Configurazione del failover attivo/attivo ASA in Firepower serie 4100

Sommario

Introduzione

In questo documento viene descritto come configurare il failover attivo/attivo nell'appliance Cisco Firepower 4145 NGFW.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di questo argomento:

- Failover attivo/standby in Cisco Adaptive Security Appliance (ASA).

Componenti usati

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

- Appliance Cisco Firepower 4145 NGFW (ASA) 9.18(3)56
- Firepower eXtensible Operating System (FXOS) 2.12(0.498)
- Windows 10

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

Premesse

Il failover attivo/attivo è disponibile solo per le appliance di sicurezza in esecuzione in modalità contesto multiplo. In questa modalità, l'ASA è divisa logicamente in più dispositivi virtuali, noti come contesti. Ogni contesto opera come dispositivo indipendente, con criteri di protezione, interfacce e amministratori specifici.

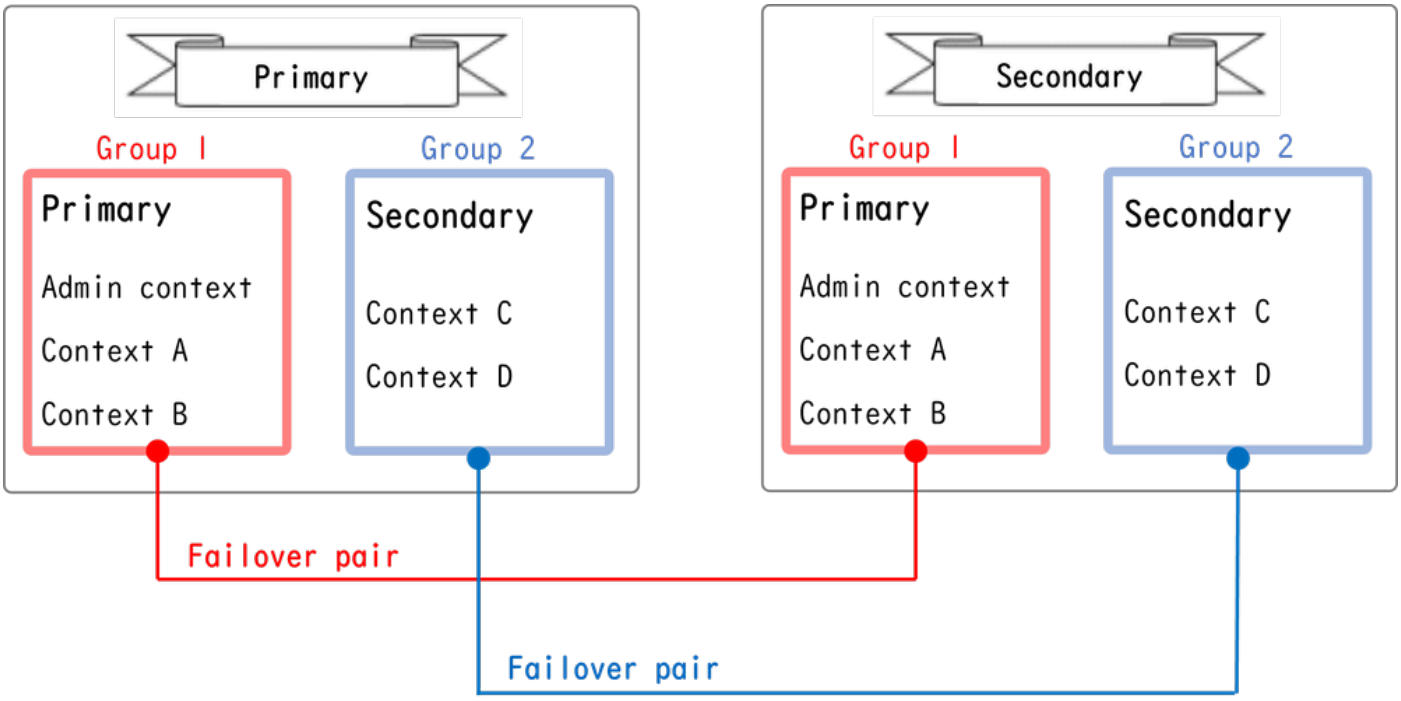
Il failover attivo/attivo è una funzione di Adaptive Security Appliance (ASA) che consente a due dispositivi Firepower di superare il traffico contemporaneamente. Questa configurazione viene in genere utilizzata per uno scenario di bilanciamento del carico in cui si desidera suddividere il traffico tra due dispositivi per massimizzare la velocità di trasmissione. Viene inoltre utilizzato per scopi di ridondanza, quindi se un'appliance ASA si guasta, l'altra può subentrare senza causare interruzioni al servizio.

Meccanismo di failover attivo/attivo dell'ASA

Ogni contesto nel failover attivo/attivo viene assegnato manualmente al gruppo 1 o al gruppo 2. Il contesto Admin viene assegnato al gruppo 1 per impostazione predefinita. Lo stesso gruppo (gruppo1 o gruppo2) nei due chassis (unità) forma una coppia di failover che sta realizzando la funzione di ridondanza. Il comportamento di ogni coppia di failover è sostanzialmente uguale a quello di un failover attivo/standby. Per ulteriori informazioni sul failover attivo/standby, vedere Configurare il failover attivo/standby. Nel failover attivo/attivo, oltre al ruolo (primario o secondario) di ogni chassis, ogni gruppo dispone anche di un ruolo (primario o secondario). Questi ruoli

vengono preimpostati manualmente dall'utente e vengono utilizzati per decidere lo stato di elevata disponibilità (HA) (Attivo o Standby) per ogni gruppo di failover.

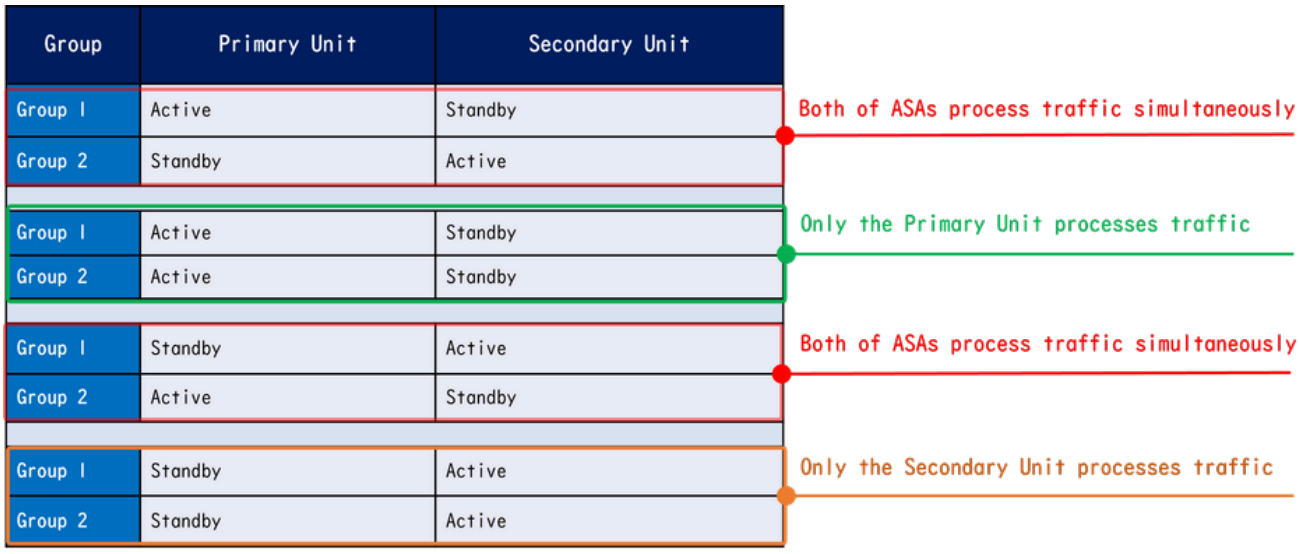
Il contesto di amministrazione è un contesto speciale che gestisce la connessione di base per la gestione dello chassis (ad esempio SSH). L'immagine mostra il failover attivo/attivo.



Coppia di failover in failover attivo/attivo

Flusso traffico

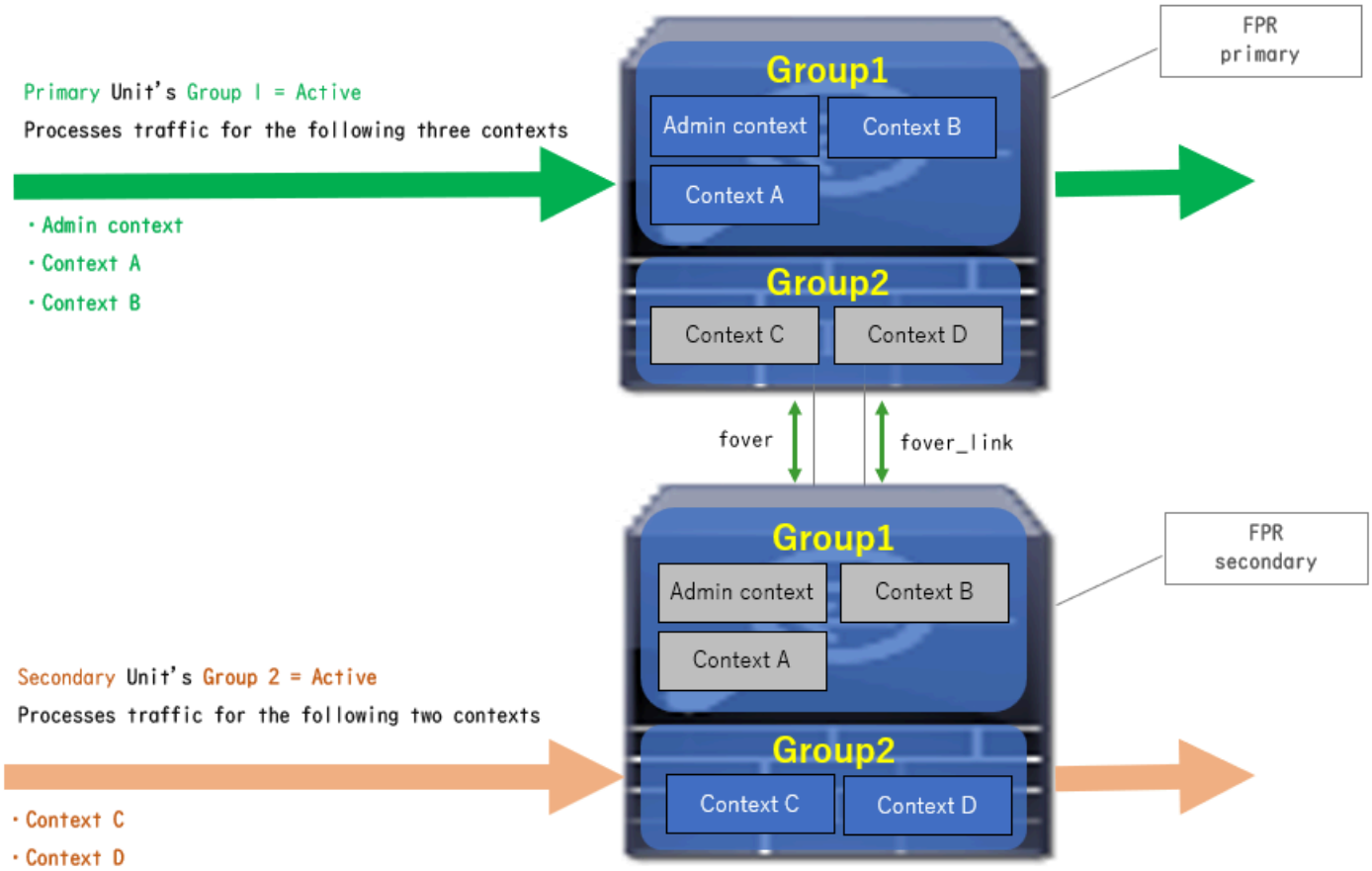
Nel failover attivo/attivo, il traffico può essere gestito in base ai diversi modelli illustrati nell'immagine seguente.



Flusso traffico

Condizione flusso traffico 1

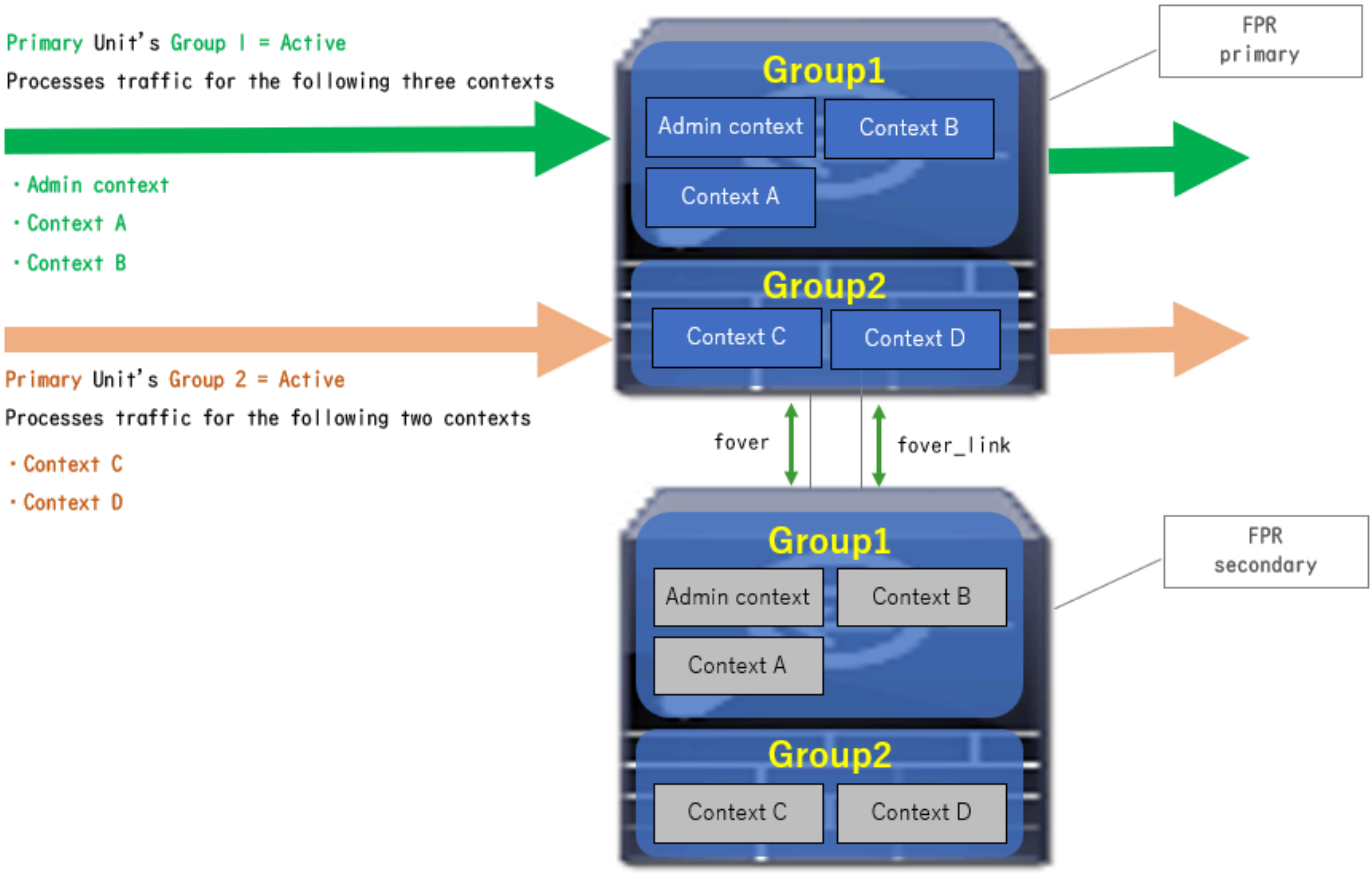
- Unità principale: Gruppo 1 = Attivo, Gruppo 2 = Standby
- Unità secondaria: Gruppo 1 = Standby, Gruppo 2 = Attivo



Condizione flusso traffico 1

Condizione flusso traffico 2

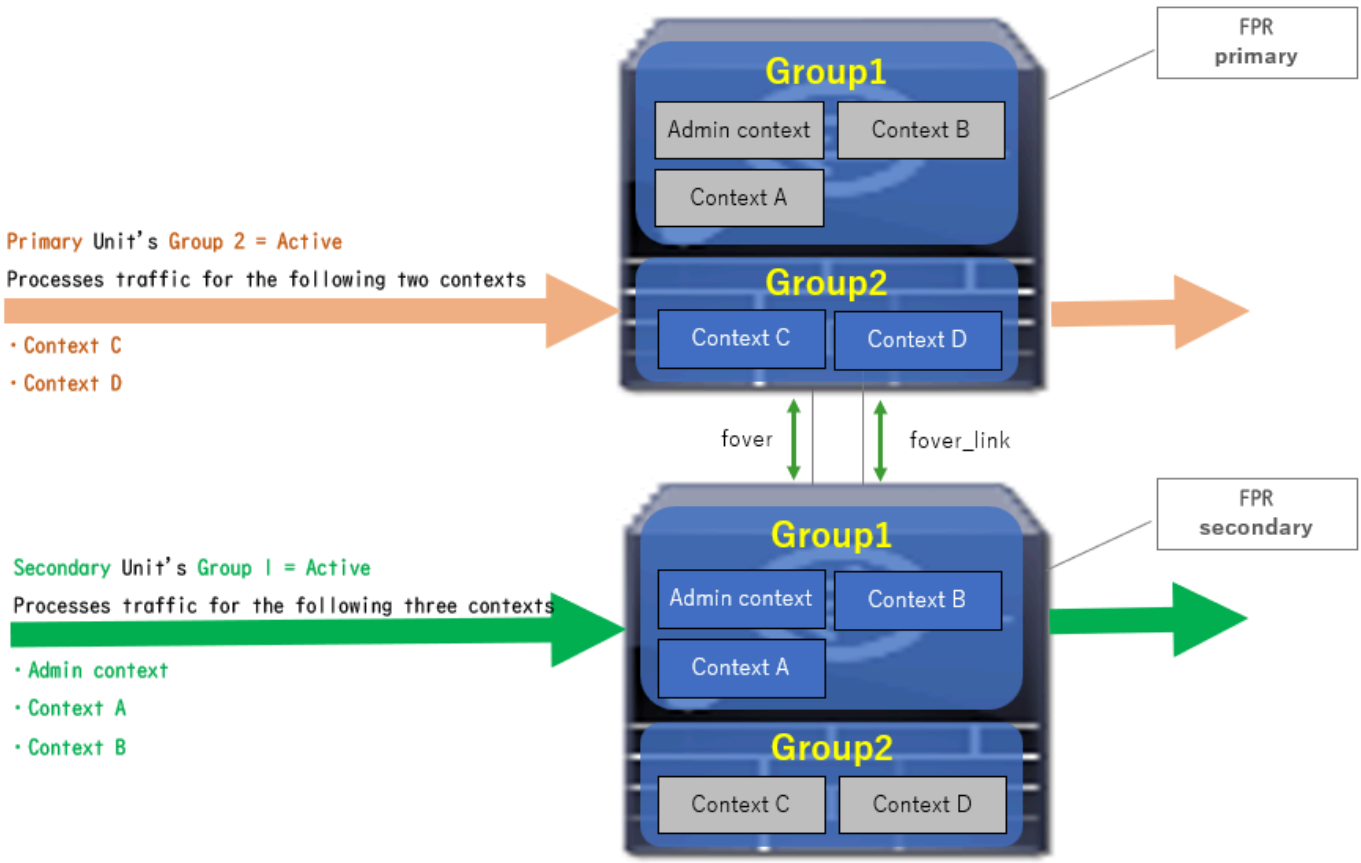
- Unità principale: Gruppo 1 = Attivo, Gruppo 2 = Attivo
- Unità secondaria: Gruppo 1 = Standby, Gruppo 2 = Standby



Condizione flusso traffico 2

Condizione flusso traffico 3

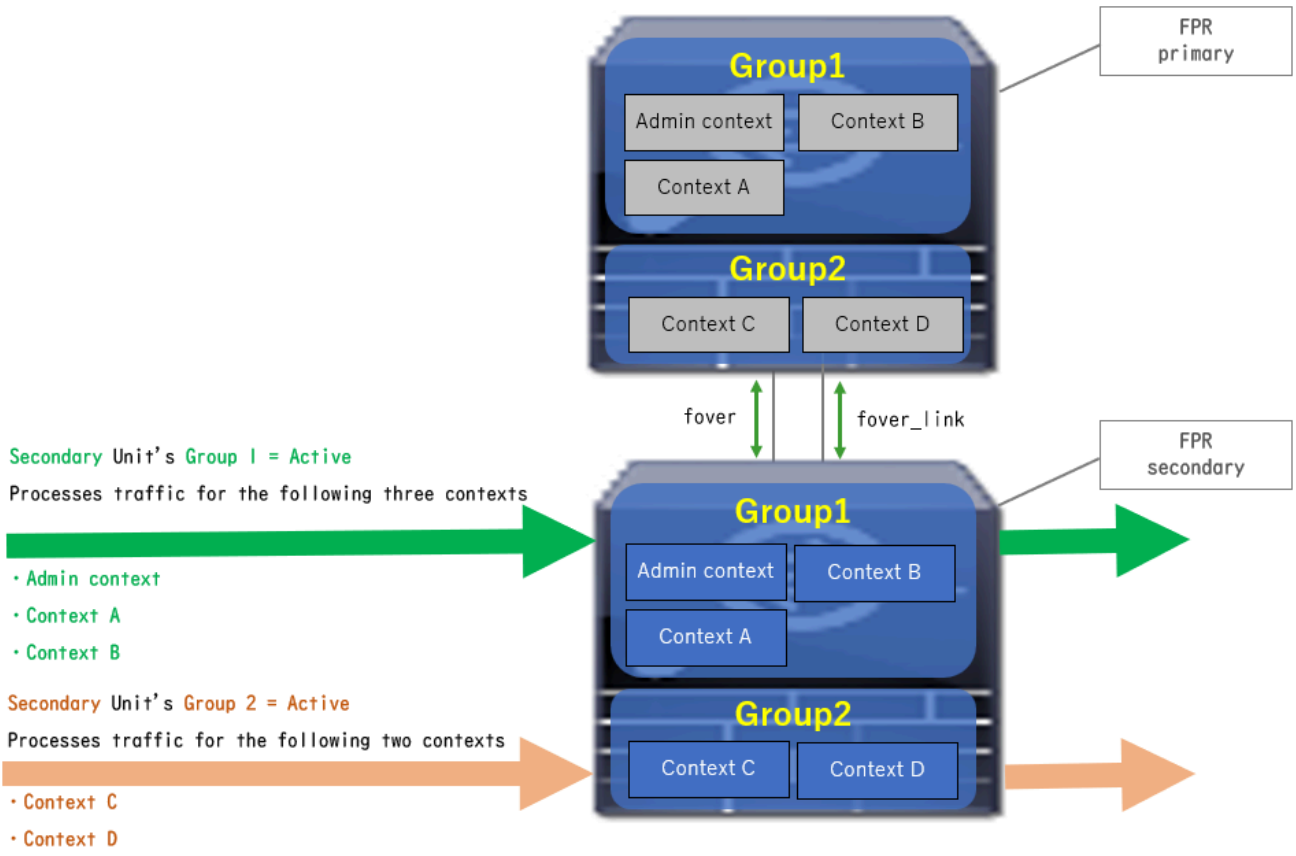
- Unità principale: Gruppo 1 = Standby, Gruppo 2 = Attivo
- Unità secondaria: Gruppo 1 = Attivo, Gruppo 2 = Standby



Condizione flusso traffico 3

Condizione flusso traffico 4

- Unità principale: Gruppo 1 = Standby, Gruppo 2 = Standby
- Unità secondaria: Gruppo 1 = Attiva, Gruppo 2 = Attiva



Condizione flusso traffico 4

Regole di selezione per Attivo/Standby

Nel failover attivo/attivo, lo stato (attivo/standby) di ogni gruppo è determinato dalle seguenti regole:

- Si supponga che due dispositivi vengano avviati quasi contemporaneamente e che una delle unità (primaria o secondaria) diventi attiva per prima.
- Una volta trascorso il tempo di priorità, il gruppo con lo stesso ruolo nello chassis e nel gruppo diventa attivo.
- Quando si verifica un evento di failover, ad esempio un'interfaccia non disponibile, lo stato del gruppo cambia come nel caso del failover attivo/standby.
- L'ora di interruzione per diritti di priorità non funziona dopo l'esecuzione manuale del failover.

Questo è un esempio della modifica dello stato.

- L'avvio di entrambi i dispositivi è quasi simultaneo. Stato A →
- Tempo di interruzione per diritti di priorità trascorso. Stato B →
- Errore del dispositivo primario (viene attivato il failover). Stato C →
- Tempo di interruzione per diritti di priorità trascorso dal ripristino da errore del dispositivo primario. Stato D →
- Attivare manualmente il failover. Stato E

Per ulteriori informazioni sui trigger di failover e sul monitoraggio dello stato, vedere Eventi di failover.

1. Entrambi i dispositivi vengono avviati quasi contemporaneamente.

Operation	Primary Unit		Secondary Unit	
	Group 1: primary	Group 2: secondary	Group 1: primary	Group 2: secondary
Both devices started simultaneously	Active	Active	Standby	Standby
	or			
	Standby	Standby	Active	Active

Stato A

2. Tempo di anticipo (30 in questo documento) trascorso.

After 30 seconds (preempt time)	Active	Standby	Standby	Active

Stato B

3. Si è verificato un errore (ad esempio Interfaccia inattiva) nel gruppo 1 dell'unità primaria.

Failover event	Standby	Standby	Active	Active

Stato C

4. Tempo di interruzione per diritti di priorità (30 in questo documento) trascorso dal ripristino da errore del gruppo 1 del dispositivo primario.

After 30 seconds since Primary Unit recovered	Active	Standby	Standby	Active

Stato D

5. Impostazione manuale del gruppo 2 dell'unità principale su Attivo.

Manual failover	Active	Active	Standby	Standby

Stato E

Esempio di rete

In questo documento vengono illustrati la configurazione e la verifica per il failover attivo/attivo basato su questo diagramma.

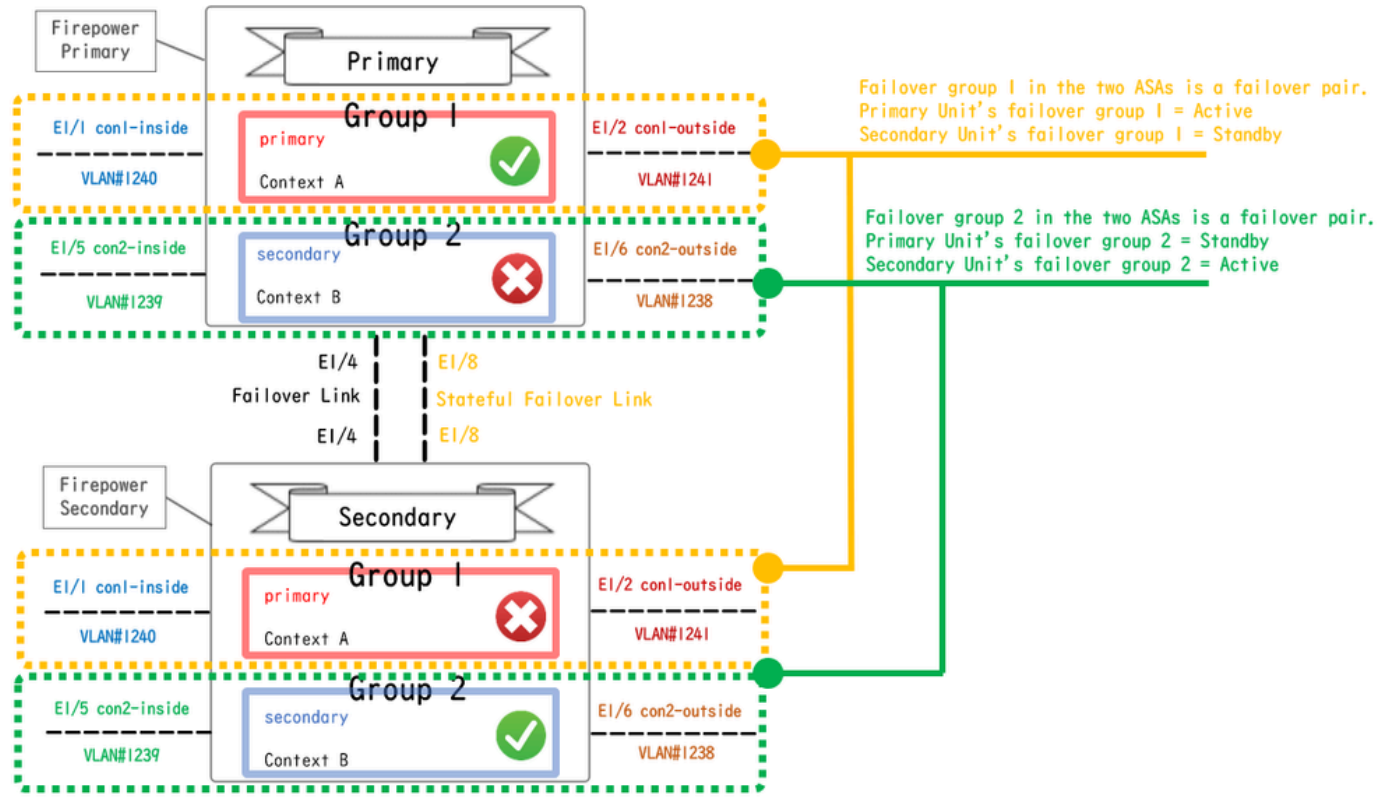


Diagramma di configurazione logica

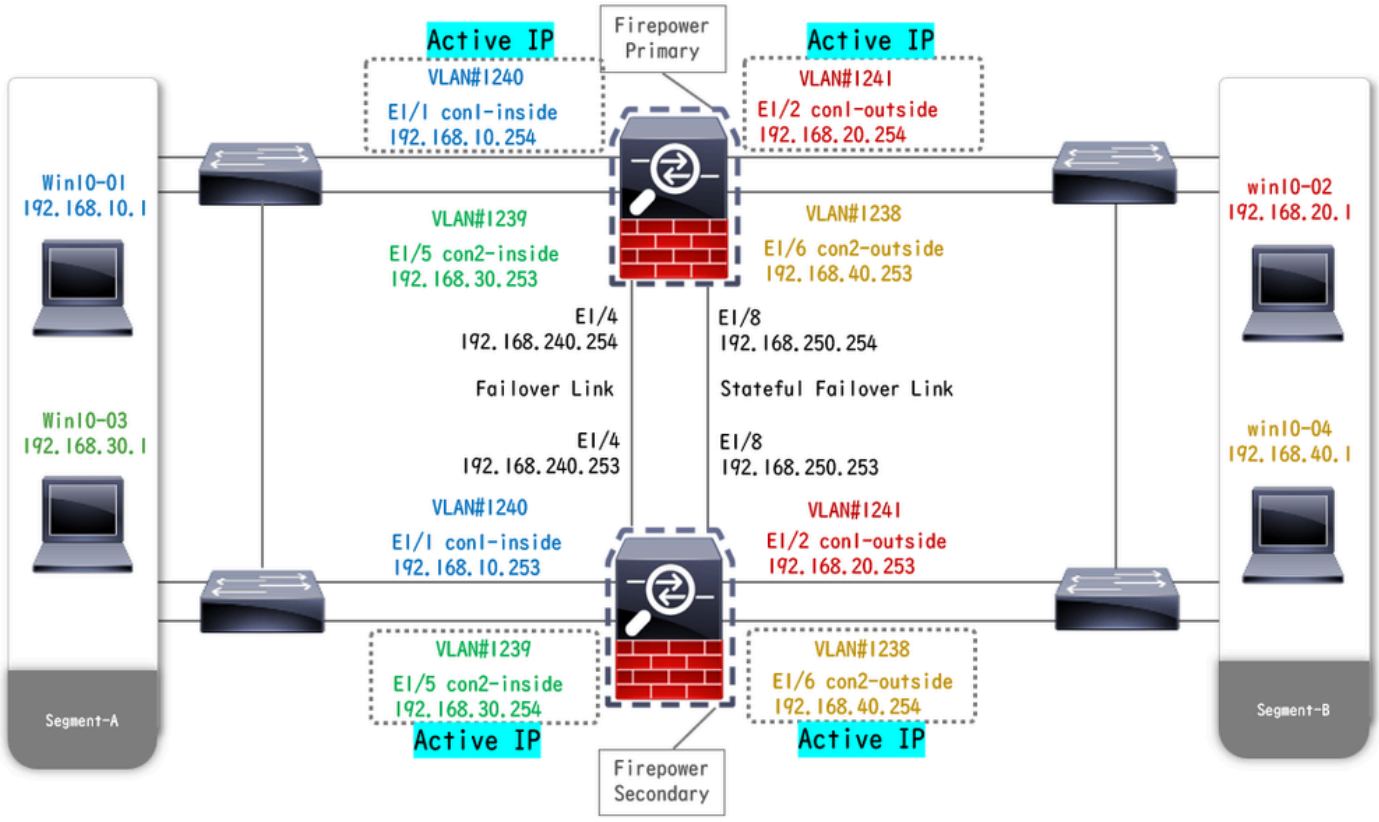
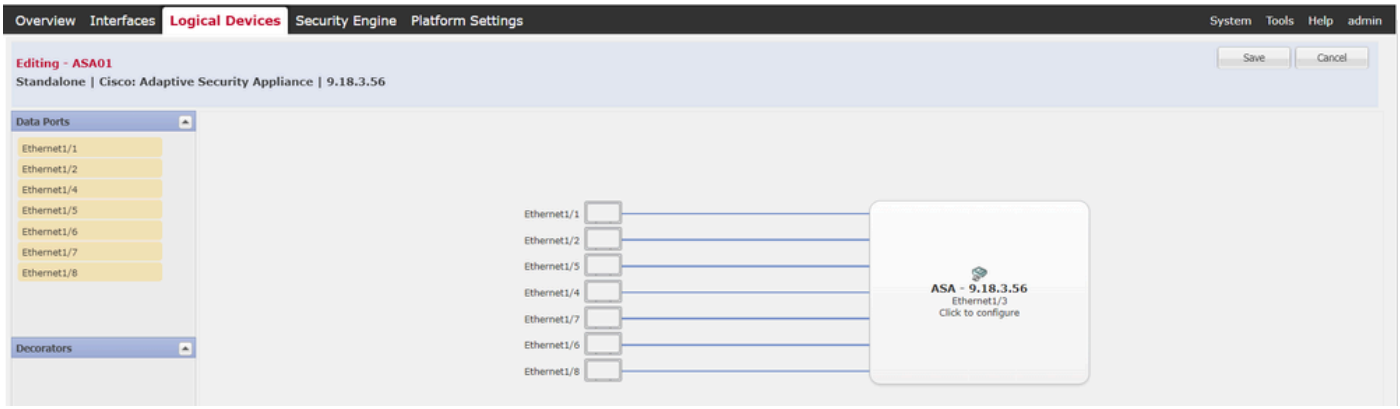


Diagramma configurazione fisica

Configurazione

Passaggio 1. Interfacce pre-configurate

Per entrambe le versioni di Firepower, accedere alla GUI di FCM. Passare a Dispositivi logici > Modifica. Aggiungere l'interfaccia dati all'appliance ASA, come mostrato nell'immagine.



Interfacce pre-configurate

Passaggio 2. Configurazione sull'unità primaria

Connettersi alla CLI principale di FXOS tramite SSH o console. Eseguire **connect module 1 console** e connect asaper accedere alla CLI di ASA.

a. Configurare il failover sull'unità primaria (eseguire il comando nel contesto di sistema dell'unità primaria).

```
<#root>
```

failover lan unit primary failover lan interface fover E1/4 failover link fover_link E1/8 failover interface ip fover 192.168.240.254 255.255.255.0 standby 1

```
failover group 1
□□□<--- group 1 is assigned to primary by default preempt 30 failover group 2 secondary preempt 30 fai
```

b. Configurare il gruppo di failover per il contesto (eseguire il comando nel contesto di sistema dell'unità primaria).

```
<#root>
```

admin-context admin

```
context admin
 <--- admin context is assigned to group 1 by default allocate-interface E1/3 config-url disk0:/admin.c
join-failover-group 1
 <--- add con1 context to group 1 ! context con2 allocate-interface E1/5 allocate-interface E1/6 config
join-failover-group 2
 <--- add con2 context to group 2
```

c. Eseguire changeto context con1 per connettere il contesto con1 dal contesto di sistema. Configurare IP per Interface del contesto con1 (eseguire il comando nel contesto con1 dell'unità primaria).

interface E1/1 nameif con1-inside ip address 192.168.10.254 255.255.255.0 standby 192.168.10.253 security-level 100 no shutdown interface E1/2 nameif

d. Eseguire changeto context con2 per connettere il contesto con2 dal contesto di sistema. Configurare IP per Interface del contesto con2 (eseguire il comando nel contesto con2 dell'unità primaria).

interface E1/5 nameif con2-inside ip address 192.168.30.254 255.255.255.0 standby 192.168.30.253 security-level 100 no shutdown interface E1/6 nameif

Passaggio 3. Configurazione sull'unità secondaria

a. Connettersi alla CLI secondaria di FXOS tramite SSH o console. Configurare il failover sull'unità secondaria (eseguire il comando nel contesto di sistema dell'unità secondaria).

failover lan unit secondary failover lan interface fover E1/4 failover link fover_link E1/8 failover interface ip fover 192.168.240.254 255.255.255.0 standby

b. Comando Run failover (eseguito nel contesto di sistema dell'unità secondaria).

failover

Passaggio 4. Conferma stato failover al termine della sincronizzazione

a. Eseguire show failover nel contesto di sistema dell'unità secondaria.

<#root>

asa#

show failover

Failover On Failover unit Secondary Failover LAN Interface: fover Ethernet1/4 (up) Version: Ours 9.18(

Secondary

<--- group 1 and group 2 are Standby status in Secondary Unit Group 1 State:

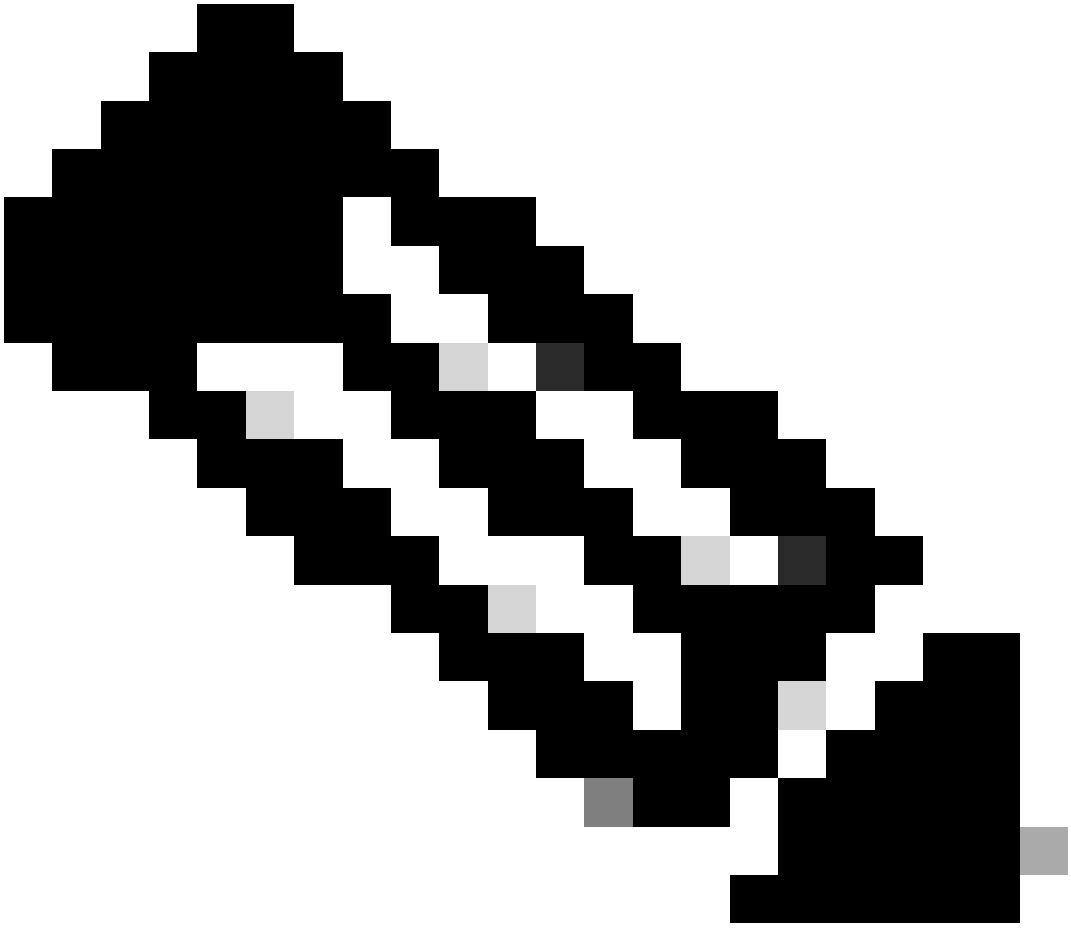
Standby Ready

```
 Active time: 0 (sec) Group 2 State:
Standby Ready
 Active time: 945 (sec) con1 Interface con1-inside (192.168.10.253): Unknown (Waiting) con1 Interface c
Primary
<--- group 1 and group 2 are Active status in Primary Unit Group 1 State:
Active
 Active time: 1637 (sec) Group 2 State:
Active
 Active time: 93 (sec) con1 Interface con1-inside (192.168.10.254): Normal (Monitored) con1 Interface c
```

b. (Facoltativo) Eseguire il **no failover active group 2** comando per passare manualmente il gruppo 2 dell'unità primaria allo stato Standby (in esecuzione nel contesto di sistema dell'unità primaria). Ciò può bilanciare il carico del traffico attraverso il firewall.

<#root>

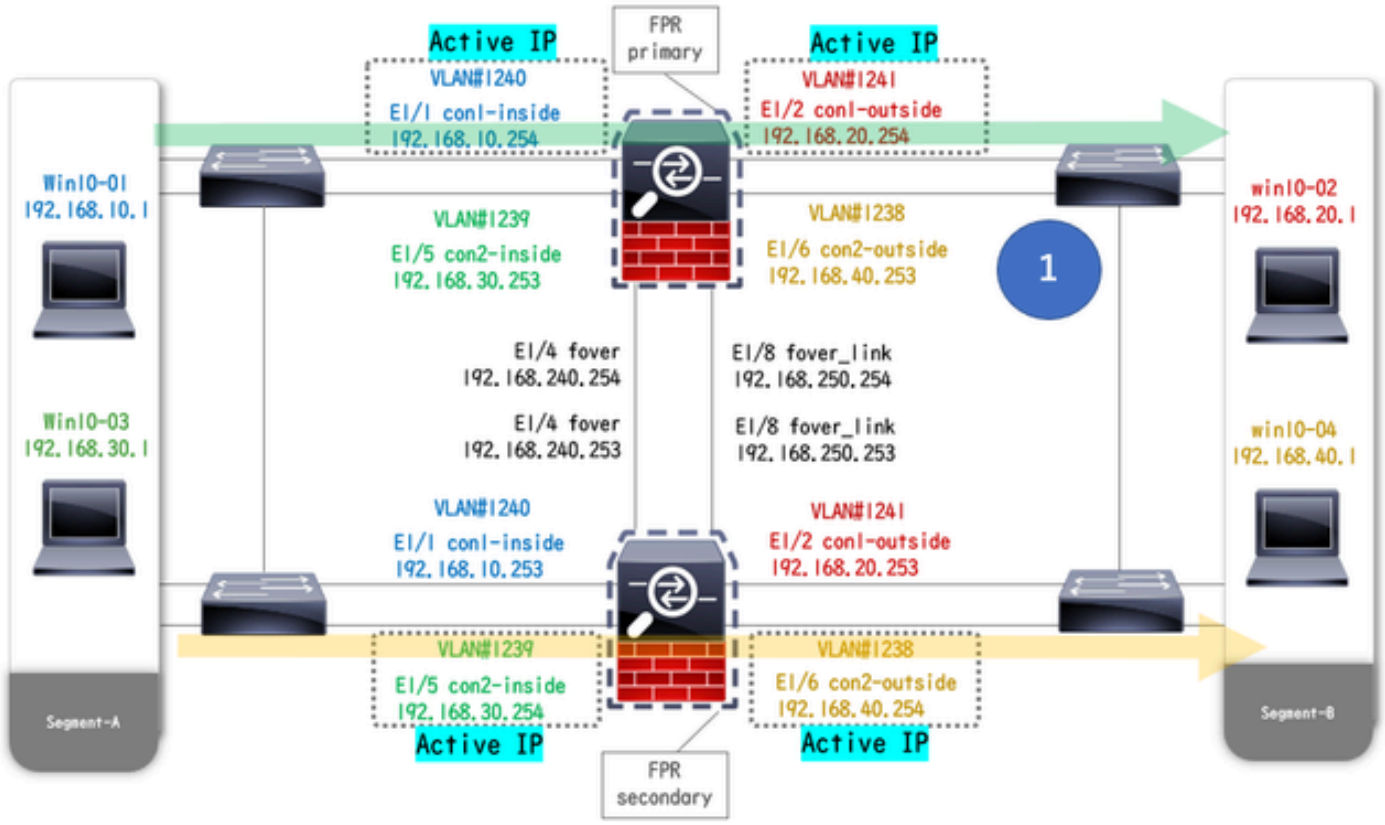
```
no failover active group 2
```



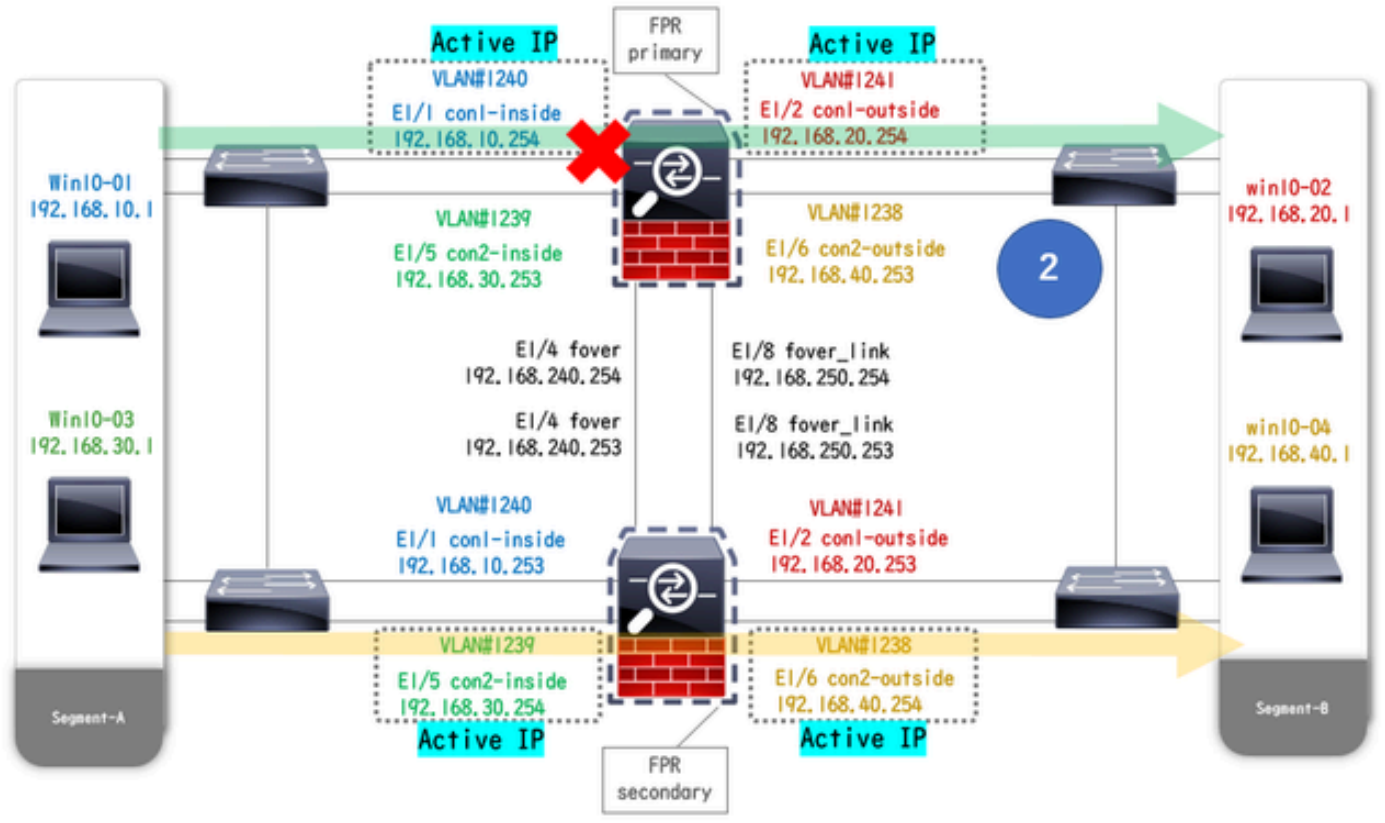
Nota: se si esegue questo comando, lo stato del failover corrisponde alla condizione 1 del flusso di traffico.

Verifica

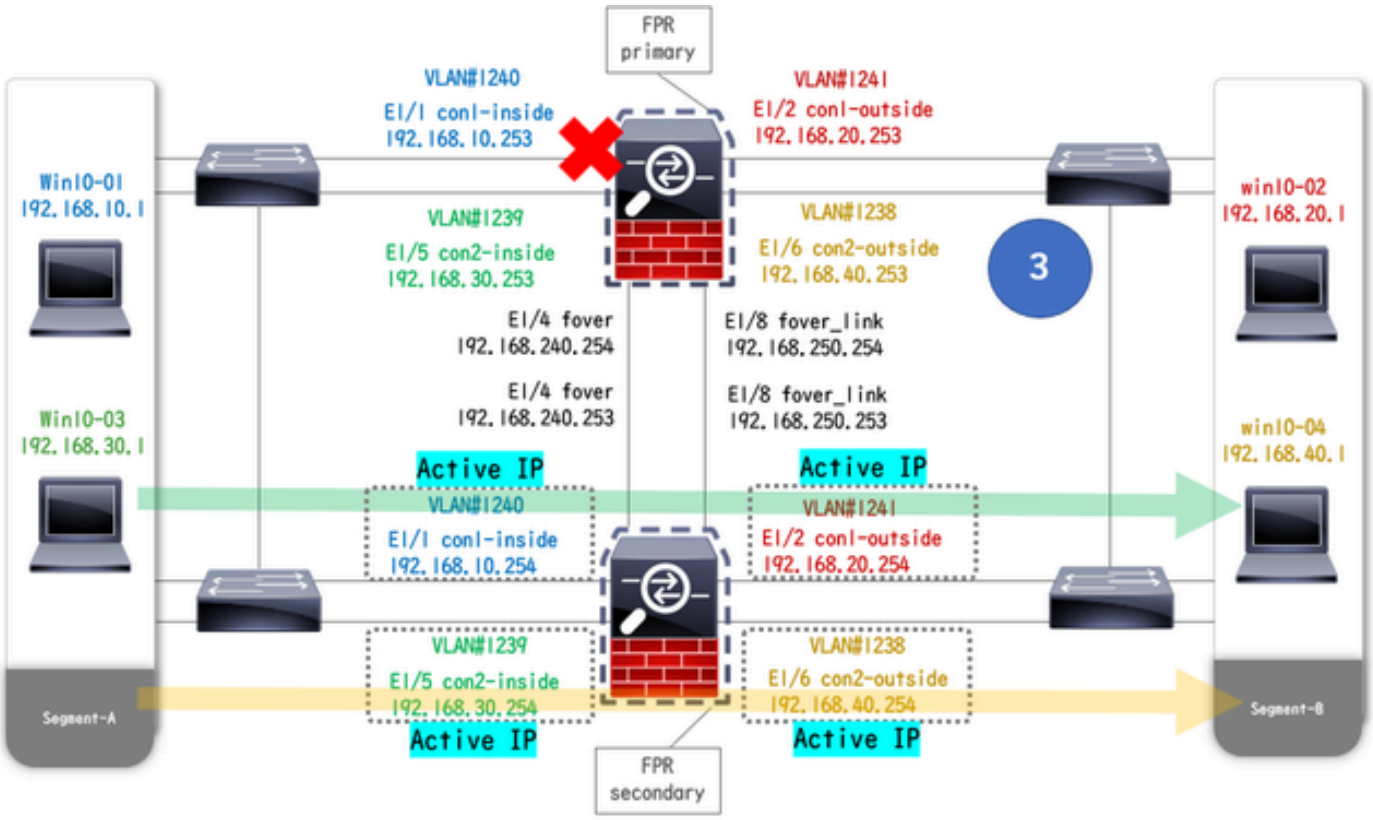
Quando E1/1 diventa INATTIVO, si attiva il failover del gruppo 1 e le interfacce dati sul lato Standby (unità secondaria) acquisiscono l'indirizzo IP e MAC dell'interfaccia attiva originale, garantendo il passaggio continuo del traffico (connessione FTP in questo documento) da parte delle appliance ASA.



Prima del collegamento



non attivo durante il collegamento non attivo



Failover attivato

Passaggio 1. Avvia connessione FTP da Win10-01 a Win10-02

Passaggio 2. Conferma connessione FTP prima del failover

Eseguire per changeto context con1 connettere il contesto con1 dal contesto di sistema. Confermare che sia stata stabilita una connessione FTP in entrambe le unità ASA.

<#root>

asa/act/pri/con1#

show conn

```
 5 in use, 11 most used
 ! --- Confirm the connection in Primary Unit TCP
```

con1-outside

192.168.20.1:21

con1-inside 192.168.10.1:49703

, idle 0:00:11, bytes 528, flags UIO asa/stby/sec/con1#

show conn

```
 5 in use, 11 most used
 ! --- Confirm the connection in Secondary Unit TCP
```

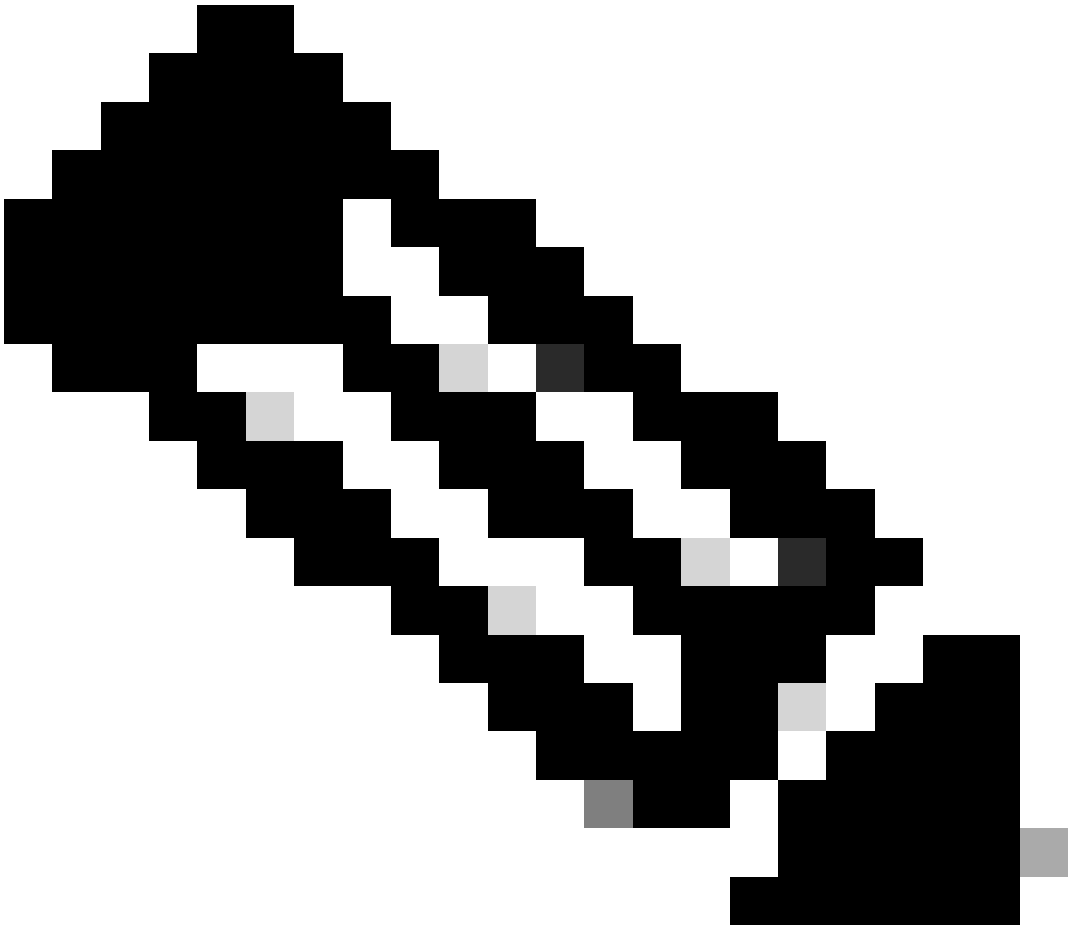
con1-outside 192.168.20.1:21 con1-inside 192.168.10.1:49703

, idle 0:00:14, bytes 528, flags UIO

Passaggio 3. LinkDOWN E1/1 dell'unità principale

Passaggio 4. Conferma stato failover

Nel contesto di sistema, verificare che il failover si verifichi nel gruppo 1.



Nota: lo stato del failover corrisponde alla condizione del flusso di traffico 4.

<#root>

asa/act/sec#

show failover

 Failover On Failover unit Secondary Failover LAN Interface: fover Ethernet1/4 (up) ..... Group 1 last

Secondary

 Group 1 State:

Active

<--- group 1 of Secondary Unit is Switching to Active Active time: 5 (sec) Group 2 State:

Active

 Active time: 10663 (sec) con1 Interface con1-inside (192.168.10.254): Normal (Waiting) con1 Interface

Primary

 Group 1 State:

Failed

<--- group 1 of Primary Unit is Switching to Failed status Active time: 434 (sec) Group 2 State:

Standby Ready

 Active time: 117 (sec) con1 Interface con1-inside (192.168.10.253): Failed (Waiting) con1 Interface co

Passaggio 5. Conferma connessione FTP dopo il failover

Eseguire per changeto context con1 connettere il contesto con1 dal contesto di sistema. Verificare che la connessione FTP non venga interrotta.

<#root>

asa/act/sec#

changeto context con1

 asa/act/sec/con1# show conn 11 in use, 11 most used
! --- Confirm the target FTP connection exists in group 1 of the Secondary Unit TCP

con1-outside 192.168.20.1:21 con1-inside 192.168.10.1:49703

, idle 0:00:09, bytes 529, flags UIO

Passaggio 6. Conferma comportamento dell'interruzione di sessione per diritti di priorità

LinkUP E1/1 dell'unità primaria e attesa per 30 s (tempo di interruzione anticipata), lo stato di failover torna allo stato originale (corrispondenza del flusso di traffico nel modello 1).

<#root>

asa/stby/pri#

Group 1 preempt mate

□□□□<--- Failover is triggered automatically, after the preempt time has passed asa/act/pri# show fail

Primary

Group 1 State:

Active

<--- group 1 of Primary Unit is switching to Active status Active time: 34 (sec) Group 2 State:

Standby Ready

Active time: 117 (sec) con1 Interface con1-inside (192.168.10.254): Normal (Monitored) con1 Interface

Secondary

Group 1 State:

Standby Ready

□□<---- group 1 of Secondary Unit is switching to Standby status Active time: 125 (sec) Group 2 State:

Active

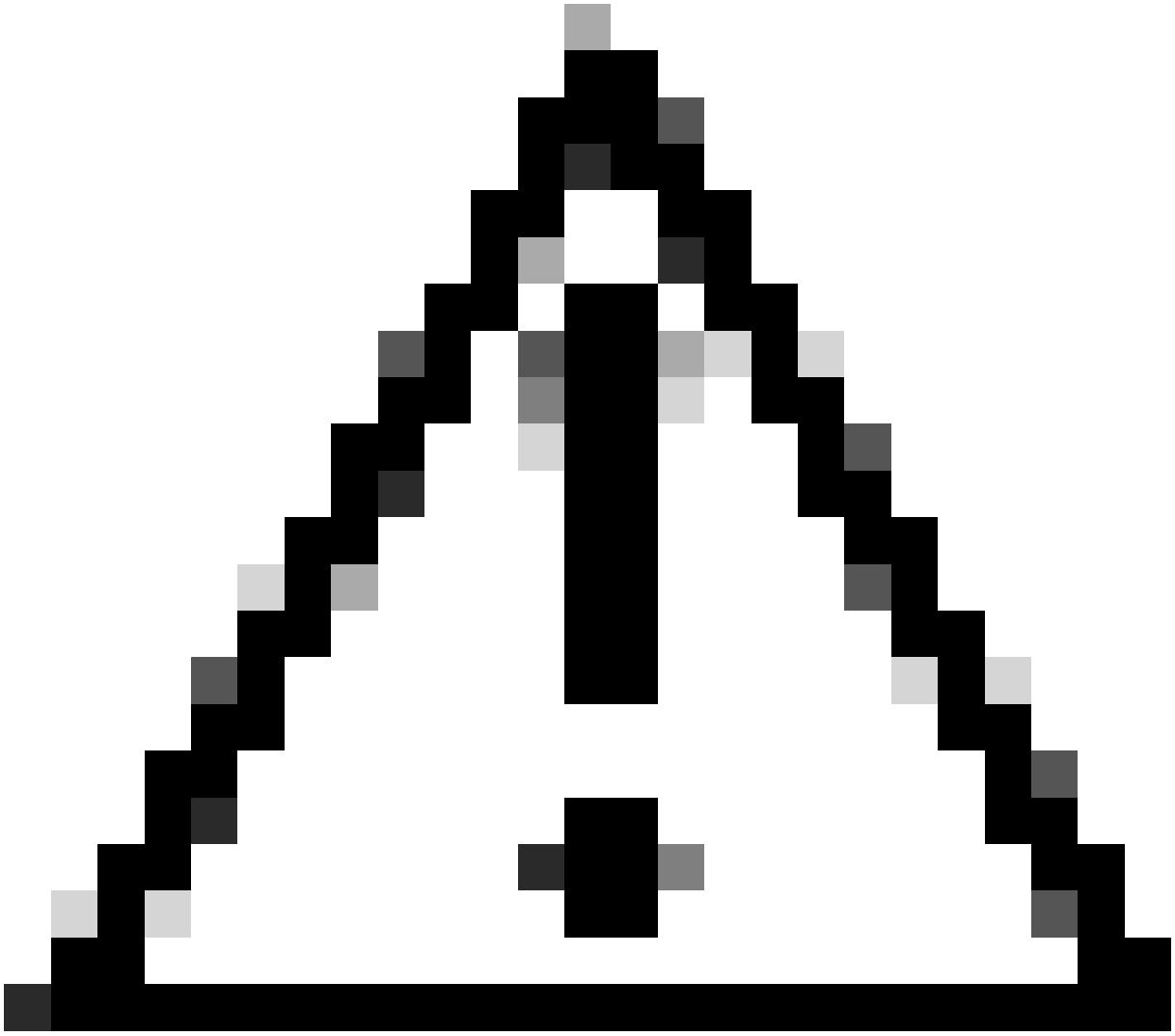
Active time: 10816 (sec) con1 Interface con1-inside (192.168.10.253): Normal (Monitored) con1 Interfac

Indirizzo MAC virtuale

In Failover attivo/attivo, viene sempre utilizzato l'indirizzo MAC virtuale (valore impostato manualmente, valore generato automaticamente o valore predefinito). L'indirizzo MAC virtuale attivo è associato all'interfaccia attiva.

Impostazione manuale dell'indirizzo MAC virtuale

Per impostare manualmente l'indirizzo MAC virtuale delle interfacce fisiche, è possibile usare il comando mac address o il comando (nella modalità di impostazione I/F) mac-address. Questo è un esempio di impostazione manuale di un indirizzo MAC virtuale per l'interfaccia fisica E1/1.



Attenzione: evitare di utilizzare questi due tipi di comandi nello stesso dispositivo.

<#root>

asa/act/pri(config)# failover group 1 asa/act/pri(config-fover-group)#

mac address E1/1 1234.1234.0001 1234.1234.0002

asa/act/pri(config-fover-group)# changeto context con1 asa/act/pri/con1(config)# show interface E1/1 |

1234.1234.0001

, MTU 1500 <--- Checking virtual MAC on the Primary Unit(con1) side asa/stby/sec# changeto context con1

1234.1234.0002

, MTU 1500 <--- Checking virtual MAC on the Secondary Unit(con1) side

O

<#root>

asa/act/pri(config)# changeto context con1 asa/act/pri/con1(config)# int E1/1 asa/act/pri/con1(config-if)#

mac-addr

1234.1234.0001 standby 1234.1234.0002

asa/act/pri/con1(config)# show interface E1/1 | in MAC MAC address

1234.1234.0001

, MTU 1500 <--- Checking virtual MAC on the Primary Unit(con1) side asa/stby/sec# changeto context con1

1234.1234.0002

, MTU 1500<--- Checking virtual MAC on the Secondary Unit(con1) side

Impostazione automatica dell'indirizzo MAC virtuale

È inoltre supportata la generazione automatica dell'indirizzo MAC virtuale. Per farlo, usare il mac-address auto <prefix prefix> comando. Il formato dell'indirizzo MAC virtuale è A2 xx.yyzz.zzzz che viene generato automaticamente.
A2: valore fisso
xx.yy : generato dall'opzione <prefix prefix> specificata nel comando (il prefisso viene convertito in esadecimale e quindi inserito in ordine inverso).
zz.zzzz : generato da un contatore interno

Questo è un esempio di generazione di un indirizzo MAC virtuale tramite un **mac-address auto** comando per l'interfaccia.

<#root>

asa/act/pri(config)#

mac-address auto

INFO: Converted to mac-address auto prefix 31

```
asa/act/pri(config)#
```

show run all context con1

```
 <--- Checking the virtual MAC addresses generated on con1 context
allocate-interface Ethernet1/1
mac-address auto Ethernet1/1 a21f.0000.0008 a21f.0000.0009
allocate-interface Ethernet1/2
mac-address auto Ethernet1/2 a21f.0000.000a a21f.0000.000b
config-url disk0:/con1.cfg
join-failover-group 1

asa/act/pri(config)#
```

show run all context con2

```
<--- Checking the virtual MAC addresses generated on con2 context
context con2
allocate-interface Ethernet1/5
mac-address auto Ethernet1/5 a21f.0000.000c a21f.0000.000d
allocate-interface Ethernet1/6
mac-address auto Ethernet1/6 a21f.0000.000e a21f.0000.000f
config-url disk0:/con2.cfg
join-failover-group 2
```

Impostazione predefinita dell'indirizzo MAC virtuale

Se non è impostata la generazione automatica o manuale di un indirizzo MAC virtuale, viene utilizzato l'indirizzo MAC virtuale predefinito.

Per ulteriori informazioni sull'indirizzo MAC virtuale predefinito, consultare il documento Command Default of mac address in Cisco Secure Firewall ASA Series Command Reference Guide.

Aggiornamento

È possibile ottenere l'aggiornamento senza tempi di inattività di una coppia di failover attivo/attivo tramite CLI o ASDM. Per ulteriori informazioni, vedere Aggiornare una coppia di failover attivo/attivo.

Informazioni correlate

- Aggiornamento di una coppia di failover attivo/attivo dalla CLI
- Indirizzo MAC
- Supporto tecnico Cisco e download

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).