Informazioni sulla funzionalità FQDN in Firepower Threat Defense (gestito da FMC)

Sommario

Introduzione

In questo documento viene descritta la configurazione della funzionalità FQDN (versione 6.3.0) in Firepower Management Center (FMC) e Firepower Threat Defense (FTD).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firepower Management Center

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

- Cisco Firepower Threat Defense (FTD) Virtual con software versione 6.3.0
- Firepower Management Center Virtual (vFMC) con software versione 6.3.0

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

In questo documento viene descritta la configurazione della funzionalità Nome di dominio completo (FQDN) introdotta dalla versione 6.3.0 del software in Firepower Management Center (FMC) e Firepower Threat Defense (FTD).

Questa funzione è presente in Cisco Adaptive Security Appliance (ASA) ma non era presente nelle versioni software iniziali di FTD.

Prima di configurare gli oggetti FQDN, verificare che siano soddisfatte le condizioni seguenti:

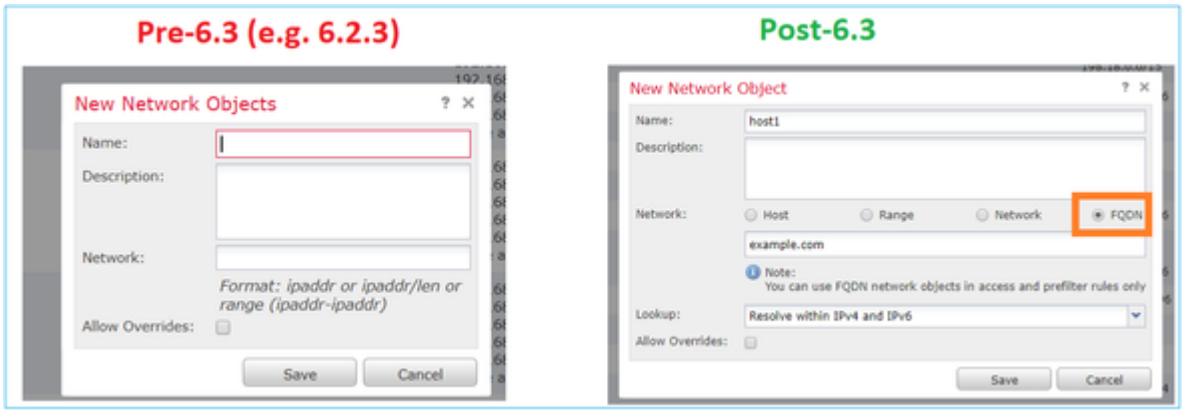
- Firepower Management Center deve eseguire la versione 6.3.0 o successive. Può essere fisico o virtuale
- Firepower Threat Defense deve eseguire la versione 6.3.0 o successiva. Può essere fisico o virtuale

Panoramica delle funzionalità

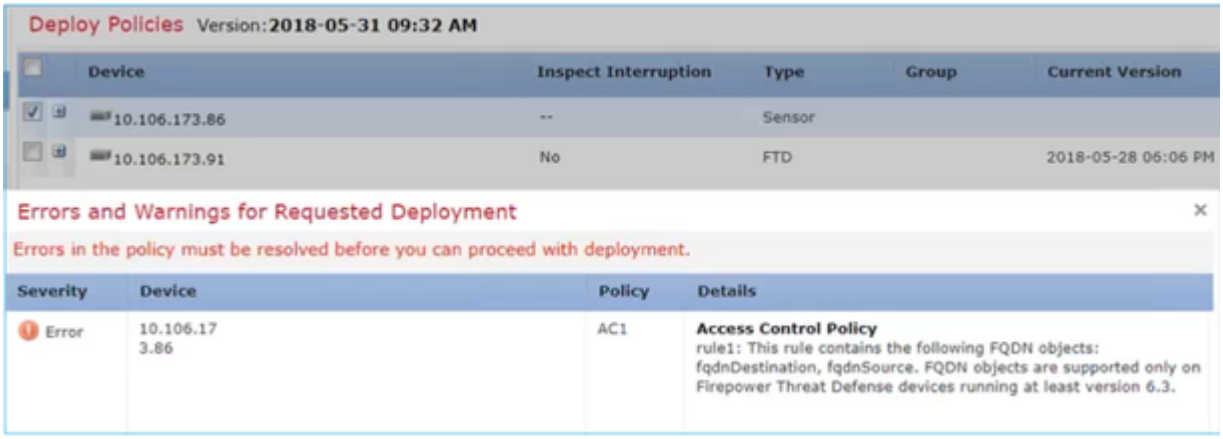
Questa funzionalità risolve un FQDN in un indirizzo IP e utilizza quest'ultimo per filtrare il traffico quando vi viene fatto riferimento da una regola di controllo dell'accesso o da un criterio di prefiltro.

E per quanto riguarda le versioni precedenti alla 6.3?

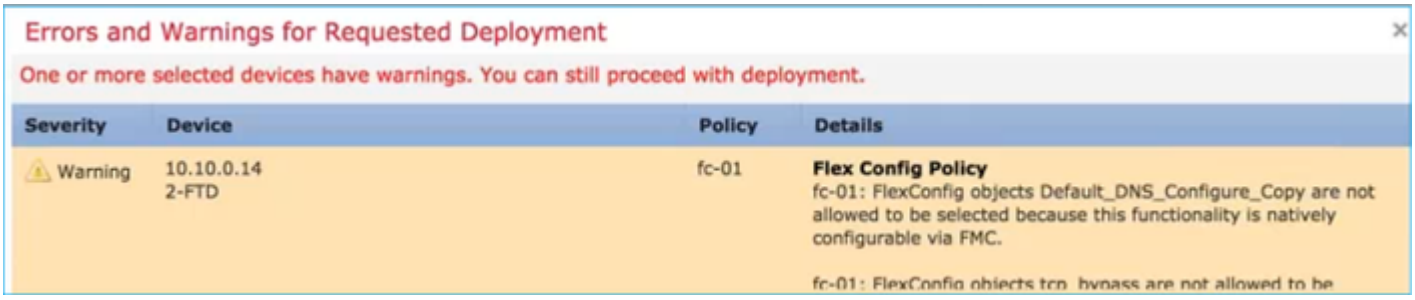
- FMC e FTD che eseguono una versione precedente alla 6.3.0 non possono configurare oggetti FQDN.



- Nel caso in cui FMC esegua la versione 6.3 o successive ma FTD esegua una versione precedente alla 6.3, nella distribuzione di un criterio viene visualizzato questo errore:

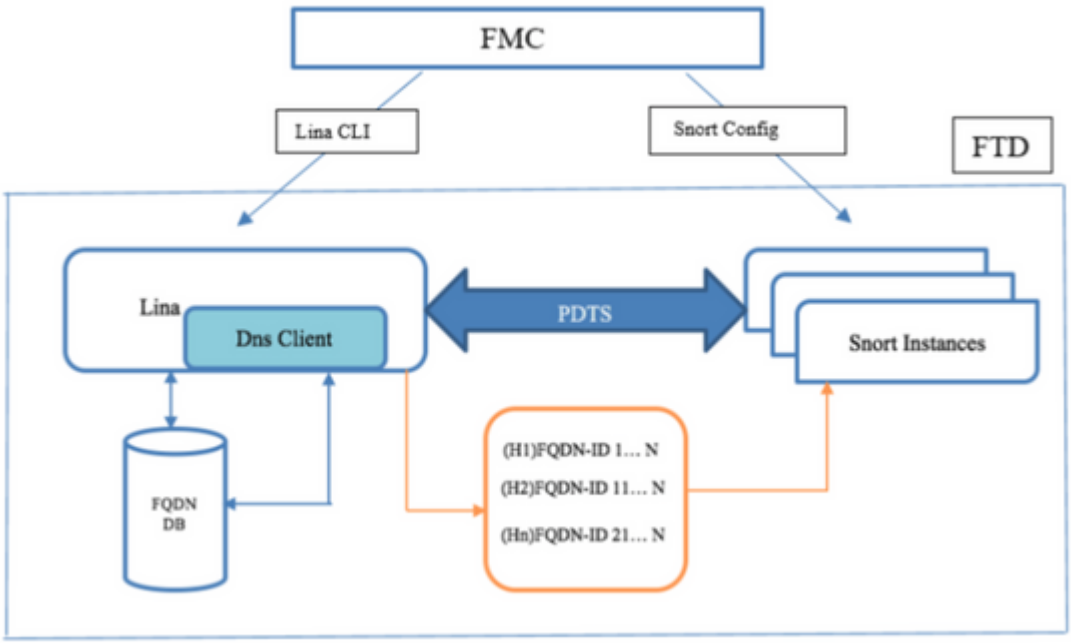


- Inoltre, se si configura tramite FlexConfig un oggetto DNS, viene visualizzato questo avviso:



Configurazione

Esempio di rete



Architettura - Punti salienti

- Risoluzione DNS (da DNS a IP) in LINA
- LINA memorizza il mapping nel proprio database
- Per ogni connessione, questa mappatura viene inviata da LINA a snort
- La risoluzione di FQDN avviene indipendentemente dalla configurazione ad alta disponibilità o cluster

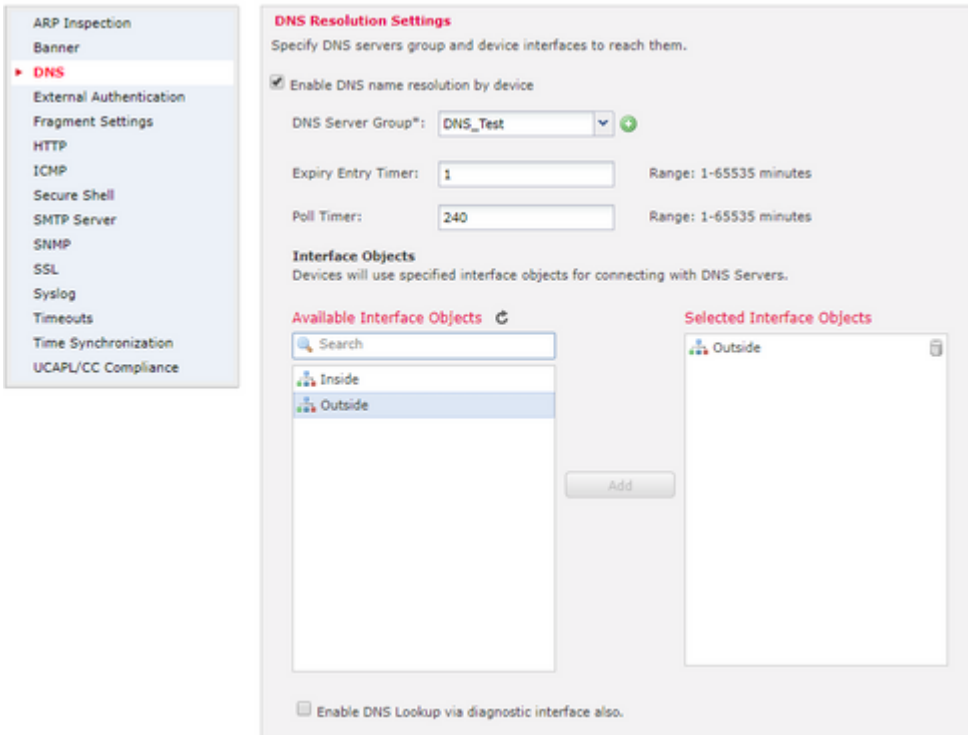
Procedura di configurazione

Passaggio 1. Configurare "Oggetto gruppo server DNS"

â€ƒ

- Il nome del gruppo di server DNS non deve superare i 63 caratteri
- In una distribuzione multidominio, i nomi degli oggetti devono essere univoci all'interno della gerarchia dei domini. Il sistema può identificare un conflitto con il nome di un oggetto che non è possibile visualizzare nel dominio corrente
- Il dominio predefinito (facoltativo) viene utilizzato per aggiungere ai nomi host non completamente qualificati
- I valori predefiniti per Tentativi e Timeout sono precompilati.
    - Tentativi: il numero di tentativi, da 0 a 10, per ripetere l'elenco dei server DNS quando il sistema non riceve una risposta. Il valore predefinito è 2.
    - Timeout: il numero di secondi, da 1 a 30, prima di un altro tentativo di passare al server DNS successivo. L'impostazione predefinita è 2 secondi. Ogni volta che il sistema ripete l'elenco dei server, questo timeout raddoppia.
- Immettere i server DNS da includere nel gruppo. Può essere un formato IPv4 o IPv6 come valori delimitati da virgole
- Il gruppo di server DNS viene utilizzato per la risoluzione con l'oggetto o gli oggetti di interfaccia configurati in Impostazioni piattaforma
- L'API REST per il CRUD dell'oggetto gruppo server DNS è supportata

Passaggio 2. Configura DNS (impostazioni piattaforma)



- (Facoltativo) Modificare i valori Timer voci scadenza e Timer polling in minuti:

L'opzione del timer della voce di scadenza specifica il limite di tempo per la rimozione dell'indirizzo IP di un FQDN risolto dalla tabella di ricerca DNS dopo la scadenza del relativo valore TTL (Time-to-Live). La rimozione di una voce richiede la ricompilazione della tabella, pertanto le rimozioni frequenti possono aumentare il carico del processo sul dispositivo. Questa impostazione estende virtualmente il valore TTL.

L'opzione poll timer specifica il limite di tempo trascorso il quale il dispositivo esegue una query sul server DNS per risolvere il nome FQDN definito in un gruppo di oggetti di rete. Un FQDN viene risolto periodicamente quando il timer di polling è scaduto o quando il valore TTL della voce IP risolta è scaduto, a seconda di quale condizione si verifica per prima.

- (Facoltativo) Selezionare gli oggetti di interfaccia richiesti dall'elenco degli oggetti disponibili e aggiungerli all'elenco Oggetti di interfaccia selezionati e verificare che il server DNS sia raggiungibile tramite le interfacce selezionate:

Per i dispositivi Firepower Threat Defense 6.3.0, se non viene selezionata alcuna interfaccia e l'interfaccia diagnostica è disabilitata per la ricerca DNS, la risoluzione DNS viene eseguita tramite qualsiasi interfaccia che include l'interfaccia diagnostica (viene applicato il comando dnsdomain-lookup any).

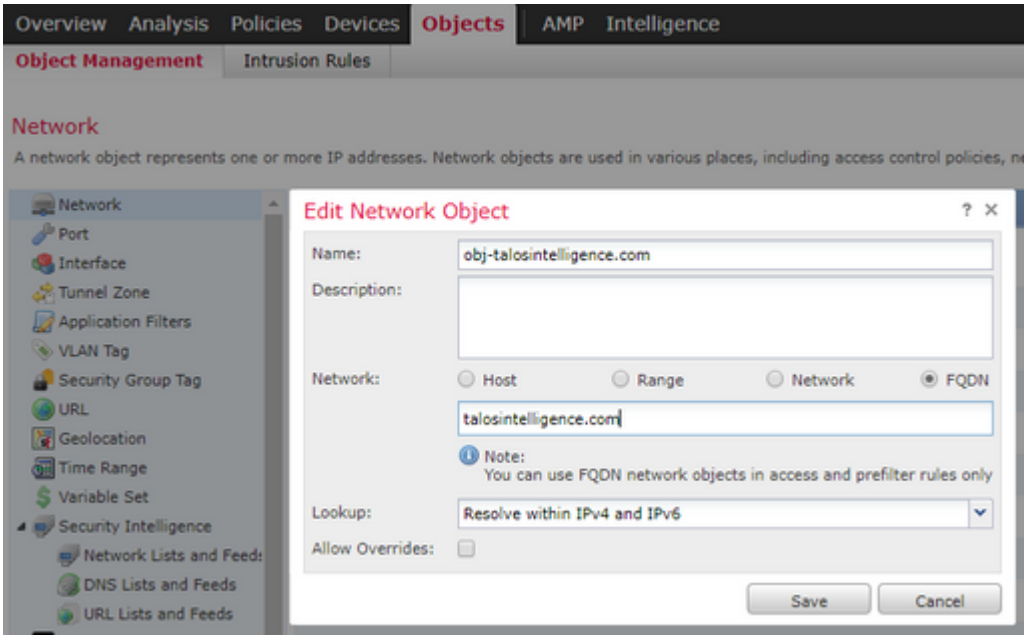
Se non si specifica alcuna interfaccia e non si abilita la ricerca DNS sull'interfaccia diagnostica, l'FTD utilizza la tabella di routing dei dati per determinare l'interfaccia. In caso contrario, viene utilizzata la tabella di routing di gestione.

- (Facoltativo) Selezionare la casella di controllo Abilita ricerca DNS anche tramite interfaccia diagnostica

Se abilitato, Firepower Threat Defense utilizza sia le interfacce dati selezionate che l'interfaccia diagnostica per le risoluzioni DNS. Assicurarsi di configurare un indirizzo IP per l'interfaccia di diagnostica nella pagina Dispositivi > Gestione dispositivi > Modifica dispositivo > Interfacce.

Passaggio 3. Configurare il nome di dominio completo (FQDN) della rete di oggetti

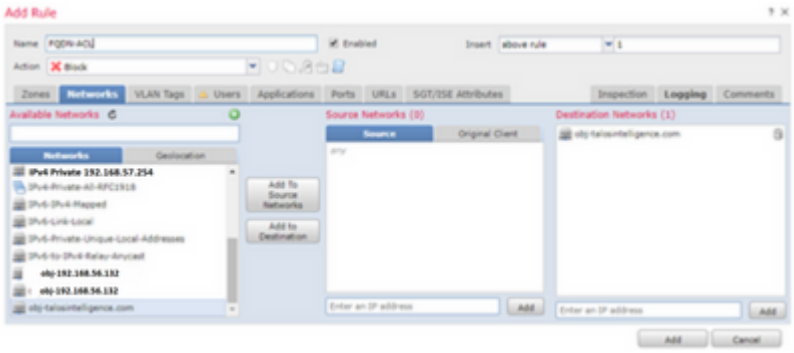
Passare a Oggetti > Gestione oggetti, all'interno di un oggetto di rete specificare selezionare l'opzione FQDN.



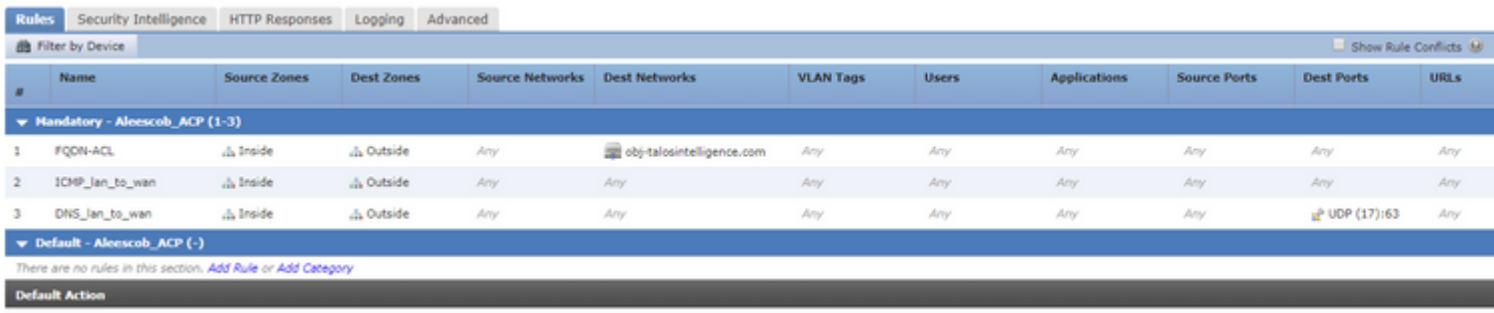
- Un ID univoco a 32 bit viene generato quando l'utente crea un oggetto FQDN
- Questo ID viene inviato da FMC a LINA e Snort
- In LINA questo ID è associato all'oggetto
- In snort, questo ID è associato alla regola di controllo d'accesso che contiene l'oggetto

Passaggio 4. Creare una regola di controllo d'accesso

Creare una regola con l'oggetto FQDN precedente e distribuire il criterio:



â€ƒ



Nota: la prima istanza della risoluzione FQDN si verifica quando l'oggetto FQDN viene distribuito in un criterio di controllo di accesso

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

- Questa è la configurazione iniziale FTD prima della distribuzione dell'FQDN:

```
aleescob# show run dns
DNS server-group DefaultDNS
```

- Questa è la configurazione dopo la distribuzione FQDN:

```
aleescob# show run dns
dns domain-lookup wan_1557
DNS server-group DNS_Test
    retries 3
    timeout 5
    name-server 172.31.200.100
    domain-name aleescob.cisco.com
DNS server-group DefaultDNS
dns-group DNS_Test
```

- Ecco l'aspetto dell'oggetto FQDN in LINA:

```
object network obj-talosintelligence.com
 fqdn talosintelligence.com id 268434436
```

- Quando è già distribuito, questo è l'aspetto dell'elenco degli accessi FQDN in LINA:

```
access-list CSM_FW_ACL_ remark rule-id 268434437: ACCESS POLICY: Aleescob_ACP - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268434437: L4 RULE: FQDN-ACL
access-list CSM_FW_ACL_ advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintelligence.com
```

- Ecco come appare in Snort (ngfw.rules):

```
# Start of AC rule.
268434437 deny 1 any  any 2 any  any any any  (log dcforward flowstart) (dstfqdn 268434436)
# End rule 268434437
```

Nota: in questo scenario, poiché l'oggetto FQDN è stato utilizzato per la destinazione, viene elencato come dstfqdn.

- Se si seleziona show dns e show fqdn commands, si noterà che la funzione ha iniziato a risolvere l'IP per tallosintelligence:

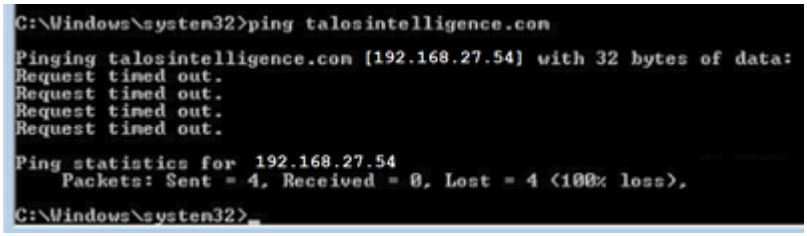
```
aleescob# show dns
Name: talosintelligence.com
  Address: 2001:DB8::6810:1b36                          TTL 00:05:43
  Address: 2001:DB8::6810:1c36                          TTL 00:05:43
  Address: 2001:DB8::6810:1d36                          TTL 00:05:43
  Address: 2001:DB8::6810:1a36                          TTL 00:05:43
  Address: 2001:DB8::6810:1936                          TTL 00:05:43
  Address: 192.168.27.54                                  TTL 00:05:43
  Address: 192.168.29.54                                  TTL 00:05:43
  Address: 192.168.28.54                                  TTL 00:05:43
  Address: 192.168.26.54                                  TTL 00:05:43
  Address: 192.168.25.54                                  TTL 00:05:43


aleescob# show fqdn
FQDN IP Table:
ip = 2001:DB8::6810:1b36, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 2001:DB8::6810:1c36, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 2001:DB8::6810:1d36, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 2001:DB8::6810:1a36, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 2001:DB8::6810:1936, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 192.168.27.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 192.168.29.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 192.168.28.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 192.168.26.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

ip = 192.168.25.54, object = obj-talosintelligence.com, domain = talosintelligence.com
        FQDN-ID = 268434436

FQDN ID Detail:
FQDN-ID = 268434436, object = obj-talosintelligence.com, domain = talosintelligence.com
        ip = 2001:DB8::6810:1b36, 2001:DB8::6810:1c36, 2001:DB8::6810:1d36, 2001:DB8::6810:1a36, 2001:DB
```

- Se si seleziona Mostra elenco accessi in LINA, è possibile notare le voci espanse per ciascuna

risoluzione e il numero di accessi:

```
firepower# show access-list
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintell
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 fqdn talosintelligence
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1b
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1c
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1d
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1a
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:19
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.27.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.29.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.28.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.26.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.25.54 (ta
```

- Come mostrato nell'immagine, il ping verso talosintelligence.com ha esito negativo perché esiste una corrispondenza per il nome FQDN nell'elenco degli accessi. La risoluzione DNS ha funzionato poiché il pacchetto ICMP è bloccato dall'FTD.



â€ƒ

- Numero di accessi da LINA per i pacchetti ICMP inviati in precedenza:

```
access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintellig
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 fqdn talosintelligence
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1b
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1c
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1d
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:1a
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 2001:DB8::6810:19
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.27.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.29.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.28.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.26.54 (ta
  access-list CSM_FW_ACL_ line 10 advanced deny ip ifc lan_v1556 any ifc wan_1557 host 192.168.25.54 (ta
```

- Le richieste ICMP vengono acquisite e visualizzate come eliminate nell'interfaccia in entrata:

aleescob# show cap in 13 pacchetti acquisiti 1: 18:03:41.558915 192.168.56.132 > 172.31.200.100 icmp: 192.168.56.132 udp port 59396 unreachable 2: 18:04:12.322126 2.168.56.132 > 172.31.4.161 icmp: richiesta echo 3: 18:04:12.479162 172.31.4.161 > 192.168.56.132 icmp: risposta echo 4: 18:04:13.309966 192.168 6.132 > 172.31.4.161 icmp: richiesta echo 5: 18:04:13.462149 172.31.4.161 > 192.168.56.132 icmp: risposta echo 6: 18:04:14.308425 192.168.56.132 > 72.31.4.161 icmp: richiesta echo 7:

18:04:14.475424 172.31.4.161> 192.168.56.132 icmp: risposta echo 8: 18:04:15.306823 192.168.56.132 > 172.31.4 2.161 icmp: richiesta echo 9: 18:04:15.46339 172.31.4.161 > 192.168.56.132 icmp: risposta echo 10: 18:04:25.713662 192.168.56.132 > 192.168.27.5 icmp: richiesta echo 11: 18:04:30.704232 192.168.56.132 > 192.168.27.54 icmp: richiesta echo 12: 18:04:35.711480 192.168.56.132 > 192.168.27.54: richiesta echo 13: 18:04:40.707528 192.168.56.132 > 192.168.27.54 icmp: richiesta echo aleescob# sho cap asp | in 192.168.27.54.162: 18:04:25.713799 192.168.56.132 > 192.168.27.54 icmp: richiesta echo 165: 18:04:30.704355 192.168.56.132 > 1 92.168.27.54 icmp: richiesta echo 168: 18:04:35.71556 192.168.56.132 > 192.168.27.54 icmp: richiesta echo 176: 18:04:40.707589 192.168.56.132 > 192.168.27.54 icmp: richiesta echo

- In questo modo la traccia cerca uno dei seguenti pacchetti ICMP:

```
aleescob# sho cap in packet-number 10 trace

13 packets captured

  10: 18:04:25.713662       192.168.56.132 > 192.168.27.54 icmp: echo request
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.57.254 using egress ifc  wan_1557

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip ifc lan_v1556 any ifc wan_1557 object obj-talosintelligence.com
access-list CSM_FW_ACL_ remark rule-id 268434437: ACCESS POLICY: Aleescob_ACP - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268434437: L4 RULE: FQDN-ACL
Additional Information:

Result:
input-interface: lan_v1556
input-status: up
input-line-status: up
output-interface: wan_1557
```

```
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

- Se l'azione per la regola di controllo di accesso è Consenti, questo è un esempio dell'output del comando system support firewall-engine-debug

```
> system support firewall-engine-debug

Please specify an IP protocol: icmp
Please specify a client IP address: 192.168.56.132
Please specify a server IP address:
Monitoring firewall engine debug messages

192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 new firewall session
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 DAQ returned DST FQDN ID: 268434436
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 Starting with minimum 2, 'FQDN-ACL', and SrcZone first wit
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 Match found for FQDN id: 268434436
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 match rule order 2, 'FQDN-ACL', action Allow
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 MidRecovery data sent for rule id: 268434437,rule_action:2
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 allow action
192.168.56.132-8 > 192.168.29.54-0 1 AS 1 I 0 deleting firewall session
```

- Quando il nome di dominio completo (FQDN) viene distribuito come parte di un prefiltro (Fastpath), viene visualizzato nel file ngfw.rules nel modo seguente:

```
iab_mode Off
# Start of tunnel and priority rules.
# These rules are evaluated by LINA. Only tunnel tags are used from the matched rule id.
268434439 fastpath any any  any any any  any any any  (log dcforward both) (tunnel -1)
268434438 allow any any  1025-65535 any any  3544 any 17  (tunnel -1)
268434438 allow any any  3544 any any  1025-65535 any 17  (tunnel -1)
268434438 allow any any  any any any  any any 47  (tunnel -1)
268434438 allow any any  any any any  any any 41  (tunnel -1)
268434438 allow any any  any any any  any any 4  (tunnel -1)
# End of tunnel and priority rules.
```

- Dal punto di vista di LINA con un pacchetto tracciato:

```
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust ip any object obj-talosintelligence.com rule-id 268434439 event-l
access-list CSM_FW_ACL_ remark rule-id 268434439: PREFILTER POLICY: Prefilter-1
access-list CSM_FW_ACL_ remark rule-id 268434439: RULE: FQDN_Prefilter
Additional Information:
```

Risoluzione dei problemi

1. Configurazione da FMC

- Verificare che i criteri e le impostazioni del server DNS siano configurati correttamente
- Verificare che la distribuzione sia riuscita

2. Distribuisci controllo su FTD

- Eseguire show dns e show access-list per verificare se l'FQDN è stato risolto e le regole AC sono state espanse
- Eseguire il comando show run object network e annotare l'ID associato all'oggetto (ad esempio X per source)
- Eseguire il comando show fqdn id X per verificare che l'FQDN sia risolto correttamente nell'IP di origine
- Verificare se nel file ngfw.rules è presente una regola CA con ID FQDN X come origine
- Eseguire il debug firewall-engine di supporto del sistema e verificare il verdetto Snort

Raccolta dei problemi relativi a FMC

Tutti i registri necessari vengono raccolti da una risoluzione dei problemi FMC. Per raccogliere tutti i registri importanti dal CCP, eseguire una procedura di risoluzione dei problemi dall'interfaccia utente del CCP. In caso contrario, dal prompt di FMC Linux eseguire sf_troubleshoot.pl. Se si riscontra un problema, inviare una segnalazione di risoluzione dei problemi FMC al Technical Assistance Center (TAC) di Cisco.

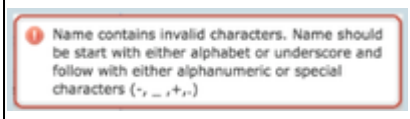
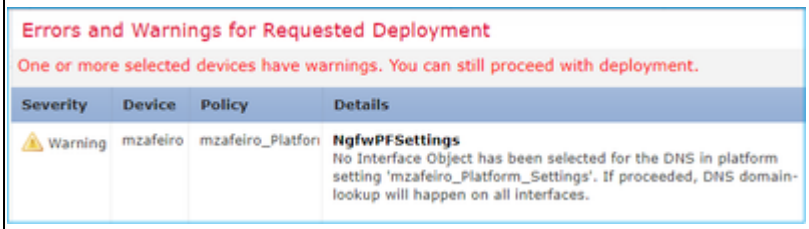
Registri FMC

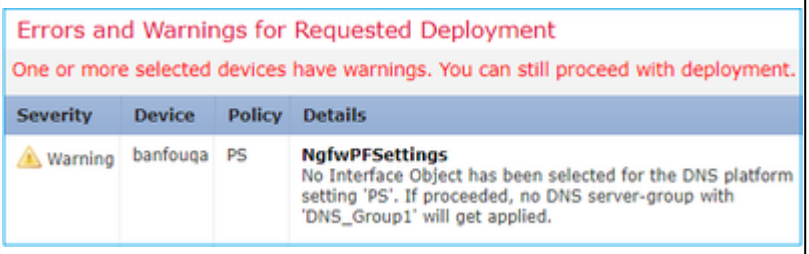
Nome/percorso file di registro	Scopo
`/opt/CSCOpx/MDC/log/operation/vmssharedsvcs.log`	Tutte le chiamate API
`/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log`	Tutte le chiamate API
`/opt/CSCOpx/MDC/log/operation/vmsbesvcs.log`	Log di generazione CLI
`/opt/CSCOpx/MDC/tomcat/logs/stdout.log`	Registri Tomcat
	Log Mojo

/var/log/mojo.log	
/var/log/CSMAgent.log	Chiamate REST tra CSM e DC
/var/log/action_queue.log	Log coda azioni del controller di dominio

Problemi comuni/Messaggi di errore

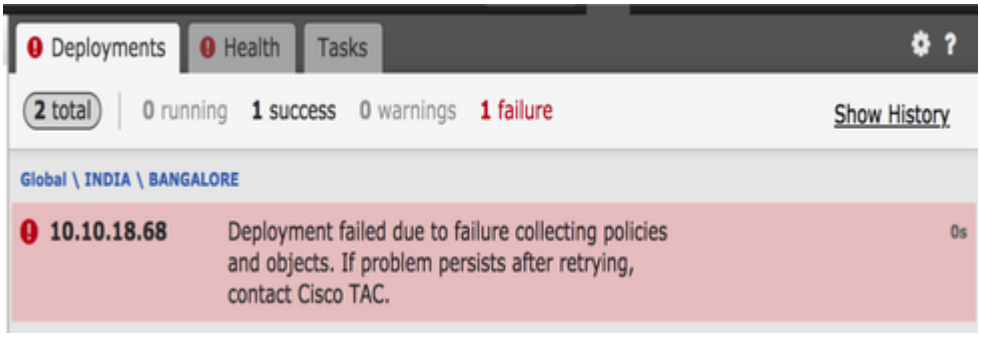
Errori/avvisi visualizzati nell'interfaccia utente per l'oggetto gruppo di server DNS e FQDN e le impostazioni DNS:

Errore/Avviso	Scenario	Descrizione
 Il nome contiene caratteri non validi. I nomi devono iniziare con un carattere alfabetico o di sottolineatura e quindi con caratteri alfanumerici o speciali. (-,_,+,.)	Utente configura un nome errato	L'utente viene informato dell'autorizzazione caratteri e intervallo massimo.
 Valore dominio predefinito non valido	L'utente configura un nome di dominio errato	L'utente viene informato sui caratteri consentiti e sull'intervallo massimo.
 Nessun oggetto interfaccia selezionato per il DNS nell'impostazione della piattaforma "mzafeiro_Platform_Settings". Se si continua, la ricerca del dominio DNS verrà eseguita a breve in tutte le interfacce	L'utente non seleziona alcuna interfaccia per la ricerca nel dominio Per un dispositivo post-6.3	L'utente viene avvisato che il DNS presto verrà applicata la CLI del gruppo di server a tutte le interfacce.

 Nessun oggetto interfaccia selezionato per il DNS nell'impostazione della piattaforma "mzafeiro_Platform_Settings". Se si continua, presto non verrà applicato alcun gruppo di server DNS con â€˜DNSâ€™	L'utente non seleziona alcuna interfaccia per la ricerca nel dominio Per un dispositivo 6.2.3	L'utente viene avvisato che il DNS la CLI del gruppo di server non generato.

Errore di distribuzione

Quando si utilizza un nome di dominio completo (FQDN) in un criterio diverso da Criterio CA/Prefiltro, è possibile che questo errore si verifichi e venga visualizzato nell'interfaccia utente di FMC:



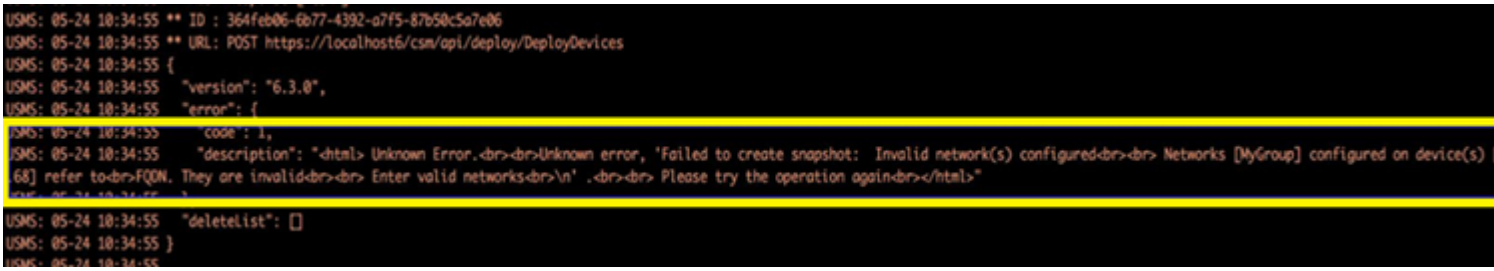
Fasi consigliate per la risoluzione dei problemi

1) Aprire il file di registro: /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log

2) Verificare la presenza di un messaggio di convalida simile al seguente:

"Configurate reti non valide. Reti [NetworksContainingFQDN] configurate sui dispositivi[DeviceNames] fare riferimento a FQDN"

â€ƒ



â€ƒ

3) Azione suggerita:

Verificare se uno o più dei criteri indicati di seguito sono già configurati con un FQDN o un gruppo che

contiene uno o più oggetti FQDN e riprovare la distribuzione dopo la rimozione di tali oggetti.

a) Politica di identità

b) Set di variabili che contengono un FQDN applicato ai criteri AC

Nessun FQDN attivato

Il sistema può visualizzare il successivo tramite la CLI FTD:

> show dns INFO: nessun FQDN attivato

Il DNS non verrà attivato fino a quando non verrà applicato un oggetto con un nome di dominio completo definito. L'applicazione di un oggetto determina la risoluzione del problema.

Domande e risposte

D: Packet-tracer con FQDN è un test valido per la risoluzione dei problemi?
R: Sì, è possibile utilizzare l'opzione fqdn con packet-tracer.

D: Con quale frequenza la regola FQDN aggiorna l'indirizzo IP del server?
R: Dipende dal valore TTL della risposta DNS. Dopo la scadenza del valore TTL, l'FQDN viene risolto di nuovo con una nuova query DNS.
Ciò dipende anche dall'attributo Poll Timer definito nella configurazione del server DNS. La regola FQDN viene risolta periodicamente quando il timer Poll DNS è scaduto o quando il valore TTL della voce IP risolta è scaduto, a seconda di quale condizione si verifica per prima.

D: Funziona per il DNS round robin?
R: Il DNS round-robin funziona senza problemi, in quanto questa funzionalità funziona sul FMC/FTD con l'utilizzo di un client DNS e la configurazione del DNS round-robin è sul lato del server DNS.

D: Esiste un limite per i valori DNS TTL bassi?
R: Se la risposta DNS arriva con 0 TTL, il dispositivo FTD vi aggiunge 60 secondi. In questo caso, il valore TTL è almeno 60 secondi.

D: Quindi per impostazione predefinita l'FTD mantiene il valore predefinito di 60 secondi?
R. L'utente può sempre ignorare il valore TTL con l'impostazione Timer voce scadenza nel server DNS.

D: Come interagisce con le risposte DNS anycast? I server DNS, ad esempio, possono fornire indirizzi IP diversi in base alla geolocalizzazione dei richiedenti. È possibile richiedere tutti gli indirizzi IP per un FQDN? Come il comando dig su Unix?
R: Sì, se il nome di dominio completo è in grado di risolvere più indirizzi IP, tutti vengono inviati al dispositivo e la regola CA si espande di conseguenza.

D: È prevista l'inclusione di un'opzione di anteprima che mostri che i comandi vengono sottoposti a push prima di qualsiasi modifica di distribuzione?
R: Fa parte dell'opzione **Preview config** disponibile tramite Flex config. L'anteprima è già presente, ma è nascosta nei criteri di configurazione Flex. C'è un piano per spostarlo e renderlo generico.

D: Quale interfaccia dell'FTD viene utilizzata per eseguire la ricerca DNS?
R: È configurabile. Quando non è configurata alcuna interfaccia, tutte le interfacce denominate su FTD sono abilitate per la ricerca DNS.

D: Ogni NGFW gestito esegue separatamente la propria risoluzione DNS e la traduzione IP del nome FQDN anche quando lo stesso criterio di accesso viene applicato a tutti i NGFW gestiti con lo stesso oggetto FQDN?
R: Sì.

D: È possibile cancellare la cache DNS per gli ACL FQDN per la risoluzione dei problemi?
R: Sì, è possibile eseguire i comandi **clear dns** e **clear dns-hosts cache** sul dispositivo.

D: Quando viene attivata esattamente la risoluzione FQDN?
R: La risoluzione FQDN si verifica quando l'oggetto FQDN viene distribuito in un criterio AC.

D: È possibile eliminare la cache solo per un singolo sito?
R: Sì. Se si conosce il nome di dominio o l'indirizzo IP, è possibile cancellarlo, ma non è disponibile alcun comando per la prospettiva degli ACL. Ad esempio, il comando **clear dns host agni.tejas.com** è presente per cancellare la cache su base host per host con la parola chiave host come in **dns host agni.tejas.com**.

D: È possibile utilizzare caratteri jolly, come *.microsoft.com?
R: No. L'FQDN deve iniziare e terminare con una cifra o una lettera. Sono consentiti solo lettere, cifre e trattini come caratteri interni.

D: La risoluzione dei nomi viene eseguita al momento della compilazione CA e non al momento della prima o delle successive richieste? Se si raggiunge un valore TTL basso (inferiore al tempo di compilazione CA, fast-flux o altro), è possibile che alcuni indirizzi IP non vengano visualizzati?
R: La risoluzione dei nomi viene eseguita subito dopo la distribuzione dei criteri di autorizzazione delle connessioni. Alla scadenza del tempo TTL, viene eseguito il rinnovo.

D: È prevista la possibilità di elaborare l'elenco di indirizzi IP cloud (XML) di Microsoft Office 365?
R: Non supportato in questo momento.

D. L'FQDN è disponibile nei criteri SSL?
R: Non per il momento (versione software 6.3.0). Gli oggetti FQDN sono supportati solo nella rete di origine e di destinazione per i criteri AC.

D. Sono presenti registri cronologici in grado di fornire informazioni sui nomi FQDN risolti? Come LINA syslogs, per esempio.
R. Per risolvere i problemi relativi all'FQDN di una determinata destinazione, è possibile utilizzare il comando **system support trace**. Le tracce mostrano l'ID FQDN del pacchetto. È possibile confrontare l'ID per la risoluzione dei problemi. È inoltre possibile abilitare i messaggi Syslog 746015, 746016 per tenere traccia dell'attività di risoluzione DNS FQDN.

D: Il dispositivo registra l'FQDN nella tabella delle connessioni con l'IP risolto?
R: Per risolvere i problemi relativi all'FQDN di una determinata destinazione, è possibile utilizzare il comando **system support trace**, dove le tracce mostrano l'ID FQDN del pacchetto. È possibile confrontare l'ID per la risoluzione dei problemi. È previsto che i registri FQDN nel visualizzatore eventi in FMC siano disponibili in futuro.

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).