanto, la modifica alla configurazione non viene salvata nella configurazione di avvio:

<#root>

```
>

configure high-availability suspend

Please ensure that no deployment operation is in progress before suspending high-availability.
Please enter 'YES' to continue if there is no deployment operation in progress and 'NO' if you wish to a

YES

Successfully suspended high-availability.
```

Failover disabilitato in running-config. In questo caso, l'unità era in modalità Standby ed è entrata nello stato pseudo-Standby come previsto per evitare uno scenario Attivo/Attivo:

<#root>

```
firepower#

show failover | include Failover

Failover Off (

pseudo-Standby

)
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/1 (up)
```

Il failover è ancora abilitato nella configurazione di avvio:

<#root>

```
firepower#

show startup | include failover



failover

failover lan unit secondary
failover lan interface FOVER Ethernet1/1
failover replication http
failover link FOVER Ethernet1/1
failover interface ip FOVER 192.0.2.1 255.255.255.0 standby 192.0.2.2
failover ipsec pre-shared-key *****
```

Riavviare il dispositivo dalla CLISH (comando **reboot**):

<#root>

```
>

reboot

This command will reboot the system.  Continue?
Please enter 'YES' or 'NO':

YES


Broadcast message from root@
Threat Defense System: CMD=-stop, CSP-ID=cisco-ftd.6.2.2.81__ftd_001_JMX2119L05CYRIBVX1, FLAG=''
Cisco FTD stopping ...
```

Una volta attivata l'unità, poiché il failover è abilitato, il dispositivo passa nella fase di negoziazione del failover e tenta di rilevare il peer remoto:

<#root>

```
User enable_1 logged in to firepower
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
firepower> .



Detected an Active mate
```

Caso 2. Riavvio dalla CLI di LINA

Il riavvio dalla CLI LINA con il comando **reload** deve essere confermato. Pertanto, se si seleziona [Y], la modifica alla configurazione viene salvata nella configurazione di avvio:

<#root>

```
firepower#

reload

System config has been modified. Save? [Y]es/[N]o:

Y <-- Be careful. This will disable the failover in the startup-config


Cryptochecksum: 31857237 8658f618 3234be7c 854d583a

8781 bytes copied in 0.940 secs
Proceed with reload? [confirm]
firepower#

show startup | include failover

no failover

failover lan unit secondary
failover lan interface FOVER Ethernet1/1
failover replication http
failover link FOVER Ethernet1/1
failover interface ip FOVER 192.0.2.1 255.255.255.0 standby 192.0.2.2
failover ipsec pre-shared-key *****
```

Dopo l'attivazione dell'unità, il failover viene disabilitato:

<#root>

```
firepower#

show failover | include Fail

Failover Off
Failover unit Secondary
Failover LAN Interface: FOVER Ethernet1/1 (up)
```

Nota: per evitare questo scenario, accertarsi di non salvare le modifiche apportate alla configurazione di avvio quando richiesto.

Informazioni correlate

- Per le versioni della guida alla configurazione di Cisco Firepower Management Center, usare questo link:

https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html#id_47280

- Per le versioni delle guide alla configurazione di FXOS Chassis Manager e della CLI, usare questo link:

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/roadmap/fxos-roadmap.html#pgfId-121950

- 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:

http://www.ciscopress.com/title/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/tsd-products-support-series-home.html

- Documentazione e supporto tecnico â€“ Cisco Systems