Esempio di configurazione EIGRP ASA 9.x

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco Adaptive Security Appliance (ASA) in modo che impari i percorsi tramite il protocollo EIGRP (Enhanced Interior Gateway Routing Protocol), supportato nel software ASA versione 9.x e successive, ed esegua l'autenticazione.

Prerequisiti

Requisiti

Prima di provare la configurazione, Cisco richiede il rispetto delle seguenti condizioni:

- Cisco ASA deve eseguire la versione 9.x o successive.

- Il protocollo EIGRP deve essere in modalità contesto singolo perché non è supportato in modalità contesto multiplo.

Componenti usati

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

- Software Cisco ASA versione 9.2.1
- Cisco Adaptive Security Device Manager (ASDM) versione 7.2.1
- Router Cisco IOS® con versione 12.4

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

Linee guida e limitazioni

- Un'istanza EIGRP è supportata in modalità singola e per contesto in modalità multimodale.
- Per ogni istanza EIGRP vengono creati due thread in modalità multimodale per contesto, che possono essere visualizzati con il processo show.
- Il riepilogo automatico è disattivato per impostazione predefinita.
- Non è stata stabilita una relazione di tipo Adiacente tra le unità cluster in modalità interfaccia singola.
- Le informazioni predefinite in [<acl>] vengono usate per filtrare il bit esterno nelle route predefinite dei candidati in ingresso.
- L'opzione Default-information out [<acl>] viene usata per filtrare il bit esterno nelle route predefinite dei candidati in uscita.

EIGRP e failover

Il codice Cisco ASA versione 8.4.4.1 e successive sincronizza i percorsi dinamici dall'unità ATTIVA all'unità STANDBY. Inoltre, l'eliminazione delle route è sincronizzata anche con l'unità STANDBY. Tuttavia, lo stato delle adiacenze tra pari non è sincronizzato; solo il dispositivo ACTIVE mantiene lo stato adiacente e partecipa attivamente al routing dinamico. Per ulteriori informazioni, fare riferimento alle domande frequenti sull'appliance ASA: Cosa succede dopo il failover se vengono sincronizzate le route dinamiche? per ulteriori informazioni.

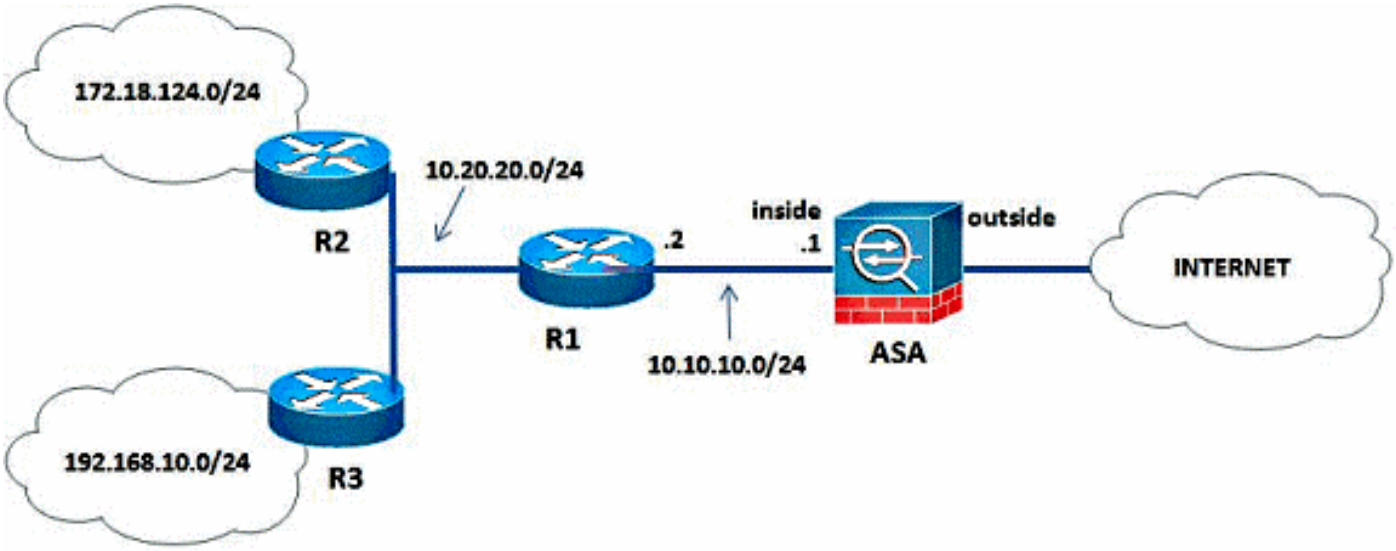
Configurazione

In questa sezione viene descritto come configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Nella topologia di rete mostrata, l'indirizzo IP dell'interfaccia interna di Cisco ASA è 10.10.10.1/24. L'obiettivo è configurare l'EIGRP sull'appliance Cisco ASA in modo che vengano appresi in modo dinamico i percorsi alle reti interne (10.20.20.0/24, 172.18.124.0/24 e 192.168.10.0/24) tramite il router adiacente (R1). R1 apprende i percorsi alle reti interne remote attraverso gli altri due router (R2 e R3).

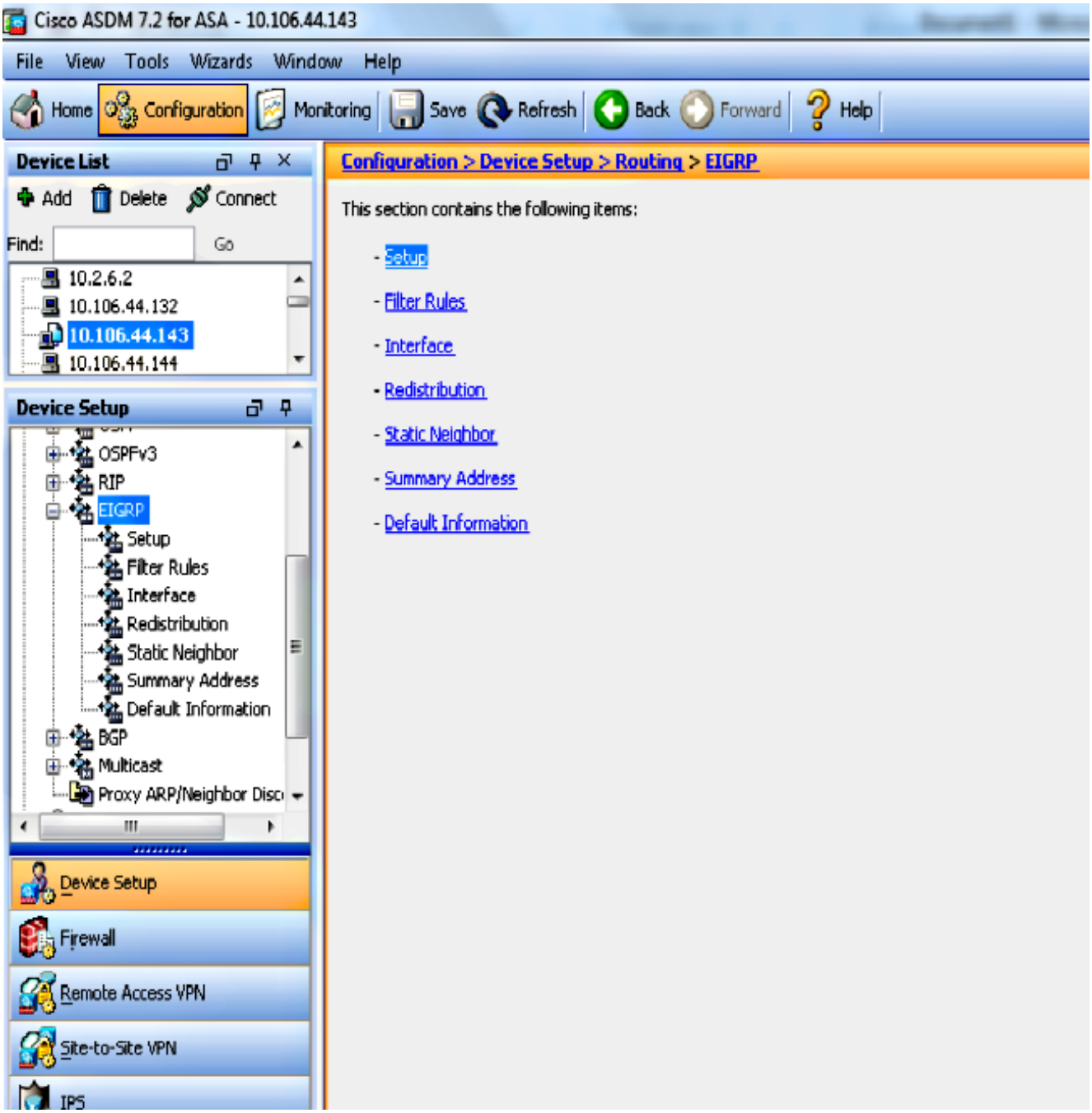
Configurazione ASDM

ASDM è un'applicazione basata su browser utilizzata per configurare e monitorare il software sui dispositivi di sicurezza. ASDM viene caricato dall'appliance di sicurezza e quindi utilizzato per configurare, monitorare e gestire il dispositivo. È inoltre possibile utilizzare l'utilità di avvio ASDM per avviare l'applicazione ASDM più rapidamente dell'applet Java. In questa sezione vengono descritte le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento con ASDM.

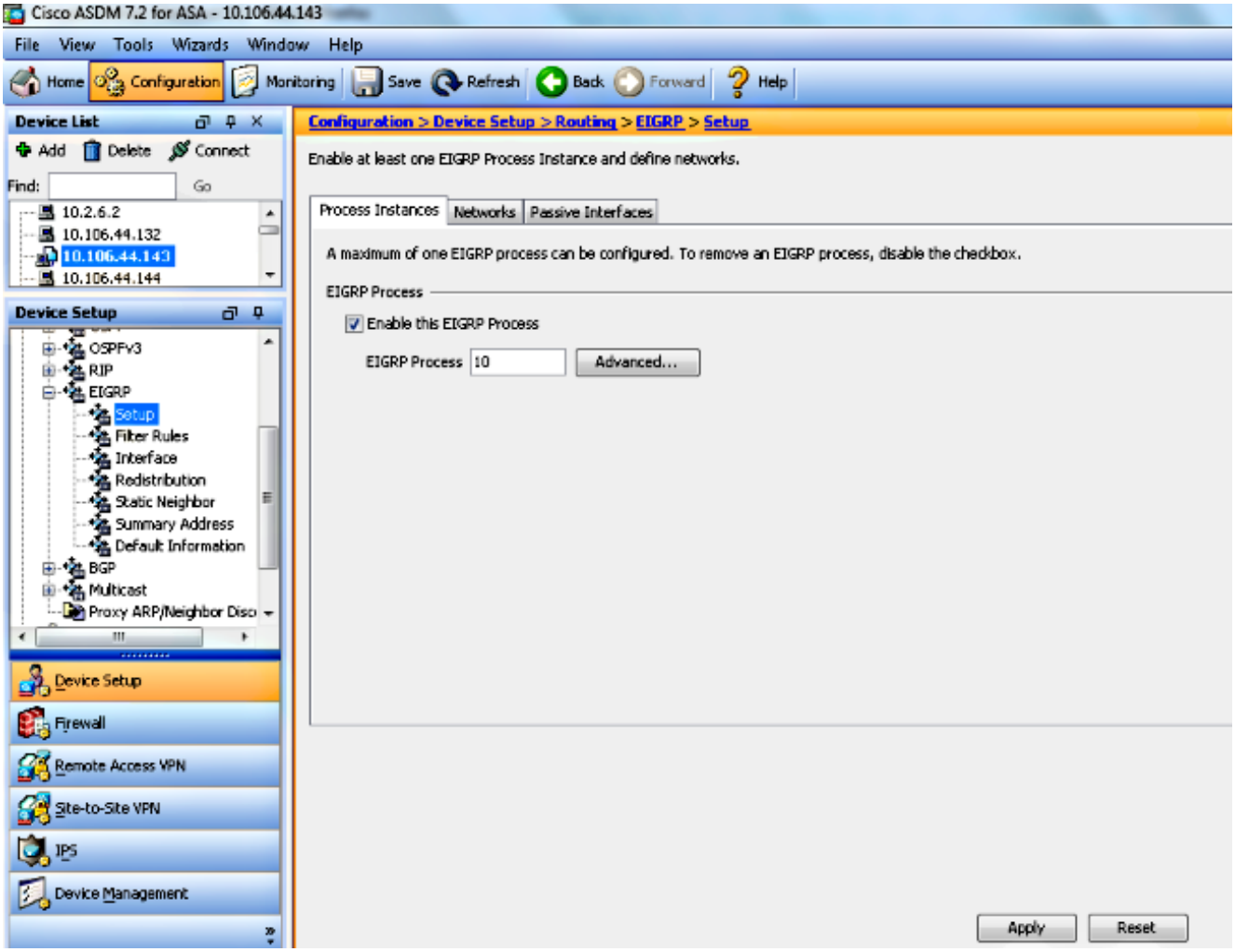
Completare questa procedura per configurare il protocollo EIGRP nell'appliance Cisco ASA.

1. Accedere all'appliance Cisco ASA con ASDM.

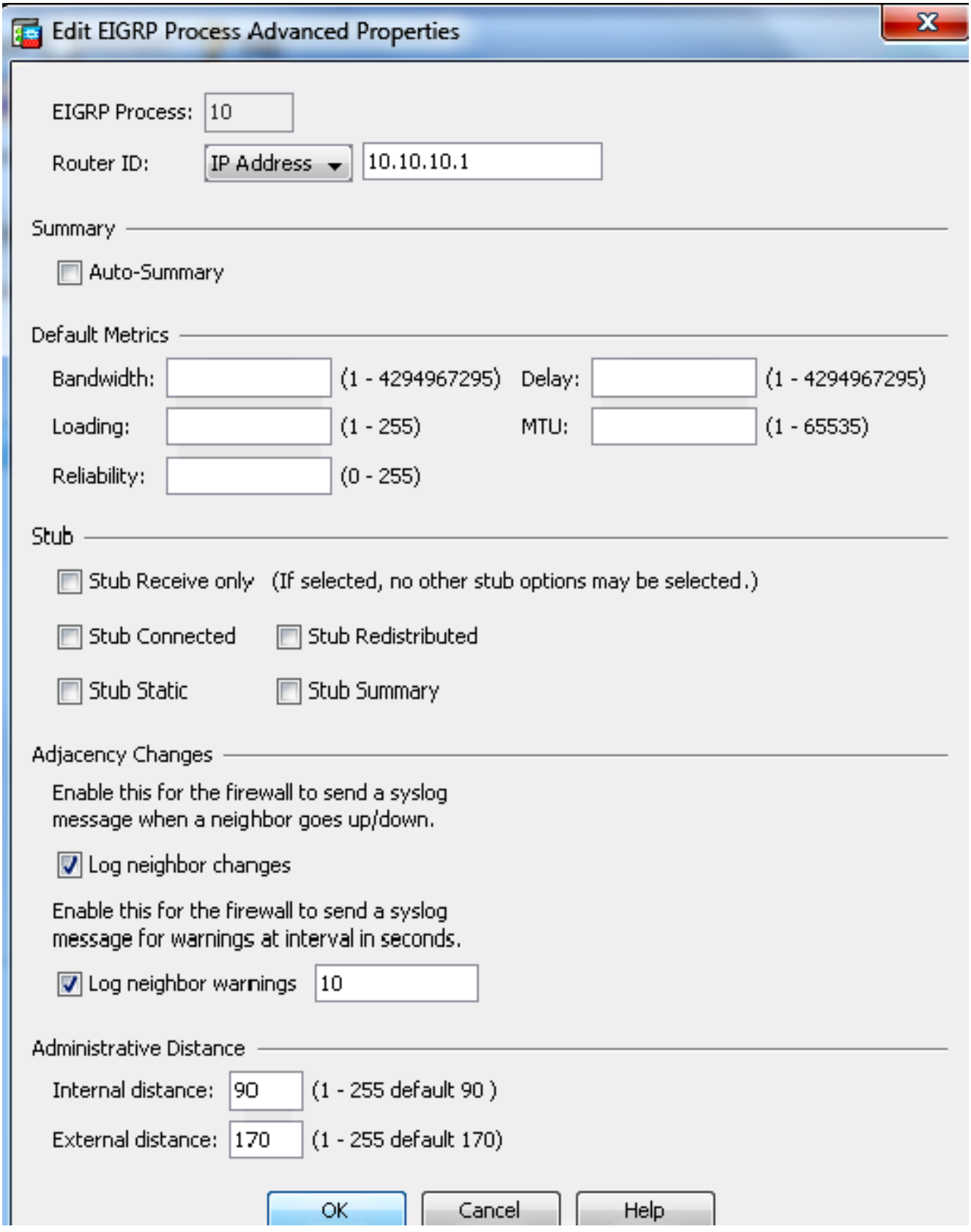
2. Passare all'area **Configurazione > Impostazione dispositivo > Routing > EIGRP** dell'interfaccia ASDM, come mostrato in questa schermata.



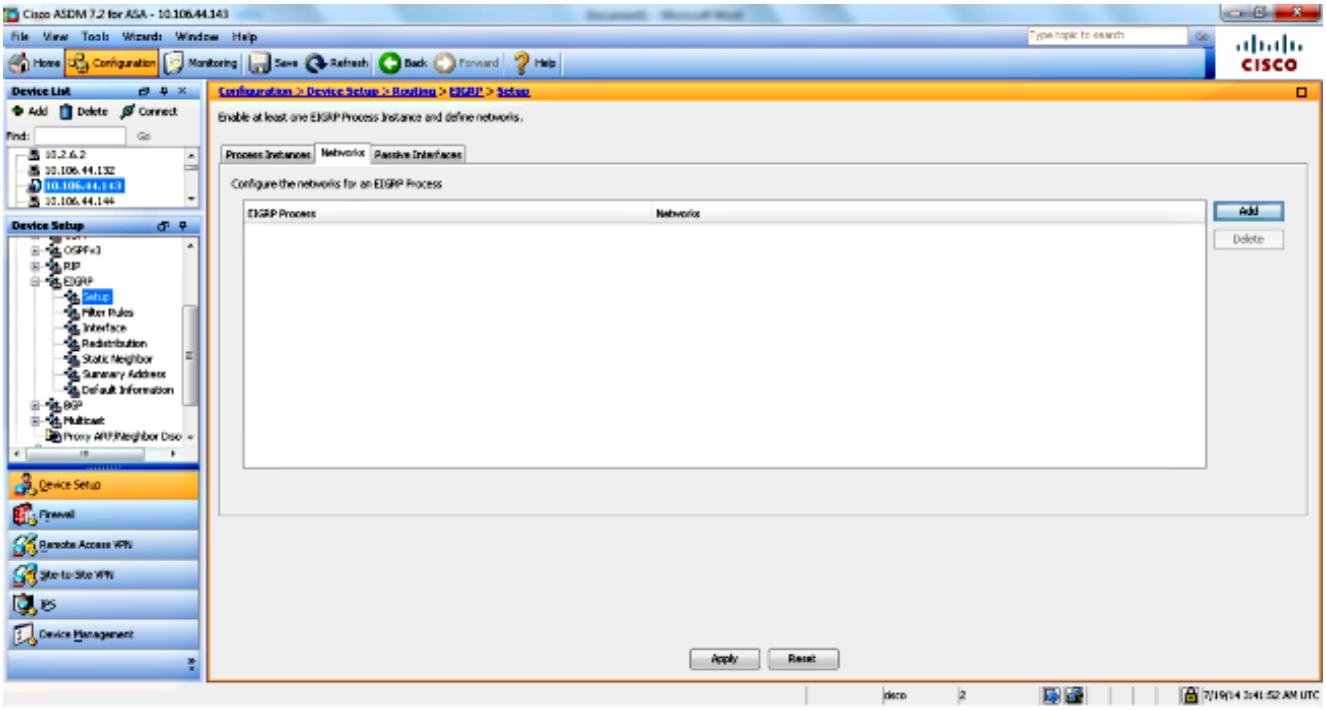
3. Abilitare il processo di instradamento EIGRP nella scheda **Impostazione > Istanze processo**, come mostrato in questa schermata. Nell'esempio, il processo EIGRP è impostato su **10**.



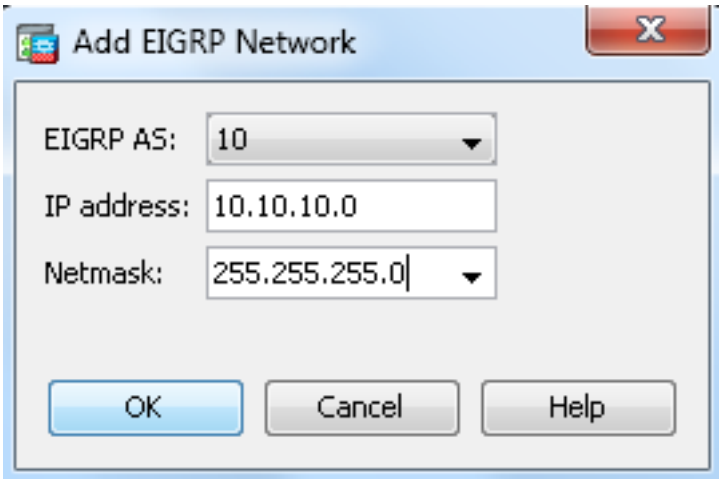
4. Èpossibile configurare i parametri opzionali del processo di instradamento EIGRP avanzato. Fare clic su **Avanzate** nella scheda **Impostazione > Istanze processo**. È possibile configurare il processo di routing EIGRP come processo di routing stub, disabilitare il riepilogo automatico delle route, definire le metriche predefinite per le route ridistribuite, modificare le distanze amministrative per le route EIGRP interne ed esterne, configurare un ID di router statico e abilitare o disabilitare la registrazione delle modifiche delle adiacenze. Nell'esempio, l'ID del router EIGRP è configurato in modo statico con l'indirizzo IP dell'interfaccia interna (10.10.10.1). Inoltre, **Riepilogo automatico** è disabilitato. Tutte le altre opzioni vengono configurate con i relativi valori predefiniti.



5. Dopo aver completato i passi precedenti, definire le reti e le interfacce che partecipano al routing EIGRP nella scheda **Imposta > Reti**. Fare clic su **Add** (Aggiungi) come mostrato in questa schermata.



6. Viene visualizzata questa schermata. Nell'esempio, l'unica rete aggiunta è la rete interna (10.10.10.0/24), in quanto il protocollo EIGRP è abilitato solo sull'interfaccia interna.



Solo le interfacce con un indirizzo IP che rientra nelle reti definite partecipano al processo di routing EIGRP. Se si dispone di un'interfaccia che non si desidera partecipare al routing EIGRP ma che è collegata a una rete che si desidera annunciare, configurare una voce di rete nella scheda **Imposta > Reti** che copra la rete a cui è collegata l'interfaccia e quindi configurare l'interfaccia come passiva in modo che l'interfaccia non possa inviare o ricevere aggiornamenti EIGRP.

Nota: Le interfacce configurate come passive non inviano o ricevono aggiornamenti EIGRP.

7. Se lo si desidera, è possibile definire filtri di instradamento nel riquadro Regole filtro. Il filtro route offre un maggiore controllo sulle route che possono essere inviate o ricevute negli aggiornamenti EIGRP.

8. Facoltativamente, è possibile configurare la ridistribuzione delle route. Cisco ASA può ridistribuire le route individuate da RIP (Routing Information Protocol) e OSPF (Open

Shortest Path First) nel processo di routing EIGRP. È inoltre possibile ridistribuire le route statiche e connesse nel processo di routing EIGRP. Non è necessario ridistribuire le route statiche o connesse se rientrano nell'intervallo di una rete configurata nella scheda **Imposta > Reti**. Definire la ridistribuzione dei cicli di lavorazione nel riquadro Ridistribuzione.

9. I pacchetti EIGRP Hello vengono inviati come pacchetti multicast. Se un router adiacente EIGRP si trova su una rete non broadcast, è necessario definirlo manualmente. Quando si definisce manualmente un router adiacente EIGRP, i pacchetti Hello vengono inviati a tale router adiacente come messaggi unicast. Per definire i router adiacenti EIGRP statici, passare al riquadro **adiacente statico**.

10. Per impostazione predefinita, le route predefinite vengono inviate e accettate. Per limitare o disabilitare l'invio e la ricezione delle informazioni sulla route predefinita, aprire il riquadro **Configurazione > Impostazione dispositivo > Routing > EIGRP >** Informazioni **predefinite**. Nel riquadro Informazioni predefinite viene visualizzata una tabella di regole per controllare l'invio e la ricezione di informazioni sulla route predefinita negli aggiornamenti EIGRP.

    Nota: È possibile avere una regola "*in"* e una "*out*" per ciascun processo di routing EIGRP. Attualmente è supportato un solo processo.

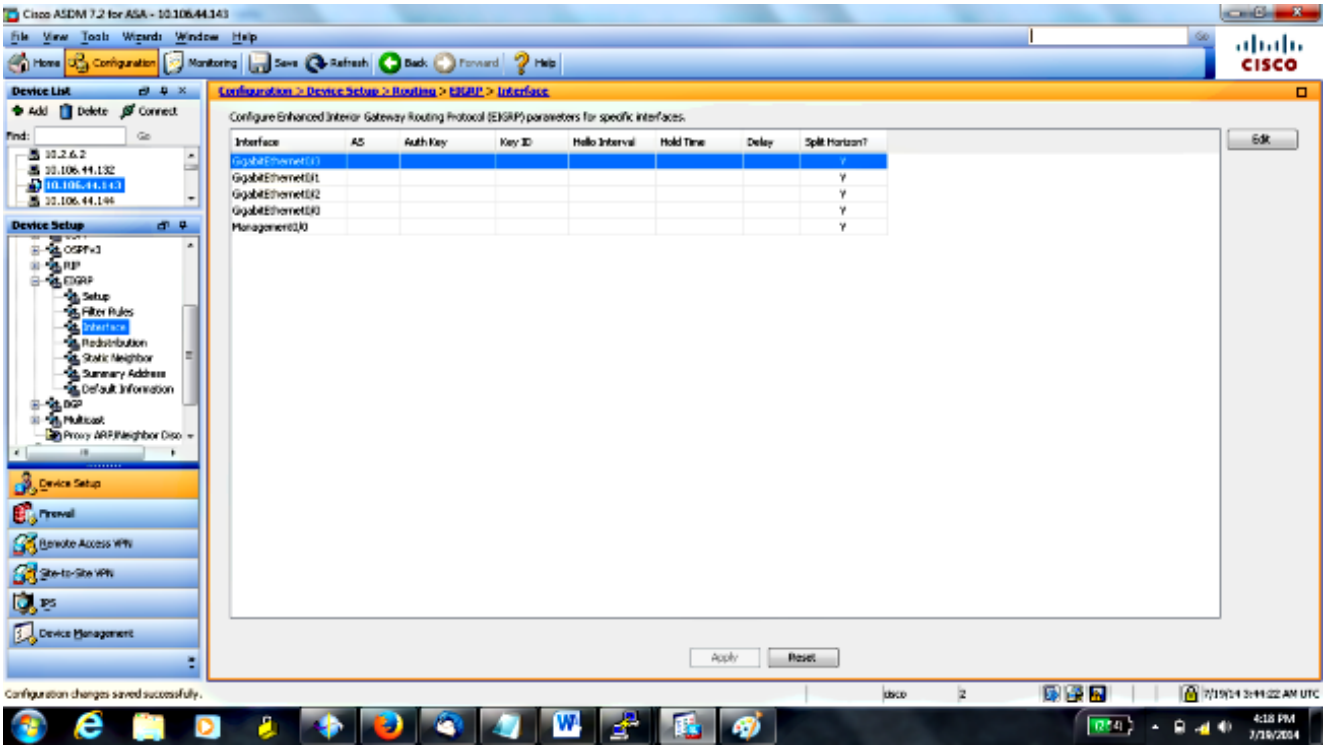
Configura autenticazione EIGRP

Cisco ASA supporta l'autenticazione MD5 degli aggiornamenti del routing dal protocollo di routing EIGRP. Il digest MD5 di ciascun pacchetto EIGRP impedisce l'introduzione di messaggi di routing non autorizzati o falsi provenienti da fonti non approvate. L'aggiunta dell'autenticazione ai messaggi EIGRP garantisce che i router e l'appliance Cisco ASA accettino solo messaggi di routing da altri dispositivi di routing configurati con la stessa chiave precondivisa. Senza questa autenticazione configurata, se un utente introduce un altro dispositivo di routing con informazioni di routing diverse o diverse sulla rete, le tabelle di routing sui router o sull'appliance Cisco ASA possono danneggiarsi e può verificarsi un attacco Denial of Service. Quando si aggiunge l'autenticazione ai messaggi EIGRP inviati tra i dispositivi di routing (inclusa l'ASA), viene impedita l'aggiunta non autorizzata di router EIGRP nella topologia di routing.

L'autenticazione route EIGRP è configurata per singola interfaccia. Tutti i router adiacenti EIGRP sulle interfacce configurate per l'autenticazione dei messaggi EIGRP devono essere configurati con la stessa modalità di autenticazione e la stessa chiave per stabilire le adiacenze.

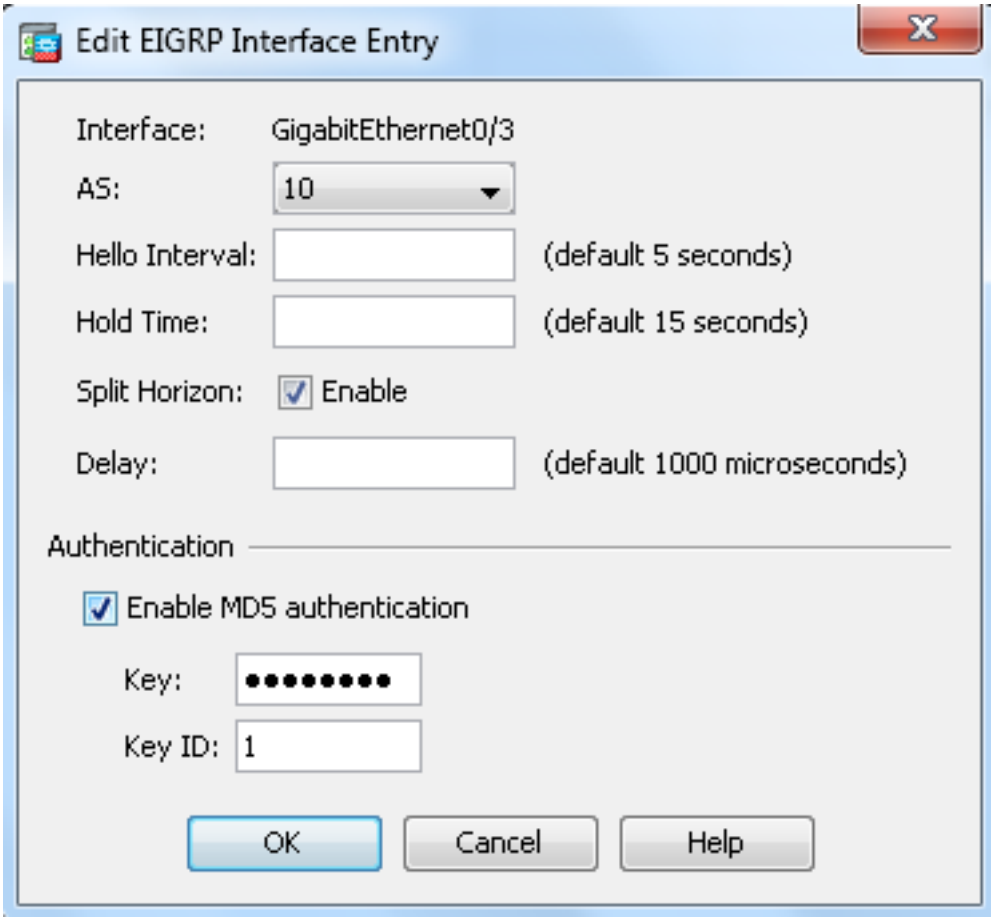
Completare questa procedura per abilitare l'autenticazione EIGRP MD5 sull'appliance Cisco ASA.

1. In ASDM, selezionare **Configurazione > Impostazione dispositivo > Routing > EIGRP > Interfaccia** come mostrato.



2. In questo caso, il protocollo EIGRP è abilitato sull'interfaccia interna (Gigabit Ethernet 0/1). Selezionare l'interfaccia **Gigabit Ethernet 0/1** e fare clic su **Edit** (Modifica).

3. In Autenticazione scegliere **Abilita autenticazione MD5**. Aggiungere qui ulteriori informazioni sui parametri di autenticazione. In questo caso, la chiave già condivisa è **cisco123** e l'ID della chiave è **1**.



EIGRP Route Filtering

Con EIGRP è possibile controllare gli aggiornamenti di routing inviati e ricevuti. Nell'esempio, gli aggiornamenti del routing vengono bloccati sull'appliance ASA per il prefisso di rete 192.168.10.0/24, che si trova dietro R1. Per il filtro delle route, è possibile usare solo **ACL STANDARD**.

```
access-list eigrp standard deny 192.168.10.0 255.255.255.0
access-list eigrp standard permit any

router eigrp 10
distribute-list eigrp in
```

Verifica

```
ASA(config)# show access-list eigrp
access-list eigrp; 2 elements; name hash: 0xd43d3adc
access-list eigrp line 1 standard deny 192.168.10.0 255.255.255.0 (hitcnt=3) 0xeb48ecd0
access-list eigrp line 2 standard permit any4 (hitcnt=12) 0x883fe5ac
```

Configurazioni

Configurazione Cisco ASA CLI

Questa è la configurazione di Cisco ASA CLI.

```
!outside interface configuration

interface GigabitEthernet0/0
description outside interface connected to the Internet
nameif outside
security-level 0
ip address 198.51.100.120 255.255.255.0
!

!inside interface configuration

interface GigabitEthernet0/1
description interface connected to the internal network
nameif inside
security-level 100
ip address 10.10.10.1 255.255.255.0
!

!EIGRP authentication is configured on the inside interface

authentication key eigrp 10 cisco123 key-id 1
authentication mode eigrp 10 md5
!

!management interface configuration

interface Management0/0
```

```
nameif management
security-level 99
ip address 10.10.20.1 255.255.255.0 management-only
!
!

!EIGRP Configuration - the CLI configuration is very similar to the
!Cisco IOS router EIGRP configuration.

router eigrp 10
no auto-summary
eigrp router-id 10.10.10.1
network 10.10.10.0 255.255.255.0
!

!This is the static default gateway configuration

route outside 0.0.0.0 0.0.0.0 198.51.100.1 1
```

Configurazione CLI del router Cisco IOS (R1)

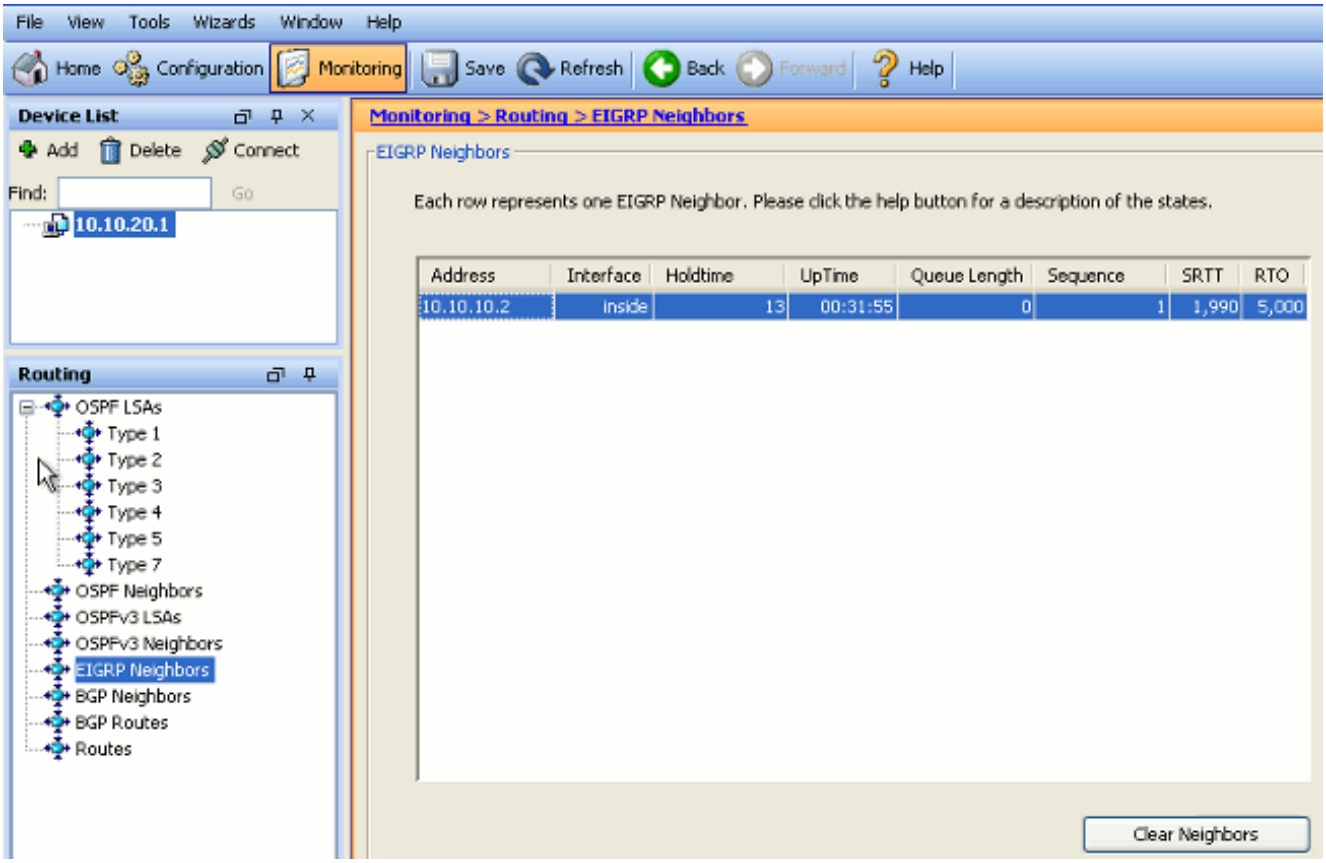
Questa è la configurazione CLI di R1 (router interno).

```
!!Interface that connects to the Cisco ASA. Notice the EIGRP authentication
paramenters.


interface FastEthernet0/0
ip address 10.10.10.2 255.255.255.0
ip authentication mode eigrp 10 md5
ip authentication key-chain eigrp 10 MYCHAIN
!
!

! EIGRP Configuration

router eigrp 10
network 10.10.10.0 0.0.0.255
network 10.20.20.0 0.0.0.255
network 172.18.124.0 0.0.0.255
network 192.168.10.0
no auto-summary
```

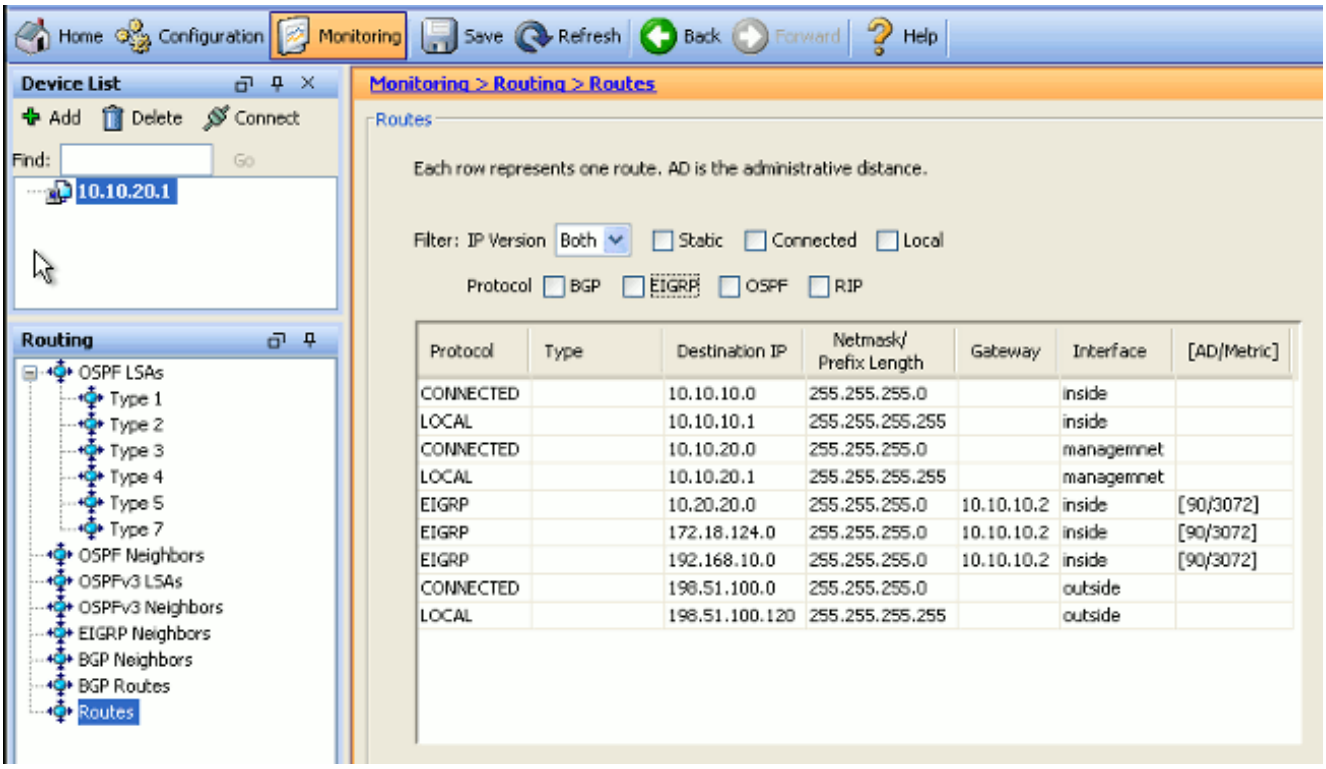
Verifica

Per verificare la configurazione, effettuare i seguenti passaggi.

1. Su ASDM, è possibile selezionare **Monitoraggio > Routing > Router adiacente EIGRP** per visualizzare tutti i router adiacenti EIGRP. In questa schermata viene mostrato il router interno (R1) come router adiacente attivo. È inoltre possibile visualizzare l'interfaccia in cui risiede il vicino, il tempo di attesa e la durata della relazione con il vicino (UpTime).



2. Inoltre, è possibile verificare la tabella di instradamento selezionando **Controllo > Instradamento > Instradamenti**. In questa schermata, è possibile vedere che le reti **192.168.10.0/24, 172.18.124.0/24** e **10.20.20.0/24** vengono apprese tramite R1 (**10.10.2**).



Dalla CLI, è possibile usare il comando **show route** per ottenere lo stesso output.

```
ciscoasa# show route
```

```
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP

D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area

N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default, U - per-user static route, o - ODR
P - periodic downloaded static route
Gateway of last resort is 100.10.10.2 to network 0.0.0.0
C 198.51.100.0 255.255.255.0 is directly connected, outside
D 192.168.10.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 172.18.124.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
C 127.0.0.0 255.255.0.0 is directly connected, cplane
D 10.20.20.0 255.255.255.0 [90/28672] via 10.10.10.2, 0:32:29, inside
C 10.10.10.0 255.255.255.0 is directly connected, inside
C 10.10.20.0 255.255.255.0 is directly connected, management
S* 0.0.0.0 0.0.0.0 [1/0] via 198.51.100.1, outside
```

Con ASA versione 9.2.1 e successive, è possibile usare il comando **show route eigrp** per visualizzare solo le route EIGRP.

```
ciscoasa(config)# show route eigrp

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

D 192.168.10.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 172.18.124.0 255.255.255.0 [90/131072] via 10.10.10.2, 0:32:29, inside
D 10.20.20.0 255.255.255.0 [90/28672] via 10.10.10.2, 0:32:29, inside
```

3. Per ulteriori informazioni sulle reti acquisite e sulla topologia EIGRP, è possibile usare il comando **show eigrp topology**.

```
    ciscoasa# show eigrp topology
EIGRP-IPv4 Topology Table for AS(10)/ID(10.10.10.1)
Codes: P - Passive, A - Active, U - Update, Q - Query, R - Reply,
r - reply Status, s - sia Status
P 10.20.20.0 255.255.255.0, 1 successors, FD is 28672
via 10.10.10.2 (28672/28416), GigabitEthernet0/1
P 10.10.10.0 255.255.255.0, 1 successors, FD is 2816
via Connected, GigabitEthernet0/1
P 192.168.10.0 255.255.255.0, 1 successors, FD is 131072
via 10.10.10.2 (131072/130816), GigabitEthernet0/1
P 172.18.124.0 255.255.255.0, 1 successors, FD is 131072
via 10.10.10.2 (131072/130816), GigabitEthernet0/1
```

4. Il comando **show eigrp neighbors** è utile anche per verificare i router adiacenti attivi e le informazioni corrispondenti. Nell'esempio vengono mostrate le stesse informazioni ottenute da ASDM nel passo 1.

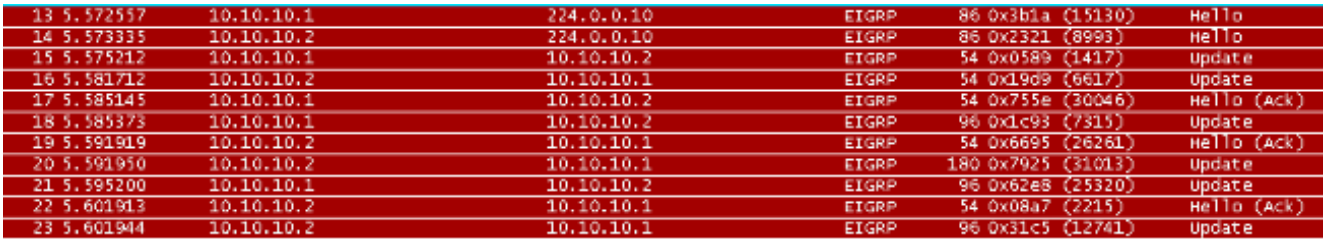
```
ciscoasa# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq (sec) (ms)Cnt Num

0 10.10.10.2 Gi0/1 12 00:39:12 107 642 0 1
```

Flusso dei pacchetti

Ecco il flusso dei pacchetti.

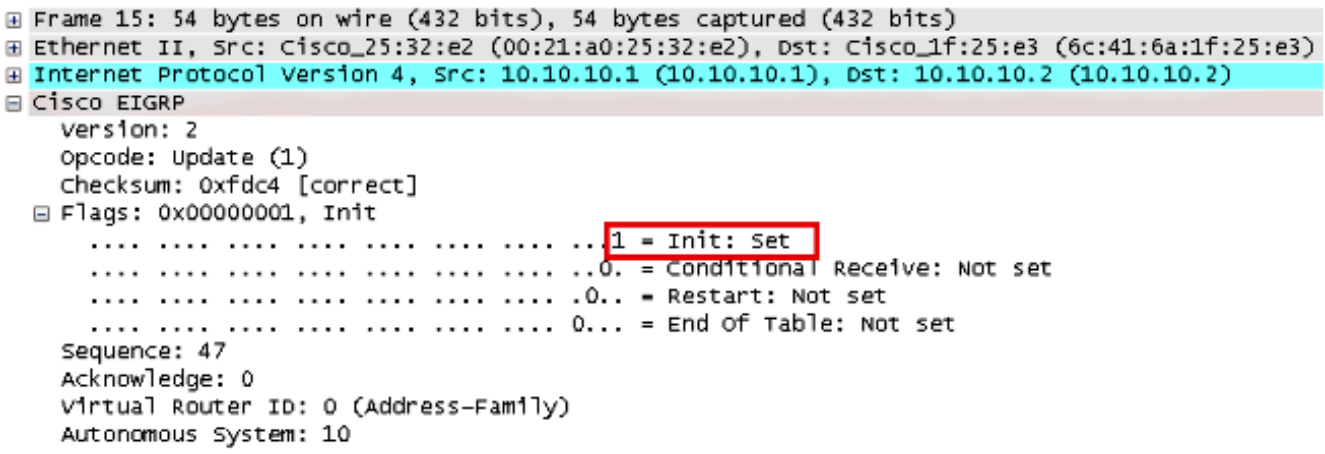
1. L'ASA arriva sul collegamento e invia un pacchetto Cast Hello tramite tutte le interfacce configurate con EIGRP.

2. R1 riceve un pacchetto Hello e lo invia.



3. L'ASA riceve il pacchetto Hello e invia un pacchetto di aggiornamento con un bit iniziale impostato, che indica che questo è il processo di inizializzazione.

4. R1 riceve un pacchetto di aggiornamento e invia un pacchetto di aggiornamento con un bit iniziale impostato, a indicare che si tratta del processo di inizializzazione.



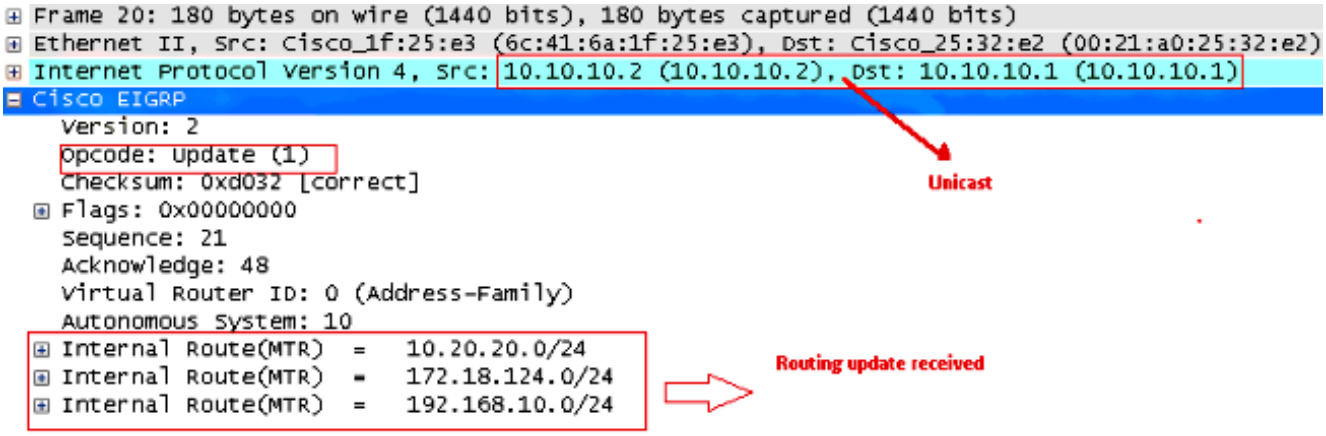
5. Dopo aver scambiato le porte ASA e R1 e aver stabilito le adiacenze, sia l'ASA che l'R1 rispondono con un pacchetto ACK, a indicare che le informazioni per l'aggiornamento sono

state ricevute.

6. L'ASA invia le informazioni di routing alla R1 in un pacchetto di aggiornamento.

7. R1 inserisce le informazioni sul pacchetto di aggiornamento nella relativa tabella della topologia. La tabella della topologia include tutte le destinazioni annunciate dai vicini. È organizzato in modo che ciascuna destinazione sia elencata, insieme a tutti i vicini che possono viaggiare verso la destinazione e le metriche associate.

8. R1 invia quindi un pacchetto di aggiornamento all'appliance ASA.



9. Dopo aver ricevuto il pacchetto di aggiornamento, l'ASA invia un pacchetto ACK a R1. Quando l'ASA e l'R1 ricevono i pacchetti di aggiornamento l'uno dall'altro, sono pronti a scegliere le route successore (migliori) e quelle possibili (di backup) nella tabella della topologia e a offrire le route successori alla tabella di routing.

Risoluzione dei problemi

In questa sezione vengono fornite informazioni sui comandi **debug** e **show** che possono essere utili per risolvere i problemi relativi al protocollo EIGRP.

Comandi per la risoluzione dei problemi

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

> **Nota:** consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug.** Per visualizzare le informazioni di debug sulla macchina a stato finito Diffusing Update Algorithm (DUAL), usare il comando **debug eigrp fsm** in modalità di esecuzione privilegiata. Questo comando consente di osservare l'attività successore possibile di EIGRP e determinare se gli aggiornamenti dei percorsi vengono installati ed eliminati dal processo di routing.

Questo è l'output del comando **debug** durante il peering con R1. È possibile visualizzare ciascuna delle diverse route installate correttamente nel sistema.

```
EIGRP-IPv4(Default-IP-Routing-Table:10): Callback: route_adjust GigabitEthernet0/1
DUAL: dest(10.10.10.0 255.255.255.0) not active
DUAL: rcvupdate: 10.10.10.0 255.255.255.0 via Connected metric 2816/0 on topoid 0
DUAL: Find FS for dest 10.10.10.0 255.255.255.0. FD is 4294967295, RD is 4294967
295 on topoid 0 found
DUAL: RT installed 10.10.10.0 255.255.255.0 via 0.0.0.0
DUAL: Send update about 10.10.10.0 255.255.255.0. Reason: metric chg on topoid
0
DUAL: Send update about 10.10.10.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(10.20.20.0 255.255.255.0) not active
DUAL: rcvupdate: 10.20.20.0 255.255.255.0 via 10.10.10.2 metric 28672/28416 on t
opoid 0
DUAL: Find FS for dest 10.20.20.0 255.255.255.0. FD is 4294967295, RD is 4294967
295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 10.20.20.0 ()
DUAL: RT installed 10.20.20.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 10.20.20.0 255.255.255.0. Reason: metric chg on topoid
0
DUAL: Send update about 10.20.20.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(172.18.124.0 255.255.255.0) not active
DUAL: rcvupdate: 172.18.124.0 255.255.255.0 via 10.10.10.2 metric 131072/130816
on topoid 0
DUAL: Find FS for dest 172.18.124.0 255.255.255.0. FD is 4294967295, RD is 42949
67295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 172.18.124.0 ()
DUAL: RT installed 172.18.124.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 172.18.124.0 255.255.255.0. Reason: metric chg on topoi
d 0
DUAL: Send update about 172.18.124.0 255.255.255.0. Reason: new if on topoid 0
DUAL: dest(192.168.10.0 255.255.255.0) not active
DUAL: rcvupdate: 192.168.10.0 255.255.255.0 via 10.10.10.2 metric 131072/130816
on topoid 0
DUAL: Find FS for dest 192.168.10.0 255.255.255.0. FD is 4294967295, RD is 42949
67295 on topoid 0 found
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 192.168.10.0 ()
DUAL: RT installed 192.168.10.0 255.255.255.0 via 10.10.10.2
DUAL: Send update about 192.168.10.0 255.255.255.0. Reason: metric chg on topoi
d 0
DUAL: Send update about 192.168.10.0 255.255.255.0. Reason: new if on topoid 0
```

Èinoltre possibile utilizzare il comando **debug eigrp neighbors**. Di seguito viene riportato l'output del comando **debug** quando Cisco ASA ha creato una nuova relazione di router adiacente con R1.

```
ciscoasa# EIGRP-IPv4(Default-IP-Routing-Table:10): Callback: route_adjust Gigabi
tEthernet0/1
EIGRP: New peer 10.10.10.2
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 10.20.20.0 ()
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 172.18.124.0 ()
EIGRP-IPv4(Default-IP-Routing-Table:10): route installed for 192.168.10.0 ()
```

Èpossibile anche usare i pacchetti EIGRP di debug per informazioni dettagliate sullo scambio di messaggi EIGRP tra l'appliance Cisco ASA e i suoi peer. In questo esempio, la chiave di autenticazione è stata modificata sul router (R1) e l'output del comando debug mostra che il problema è una mancata corrispondenza dell'autenticazione.

```
ciscoasa# EIGRP: Sending HELLO on GigabitEthernet0/1
AS 655362, Flags 0x0, Seq 0/0 interfaceQ 1/1 iidbQ un/rely 0/0
EIGRP: pkt key id = 1, authentication mismatch
EIGRP: GigabitEthernet0/1: ignored packet from 10.10.10.2, opcode = 5
(invalid authentication)
```

Il Villaggio EIGRP crolla con Syslogs ASA-5-336010

L'ASA elimina il vicinato EIGRP quando vengono apportate modifiche alla lista di distribuzione EIGRP. Questo messaggio Syslog viene visualizzato.

```
EIGRP Nieghborship Resets with syslogs ASA-5-336010: EIGRP-IPv4: PDM(314 10:
Neighbor 10.15.0.30 (GigabitEthernet0/0) is down: route configuration changed
```

Con questa configurazione, quando si **aggiunge** una **nuova voce** nell'ACL, il livello di vicinanza **Eigrp-network-list** EIGRP viene reimpostato.

```
router eigrp 10
distribute-list Eigrp-network-list in
network 10.10.10.0 255.0.0.0
passive-interface default
no passive-interface inside
redistribute static

access-list Eigrp-network-list standard permit any
```

Èpossibile osservare che la relazione di prossimità è attiva con il dispositivo adiacente.

```
ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 10 00:01:22 1 5000 0 5

ciscoasa(config)# show eigrp neighbors
EIGRP-IPv4 neighbors for process 10
H Address Interface Hold Uptime SRTT RTO Q Seq
(sec) (ms) Cnt Num
0 10.10.10.2 Gi0/3 13 00:01:29 1 5000 0 5
```

A questo punto, è possibile aggiungere all'elenco degli **accessi lo standard Eigrp-network-list deny 172.18.24.0 255.255.255.0**.

```
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 0.0.0.0, executed 'debug
eigrp fsm'
%ASA-7-111009: User 'enable_15' executed cmd: show access-list
%ASA-5-111008: User 'enable_15' executed the 'access-list Eigrp-network-list line
1 permit 172.18.24.0 255.255.255.0' command.
%ASA-5-111010: User 'enable_15', running 'CLI' from IP 0.0.0.0, executed 'access-list
Eigrp-network-list line 1 permit 172.18.24.0 255.255.255.0'
%ASA-7-111009: User 'enable_15' executed cmd: show eigrp neighbors
%ASA-5-336010: EIGRP-IPv4: PDM(599 10: Neighbor 10.10.10.2 (GigabitEthernet0/3) is
down: route configuration changed
%ASA-5-336010: EIGRP-IPv4: PDM(599 10: Neighbor 10.10.10.2 (GigabitEthernet0/3) is
up: new adjacency
```

I log possono essere visualizzati in **debug eigrp fsm**.

```
IGRP2: linkdown: start - 10.10.10.2 via GigabitEthernet0/3
DUAL: Destination 10.10.10.0 255.255.255.0 for topoid 0
DUAL: linkdown: finish
```

Questo è il comportamento previsto in tutte le nuove versioni di ASA da 8.4 e da 8.6 a 9.1. Lo stesso è stato osservato nei router che eseguono i code module da 12.4 a 15.1. Tuttavia, questo

comportamento non è osservato nelle versioni 8.2 e precedenti del software ASA, perché le modifiche apportate a un ACL non reimpostano le adiacenze EIGRP.

Dal momento che EIGRP invia l'intera tabella di topologia a un router adiacente quando il router adiacente si presenta per la prima volta e quindi invia solo le modifiche, la configurazione di una lista di distribuzione con la natura basata sugli eventi di EIGRP renderebbe difficile l'applicazione delle modifiche senza un ripristino completo della relazione con il router adiacente. I router devono tenere traccia di tutte le route inviate e ricevute da un router adiacente per poter sapere quale route è stata modificata (ossia, verrà inviata o meno) per applicare le modifiche come stabilito dalla lista di distribuzione corrente. è molto più semplice abbattere e ristabilire l'adiacenza tra vicini.

Quando un'adiacenza viene demolita e ristabilita, tutti i percorsi appresi tra particolari vicini vengono semplicemente dimenticati e l'intera sincronizzazione tra i vicini viene eseguita di nuovo, con la nuova lista di distribuzione.

La maggior parte delle tecniche EIGRP usate per risolvere i problemi dei router Cisco IOS può essere applicata sull'appliance Cisco ASA. Per risolvere i problemi relativi a EIGRP, usare il diagramma di flusso per la risoluzione dei problemi principale; iniziare dalla casella contrassegnata come **Main** (Principale).