Informazioni sull'espansione delle regole sui dispositivi FirePOWER

Sommario

Introduzione

Questo documento descrive la conversione delle regole di controllo di accesso nel sensore quando viene distribuito da Firepower Management Center (FMC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza della tecnologia Firepower
- Informazioni sulla configurazione dei criteri di controllo di accesso in FMC

Componenti usati

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

- Firepower Management Center versione 6.0.0 e successive
- ASA Firepower Defense Image (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) con software versione 6.0.1 e successive

- ASA Firepower SFR Image (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X, ASA 5585-X) con software versione 6.0.0 e successive

- Firepower serie 7000/8000 sensor versione 6.0.0 e successive

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

Premesse

Una regola di controllo d'accesso viene creata utilizzando una o più combinazioni dei seguenti parametri:

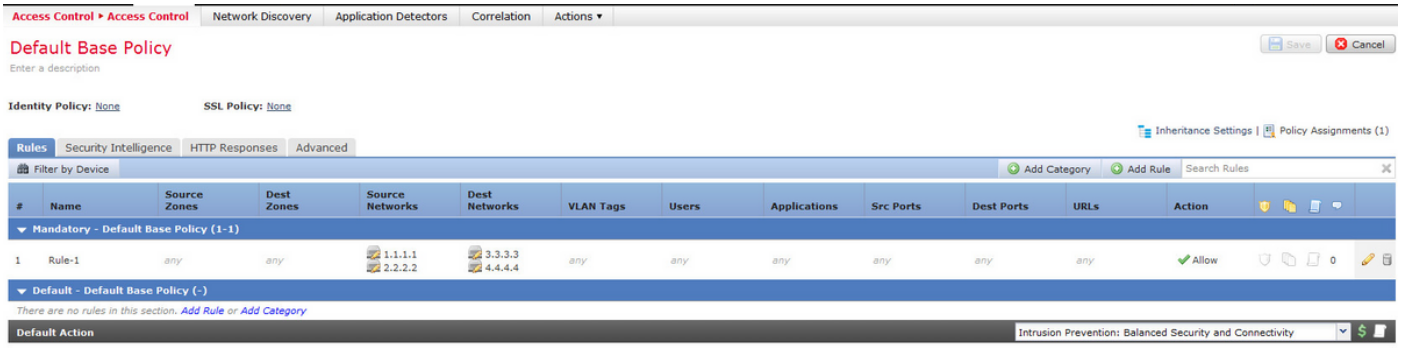
- Indirizzo IP (origine e destinazione)
- Porte (origine e destinazione)
- URL (categorie fornite dal sistema e URL personalizzati)
- Rilevatori applicazioni
- VLAN
- Zone

In base alla combinazione di parametri utilizzata nella regola di accesso, l'espansione della regola nel sensore cambia. Il presente documento mette in evidenza varie combinazioni di norme relative al CCP e le rispettive espansioni associate sui sensori.

Informazioni sull'espansione delle regole

Espansione di una regola basata su IP

Prendere in considerazione la configurazione di una regola di accesso da FMC, come illustrato nell'immagine:



Si tratta di una regola singola nel centro di gestione. Tuttavia, dopo averlo distribuito al sensore, si espande in **quattro** regole, come mostrato nell'immagine:

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart)
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart)
```

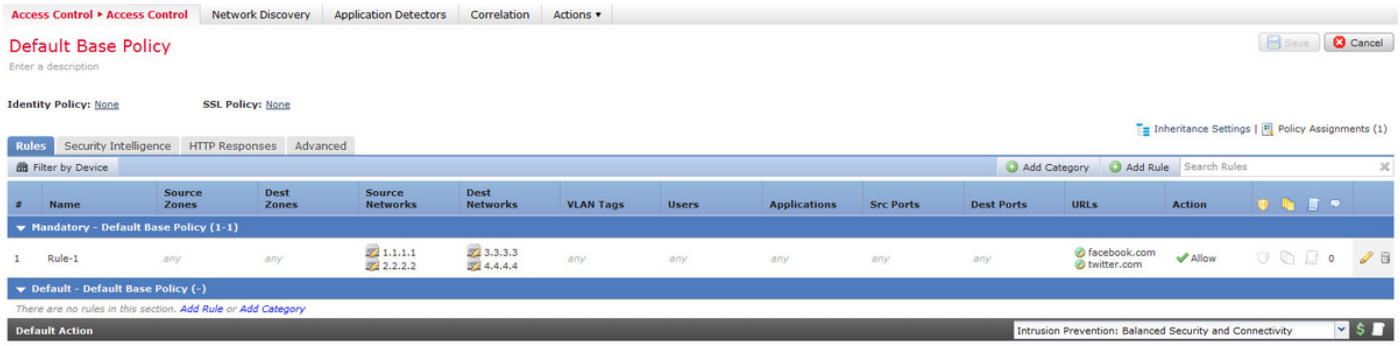
```
268435456 allow any any  any any any  any any any  (ipspolicy 2)
```

Quando si distribuisce una regola con due subnet configurate come origine e due host configurati come indirizzi di destinazione, questa regola viene espansa a quattro regole sul sensore.

> **Nota:** Se il requisito è quello di bloccare l'accesso in base alle reti di destinazione, un modo migliore per eseguire questa operazione è utilizzare la funzione delle liste nere in Security Intelligence.

Espansione di una regola basata su IP tramite URL personalizzato

Prendere in considerazione la configurazione di una regola di accesso da FMC, come illustrato nell'immagine:



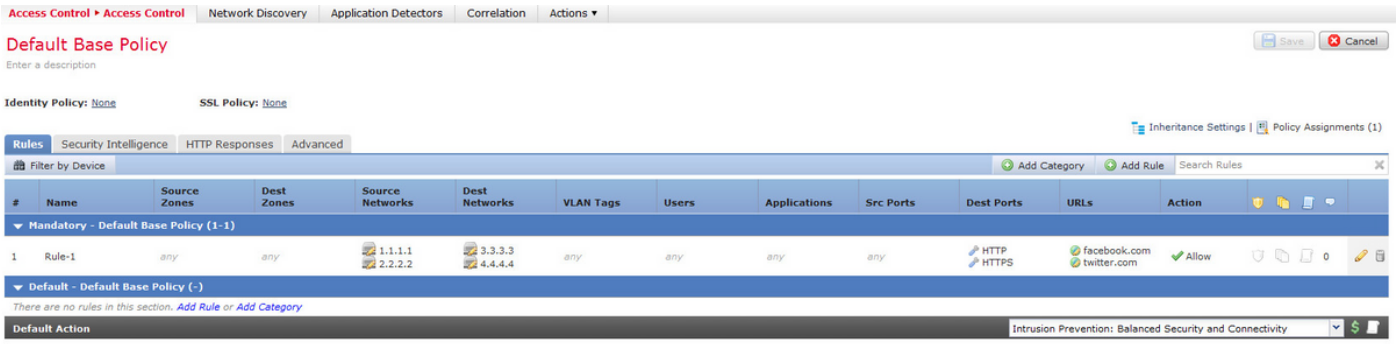
Si tratta di una regola singola nel centro di gestione. Tuttavia, dopo averla distribuita al sensore, viene espansa in otto regole, come mostrato nell'immagine:

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any  (log dcforward flowstart) (url
"twitter.com")
268435456 allow any any  any any any  any any any  (ipspolicy 2)
```

Quando si distribuisce una regola con due subnet configurate come origine, due host configurati come indirizzi di destinazione e due oggetti URL personalizzati in una singola regola nel centro di gestione, questa regola viene espansa a otto regole sul sensore. Ciò significa che per ciascuna categoria di URL personalizzati è disponibile una combinazione di intervalli di porte/IP di origine e di destinazione, che vengono configurati e creati.

Espansione di una regola basata su IP tramite porte

Prendere in considerazione la configurazione di una regola di accesso da FMC, come illustrato nell'immagine:



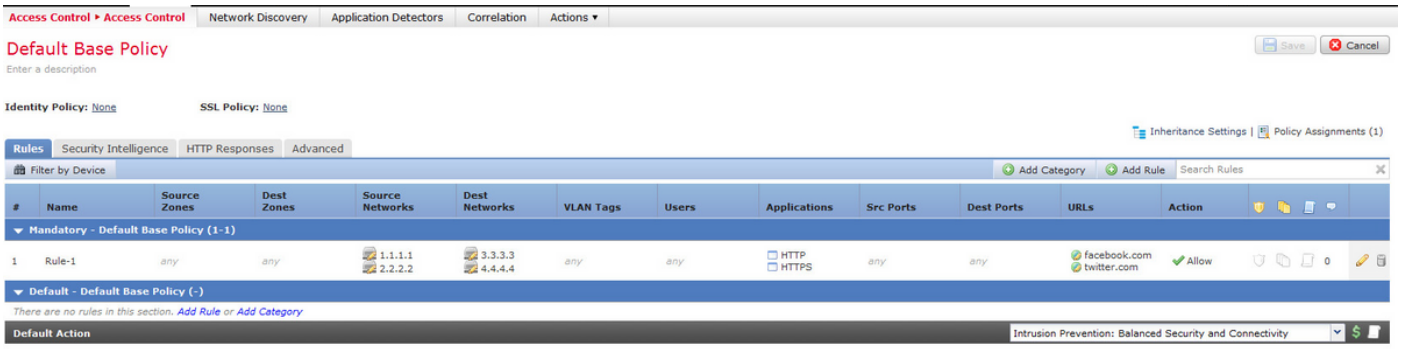
Si tratta di una regola singola nel centro di gestione. Tuttavia, dopo averlo distribuito al sensore, viene espanso in sedici regole, come mostrato nell'immagine:

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 80 any 6 (log dcforward flowstart) (url
"twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 443 any 6 (log dcforward flowstart) (url
"twitter.com")
268435456 allow any any any any any any any any (ipspolicy 2)
```

Quando si distribuisce una regola con due subnet configurate come origine, due host configurati come indirizzi di destinazione e due oggetti URL personalizzati destinati a due porte, questa regola si espande a sedici regole sul sensore.

> **Nota**: se è necessario utilizzare le porte nella regola di accesso, utilizzare **i rilevatori applicazioni** presenti per le applicazioni standard. In questo modo l'espansione delle regole può avvenire in modo efficiente.

Prendere in considerazione la configurazione di una regola di accesso da FMC, come illustrato nell'immagine:

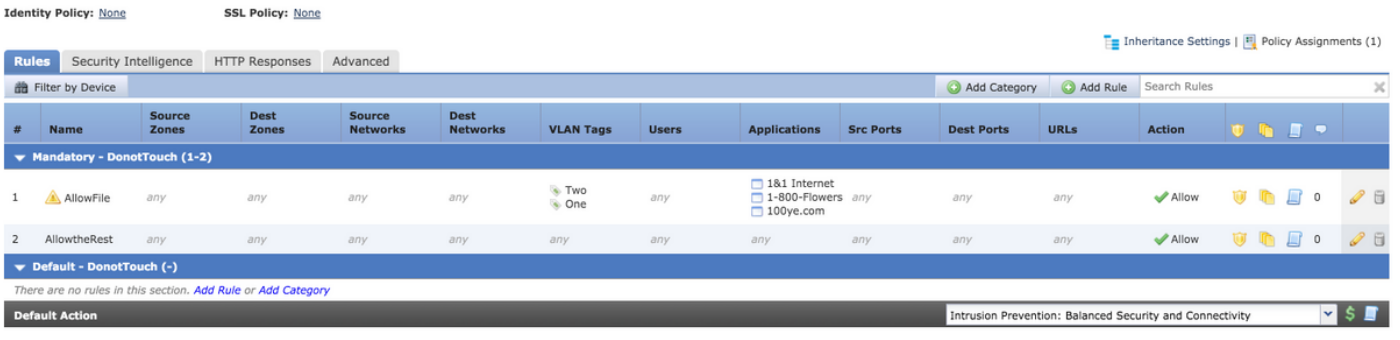


Quando si utilizzano i rilevatori di applicazioni invece delle porte, il numero di regole espanse si riduce da sedici a otto, come mostrato nell'immagine:

```
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 1.1.1.1 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 1.1.1.1 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 2.2.2.2 32 any any 3.3.3.3 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "facebook.com")
268436480 allow any 2.2.2.2 32 any any 4.4.4.4 32 any any any (log dcforward flowstart) (appid
676:1, 1122:1) (url "twitter.com")
```

Espansione di una regola IP tramite VLAN

Prendere in considerazione la configurazione di una regola di accesso da FMC, come illustrato nell'immagine:



La regola **AllowFile** ha una sola riga che corrisponde a due ID VLAN con alcuni rilevatori di applicazioni, criteri per le intrusioni e criteri per i file. La regola AllowFile si espanderà a due regole.

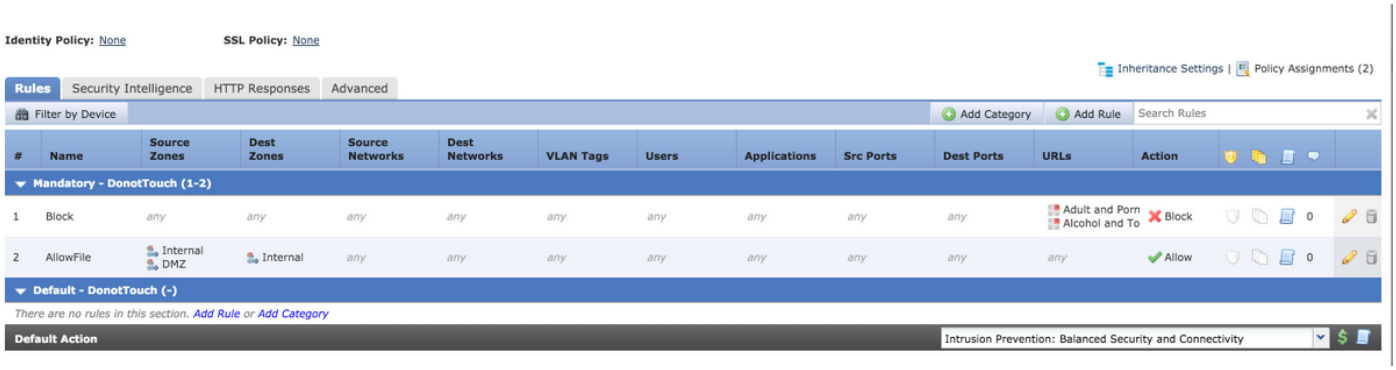
```
268436480 allow any any any any any any 1 any (log dcforward flowstart) (ipspolicy 5)
(filepolicy 1 enable) (appid 535:4, 1553:4, 3791:4)
```

```
268436480 allow any any any any any any 2 any (log dcforward flowstart) (ipspolicy 5)
(filepolicy 1 enable) (appid 535:4, 1553:4, 3791:4)
```

I criteri IPS e i criteri file sono univoci per ogni regola di controllo di accesso, ma più rilevatori di applicazioni fanno riferimento alla stessa regola e pertanto non partecipano all'espansione. Se si considera una regola con due ID VLAN e tre rilevatori di applicazioni, esistono solo due regole, una per ciascuna VLAN.

Espansione di una regola basata su IP con categorie URL

Prendere in considerazione la configurazione di una regola di accesso da FMC, come illustrato nell'immagine:



La regola di blocco blocca le categorie URL per **adulto e pornografia Qualsiasi reputazione** e **reputazione alcol e tabacco 1-3.** Si tratta di una regola singola nel centro di gestione, ma quando la si distribuisce al sensore viene espansa in due regole, come mostrato di seguito:

```
268438530 deny any any  any any any  any any any  (log dcforward flowstart) (urlcat 11)
268438530 deny any any  any any any  any any any  (log dcforward flowstart) (urlcat 76) (urlrep
le 60)
```

Quando si distribuisce una singola regola con due subnet configurate come origine e due host configurati come indirizzi di destinazione, insieme a due oggetti URL personalizzati destinati a due porte con due categorie URL, questa regola si espande a trentadue regole sul sensore.

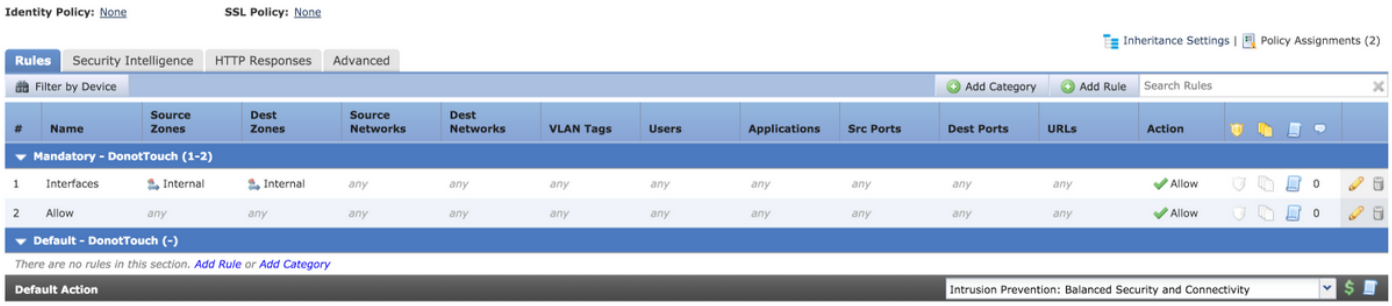
Espansione di una regola IP con zone

Alle zone vengono assegnati numeri a cui si fa riferimento nei criteri.

Se in un criterio viene fatto riferimento a un'area che non è assegnata ad alcuna interfaccia nel dispositivo a cui viene applicato il criterio, l'area viene considerata come **qualsiasi** e **qualsiasi** non comporta l'espansione delle regole.

Se la zona di origine e la zona di destinazione coincidono nella regola, il fattore di zona viene considerato come **qualsiasi** e viene aggiunta una sola regola poiché ANY non determina l'espansione delle regole.

Prendere in considerazione la configurazione di una regola di accesso da FMC, come illustrato nell'immagine:



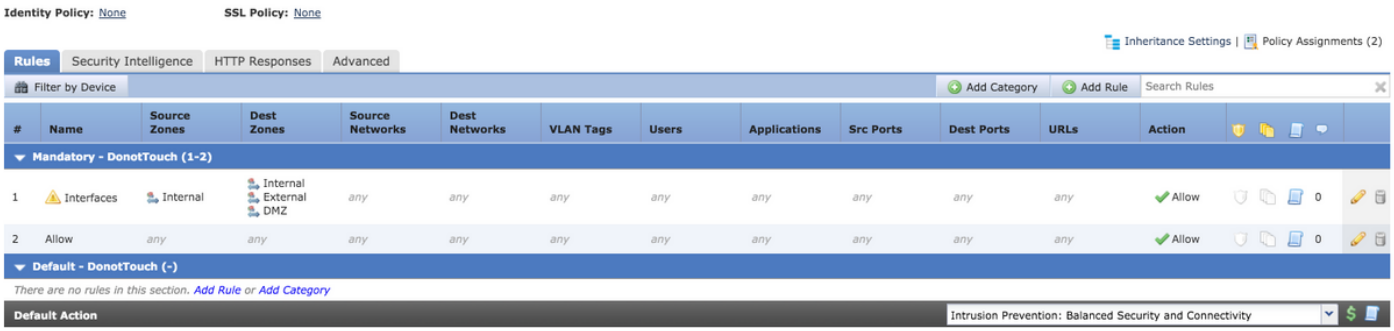
Ci sono due regole. In una regola sono configurate zone, ma la zona di origine e la zona di destinazione sono uguali. L'altra regola non ha una configurazione specifica. In questo esempio, la regola di accesso **Interfacce** non viene convertita in una regola.

```
268438531 allow any any any any any any any any (log dcforward flowstart)<-----Allow Access Rule
268434432 allow any any any any any any any any (log dcforward flowstart) (ipspolicy 17)<-------
---Default Intrusion Prevention Rule
```

Sul sensore entrambe le regole appaiono identiche perché il controllo basato su zona che coinvolge le stesse interfacce non porta ad un'espansione.

L'espansione delle regole per l'accesso alle regole di controllo d'accesso basate sulle zone si verifica quando la zona a cui si fa riferimento nella regola viene assegnata a un'interfaccia sul dispositivo.

Considerare la configurazione di una regola di accesso dal FMC come illustrato di seguito:



La regola Interfacce interessa le regole basate sulla zona con la zona di origine come zona interna e le zone di destinazione come interna, esterna e DMZ. In questa regola, le zone interfaccia interna e DMZ sono configurate sulle interfacce e l'area Esterna non esiste sul dispositivo. Questa è l'espansione della stessa:

```
268436480 allow 0 any any 2 any any any any (log dcforward flowstart) <------Rule for Internal
to DMZ)
268438531 allow any any any any any any any any (log dcforward flowstart)<--------Allow Access
rule
268434432 allow any any any any any any any any (log dcforward flowstart) (ipspolicy 17)<-------
-Default Intrusion Prevention: Balanced Security over Connectivity
```

Viene creata una regola per una coppia di interfacce specifica, ovvero **Interno > DMZ** con specifica clear zone e non viene creata una regola **Interno >Interno**.

Il numero di regole espanse è proporzionale al numero di coppie di origine e destinazione delle

zone che possono essere create per zone associate **valide** e che includono le stesse regole di origine e di destinazione.

> **Nota:** Durante la distribuzione dei criteri, le regole disattivate dal CCP non vengono propagate e non vengono espanse al sensore.

Formula generale per espansione regola

Numero di regole sul sensore = (Numero di subnet o host di origine) * (Numero di porte di destinazione) * (Numero di porte di origine) * (Numero di porte di destinazione) * (Numero di URL personalizzati)* (Numero di tag VLAN)* (Numero di categorie URL)* (Numero di coppie di zone di origine e destinazione valide)

> **Nota:** Per i calcoli, **qualsiasi** valore nel campo viene sostituito da 1. Il valore **any** nella combinazione di regole viene considerato come 1 e non aumenta né espande la regola.

Risoluzione dei problemi di distribuzione a causa dell'espansione delle regole

Se si verifica un errore di distribuzione dopo aver aggiunto la regola di accesso, eseguire la procedura indicata di seguito per i casi in cui è stato raggiunto il limite di espansione della regola

Controllare se nel file **/var/log/action.queue.log sono presenti** messaggi con le seguenti parole chiave:

Errore - troppe regole - scrittura regola 28, numero massimo regole 9094

Il messaggio precedente indica che si è verificato un problema con il numero di regole da espandere. Controllare la configurazione del CCP per ottimizzare le regole in base a quanto descritto sopra.

Informazioni correlate

- Guida alla configurazione di Firepower Management Center, versione 6.0
- Documentazione e supporto tecnico – Cisco Systems