ASA/PIX mit OSPF-Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Cisco ASA so konfiguriert wird, dass Routen mithilfe von Open Shortest Path First (OSPF) erfasst, authentifiziert und neu verteilt werden.

Weitere Informationen finden Sie unter PIX/ASA 8.X: Konfigurieren von EIGRP auf der Cisco Adaptive Security Appliance (ASA) für weitere Informationen zur EIGRP-Konfiguration

Hinweis: Asymmetrisches Routing wird in ASA/PIX nicht unterstützt.

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese

Konfiguration durchzuführen:

- Cisco ASA/PIX muss Version 7.x oder höher ausführen.
- OSPF wird im Multi-Context-Modus nicht unterstützt. Es wird nur im Einzelmodus unterstützt.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Adaptive Security Appliance (ASA) der Serie 5500 mit Softwareversion 8.0 und höher
- Cisco Adaptive Security Device Manager (ASDM)-Software, Version 6.0 und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Zugehörige Produkte

Die Informationen in diesem Dokument gelten auch für die Cisco PIX-Firewall der Serie 500, die die Softwareversion 8.0 und höher ausführt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

OSPF verwendet einen Link-State-Algorithmus, um den kürzesten Pfad zu allen bekannten Zielen zu erstellen und zu berechnen. Jeder Router in einem OSPF-Bereich enthält eine identische Link-State-Datenbank, die eine Liste der jeweils verwendbaren Router-Schnittstellen und der erreichbaren Nachbarn darstellt.

OSPF bietet gegenüber RIP folgende Vorteile:

- OSPF-Aktualisierungen für Link-State-Datenbanken werden weniger häufig als RIP-Aktualisierungen gesendet, und die Link-State-Datenbank wird sofort und nicht schrittweise aktualisiert, wenn veraltete Informationen abgelaufen sind.
- Routing-Entscheidungen basieren auf Kosten. Dies ist ein Hinweis auf den Overhead, der zum Senden von Paketen über eine bestimmte Schnittstelle erforderlich ist. Die Sicherheits-Appliance berechnet die Kosten einer Schnittstelle basierend auf der Verbindungsbandbreite und nicht auf der Anzahl der Hops bis zum Ziel. Die Kosten können so konfiguriert werden, dass bevorzugte Pfade festgelegt werden.

Der Nachteil von Kurzstreckenalgorithmen besteht darin, dass sie eine Menge CPU-Zyklen und Arbeitsspeicher benötigen.

Die Security Appliance kann zwei Prozesse des OSPF-Protokolls gleichzeitig auf verschiedenen Schnittstellensätzen ausführen. Sie können zwei Prozesse ausführen, wenn Sie über

Schnittstellen verfügen, die die gleichen IP-Adressen verwenden (NAT ermöglicht das parallele Ausführen dieser Schnittstellen, OSPF jedoch nicht das Überschneiden von Adressen). Oder Sie möchten einen Prozess auf der Innenseite und einen anderen auf der Außenseite ausführen und einen Teil der Routen zwischen den beiden Prozessen neu verteilen. Ebenso müssen Sie möglicherweise private Adressen von öffentlichen Adressen trennen.

Sie können Routen über einen anderen OSPF-Routing-Prozess, einen RIP-Routing-Prozess oder über statische und verbundene Routen, die auf OSPF-fähigen Schnittstellen konfiguriert sind, in einen OSPF-Routing-Prozess neu verteilen.

Die Sicherheits-Appliance unterstützt folgende OSPF-Funktionen:

- Unterstützung von Intra-Area-, Interarea- und externen Routen (Typ I und Typ II).
- Unterstützung einer virtuellen Verbindung.
- OSPF LSA-Flooding
- Authentifizierung von OSPF-Paketen (sowohl Kennwort als auch MD5-Authentifizierung).
- Unterstützung für die Konfiguration der Sicherheits-Appliance als designierter Router oder designierter Backup-Router. Die Sicherheits-Appliance kann auch als ABR eingerichtet werden. Die Konfiguration der Sicherheits-Appliance als ASBR ist jedoch auf Standardinformationen beschränkt (z. B. das Einschleusen einer Standardroute).
- Unterstützung für Stub-Bereiche und nicht so stubby-Bereiche.
- Bereichsbegrenzter Router-Typ-3-LSA-Filterung.

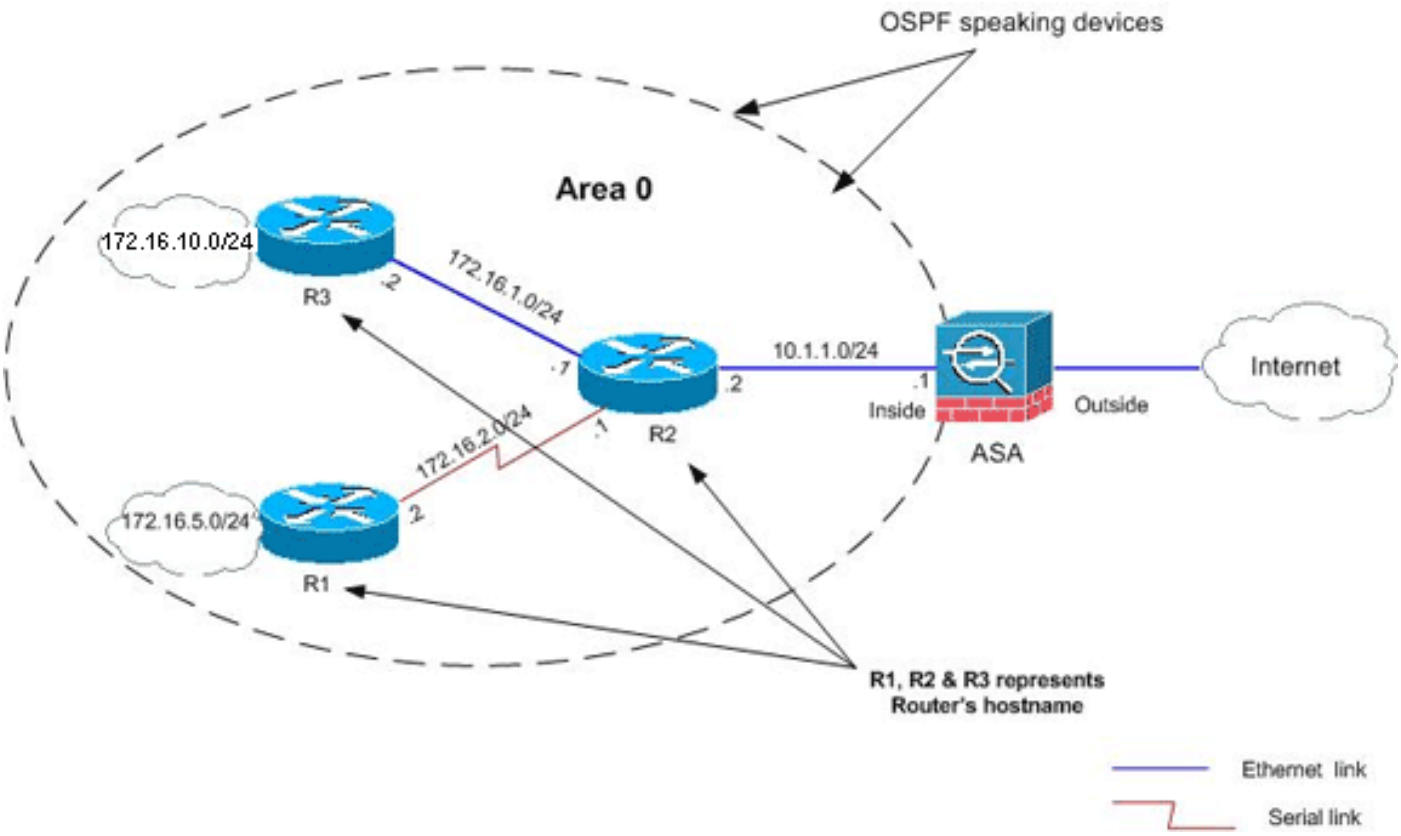
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Hinweis: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



In dieser Netzwerktopologie lautet die interne IP-Adresse der Cisco ASA-Schnittstelle 10.1.1.1/24. Ziel ist es, OSPF auf der Cisco ASA zu konfigurieren, um Routen zu den internen Netzwerken (172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24 und 172.16.10.0/24) dynamisch über den benachbarten Router (R2) zu erfassen. R2 erfasst die Routen zu internen Remote-Netzwerken über die anderen beiden Router (R1 und R3).

Konfigurationen

In diesem Dokument werden folgende Konfigurationen verwendet:

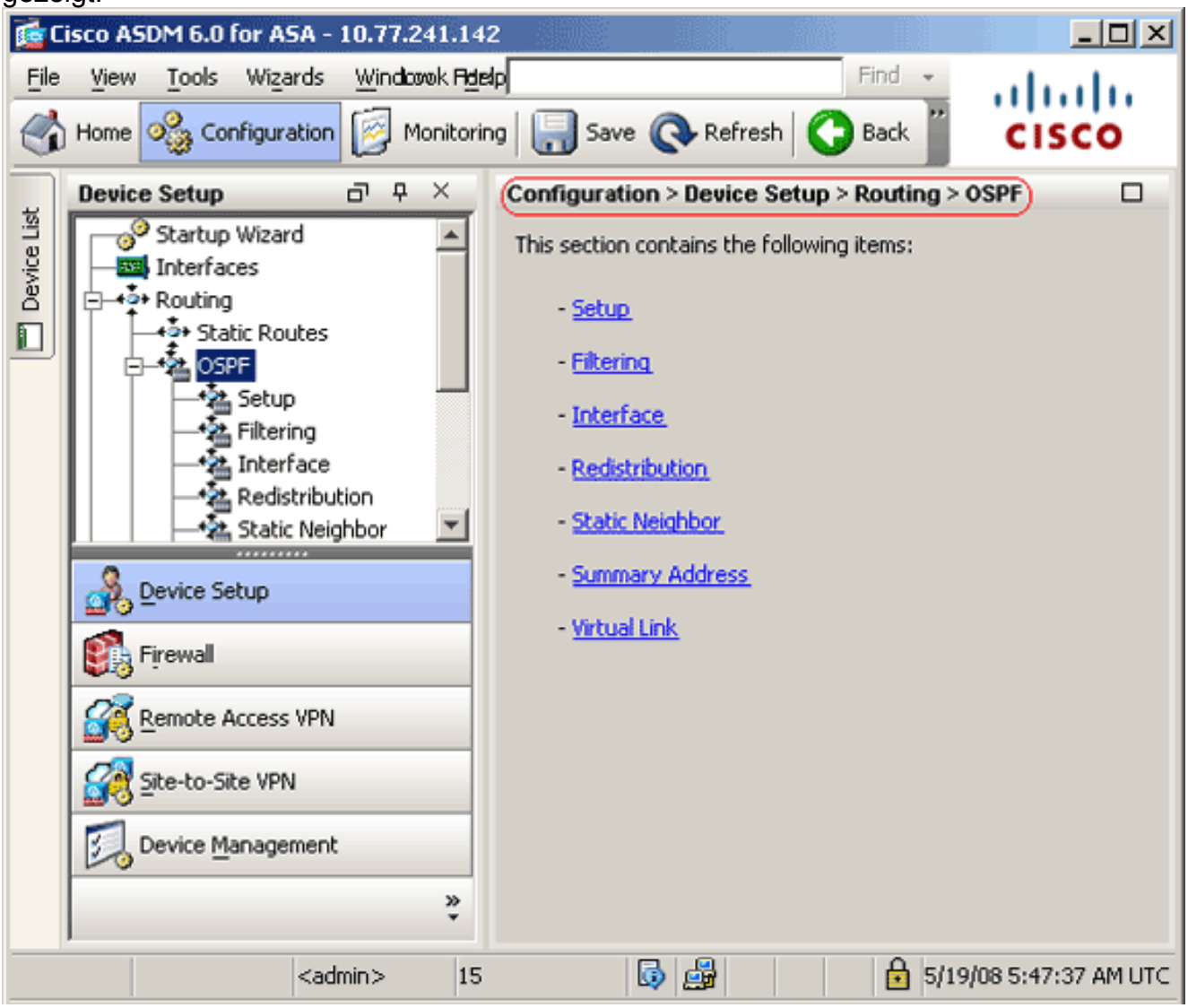
- ASDM-Konfiguration
- Konfigurieren der OSPF-Authentifizierung
- Cisco ASA CLI-Konfiguration
- CLI-Konfiguration des Cisco IOS Routers (R2)
- CLI-Konfiguration des Cisco IOS Routers (R1)
- CLI-Konfiguration des Cisco IOS Routers (R3)
- Neuverteilung in OSPF mit ASA

ASDM-Konfiguration

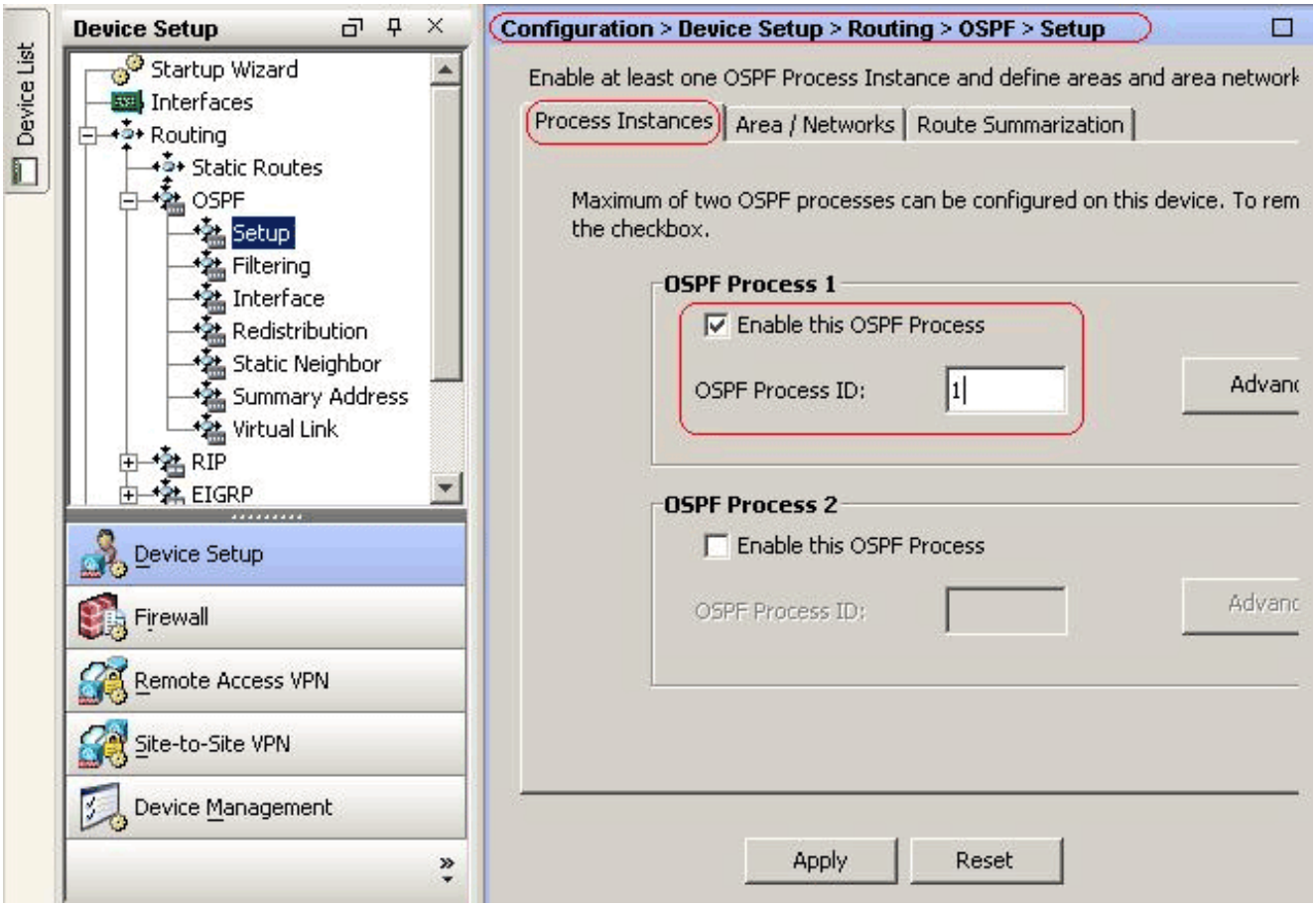
Adaptive Security Device Manager (ASDM) ist eine browserbasierte Anwendung zur Konfiguration und Überwachung der Software auf Sicherheitsgeräten. ASDM wird von der Sicherheits-Appliance geladen und anschließend zur Konfiguration, Überwachung und Verwaltung des Geräts verwendet. Sie können auch den ASDM Launcher (nur Windows) verwenden, um die ASDM-Anwendung schneller als das Java-Applet zu starten. In diesem Abschnitt werden die Informationen beschrieben, die Sie benötigen, um die in diesem Dokument beschriebenen Funktionen mit ASDM zu konfigurieren.

Gehen Sie wie folgt vor, um OSPF in der Cisco ASA zu konfigurieren:

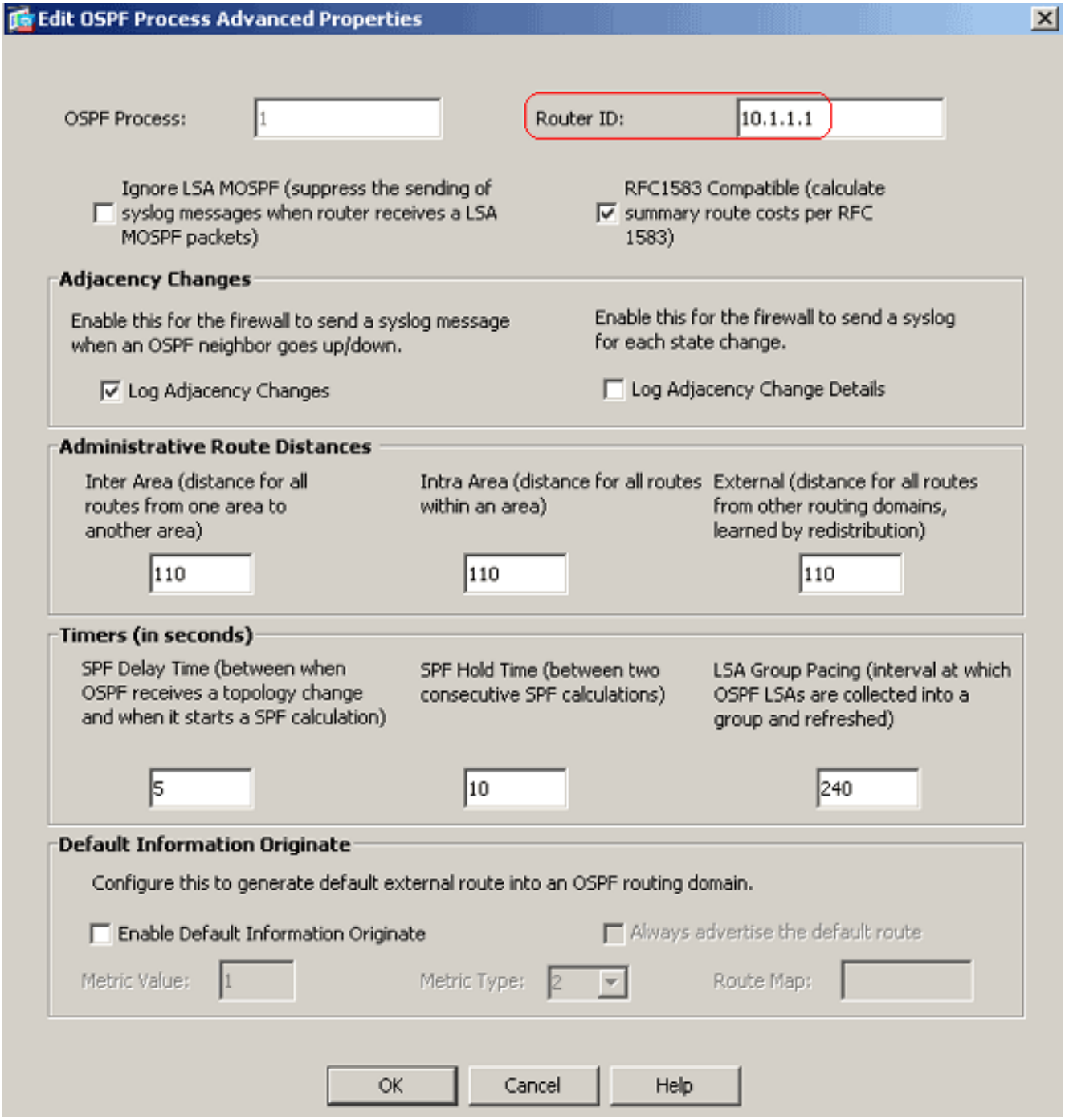
1. Melden Sie sich mit ASDM bei der Cisco ASA an.
2. Navigieren Sie zum Bereich **Konfiguration > Device Setup > Routing > OSPF** der ASDM-Schnittstelle, wie in diesem Bild gezeigt.



3. Aktivieren Sie den OSPF-Routing-Prozess auf der Registerkarte **Setup > Process Instances** (**Setup > Process Instanzen**), wie in diesem Bild gezeigt. In diesem Beispiel lautet der OSPF-ID-Prozess
1.



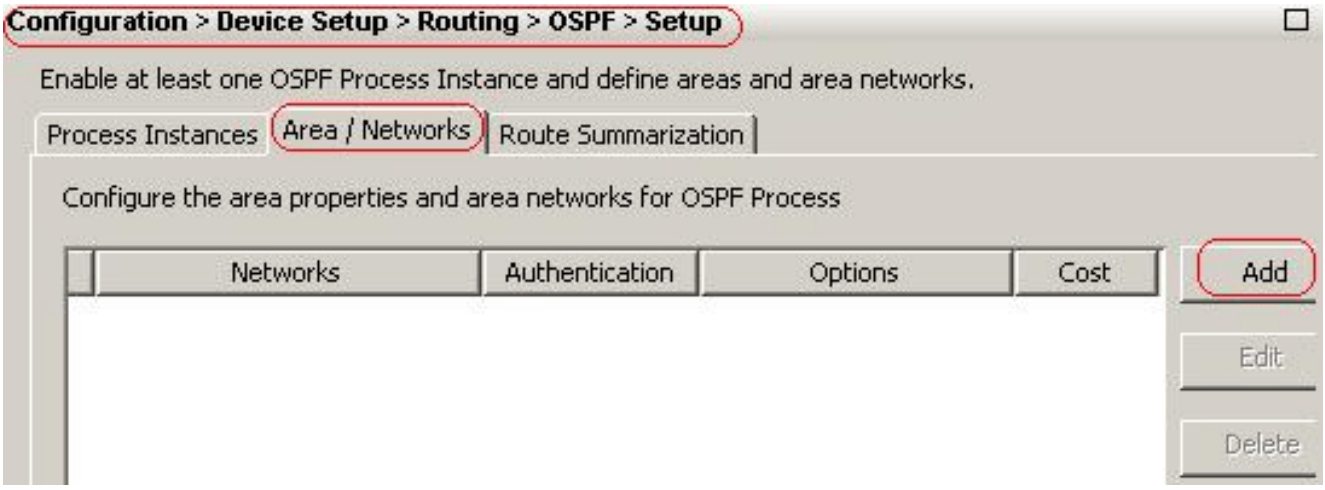
4. Sie können auf der Registerkarte **Setup > Process Instances (Setup > Prozessinstanzen)** auf **Advanced (Erweitert)** klicken, um optionale erweiterte OSPF-Routingprozessparameter zu konfigurieren. Sie können prozessspezifische Einstellungen bearbeiten, z. B. die Router-ID, Adjacency-Änderungen, Administrative Route Distances, Timer und die Einstellungen für die Standard-Informationsursprungskonfiguration.



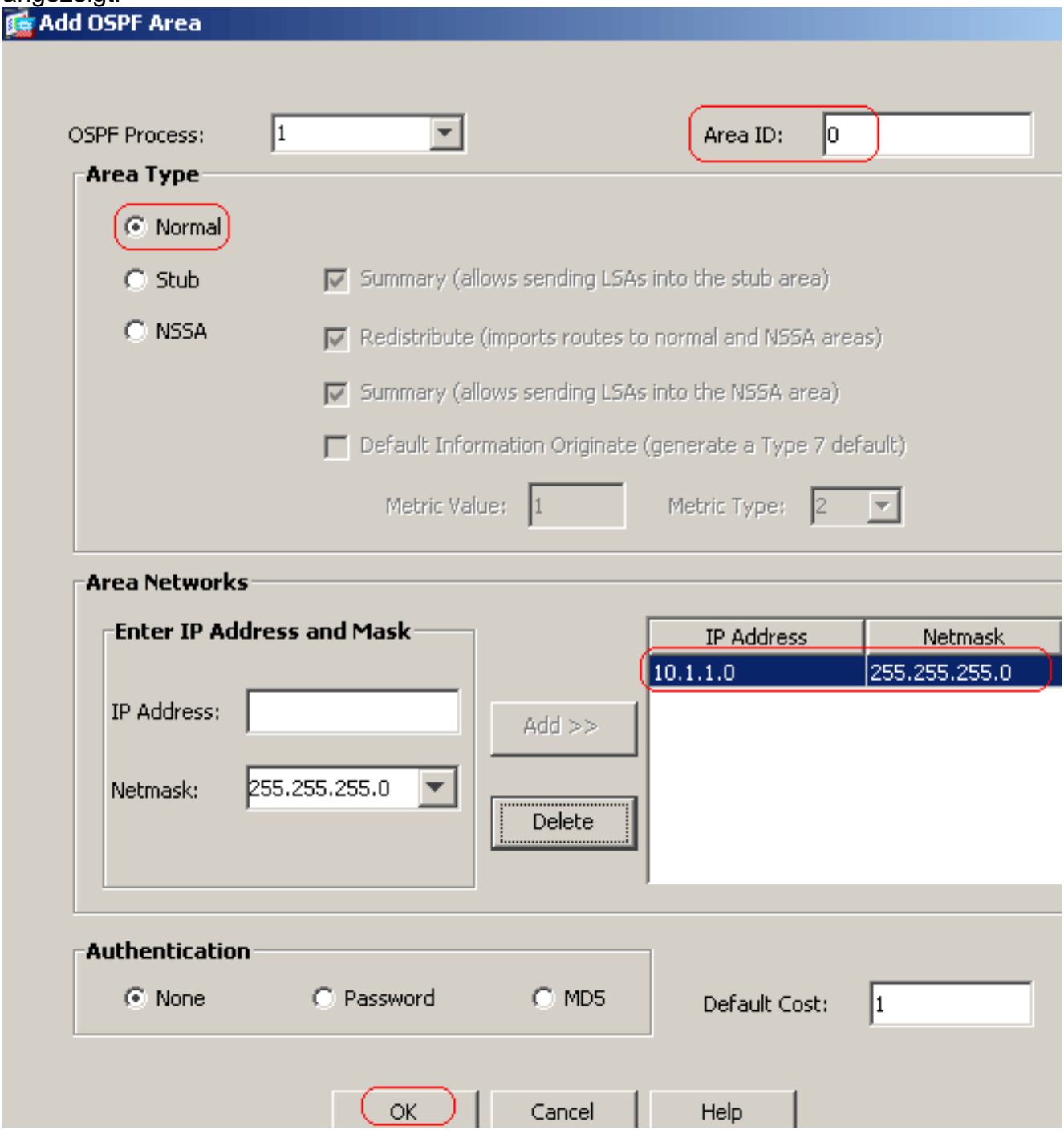
Diese Liste beschreibt die einzelnen Felder:OSPF Process (OSPF-Prozess): Zeigt den OSPF-Prozess an, den Sie konfigurieren. Dieser Wert kann nicht geändert werden.Router ID (Router-ID): Um eine feste Router-ID zu verwenden, geben Sie im Feld Router ID (Router-ID) eine Router-ID im IP-Adressformat ein. Wenn Sie diesen Wert leer lassen, wird die IP-Adresse der Sicherheitsappliance auf höchster Ebene als Router-ID verwendet.In diesem Beispiel wird die Router-ID statisch mit der IP-Adresse der internen Schnittstelle (10.1.1.1) konfiguriert.Ignore LSA MOSPF (LSA-MOSPF ignorieren) - Aktivieren Sie dieses Kontrollkästchen, um das Senden von Systemprotokollmeldungen zu unterdrücken, wenn die Sicherheits-Appliance LSA-Pakete vom Typ 6 (MOSPF) empfängt. Diese Einstellung ist standardmäßig deaktiviert.RFC 1583 Compatible (RFC 1583-kompatibel): Aktivieren Sie dieses Kontrollkästchen, um die zusammengefassten Routenkosten pro RFC 1583 zu berechnen. Deaktivieren Sie dieses Kontrollkästchen, um die zusammengefassten Routenkosten gemäß RFC 2328 zu berechnen. Um die Wahrscheinlichkeit von Routing-Schleifen zu minimieren, sollten für alle OSPF-Geräte in einer OSPF-Routing-Domäne die RFC-Kompatibilität identisch eingestellt sein. Diese Einstellung ist standardmäßig

ausgewählt.Adjacency Changes (Änderungen der Adjacency): Enthält Einstellungen, die die Adjacency-Änderungen definieren, die das Senden von Systemprotokollmeldungen verursachen.Änderungen an der Adjazenz protokollieren - Aktivieren Sie dieses Kontrollkästchen, um die Sicherheits-Appliance dazu zu veranlassen, bei jedem Ein- oder Ausschalten eines OSPF-Nachbarn eine Systemprotokollmeldung zu senden. Diese Einstellung ist standardmäßig ausgewählt.Log Adjacency Changes Detail (Änderungsdetails für Adjazenz protokollieren): Aktivieren Sie dieses Kontrollkästchen, um die Sicherheits-Appliance dazu zu veranlassen, bei jeder Statusänderung eine Systemprotokollmeldung zu senden, nicht nur beim Hochfahren oder Herunterfahren eines Nachbarn. Diese Einstellung ist standardmäßig deaktiviert.Administrative Route Distances (Administrative Route Distances) - Enthält die Einstellungen für die administrativen Entfernungen von Routen, die auf dem Routentyp basieren.Inter Area - Legt die administrative Distanz für alle Routen zwischen Bereichen fest. Gültige Werte liegen zwischen 1 und 255. Der Standardwert ist 100.Intra Area (Intra Area): Legt die administrative Distanz für alle Routen innerhalb eines Bereichs fest. Gültige Werte liegen zwischen 1 und 255. Der Standardwert ist 100.External - Legt die administrative Distanz für alle Routen von anderen Routing-Domänen fest, die durch Neuverteilung erfasst werden. Gültige Werte liegen zwischen 1 und 255. Der Standardwert ist 100.Timers (Timer): Enthält die Einstellungen, die zum Konfigurieren von LSA-Pacing- und SPF-Berechnungs-Timern verwendet werden.SPF Delay Time (SPF-Verzögerungszeit): Gibt die Zeit zwischen dem Empfang einer Topologieänderung durch OSPF und dem Beginn der SPF-Berechnung an. Gültige Werte liegen zwischen 0 und 65.535. Der Standardwert ist 5.SPF Hold Time (SPF-Haltezeit): Gibt die Haltezeit zwischen aufeinander folgenden SPF-Berechnungen an.Gültige Werte liegen zwischen 1 und 65534. Der Standardwert ist 10.LSA Group Pacing (LSA-Gruppen-Pacing): Gibt das Intervall an, in dem LSAs in einer Gruppe gesammelt und aktualisiert, überprüft oder veraltet werden. Gültige Werte liegen zwischen 10 und 1800. Der Standardwert ist 240.Default Information Originate (Standardinformationsquelle) - Enthält die Einstellungen, die ein ASBR verwendet, um eine externe Standardroute in eine OSPF-Routing-Domäne zu generieren.Enable Default Information Originate (Standardinformationsquelle aktivieren) - Aktivieren Sie dieses Kontrollkästchen, um die Generierung der Standardroute in die OSPF-Routing-Domäne zu aktivieren.Immer die Standard-Route ankündigen: Aktivieren Sie dieses Kontrollkästchen, um immer die Standard-Route anzukündigen. Diese Option ist standardmäßig deaktiviert.Metric Value (Metrischer Wert): Gibt die OSPF-Standardmetrik an. Gültige Werte liegen zwischen 0 und 16777214. Der Standardwert ist 2.Metric Type (Metrischer Typ): Gibt den externen Verbindungstyp an, der der in der OSPF-Routing-Domäne angegebenen Standardroute zugeordnet ist. Gültige Werte sind 1 oder 2, die auf eine externe Route vom Typ 1 oder Typ 2 hinweisen. Der Standardwert ist 2.Route Map - (*optional*) Der Name der anzuwendenden Route Map. Der Routing-Prozess generiert die Standardroute, wenn die Routenzuordnung eingehalten wird.

5. Nachdem Sie die vorherigen Schritte ausgeführt haben, definieren Sie die Netzwerke und Schnittstellen, die am OSPF-Routing teilnehmen, auf der Registerkarte **Setup > Area/Networks** (**Setup > Bereich/Netzwerke**), und klicken Sie dann auf **Add (Hinzufügen)**, wie in diesem Bild
gezeigt:



Das Dialogfeld OSPF-Bereich hinzufügen wird angezeigt.



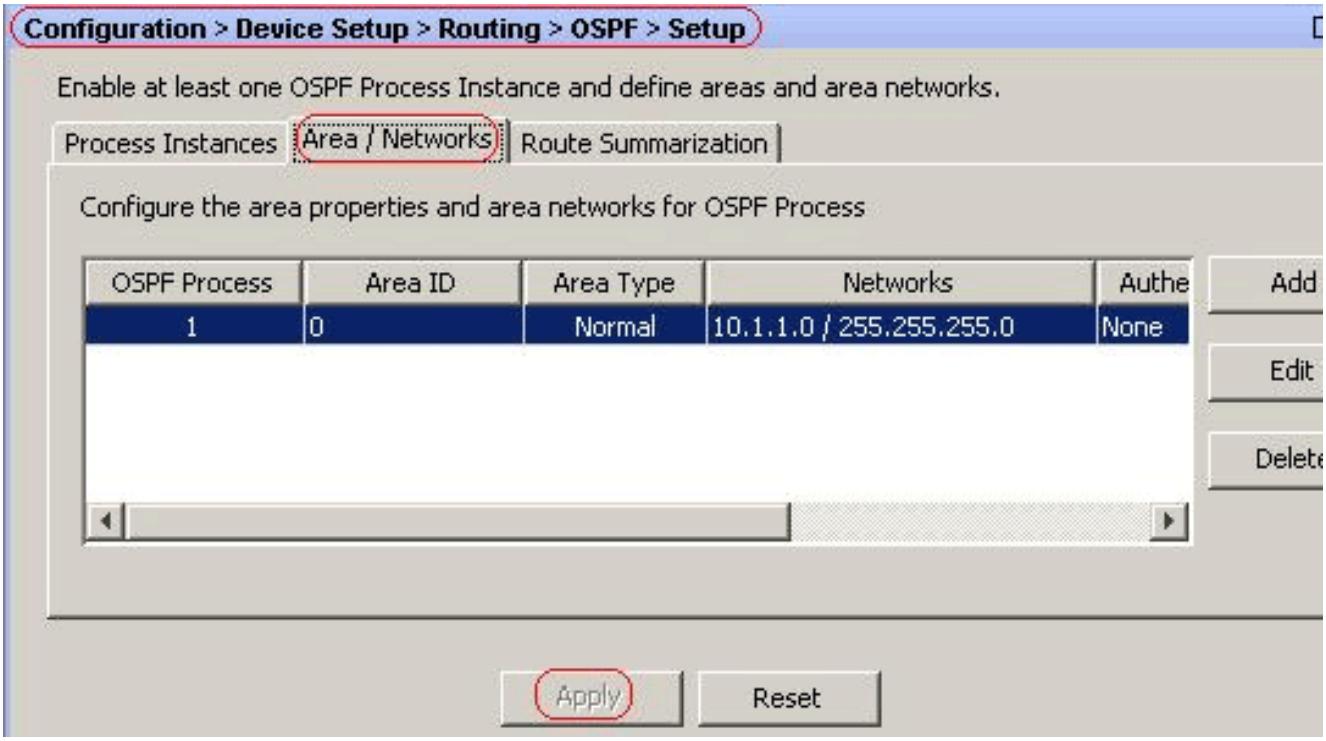
In diesem Beispiel wird nur das interne Netzwerk (10.1.1.0/24) hinzugefügt, da OSPF nur für die interne Schnittstelle aktiviert ist.**Hinweis:** Nur Schnittstellen mit einer IP-Adresse, die zu

den definierten Netzwerken gehören, sind am OSPF-Routing-Prozess beteiligt.

6. Klicken Sie auf **OK**.In dieser Liste werden die einzelnen Felder beschrieben:OSPF-Prozess - Wenn Sie einen neuen Bereich hinzufügen, wählen Sie die ID für den OSPF-Prozess aus. Wenn auf der Sicherheits-Appliance nur ein OSPF-Prozess aktiviert ist, wird dieser Prozess standardmäßig ausgewählt. Wenn Sie einen vorhandenen Bereich bearbeiten, können Sie die OSPF-Prozess-ID nicht ändern.Area ID (Area-ID): Wenn Sie einen neuen Bereich hinzufügen, geben Sie die Area-ID ein. Sie können die Bereich-ID entweder als Dezimalzahl oder als IP-Adresse angeben. Gültige Dezimalwerte liegen zwischen 0 und 4294967295. Sie können die Bereich-ID nicht ändern, wenn Sie einen vorhandenen Bereich bearbeiten.In diesem Beispiel ist die Area-ID **0**.Area Type (Bereichstyp): Enthält die Einstellungen für den zu konfigurierenden Bereichstyp.Normal (Normal) - Wählen Sie diese Option aus, um den Bereich zu einem standardmäßigen OSPF-Bereich zu machen. Diese Option ist beim ersten Erstellen eines Bereichs standardmäßig aktiviert.Stub - Wählen Sie diese Option, um aus dem Bereich einen Stub-Bereich zu machen. Stub-Bereiche haben keine Router oder Bereiche darüber hinaus. Stub-Bereiche verhindern, dass AS External LSAs (Typ 5 LSAs) in den Stub-Bereich überflutet werden. Wenn Sie einen Stub-Bereich erstellen, können Sie das Kontrollkästchen Zusammenfassung deaktivieren, um zu verhindern, dass zusammengefasste LSAs (Typ 3 und 4) in den Bereich überflutet werden.Summary (Zusammenfassung): Wenn der definierte Bereich ein Stub-Bereich ist, deaktivieren Sie dieses Kontrollkästchen, um zu verhindern, dass LSAs in den Stub-Bereich gesendet werden. Dieses Kontrollkästchen ist standardmäßig für Stub-Bereiche aktiviert.NSSA (NSSA): Wählen Sie diese Option, um den Bereich als nicht besonders stubby-Bereich zu definieren. NSSAs akzeptieren Typ-7-LSAs. Wenn Sie ein NSSA erstellen, können Sie das Kontrollkästchen Übersicht deaktivieren, um zu verhindern, dass zusammengefasste LSAs in den Bereich überflutet werden. Darüber hinaus können Sie das Kontrollkästchen Redistribution (Neuverteilung) deaktivieren und Default Information Originate aktivieren, um die Neuverteilung der Route zu deaktivieren.Redistribute (Neuverteilung): Deaktivieren Sie dieses Kontrollkästchen, um zu verhindern, dass Routen in den NSSA importiert werden. Dieses Kontrollkästchen ist standardmäßig aktiviert.Summary (Zusammenfassung): Wenn es sich bei dem definierten Bereich um einen NSSA handelt, deaktivieren Sie dieses Kontrollkästchen, um zu verhindern, dass LSAs in den Stub-Bereich gesendet werden. Dieses Kontrollkästchen ist standardmäßig für NSSAs aktiviert.Default Information Originate (Standardinformationsquelle) - Aktivieren Sie dieses Kontrollkästchen, um einen Standard vom Typ 7 im NSSA zu generieren. Dieses Kontrollkästchen ist standardmäßig deaktiviert.Metric Value (Metrischer Wert): Geben Sie einen Wert ein, um den OSPF-Metrikwert für die Standardroute anzugeben. Gültige Werte liegen zwischen 0 und 16777214. Der Standardwert ist 2.Metric Type (Metrischer Typ): Wählen Sie einen Wert aus, um den metrischen OSPF-Typ für die Standardroute anzugeben. Sie können zwischen 1 (Typ 1) und 2 (Typ 2) wählen. Der Standardwert ist 2.Area Networks (Bereichsnetzwerke): Enthält die Einstellungen, die einen OSPF-Bereich definieren.Enter IP Address and Mask (IP-Adresse und -Maske eingeben): Enthält die Einstellungen, die zum Definieren der Netzwerke im Bereich verwendet werden.IP Address (IP-Adresse): Geben Sie die IP-Adresse des Netzwerks oder Hosts ein, der dem Bereich hinzugefügt werden soll. Verwenden Sie 0.0.0.0 mit der Netzmaske 0.0.0.0, um den Standardbereich zu erstellen. Sie können 0.0.0.0 nur in einem Bereich verwenden.Netzmaske - Wählen Sie die Netzwerkmaske für die IP-Adresse oder den Host aus, die dem Bereich hinzugefügt werden soll. Wenn Sie einen Host hinzufügen, wählen Sie die Maske 255.255.255.255 aus.In diesem Beispiel ist das zu konfigurierende Netzwerk **10.1.1.0/24**.Add (Hinzufügen): Fügt dem

Bereich das Netzwerk hinzu, das im Bereich "Enter IP Address" (IP-Adresse eingeben) und "Mask" (Maske) definiert ist. Das hinzugefügte Netzwerk wird in der Tabelle Area Networks (Bereichsnetzwerke) angezeigt.Delete (Löschen): Löscht das ausgewählte Netzwerk aus der Tabelle Area Networks (Bereichsnetzwerke).Area Networks (Bereichsnetzwerke): Zeigt die für den Bereich definierten Netzwerke an.IP Address (IP-Adresse): Zeigt die IP-Adresse des Netzwerks an.Netmask (Netzmaske): Zeigt die Netzwerkmaske für das Netzwerk an.Authentication (Authentifizierung) - Enthält die Einstellungen für die OSPF-Bereichsauthentifizierung.None (Keine): Wählen Sie diese Option aus, um die OSPF-Bereichsauthentifizierung zu deaktivieren. Dies ist die Standardeinstellung.Password (Kennwort): Wählen Sie diese Option aus, um ein Klartext-Kennwort für die Bereichsauthentifizierung zu verwenden. Diese Option wird nicht empfohlen, wenn die Sicherheit ein Anliegen ist.MD5: Wählen Sie diese Option aus, um die MD5-Authentifizierung zu verwenden.Default Cost (Standardkosten): Geben Sie die Standardkosten für den Bereich an. Gültige Werte liegen zwischen 0 und 65.535. Der Standardwert ist 2.

7. Klicken Sie auf **Übernehmen**.



8. Optional können Sie im Bereich Filterregeln Weiterleitungsfilter definieren. Die Routenfilterung bietet mehr Kontrolle über die Routen, die in OSPF-Updates gesendet oder empfangen werden dürfen.
9. Optional können Sie die Routen-Neuverteilung konfigurieren. Die Cisco ASA kann die von RIP und EIGRP erkannten Routen über den OSPF-Routing-Prozess neu verteilen. Sie können statische und verbundene Routen auch über den OSPF-Routing-Prozess neu verteilen. Definieren Sie die Neuverteilung von Routen im Bereich "Neuverteilung".
10. OSPF-Hello-Pakete werden als Multicast-Pakete gesendet. Wenn sich ein OSPF-Nachbar in einem Nicht-Broadcast-Netzwerk befindet, müssen Sie diesen Nachbar manuell definieren. Wenn Sie einen OSPF-Nachbarn manuell definieren, werden Hello-Pakete als Unicast-Nachrichten an diesen Nachbarn gesendet. Um statische OSPF-Nachbarn zu definieren, gehen Sie zum Bereich Static Neighbor (Statischer Nachbar).
11. Routen, die von anderen Routing-Protokollen gelernt wurden, können zusammengefasst werden. Die Kennzahl für die Anzeige der Zusammenfassung ist die kleinste Kennzahl aller

spezifischeren Routen. Zusammenfassende Routen tragen dazu bei, die Größe der Routing-Tabelle zu reduzieren.Die Verwendung von zusammengefassten Routen für OSPF veranlasst einen OSPF-ASBR, eine externe Route als Aggregat für alle neu verteilten Routen anzukündigen, die von der Adresse abgedeckt werden. Nur Routen von anderen Routing-Protokollen, die in OSPF neu verteilt werden, können zusammengefasst werden.

12. Im Bereich "Virtuelle Verbindung" können Sie einem OSPF-Netzwerk einen Bereich hinzufügen. Es ist nicht möglich, den Bereich direkt mit dem Backbone-Bereich zu verbinden. müssen Sie einen virtuellen Link erstellen. Eine virtuelle Verbindung verbindet zwei OSPF-Geräte mit einem gemeinsamen Bereich, dem so genannten Transit Area. Eines der OSPF-Geräte muss mit dem Backbone-Bereich verbunden werden.

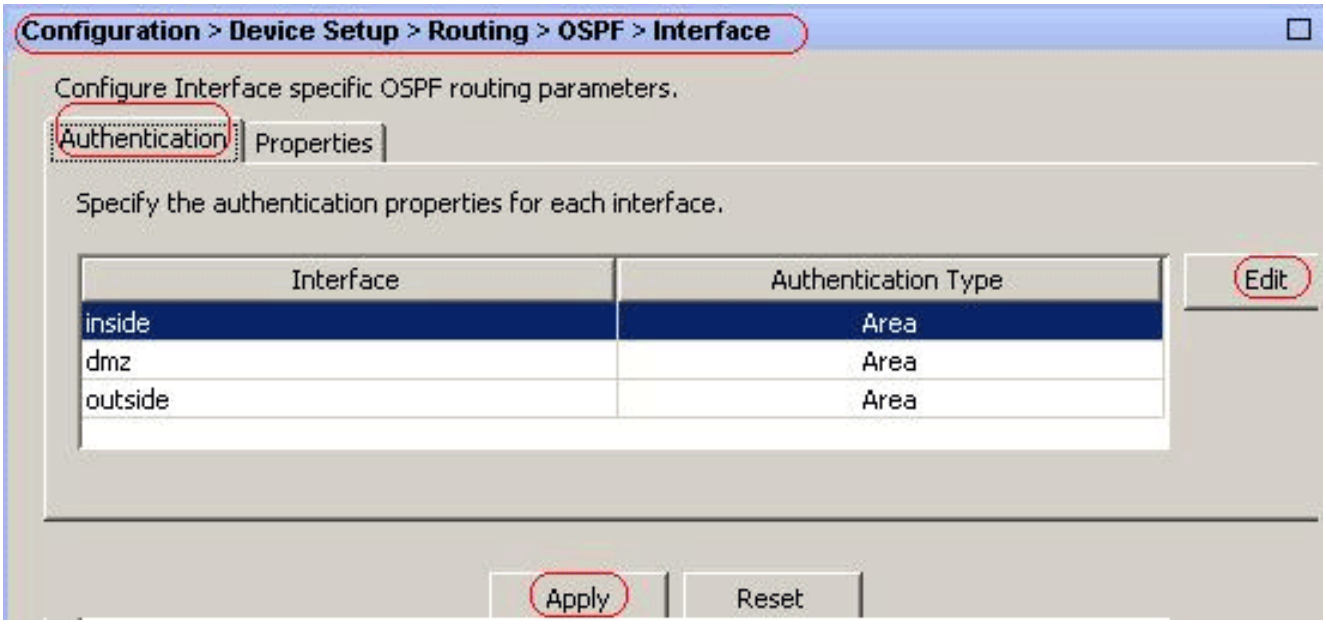
Konfigurieren der OSPF-Authentifizierung

Die Cisco ASA unterstützt die MD5-Authentifizierung von Routing-Updates über das OSPF-Routing-Protokoll. Der MD5-verschlüsselte Digest in jedem OSPF-Paket verhindert die Einführung von nicht autorisierten oder falschen Routing-Nachrichten aus nicht genehmigten Quellen. Durch das Hinzufügen einer Authentifizierung zu Ihren OSPF-Nachrichten wird sichergestellt, dass Ihre Router und die Cisco ASA nur Routing-Nachrichten von anderen Routing-Geräten akzeptieren, die mit demselben vorinstallierten Schlüssel konfiguriert sind. Wenn diese Authentifizierung nicht konfiguriert ist und jemand ein anderes Routing-Gerät mit anderen oder gegenteiligen Routing-Informationen in das Netzwerk einführt, können die Routing-Tabellen auf Ihren Routern oder der Cisco ASA beschädigt werden, und es kann zu einem Denial-of-Service-Angriff kommen. Wenn Sie den EIGRP-Nachrichten, die zwischen den Routing-Geräten gesendet werden (einschließlich der ASA), Authentifizierung hinzufügen, wird das gezielte oder versehentliche Hinzufügen eines anderen Routers zum Netzwerk und jedes Problem verhindert.

Die OSPF-Routenauthentifizierung wird auf Schnittstellenbasis konfiguriert. Alle OSPF-Nachbarn auf für die OSPF-Nachrichtenauthentifizierung konfigurierten Schnittstellen müssen mit demselben Authentifizierungsmodus und Schlüssel konfiguriert werden, damit Nachbarschaften eingerichtet werden können.

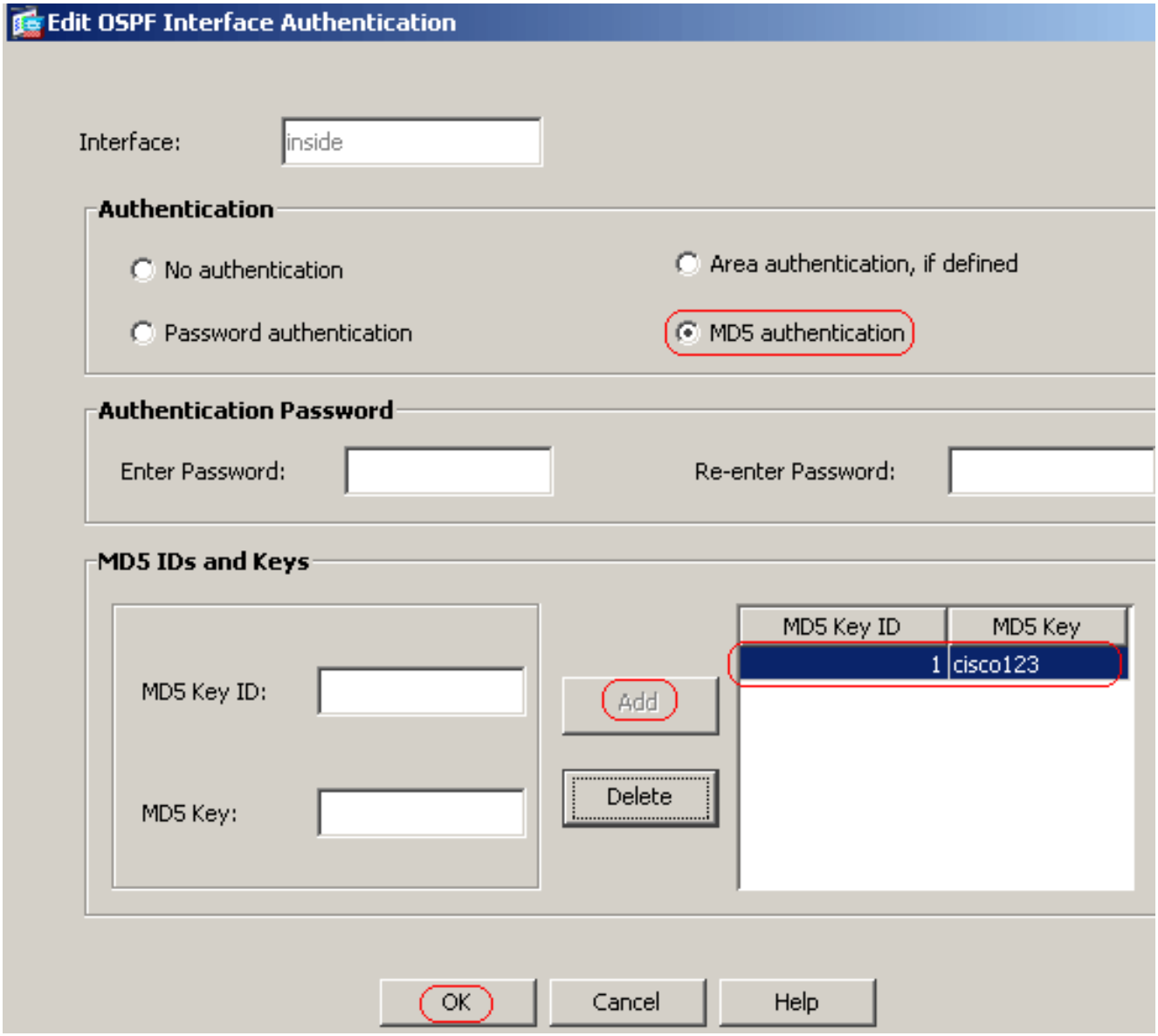
Gehen Sie wie folgt vor, um die OSPF MD5-Authentifizierung auf der Cisco ASA zu aktivieren:

1. Navigieren Sie im ASDM zu **Configuration > Device Setup > Routing > OSPF > Interface**, und klicken Sie dann auf die **Authentication (Authentifizierung)** Registerkarte, wie in diesem Bild
gezeigt.

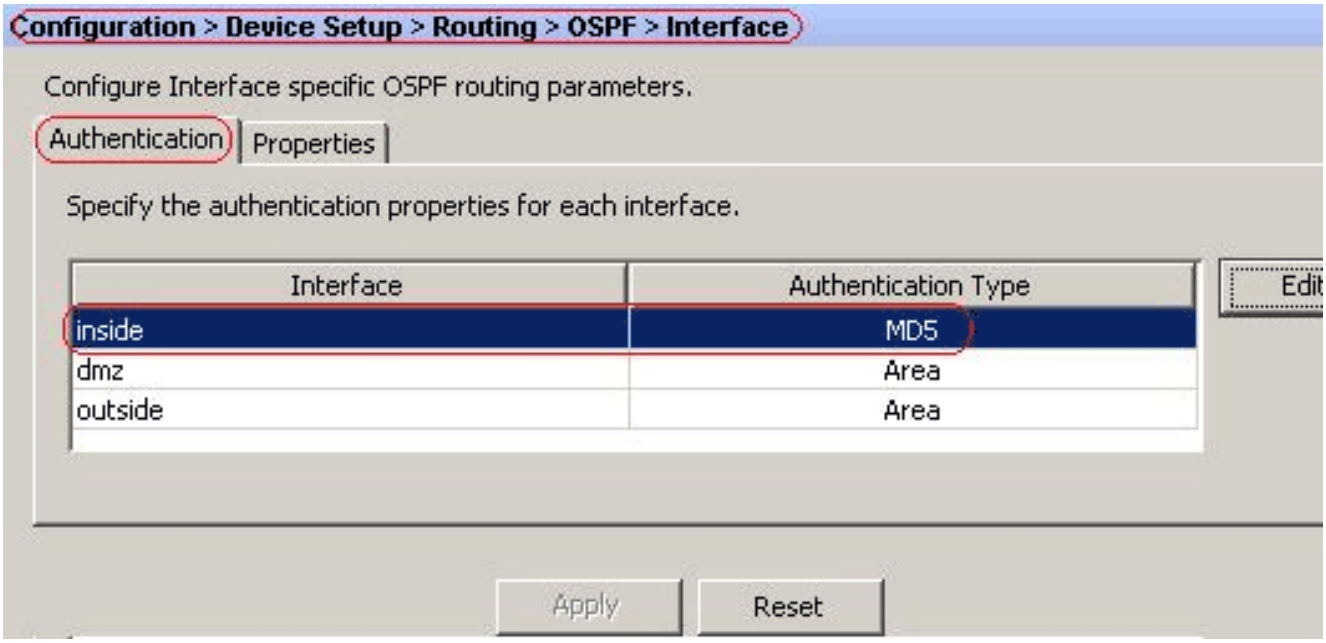


In diesem Fall ist OSPF auf der internen Schnittstelle aktiviert.

2. Wählen Sie die **interne** Schnittstelle aus, und klicken Sie auf **Bearbeiten**.
3. Wählen Sie unter Authentication (Authentifizierung) die Option **MD5-Authentifizierung aus**, und fügen Sie hier weitere Informationen zu Authentifizierungsparametern hinzu.In diesem Fall ist der vorinstallierte Schlüssel **cisco123** und die Schlüssel-ID **1**.



4. Klicken Sie auf **OK** und dann auf **Übernehmen**.



Cisco ASA CLI-Konfiguration

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#
```

CLI-Konfiguration des Cisco IOS Routers (R2)

Cisco IOS-Router (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
```

CLI-Konfiguration des Cisco IOS Routers (R1)

Cisco IOS-Router (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
```

CLI-Konfiguration des Cisco IOS Routers (R3)

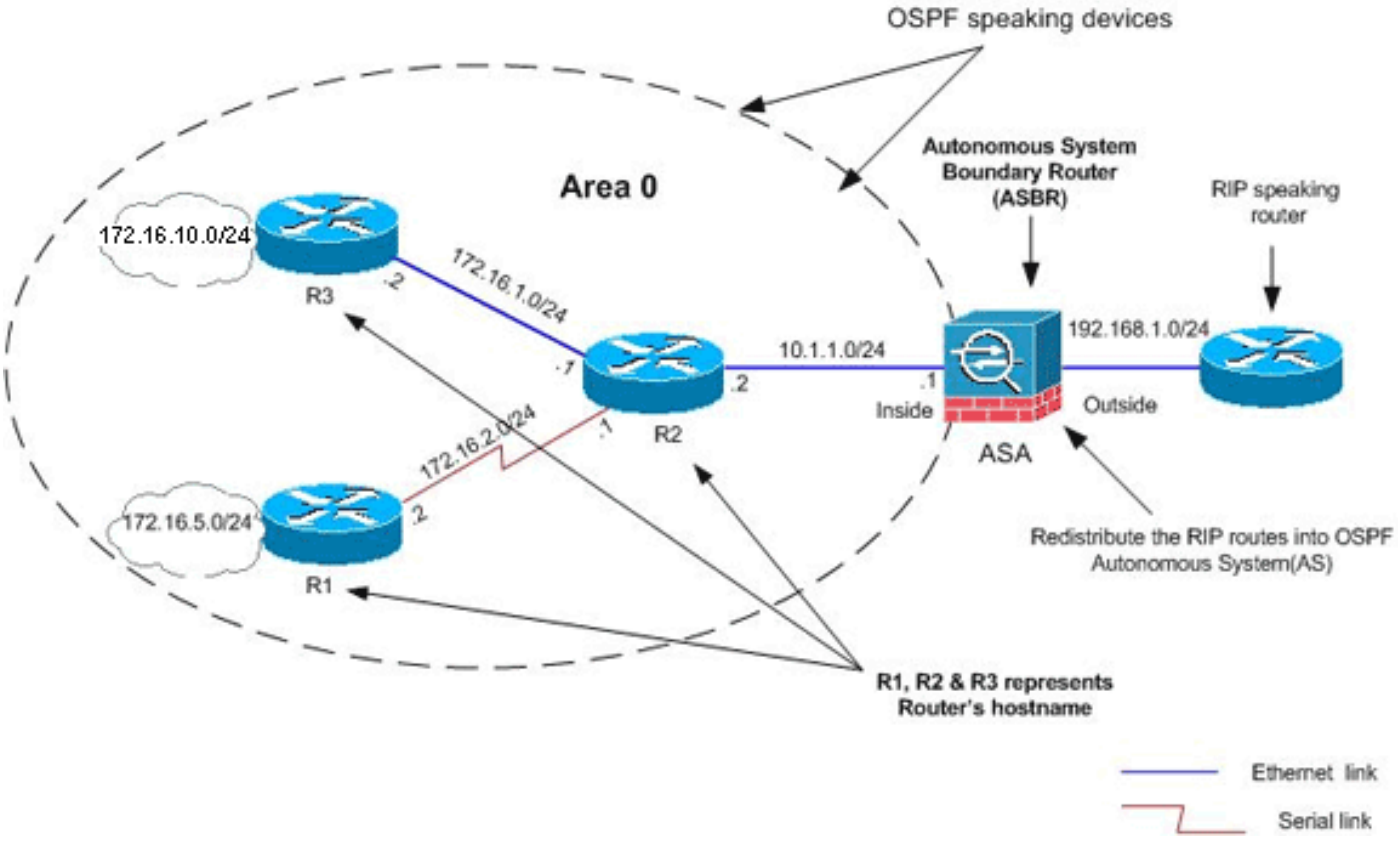
Cisco IOS-Router (R3)

```
!--- 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
```

Neuverteilung in OSPF mit ASA

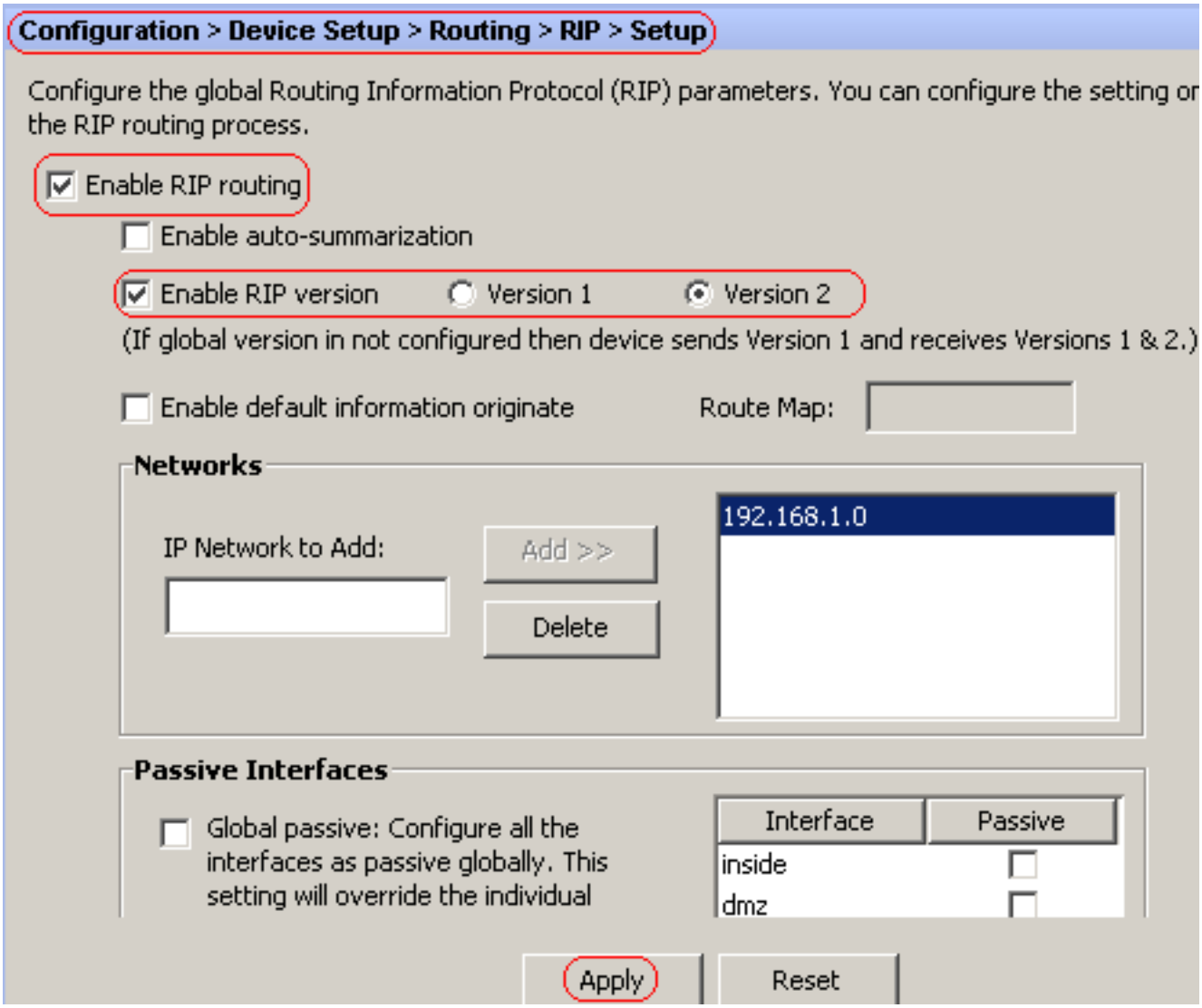
Wie bereits erwähnt, können Sie Routen über einen anderen OSPF-Routing-Prozess, einen RIP-Routing-Prozess oder über statische und verbundene Routen, die auf OSPF-fähigen Schnittstellen konfiguriert sind, in einen OSPF-Routing-Prozess neu verteilen.

In diesem Beispiel wird die Neuverteilung der RIP-Routen in OSPF mit dem Netzwerkdiagramm wie folgt beschrieben:

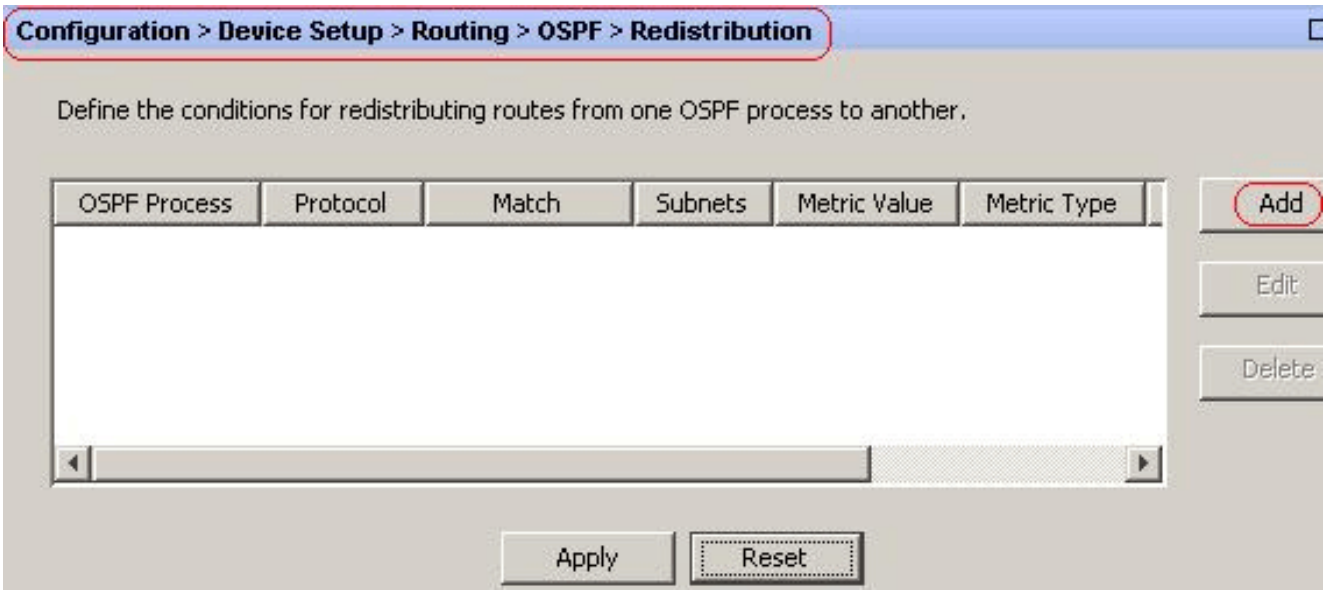


ASDM-Konfiguration

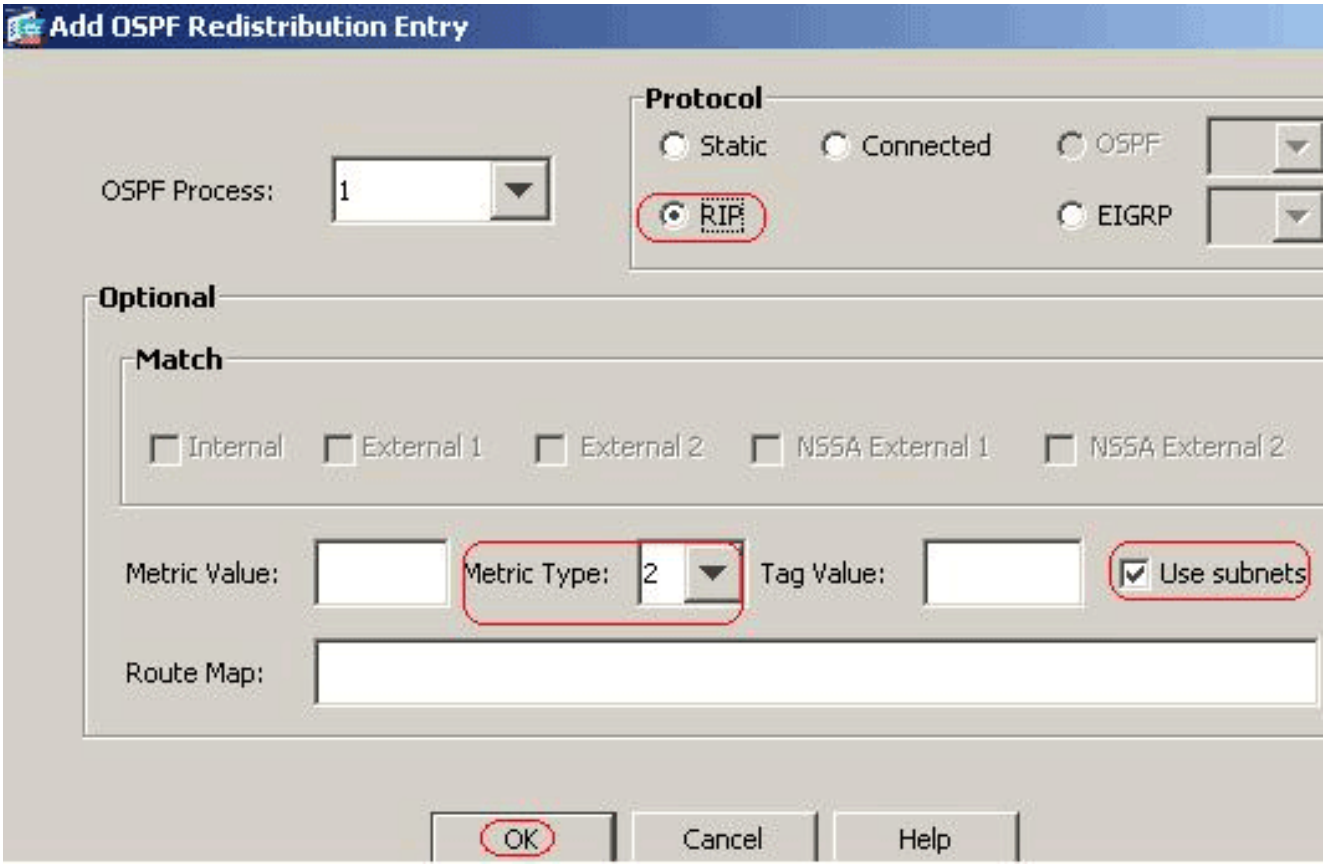
1. Wählen Sie **Configuration > Device Setup > Routing > RIP > Setup**, um RIP zu aktivieren, und fügen Sie das Netzwerk 192.168.1.0 hinzu, wie in diesem Bild gezeigt.



2. Klicken Sie auf **Übernehmen**.
3. Wählen Sie **Configuration > Device Setup > Routing > OSPF > Redistribution > Add (Konfiguration > Geräte-Setup > Routing > OSPF > Umverteilung > Hinzufügen** aus, um RIP-Routen in OSPF umzuverteilen.



4. Klicken Sie auf **OK** und dann auf **Übernehmen**.



Entsprechende CLI-Konfiguration

CLI-Konfiguration der ASA zur Neuverteilung von 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

Sie sehen die Routing-Tabelle des benachbarten IOS-Routers (R2) nach der Neuverteilung von RIP-Routen in OSPF AS.

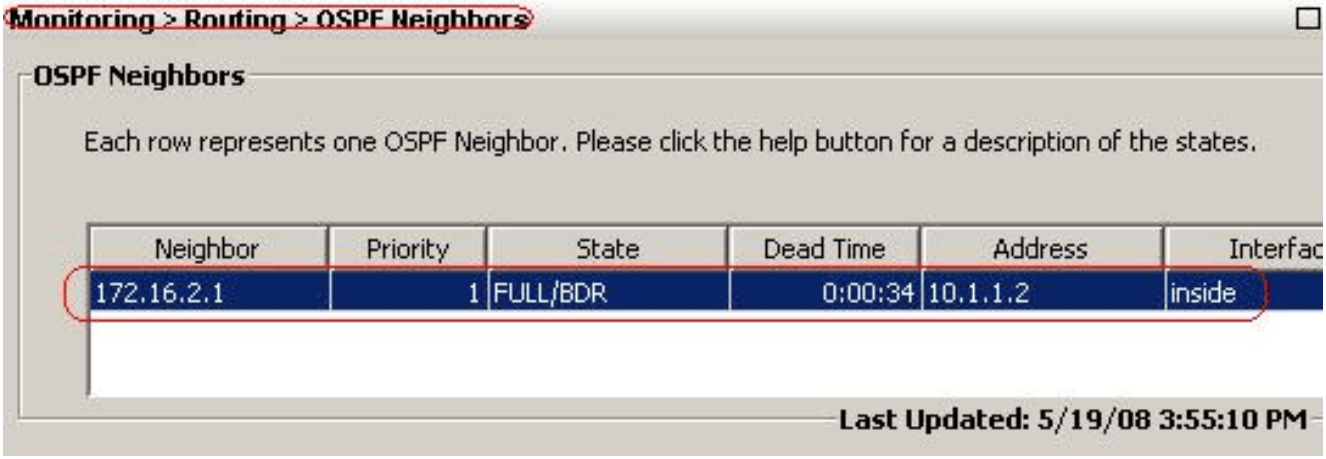
```
R2#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       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 adverstied by Cisco ASA
```

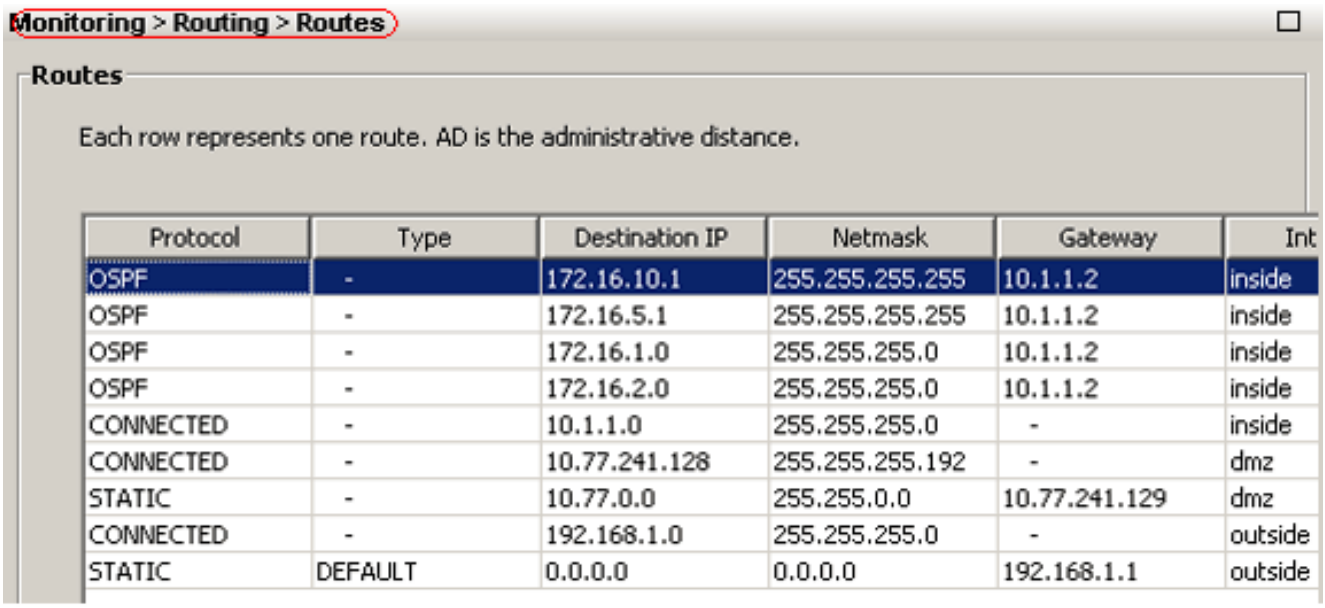
Überprüfen

Gehen Sie wie folgt vor, um Ihre Konfiguration zu überprüfen:

1. Auf dem ASDM können Sie zu **Monitoring > Routing > OSPF Neighbors** navigieren, um die einzelnen OSPF-Nachbarn anzuzeigen. Dieses Bild zeigt den internen Router (R2) als aktiven Nachbarn. Sie können auch die Schnittstelle sehen, auf der sich dieser Nachbar befindet, die Nachbarrouter-ID, den Status und die Ausfallzeit.



2. Darüber hinaus können Sie die Routing-Tabelle überprüfen, wenn Sie zu **Monitoring > Routing > Routes** navigieren. In diesem Bild werden die Netzwerke 172.16.1.0/24, 172.16.2.0/24, 172.16.5.0/24 und 172.16.10.0/24 durch R2 (10.1.1.2) erfasst.



3. In der CLI können Sie den Befehl **show route** verwenden, um dieselbe Ausgabe zu erhalten.

```
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. Sie können auch den Befehl **show ospf database** verwenden, um Informationen über die erlernten Netzwerke und die OSPF-Topologie abzurufen.

```
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. Der Befehl **show ospf neighbors** ist ebenfalls hilfreich, um die aktiven Nachbarn und die entsprechenden Informationen zu überprüfen. Dieses Beispiel zeigt die gleichen Informationen, die Sie von ASDM in Schritt 1 erhalten haben.

```
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
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die die Behebung von OSPF-Problemen erleichtern können.

Statische Nachbarkonfiguration für ein Point-to-Point-Netzwerk

Wenn Sie *OSPF-Netzwerk-Point-to-Point-Non-Broadcast* auf der ASA konfiguriert haben, müssen Sie statische OSPF-Nachbarn definieren, um OSPF-Routen über ein Point-to-Point-Nicht-Broadcast-Netzwerk anzukündigen. Weitere Informationen finden Sie unter Definieren statischer OSPF-Nachbarn.

Befehle zur Fehlerbehebung

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

Hinweis: Beachten Sie vor der Verwendung von **Debug-**Befehlen die Informationen zu Debug-Befehlen.

- **debug ospf events**: Aktiviert das Debuggen von OSPF-Ereignissen.

```
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: Send with youngest Key 1
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: 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
```

Hinweis: Weitere Informationen zu verschiedenen Befehlen, die zur Behebung des Problems nützlich sind, finden Sie im Abschnitt debug ospf der Cisco Security Appliance Command Reference, Version 8.0.

Zugehörige Informationen

- Support-Seite für Cisco Adaptive Security Appliances der Serie 5500
- Support-Seite für Cisco PIX der Serie 500
- PIX/ASA 8.X: Konfigurieren von EIGRP auf der Cisco Adaptive Security Appliance (ASA)
- Technischer Support und Dokumentation - Cisco Systems