

Esempio di configurazione ASA/PIX con OSPF

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Prodotti correlati](#)

[Convenzioni](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione ASDM](#)

[Configura autenticazione OSPF](#)

[Configurazione Cisco ASA CLI](#)

[Configurazione CLI del router Cisco IOS \(R2\)](#)

[Configurazione CLI del router Cisco IOS \(R1\)](#)

[Configurazione CLI del router Cisco IOS \(R3\)](#)

[Ridistribuzione in OSPF con ASA](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Configurazione statica router adiacente per rete point-to-point](#)

[Comandi per la risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare Cisco ASA in modo che impari le route tramite Open Shortest Path First (OSPF), esegua l'autenticazione e la redistribuzione.

Per ulteriori informazioni, fare riferimento al documento [PIX/ASA 8.X: Configurazione di EIGRP su Cisco Adaptive Security Appliance \(ASA\)](#) per ulteriori informazioni sulla configurazione EIGRP.

Nota: il routing asimmetrico non è supportato in ASA/PIX.

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Cisco ASA/PIX deve eseguire la versione 7.x o successive.
- OSPF non supportato in modalità contesto multiplo; è supportato solo in modalità singola.

Componenti usati

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

- Cisco serie 5500 Adaptive Security Appliance (ASA) con software versione 8.0 e successive
- Software Cisco Adaptive Security Device Manager (ASDM) versione 6.0 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.

Prodotti correlati

Le informazioni discusse in questo documento sono valide anche per il Cisco serie 500 PIX firewall con software versione 8.0 e successive.

Convenzioni

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

Premesse

Per creare e calcolare il percorso più breve a tutte le destinazioni note, OSPF utilizza un algoritmo dello stato del collegamento. Ogni router di un'area OSPF contiene un database dello stato del collegamento identico, ovvero un elenco di tutte le interfacce utilizzabili del router e dei router adiacenti raggiungibili.

I vantaggi di OSPF rispetto a RIP includono:

- Gli aggiornamenti del database allo stato di collegamento OSPF vengono inviati con minore frequenza rispetto agli aggiornamenti RIP e il database allo stato di collegamento viene aggiornato in modo istantaneo invece che in modo graduale a causa del timeout delle informazioni non aggiornate.
- Le decisioni relative al routing si basano sui costi, che indicano il sovraccarico necessario per inviare i pacchetti attraverso una determinata interfaccia. L'appliance di sicurezza calcola il costo di un'interfaccia in base alla larghezza di banda del collegamento anziché al numero di hop verso la destinazione. Il costo può essere configurato per specificare i percorsi preferiti.

Lo svantaggio degli algoritmi "path first" più brevi è che richiedono molti cicli della CPU e molta memoria.

L'appliance di sicurezza può eseguire due processi del protocollo OSPF contemporaneamente su set diversi di interfacce. È possibile eseguire due processi se si dispone di interfacce che utilizzano gli stessi indirizzi IP (NAT consente la coesistenza di queste interfacce, ma OSPF non consente la sovrapposizione di indirizzi). In alternativa, è possibile eseguire un processo all'interno

e un altro all'esterno e ridistribuire un sottoinsieme di route tra i due processi. Analogamente, potrebbe essere necessario separare gli indirizzi privati dagli indirizzi pubblici.

È possibile ridistribuire le route in un processo di routing OSPF da un altro processo di routing OSPF, da un processo di routing RIP o da route statiche e connesse configurate su interfacce abilitate OSPF.

L'appliance di sicurezza supporta le seguenti funzionalità OSPF:

- Supporto di percorsi intra-area, interarea ed esterni (tipo I e tipo II).
- Supporto di un collegamento virtuale.
- Inondazione OSPF LSA.
- Autenticazione su pacchetti OSPF (password e autenticazione MD5).
- Supporto per la configurazione dell'appliance di sicurezza come router designato o router di backup designato. L'appliance di sicurezza può anche essere configurata come ABR. La possibilità di configurare l'appliance di sicurezza come ASBR è tuttavia limitata alle sole informazioni predefinite, ad esempio l'inserimento di un percorso predefinito.
- Supporto per aree di stub e non di stubby.
- Filtraggio LSA tipo 3 router di confine area.

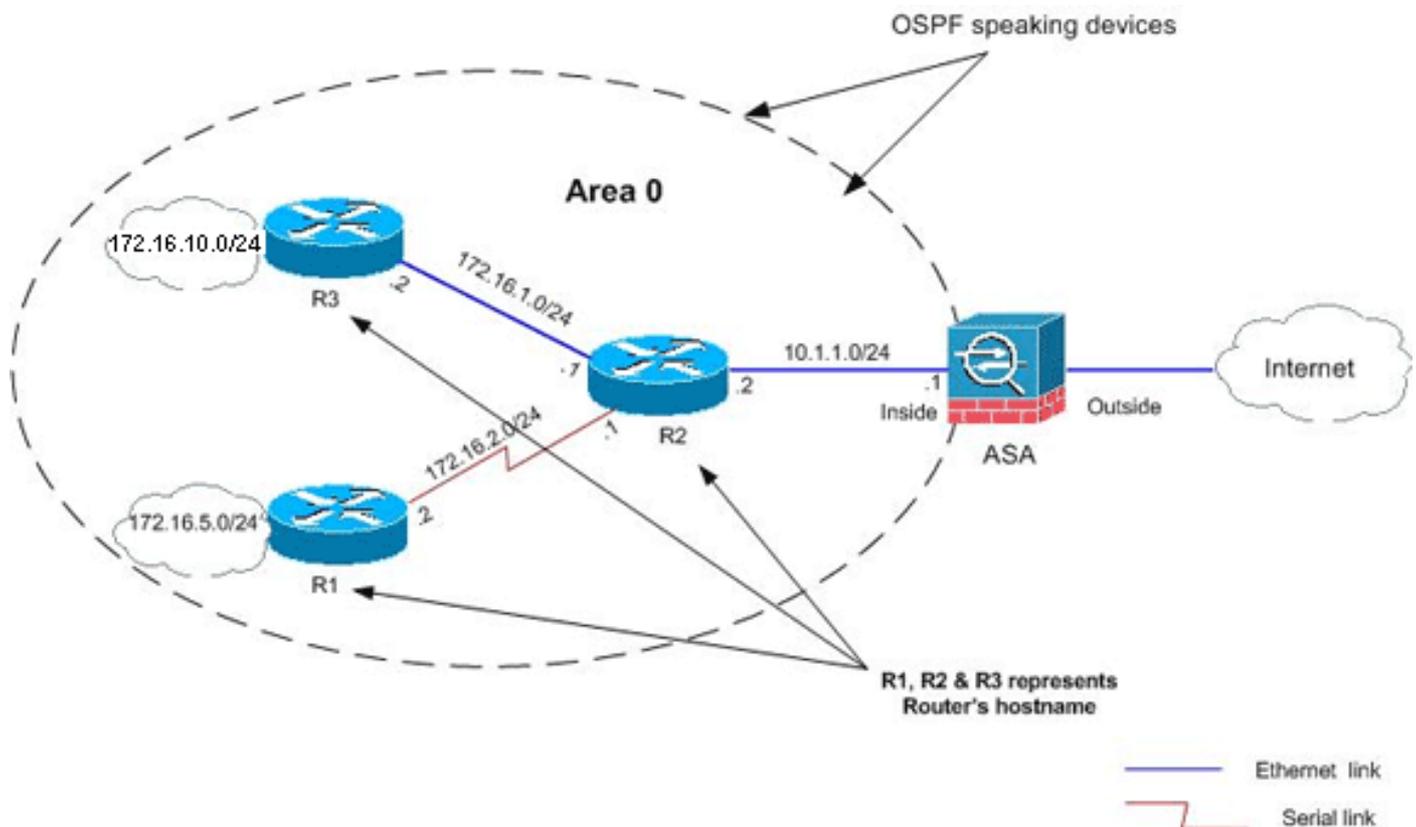
[Configurazione](#)

In questa sezione vengono presentate le informazioni necessarie per 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:



In questa topologia di rete, l'indirizzo IP dell'interfaccia interna di Cisco ASA è 10.1.1.1/24. L'obiettivo è configurare OSPF sull'appliance Cisco ASA in modo che apprenda dinamicamente le route alle reti interne (172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24 e 172.16.10.0/24) tramite il router adiacente (R2). R2 apprende le route alle reti interne remote attraverso gli altri due router (R1 e R3).

Configurazioni

Nel documento vengono usate queste configurazioni:

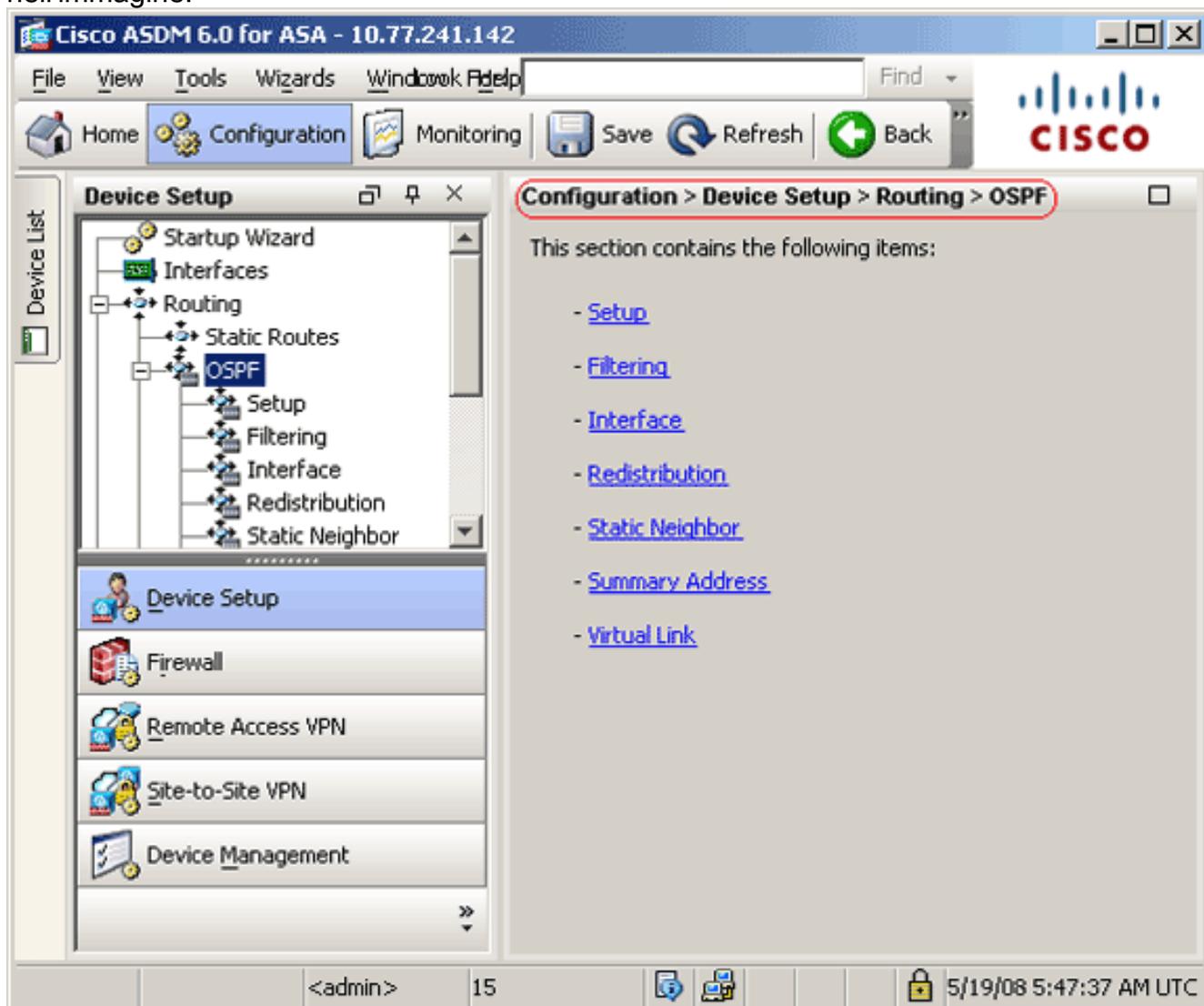
- [Configurazione ASDM](#)
- [Configura autenticazione OSPF](#)
- [Configurazione Cisco ASA CLI](#)
- [Configurazione CLI del router Cisco IOS \(R2\)](#)
- [Configurazione CLI del router Cisco IOS \(R1\)](#)
- [Configurazione CLI del router Cisco IOS \(R3\)](#)
- [Ridistribuzione in OSPF con ASA](#)

Configurazione ASDM

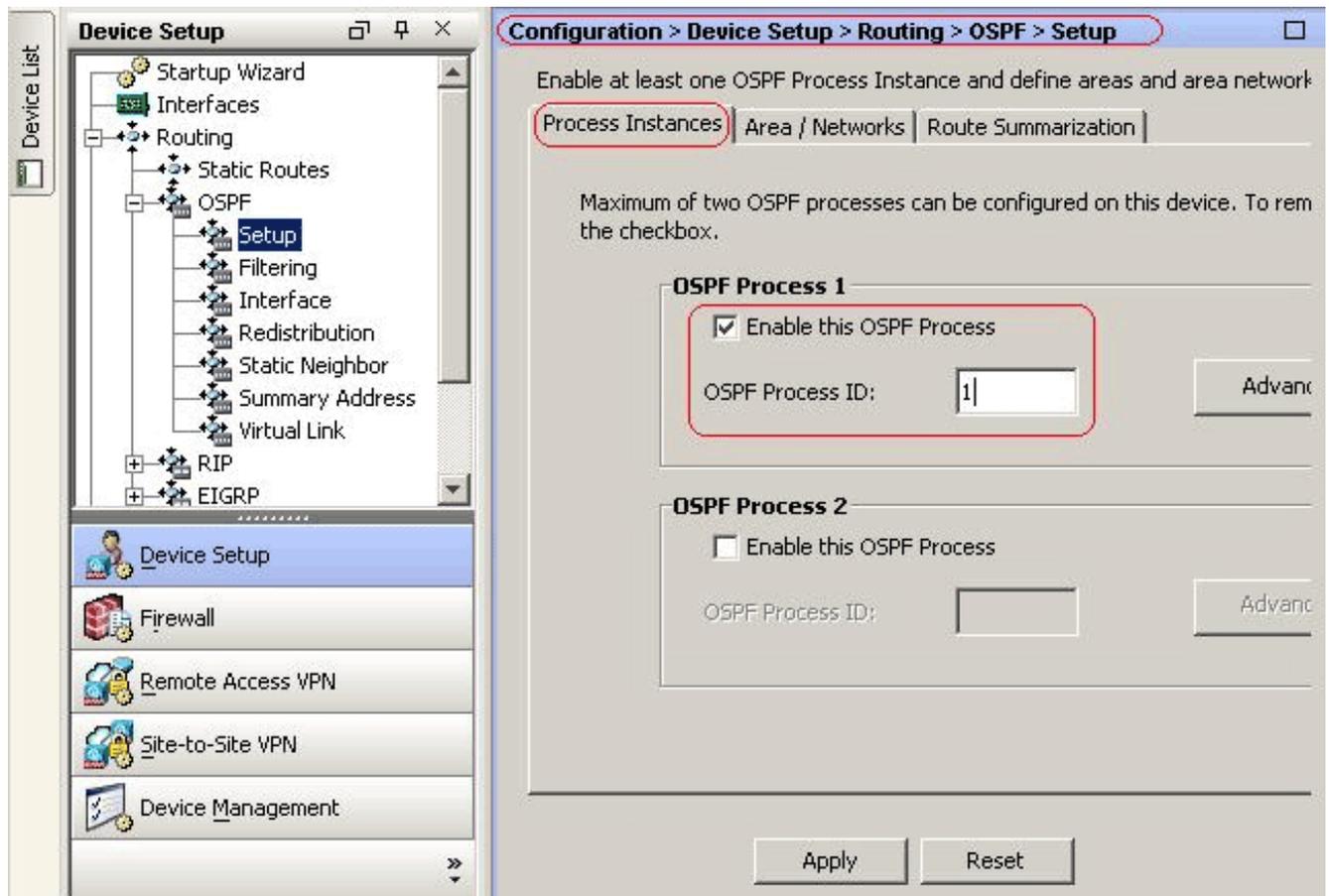
Adaptive Security Device Manager (ASDM) è un'applicazione basata su browser utilizzata per configurare e monitorare il software sui dispositivi di sicurezza. ASDM viene caricato dall'appliance di sicurezza e quindi utilizzato per configurare, monitorare e gestire il dispositivo. È inoltre possibile utilizzare l'utilità di avvio ASDM (solo Windows) 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 questi passaggi per configurare OSPF nell'appliance Cisco ASA:

1. Accedere all'appliance Cisco ASA con ASDM.
2. Passare all'area **Configurazione > Impostazione dispositivo > Routing > OSPF** dell'interfaccia ASDM, come mostrato nell'immagine.



3. Abilitare il processo di routing OSPF nella scheda **Imposta > Istanze processo**, come mostrato nell'immagine. Nell'esempio, il processo ID OSPF è 1.



4. È possibile fare clic su **Advanced** (Avanzate) nella scheda **Setup > Process Instances** (Impostazione > Istanze processo) per configurare i parametri opzionali avanzati del processo di routing OSPF. È possibile modificare le impostazioni specifiche del processo, ad esempio l'ID del router, le modifiche alle adiacenze, le distanze di instradamento amministrativo, i timer e le impostazioni di origine delle informazioni predefinite.

Edit OSPF Process Advanced Properties

OSPF Process: Router ID:

Ignore LSA MOSPF (suppress the sending of syslog messages when router receives a LSA MOSPF packets) RFC1583 Compatible (calculate summary route costs per RFC 1583)

Adjacency Changes

Enable this for the firewall to send a syslog message when an OSPF neighbor goes up/down. Log Adjacency Changes

Enable this for the firewall to send a syslog for each state change. Log Adjacency Change Details

Administrative Route Distances

Inter Area (distance for all routes from one area to another area)	Intra Area (distance for all routes within an area)	External (distance for all routes from other routing domains, learned by redistribution)
<input type="text" value="110"/>	<input type="text" value="110"/>	<input type="text" value="110"/>

Timers (in seconds)

SPF Delay Time (between when OSPF receives a topology change and when it starts a SPF calculation)	SPF Hold Time (between two consecutive SPF calculations)	LSA Group Pacing (interval at which OSPF LSAs are collected into a group and refreshed)
<input type="text" value="5"/>	<input type="text" value="10"/>	<input type="text" value="240"/>

Default Information Originate

Configure this to generate default external route into an OSPF routing domain.

Enable Default Information Originate Always advertise the default route

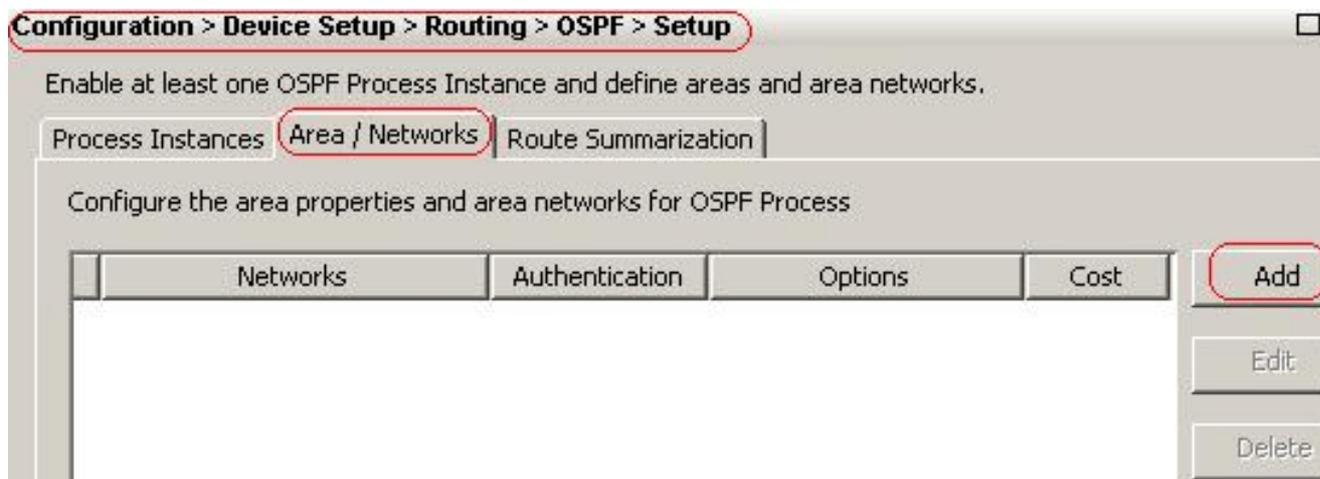
Metric Value: Metric Type: Route Map:

OK Cancel Help

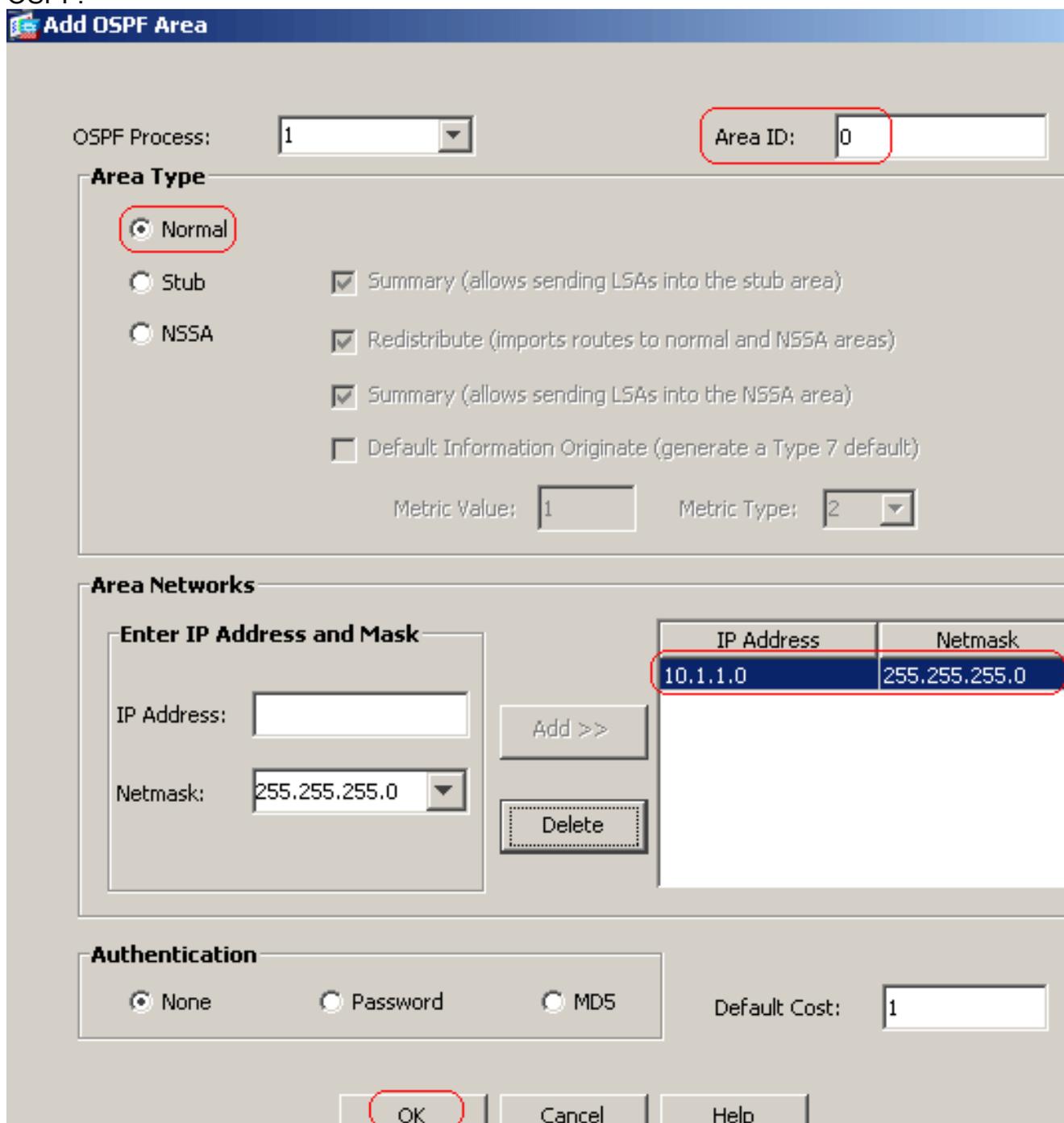
In questo elenco vengono descritti i singoli campi: Processo OSPF: visualizza il processo OSPF che si sta configurando. Non è possibile modificare questo valore. ID router: per utilizzare un ID di router fisso, immettere un ID di router in formato indirizzo IP nel campo ID router. Se si lascia vuoto questo valore, come ID del router verrà utilizzato l'indirizzo IP di livello più alto sull'accessorio di sicurezza. Nell'esempio, l'ID del router è configurato in modo statico con l'indirizzo IP dell'interfaccia interna (10.1.1.1). Ignora MOSPF LSA: selezionare questa casella di controllo per non inviare messaggi di registro del sistema quando l'appliance di sicurezza riceve pacchetti LSA tipo 6 (MOSPF). Questa impostazione è deselezionata per impostazione predefinita. RFC 1583 compatibile: selezionare questa casella di controllo per calcolare il riepilogo dei costi di instradamento per RFC 1583. Deselezionare questa casella di controllo per calcolare il riepilogo dei costi dei cicli di lavorazione per RFC 2328. Per ridurre al minimo la possibilità di loop di routing, tutti i dispositivi OSPF in un dominio di routing OSPF devono avere la compatibilità RFC impostata in modo identico. Questa impostazione è selezionata per impostazione predefinita. Modifiche adiacenze (Adjacency Changes) - Contiene le impostazioni che definiscono le modifiche

delle adiacenze che causano l'invio dei messaggi di registro del sistema. Registra modifiche adiacenze: selezionare questa casella di controllo per fare in modo che l'appliance di sicurezza invii un messaggio di registro di sistema ogni volta che un router adiacente OSPF diventa attivo o inattivo. Questa impostazione è selezionata per impostazione predefinita. Registra dettagli modifiche adiacenze: selezionare questa casella di controllo per fare in modo che l'appliance di sicurezza invii un messaggio di registro del sistema ogni volta che si verifica un cambiamento di stato, non solo quando un router adiacente diventa attivo o inattivo. Questa impostazione è deselezionata per impostazione predefinita. Distanze route amministrative (Administrative Route Distances) - Contiene le impostazioni per le distanze amministrative delle route in base al tipo di route. Tra aree (Inter Area) - Imposta la distanza amministrativa per tutte le route da un'area all'altra. I valori validi sono compresi tra 1 e 255. Il valore predefinito è 100. Intra area - Imposta la distanza amministrativa per tutte le route all'interno di un'area. I valori validi sono compresi tra 1 e 255. Il valore predefinito è 100. Esterna (External) - Imposta la distanza amministrativa per tutte le route dagli altri domini di routing appresi mediante la redistribuzione. I valori validi sono compresi tra 1 e 255. Il valore predefinito è 100. Timer (Timers) - Contiene le impostazioni utilizzate per configurare il passo LSA e i timer di calcolo SPF. Ritardo SPF - Specifica il tempo che intercorre tra il momento in cui OSPF riceve una modifica della topologia e l'inizio del calcolo SPF. I valori validi sono compresi tra 0 e 65535. Il valore predefinito è 5. Tempo blocco SPF (SPF Hold Time) - Specifica il tempo di blocco tra i calcoli SPF consecutivi. I valori validi sono compresi tra 1 e 65534. Il valore predefinito è 10. Pacing gruppo LSA (LSA Group Pacing) - Specifica l'intervallo in base al quale le LSA vengono raccolte in un gruppo e aggiornate, sottoposte a checksum o sottoposte a aging. I valori validi sono compresi tra 10 e 1800. Il valore predefinito è 240. Origine informazioni di default (Default Information Origine) - Contiene le impostazioni utilizzate da un ASBR per generare una route esterna di default in un dominio di routing OSPF. Abilita origine informazioni predefinita: selezionare questa casella di controllo per abilitare la generazione della route predefinita nel dominio di routing OSPF. Annuncia sempre la route predefinita: selezionare questa casella di controllo per annunciare sempre la route predefinita. Questa opzione è deselezionata per impostazione predefinita. Valore metrica (Metric Value) - Specifica la metrica di default OSPF. I valori validi sono compresi tra 0 e 16777214. Il valore predefinito è 1. Tipo di metrica: specifica il tipo di collegamento esterno associato alla route predefinita annunciata nel dominio di routing OSPF. I valori validi sono 1 o 2 e indicano un instradamento esterno di tipo 1 o 2. Il valore predefinito è 2. Mappa route - (*facoltativo*) il nome della mappa route da applicare. Il processo di instradamento genera il instradamento predefinito se la mappa del instradamento è soddisfatta.

5. Dopo aver completato i passaggi precedenti, definire le reti e le interfacce che partecipano al routing OSPF nella scheda **Imposta > Area/Reti** e quindi fare clic su **Aggiungi** come mostrato nell'immagine:



Viene visualizzata la finestra di dialogo Aggiungi area OSPF.



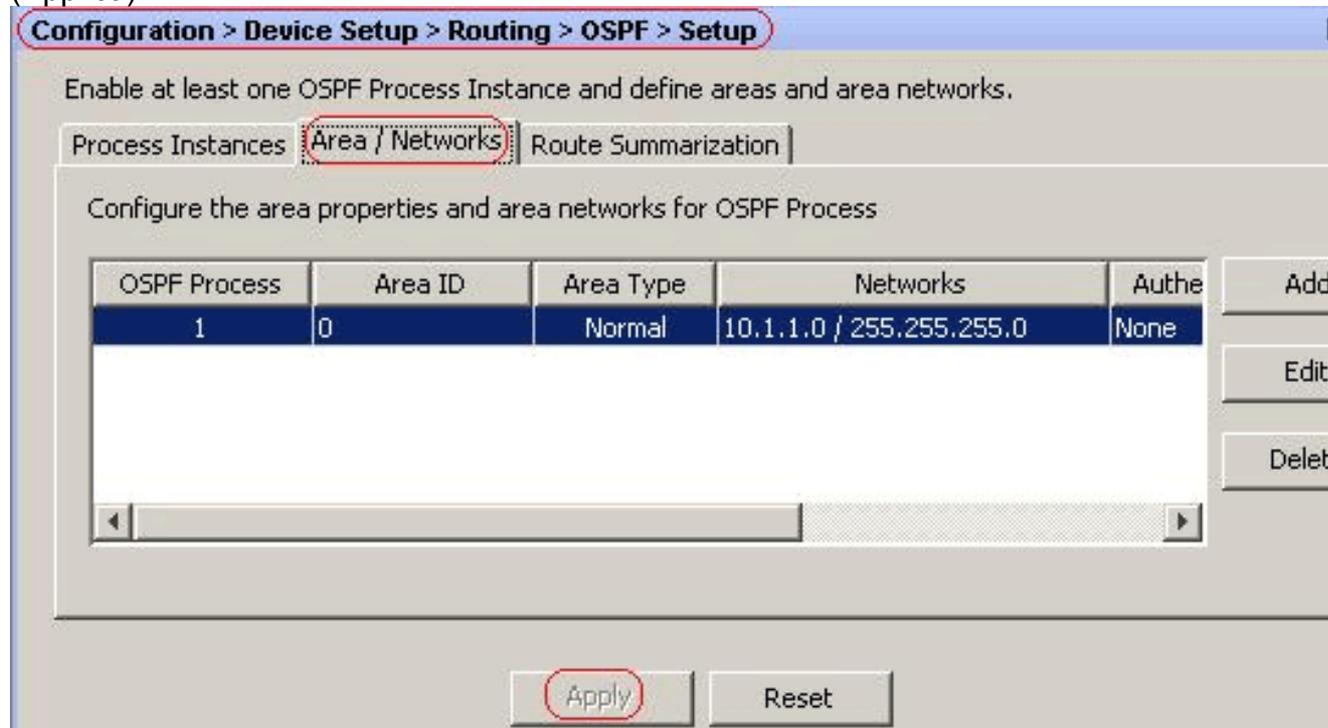
Nell'esempio, l'unica rete aggiunta è la rete interna (10.1.1.0/24), in quanto OSPF è abilitato solo sull'interfaccia interna. **Nota:** solo le interfacce con un indirizzo IP che rientrano nelle reti

definite partecipano al processo di routing OSPF.

6. Fare clic su **OK**. In questo elenco vengono descritti i singoli campi:
- Processo OSPF:** quando si aggiunge una nuova area, scegliere l'ID per il processo OSPF. Se sull'accessorio di protezione è abilitato un solo processo OSPF, per impostazione predefinita tale processo viene selezionato. Quando si modifica un'area esistente, non è possibile modificare l'ID del processo OSPF.
 - ID area (Area ID) -** Quando aggiungete una nuova area, immettete l'ID dell'area. È possibile specificare l'ID dell'area come numero decimale o come indirizzo IP. I valori decimali validi sono compresi tra 0 e 4294967295. Non è possibile modificare l'ID area quando si modifica un'area esistente. Nell'esempio, l'ID area è 0.
 - Tipo area (Area Type) -** Contiene le impostazioni per il tipo di area da configurare.
 - Normale (Normal) -** Selezionate questa opzione per rendere l'area un'area OSPF standard. Questa opzione è selezionata per impostazione predefinita quando si crea un'area.
 - Stub -** Selezionate questa opzione per rendere l'area un'area di stub. Le aree di stub non hanno router o aree oltre. Le aree di stub impediscono che le LSA esterne (LSA di tipo 5) vengano inondate nell'area di stub. Quando si crea un'area di stub, è possibile deselegionare la casella di controllo Riepilogo per evitare che le LSA di riepilogo (tipo 3 e 4) vengano inondate nell'area.
 - Riepilogo (Summary) -** Se l'area da definire è un'area di stub, deselegionare questa casella di controllo per impedire l'invio di LSA nell'area di stub. Questa casella di controllo è selezionata per default per le aree di stub.
 - NSSA (NSSA) -** Selezionate questa opzione per rendere l'area un'area non di tipo stubby. Gli NSA accettano LSA di tipo 7. Quando si crea un'associazione di protezione (LSA) di riepilogo, è possibile deselegionare la casella di controllo Riepilogo per impedire che le associazioni di protezione di riepilogo vengano propagate nell'area. Inoltre, è possibile deselegionare la casella di controllo Ridistribuisce e abilitare Origine informazioni predefinite per disabilitare la redistribuzione della route.
 - Ridistribuisce (Redistribute) -** Deselegionare questa casella di controllo per impedire l'importazione delle route nell'NSSA. Questa casella di controllo è selezionata per impostazione predefinita.
 - Riepilogo: se l'area da definire è un'area NSSA, deselegionare questa casella di controllo per impedire l'invio delle LSA nell'area di stub. Questa casella di controllo è selezionata per impostazione predefinita per le NSSA.**
 - Origine informazioni di default (Default Information Origine) -** Selezionate questa casella di controllo per generare un default di tipo 7 nell'NSSA. Per impostazione predefinita, questa casella di controllo è deselegionata.
 - Valore metrica:** immettere un valore per specificare il valore della metrica OSPF per la route predefinita. I valori validi sono compresi tra 0 e 16777214. Il valore predefinito è 1.
 - Tipo di metrica:** scegliere un valore per specificare il tipo di metrica OSPF per la route predefinita. Le opzioni disponibili sono 1 (tipo 1) o 2 (tipo 2). Il valore predefinito è 2.
 - Reti ad area:** contiene le impostazioni che definiscono un'area OSPF.
 - Enter IP Address and Mask -** Contiene le impostazioni utilizzate per definire le reti nell'area.
 - Indirizzo IP:** immettere l'indirizzo IP della rete o dell'host da aggiungere all'area. Utilizzate 0.0.0.0 con una maschera di rete di 0.0.0.0 per creare l'area di default. Potete utilizzare 0.0.0.0 in una sola area.
 - Netmask:** scegliere la maschera di rete per l'indirizzo IP o l'host da aggiungere all'area. Se si aggiunge un host, scegliere la maschera 255.255.255.255. Nell'esempio, **10.1.1.0/24** è la rete da configurare.
 - Aggiungi (Add) -** Aggiunge all'area la rete definita nell'area. Immetti indirizzo IP e maschera (Enter IP Address and Mask). La rete aggiunta viene visualizzata nella tabella Reti LAN.
 - Elimina (Delete) -** Elimina la rete selezionata dalla tabella Reti ad area (Area Networks).
 - Reti area (Area Networks) -** Visualizza le reti definite per l'area.
 - Indirizzo IP:** visualizza l'indirizzo IP della rete.
 - Maschera di rete (Netmask) -** Visualizza la maschera di rete per la rete.
 - Autenticazione:** contiene le impostazioni per l'autenticazione dell'area OSPF.
 - Nessuna:** scegliere questa opzione per disabilitare l'autenticazione dell'area OSPF. Si tratta dell'impostazione

predefinita. Password: scegliere questa opzione per utilizzare una password non crittografata per l'autenticazione dell'area. Questa opzione non è consigliata quando la sicurezza rappresenta un problema. MD5: selezionare questa opzione per utilizzare l'autenticazione MD5. Costo di default (Default Cost) - Consente di specificare un costo di default per l'area. I valori validi sono compresi tra 0 e 65535. Il valore predefinito è 1.

7. Fare clic su **Apply** (Applica).



8. Facoltativamente, 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 OSPF.
9. Facoltativamente, è possibile configurare la redistribuzione delle route. Cisco ASA può redistribuire le route individuate da RIP e EIGRP nel processo di routing OSPF. È inoltre possibile redistribuire le route statiche e connesse nel processo di routing OSPF. Definire la redistribuzione dei cicli di lavorazione nel riquadro Ridistribuzione.
10. I pacchetti hello OSPF vengono inviati come pacchetti multicast. Se una risorsa adiacente OSPF si trova su una rete non broadcast, è necessario definirla manualmente. Quando si definisce manualmente un router adiacente OSPF, i pacchetti hello vengono inviati a tale router adiacente come messaggi unicast. Per definire i router adiacenti OSPF statici, passare al riquadro adiacente statico.
11. È possibile riepilogare le route apprese da altri protocolli di routing. La metrica utilizzata per annunciare il riepilogo è la più piccola di tutte le route più specifiche. Le route di riepilogo consentono di ridurre le dimensioni della tabella di routing. L'utilizzo di route di riepilogo per OSPF fa sì che un OSPF ASBR annunci una route esterna come aggregazione per tutte le route redistribute coperte dall'indirizzo. È possibile riepilogare solo le route di altri protocolli di routing redistribuiti in OSPF.
12. Nel riquadro Virtual Link è possibile aggiungere un'area a una rete OSPF e non è possibile collegarla direttamente all'area backbone. È necessario creare un collegamento virtuale. Un collegamento virtuale collega due dispositivi OSPF che hanno un'area comune, denominata area di transito. Uno dei dispositivi OSPF deve essere collegato all'area backbone.

Configura autenticazione OSPF

Cisco ASA supporta l'autenticazione MD5 degli aggiornamenti di routing dal protocollo di routing OSPF. Il digest con chiave MD5 in ciascun pacchetto OSPF impedisce l'introduzione di messaggi di routing non autorizzati o falsi provenienti da origini non approvate. L'aggiunta dell'autenticazione ai messaggi OSPF assicura che i router e l'appliance Cisco ASA accettino solo messaggi di routing da altri dispositivi di routing configurati con la stessa chiave precondivisa. Se non si configura questa autenticazione, se un altro utente immette nella rete un'altra periferica di routing con informazioni di routing diverse o contrarie, le tabelle di routing sui router o sull'appliance Cisco ASA possono danneggiarsi e può verificarsi un attacco Denial of Service. L'aggiunta dell'autenticazione ai messaggi EIGRP inviati tra i dispositivi di routing (compresa l'ASA) impedisce l'aggiunta intenzionale o accidentale di un altro router alla rete e qualsiasi problema.

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

Completare questi passaggi per abilitare l'autenticazione OSPF MD5 sull'appliance Cisco ASA:

1. In ASDM, selezionare **Configuration > Device Setup > Routing > OSPF > Interface** (Configurazione > Impostazione dispositivo > Routing > OSPF > Interfaccia), quindi fare clic sulla scheda **Authentication** (Autenticazione), come mostrato nell'immagine.



In questo caso, OSPF è abilitato sull'interfaccia interna.

2. Scegliere l'interfaccia **interna** e fare clic su **Modifica**.
3. In Autenticazione scegliere **Autenticazione MD5** e aggiungere qui ulteriori informazioni sui parametri di autenticazione. In questo caso, la chiave già condivisa è **cisco123** e l'ID della chiave è
1.

Edit OSPF Interface Authentication

Interface:

Authentication

No authentication
 Area authentication, if defined
 MD5 authentication

Authentication Password

Enter Password: Re-enter Password:

MD5 IDs and Keys

MD5 Key ID:

MD5 Key:

MD5 Key ID	MD5 Key
1	cisco123

4. Fare clic su **OK**, quindi su **Applica**.

Configuration > Device Setup > Routing > OSPF > Interface

Configure Interface specific OSPF routing parameters.

Specify the authentication properties for each interface.

Interface	Authentication Type
inside	MD5
dmz	Area
outside	Area

Cisco ASA

```
ciscoasa#show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname ciscoasa
enable password 8Ry2YjIyt7RRXU24 encrypted
names

!--- Inside interface configuration interface
Ethernet0/1 nameif inside security-level 100 ip address
10.1.1.1 255.255.255.0 ospf cost 10 !--- OSPF
authentication is configured on the inside interface
ospf message-digest-key 1 md5 <removed> ospf
authentication message-digest ! !--- Outside interface
configuration interface Ethernet0/2 nameif outside
security-level 0 ip address 192.168.1.2 255.255.255.0
ospf cost 10 ! !--- Output Suppressed icmp unreachable
rate-limit 1 burst-size 1 asdm image disk0:/asdm-602.bin
no asdm history enable arp timeout 14400 ! !--- OSPF
Configuration router ospf 1
  network 10.1.1.0 255.255.255.0 area 0
  log-adj-changes
!

!--- This is the static default gateway configuration in
order to reach Internet route outside 0.0.0.0 0.0.0.0
192.168.1.1 1 ciscoasa#
```

Configurazione CLI del router Cisco IOS (R2)

Router Cisco IOS (R2)

```
!--- Interface that connects to the Cisco ASA. !---
Notice the OSPF authentication parameters interface
Ethernet0
  ip address 10.1.1.2 255.255.255.0
  ip ospf authentication message-digest
  ip ospf message-digest-key 1 md5 cisco123

!--- Output Suppressed !--- OSPF Configuration router
ospf 1
  log-adjacency-changes
  network 10.1.1.0 0.0.0.255 area 0
  network 172.16.1.0 0.0.0.255 area 0
  network 172.16.2.0 0.0.0.255 area 0
```

Configurazione CLI del router Cisco IOS (R1)

Router Cisco IOS (R1)

```
!--- Output Suppressed !--- OSPF Configuration router
ospf 1
  log-adjacency-changes
```

```
network 172.16.5.0 0.0.0.255 area 0
network 172.16.2.0 0.0.0.255 area 0
```

Configurazione CLI del router Cisco IOS (R3)

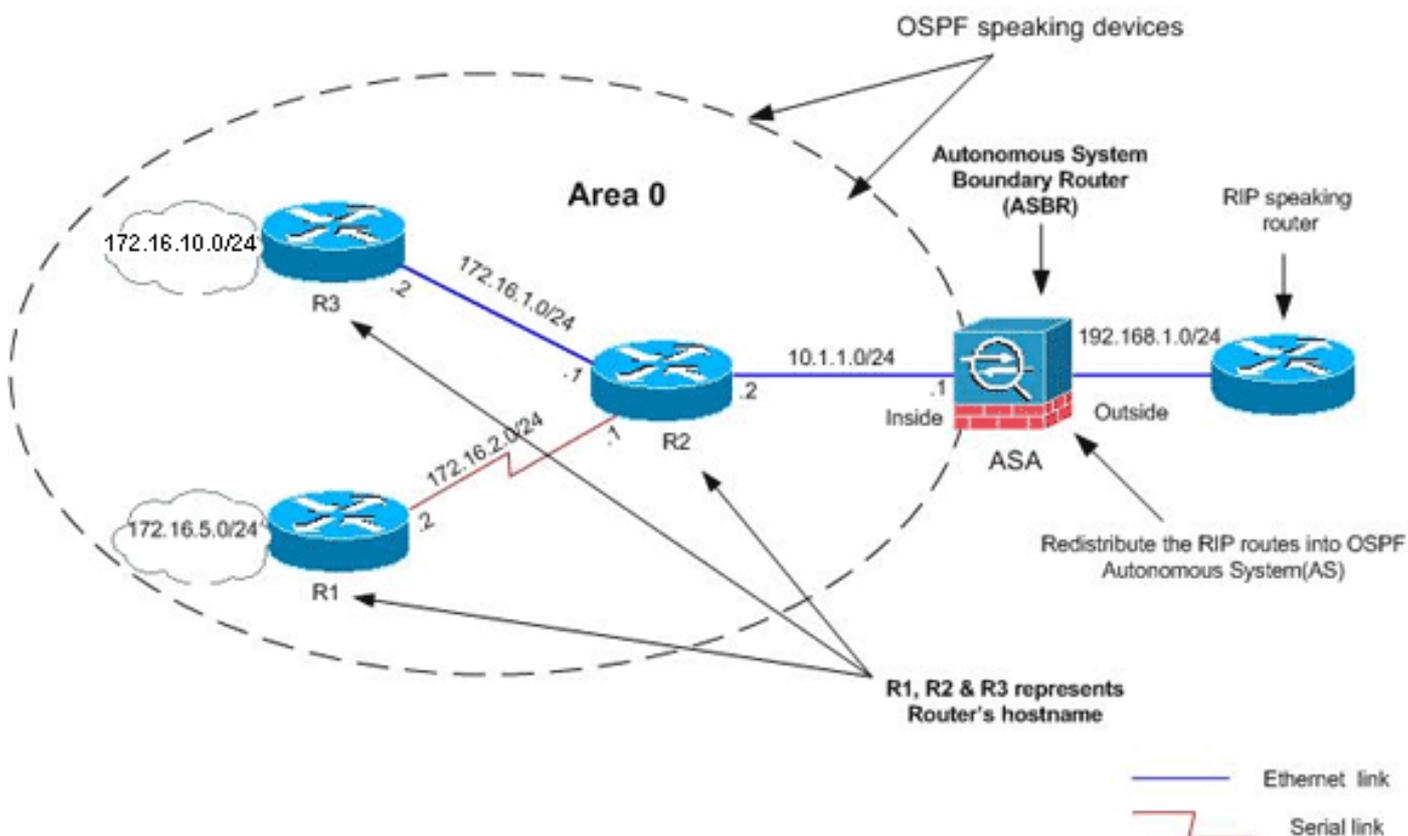
Router Cisco IOS (R3)

```
!--- Output Suppressed !--- OSPF Configuration router
ospf 1
log-adjacency-changes
network 172.16.1.0 0.0.0.255 area 0
network 172.16.10.0 0.0.0.255 area 0
```

Ridistribuzione in OSPF con ASA

Come accennato in precedenza, è possibile redistribuire le route in un processo di routing OSPF da un altro processo di routing OSPF, da un processo di routing RIP o da route statiche e connesse configurate su interfacce abilitate OSPF.

In questo esempio, redistribuire le route RIP in OSPF con il diagramma di rete come mostrato:



Configurazione ASDM

1. Scegliere **Configurazione > Configurazione dispositivo > Routing > RIP > Impostazioni** per abilitare RIP e aggiungere la rete 192.168.1.0 come mostrato nell'immagine.

Configuration > Device Setup > Routing > RIP > Setup

Configure the global Routing Information Protocol (RIP) parameters. You can configure the setting of the RIP routing process.

Enable RIP routing

Enable auto-summarization

Enable RIP version Version 1 Version 2

(If global version in not configured then device sends Version 1 and receives Versions 1 & 2.)

Enable default information originate Route Map:

Networks

IP Network to Add:

192.168.1.0

Passive Interfaces

Global passive: Configure all the interfaces as passive globally. This setting will override the individual

Interface	Passive
inside	<input type="checkbox"/>
dmz	<input type="checkbox"/>

2. Fare clic su **Apply** (Applica).
3. Scegliere **Configurazione > Configurazione dispositivo > Routing > OSPF > Ridistribuzione > Aggiungi** per ridistribuire le route RIP in OSPF.

Configuration > Device Setup > Routing > OSPF > Redistribution

Define the conditions for redistributing routes from one OSPF process to another.

OSPF Process	Protocol	Match	Subnets	Metric Value	Metric Type

4. Fare clic su **OK**, quindi su **Applica**.

Configurazione CLI equivalente

Configurazione CLI di ASA per la redistribuzione di RIP in OSPF AS

```

router ospf 1
 network 10.1.1.0 255.255.255.0 area 0
 log-adj-changes
 redistribute rip subnets

router rip
 network 192.168.1.0

```

Dopo aver redistribuito le route RIP in OSPF AS, è possibile visualizzare la tabella di routing del router IOS (R2) adiacente.

R2#show ip 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, 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

```

Gateway of last resort is not set

```

172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
O       172.16.10.1/32 [110/11] via 172.16.1.2, 01:17:29, Ethernet1
O       172.16.5.1/32 [110/65] via 172.16.2.2, 01:17:29, Serial1
C       172.16.1.0/24 is directly connected, Ethernet1
C       172.16.2.0/24 is directly connected, Serial1
10.0.0.0/24 is subnetted, 1 subnets

```

```
C 10.1.1.0 is directly connected, Ethernet0
O E2 192.168.1.0/24 [110/20] via 10.1.1.1, 01:17:29, Ethernet0
!--- Redistributed route advertised by Cisco ASA
```

Verifica

Per verificare la configurazione, attenersi alla procedura seguente:

1. Su ASDM, è possibile passare a **Monitoraggio > Routing > Router OSPF** per visualizzare ogni router adiacente OSPF. Nell'immagine viene mostrato il router interno (R2) come router adiacente attivo. È inoltre possibile visualizzare l'interfaccia in cui risiede il router adiacente, l'ID del router adiacente, lo stato del ciclo di vita e il tempo di inattività.

Monitoring > Routing > OSPF Neighbors

OSPF Neighbors

Each row represents one OSPF Neighbor. Please click the help button for a description of the states.

Neighbor	Priority	State	Dead Time	Address	Interface
172.16.2.1	1	FULL/BDR	0:00:34	10.1.1.2	inside

Last Updated: 5/19/08 3:55:10 PM

2. Inoltre, è possibile verificare la tabella di instradamento selezionando **Controllo > Instradamento > Instradamenti**. In questa immagine, le reti 172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24 e 172.16.10.0/24 vengono apprese tramite R2 (10.1.1.2).

Monitoring > Routing > Routes

Routes

Each row represents one route. AD is the administrative distance.

Protocol	Type	Destination IP	Netmask	Gateway	Int
OSPF	-	172.16.10.1	255.255.255.255	10.1.1.2	inside
OSPF	-	172.16.5.1	255.255.255.255	10.1.1.2	inside
OSPF	-	172.16.1.0	255.255.255.0	10.1.1.2	inside
OSPF	-	172.16.2.0	255.255.255.0	10.1.1.2	inside
CONNECTED	-	10.1.1.0	255.255.255.0	-	inside
CONNECTED	-	10.77.241.128	255.255.255.192	-	dmz
STATIC	-	10.77.0.0	255.255.0.0	10.77.241.129	dmz
CONNECTED	-	192.168.1.0	255.255.255.0	-	outside
STATIC	DEFAULT	0.0.0.0	0.0.0.0	192.168.1.1	outside

3. 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 192.168.1.1 to network 0.0.0.0

```
O 172.16.10.1 255.255.255.255 [110/21] via 10.1.1.2, 0:00:06, inside
O 172.16.5.1 255.255.255.255 [110/75] via 10.1.1.2, 0:00:06, inside
O 172.16.1.0 255.255.255.0 [110/20] via 10.1.1.2, 0:00:06, inside
O 172.16.2.0 255.255.255.0 [110/74] via 10.1.1.2, 0:00:06, inside
C 10.1.1.0 255.255.255.0 is directly connected, inside
C 10.77.241.128 255.255.255.192 is directly connected, dmz
S 10.77.0.0 255.255.0.0 [1/0] via 10.77.241.129, dmz
C 192.168.1.0 255.255.255.0 is directly connected, outside
S* 0.0.0.0 0.0.0.0 [1/0] via 192.168.1.1, outside
```

4. È inoltre possibile utilizzare il comando **show ospf database** per ottenere informazioni sulle reti e sulla topologia ospf apprese.

```
ciscoasa#show ospf database
```

OSPF Router with ID (192.168.1.2) (Process ID 1)

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
172.16.1.2	172.16.1.2	123	0x80000039	0xfd1d	2
172.16.2.1	172.16.2.1	775	0x8000003c	0x9b42	4
172.16.5.1	172.16.5.1	308	0x80000038	0xb91b	3
192.168.1.2	192.168.1.2	1038	0x80000037	0x29d7	1

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
10.1.1.1	192.168.1.2	1038	0x80000034	0x72ee
172.16.1.1	172.16.2.1	282	0x80000036	0x9e68

5. Il comando **show ospf neighbors** è utile anche per verificare i router adiacenti attivi e le informazioni corrispondenti. Questo esempio mostra le stesse informazioni ottenute da ASDM nel passo 1.

```
ciscoasa#show ospf neighbor
```

Neighbor ID	Pri	State	Dead Time	Address	Interface
172.16.2.1	1	FULL/BDR	0:00:36	10.1.1.2	inside

Risoluzione dei problemi

In questa sezione vengono fornite informazioni che possono facilitare la risoluzione dei problemi OSPF.

Configurazione statica router adiacente per rete point-to-point

Se è stata configurata la *rete OSPF point-to-point non-broadcast* sull'appliance ASA, è necessario definire router adiacenti OSPF statici per annunciare le route OSPF su una rete point-to-point non broadcast. Per ulteriori informazioni, fare riferimento a [Definizione dei router adiacenti OSPF statici](#).

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**.

- **debug ospf events:** abilita il debug degli eventi OSPF.

```
ciscoasa(config)#debug ospf events
OSPF events debugging is on
ciscoasa(config)# int e0/1
ciscoasa(config-if)# no shu
ciscoasa(config-if)#
OSPF: Interface inside going Up
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: 2 Way Communication to 172.16.2.1 on inside, state 2WAY
OSPF: Backup seen Event before WAIT timer on inside
OSPF: DR/BDR election on inside
OSPF: Elect BDR 172.16.2.1
OSPF: Elect DR 172.16.2.1
      DR: 172.16.2.1 (Id)   BDR: 172.16.2.1 (Id)
OSPF: Send DBD to 172.16.2.1 on inside seq 0x1abd opt 0x2 flag 0x7 len 32
OSPF: Send with youngest Key 1
OSPF: End of hello processing
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x12f3 opt 0x42 flag 0x7 len 32  mtu
 1500 state EXSTART
OSPF: First DBD and we are not SLAVE
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x1abd opt 0x42 flag 0x2 len 152  mt
u 1500 state EXSTART
OSPF: NBR Negotiation Done. We are the MASTER
OSPF: Send DBD to 172.16.2.1 on inside seq 0x1abe opt 0x2 flag 0x3 len 132
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Database request to 172.16.2.1
OSPF: sent LS REQ packet to 10.1.1.2, length 12
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x1abe opt 0x42 flag 0x0 len 32  mtu
 1500 state EXCHANGE
OSPF: Send DBD to 172.16.2.1 on inside seq 0x1abf opt 0x2 flag 0x1 len 32
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Rcv DBD from 172.16.2.1 on inside seq 0x1abf opt 0x42 flag 0x0 len 32  mtu
 1500 state EXCHANGE
OSPF: Exchange Done with 172.16.2.1 on inside
OSPF: Synchronized with 172.16.2.1 on inside, state FULL
OSPF: Send with youngest Key 1
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: Neighbor change Event on interface inside
OSPF: DR/BDR election on inside
OSPF: Elect BDR 192.168.1.2
OSPF: Elect DR 172.16.2.1
OSPF: Elect BDR 192.168.1.2
OSPF: Elect DR 172.16.2.1
      DR: 172.16.2.1 (Id)   BDR: 192.168.1.2 (Id)
OSPF: End of hello processing
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
```

```
OSPF: End of hello processing
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
OSPF: Send with youngest Key 1
OSPF: Rcv hello from 172.16.2.1 area 0 from inside 10.1.1.2
OSPF: End of hello processing
```

Nota: per ulteriori informazioni sui vari comandi che sono utili per la risoluzione del problema, consultare la sezione [debug ospf](#) della guida di riferimento dei comandi di Cisco Security Appliance, versione 8.0.

[Informazioni correlate](#)

- [Cisco serie 5500 Adaptive Security Appliance - Pagina di supporto](#)
- [Cisco serie 500 PIX Support Page](#)
- [PIX/ASA 8.X: Configurazione di EIGRP su Cisco Adaptive Security Appliance \(ASA\)](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)