ASA 9.x EIGRP-Konfigurationsbeispiel

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die Cisco Adaptive Security Appliance (ASA) konfigurieren, um Routen durch das Enhanced Interior Gateway Routing Protocol (EIGRP) zu erlernen, das von der ASA Software Version 9.x und höher unterstützt wird, und um eine Authentifizierung durchzuführen.

Voraussetzungen

Anforderungen

Cisco verlangt, dass Sie diese Bedingungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Cisco ASA muss Version 9.x oder höher ausführen.
- EIGRP muss sich im Single-Context-Modus befinden, da es im Multi-Context-Modus nicht unterstützt wird.

Verwendete Komponenten

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

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

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.

Hintergrundinformationen

Richtlinien und Einschränkungen

- Eine EIGRP-Instanz wird im Einzelmodus und pro Kontext im Multimodus unterstützt.
- Zwei Threads werden pro Kontext pro EIGRP-Instanz im Multimode erstellt und können mit dem Anzeigeprozess angezeigt werden.
- Die automatische Zusammenfassung ist standardmäßig deaktiviert.
- Im individuellen Schnittstellenmodus wird zwischen den Cluster-Einheiten keine Nachbarbeziehung hergestellt.
- Die Standardinformationen in [<acl>] werden verwendet, um das Exterior-Bit in eingehenden Standard-Routen zu filtern.
- Default-information out [<acl>] wird verwendet, um das Exterior-Bit in ausgehenden, standardmäßigen Standardrouten von Kandidaten zu filtern.

EIGRP und Failover

Cisco ASA Code Version 8.4.4.1 und höher synchronisiert dynamische Routen von der AKTIVEN Einheit zur STANDBY-Einheit. Darüber hinaus wird das Löschen von Routen auch mit der STANDBY-Einheit synchronisiert. Der Zustand der Peer-Adjacencies wird jedoch nicht synchronisiert. Nur das ACTIVE-Gerät behält den Nachbarstatus bei und beteiligt sich aktiv am dynamischen Routing. Siehe ASA FAQ: Was geschieht nach dem Failover, wenn dynamische Routen synchronisiert werden? für weitere Informationen.

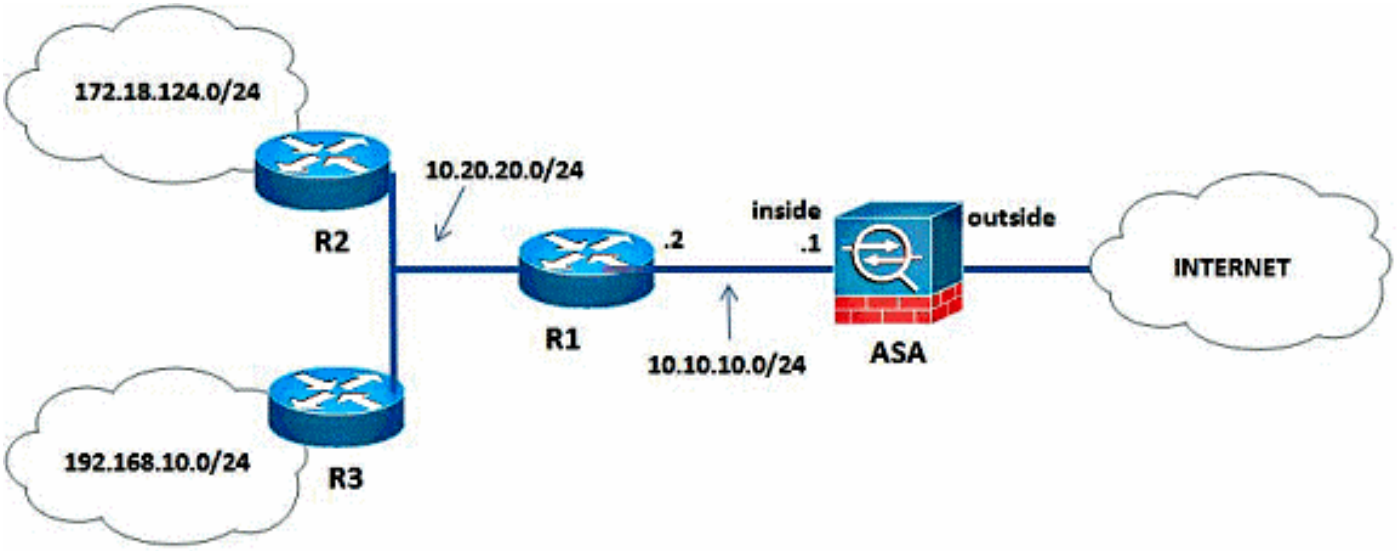
Konfigurieren

In diesem Abschnitt wird beschrieben, wie Sie die in diesem Dokument behandelten Funktionen konfigurieren.

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 der abgebildeten Netzwerktopologie lautet die IP-Adresse der Cisco ASA-internen Schnittstelle 10.10.10.1/24. Ziel ist es, EIGRP auf der Cisco ASA zu konfigurieren, um über den benachbarten Router (R1) dynamisch Routen zu den internen Netzwerken (10.20.20.0/24, 172.18.124.0/24 und 192.168.10.0/24) zu erfassen. R1 erfasst die Routen zu internen Remote-Netzwerken über die anderen beiden Router (R2 und R3).

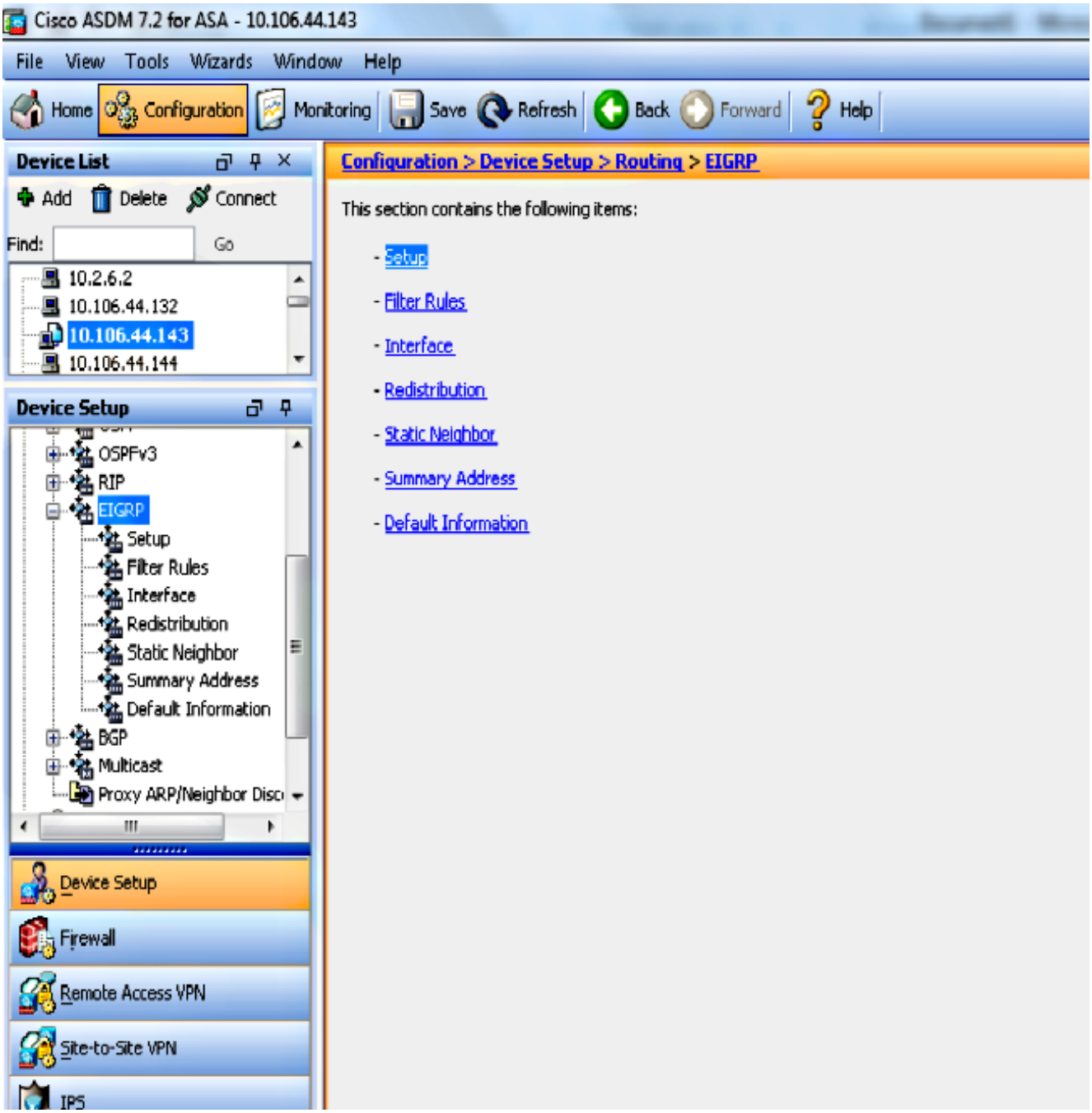
ASDM-Konfiguration

ASDM ist eine browserbasierte Anwendung zur Konfiguration und Überwachung der Software auf Security Appliances. ASDM wird von der Sicherheits-Appliance geladen und anschließend zur Konfiguration, Überwachung und Verwaltung des Geräts verwendet. Sie können auch den ASDM Launcher 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.

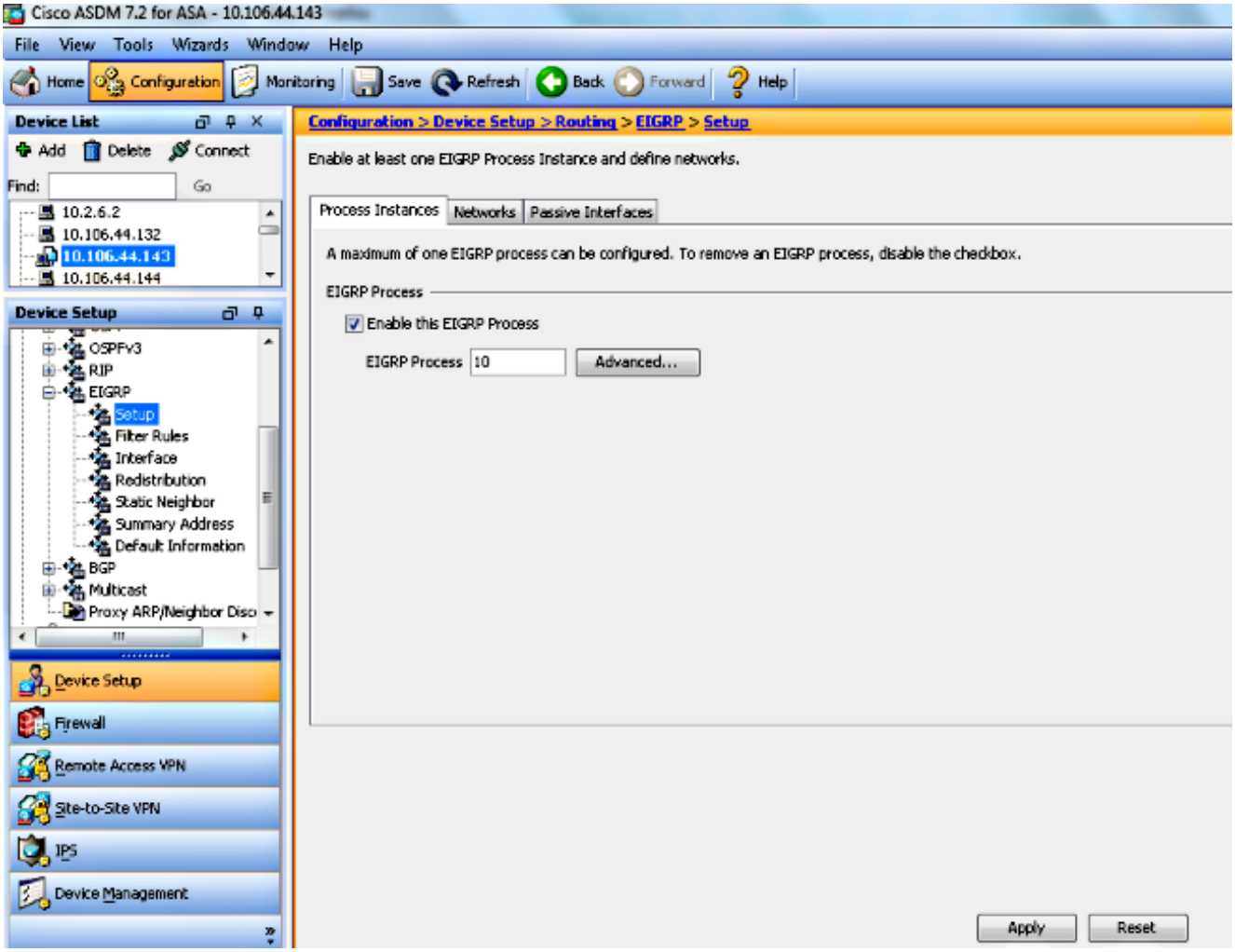
Führen Sie diese Schritte aus, um EIGRP in der Cisco ASA zu konfigurieren.

1. Melden Sie sich mit dem ASDM bei der Cisco ASA an.

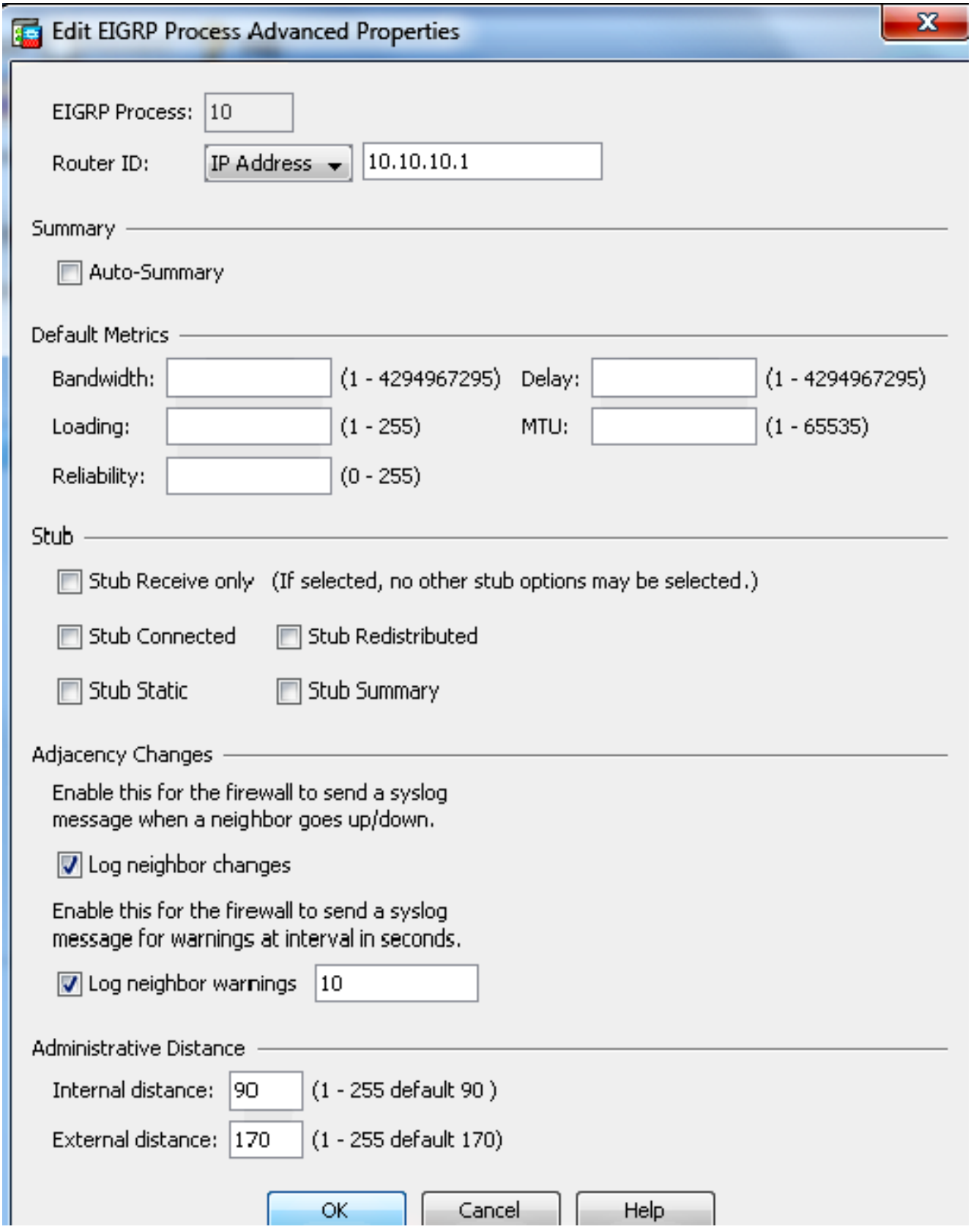
2. Navigieren Sie zum Bereich **Configuration > Device Setup > Routing > EIGRP** der ASDM-Schnittstelle, wie in diesem Screenshot gezeigt.



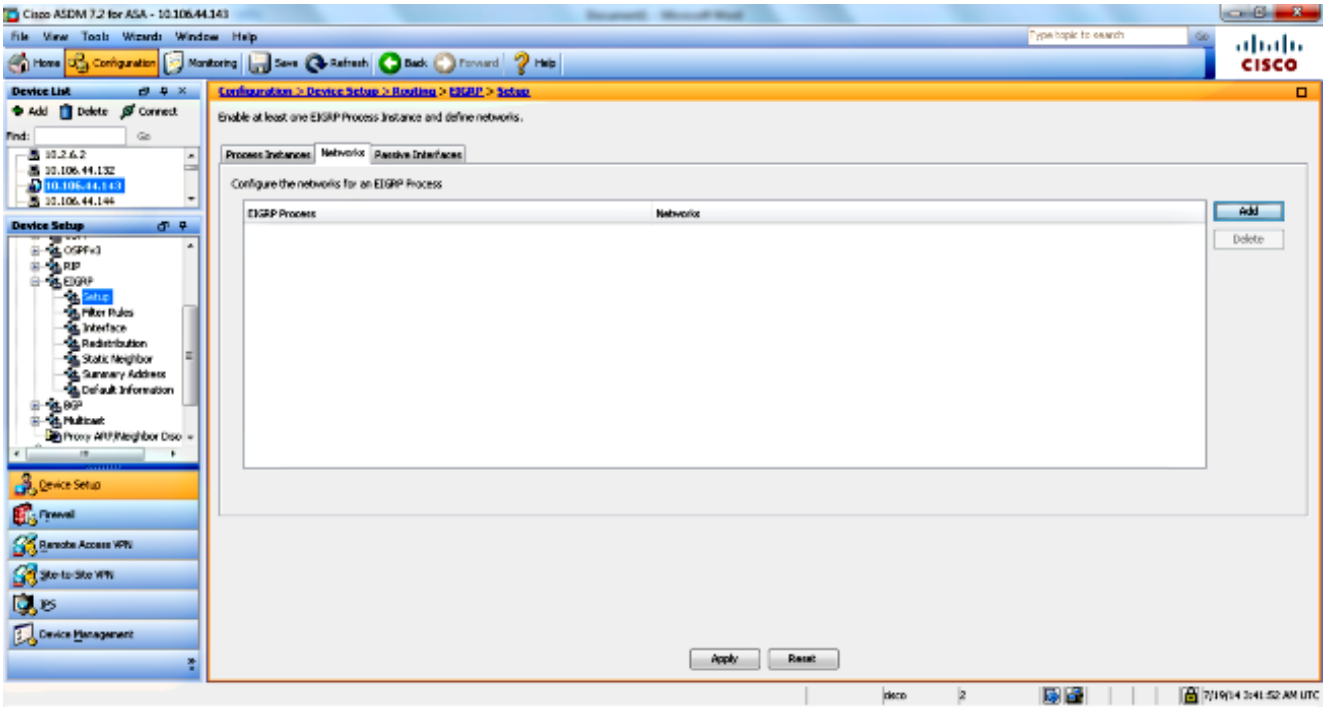
3. Aktivieren Sie den EIGRP-Routing-Prozess auf der Registerkarte **Setup > Process Instances** (**Setup > Process Instanzen**), wie in diesem Screenshot gezeigt. In diesem Beispiel ist der EIGRP-Prozess **10**.



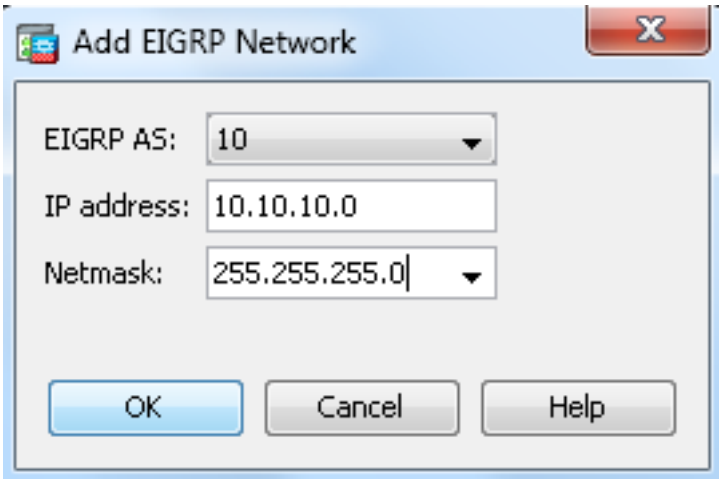
4. Sie können optionale erweiterte EIGRP-Routing-Prozessparameter konfigurieren. Klicken Sie auf der Registerkarte **Setup > Process Instances (Setup > Prozessinstanzen)** auf **Erweitert**. Sie können den EIGRP-Routing-Prozess als Stub-Routing-Prozess konfigurieren, die automatische Routenzusammenfassung deaktivieren, die Standardmetriken für neu verteilte Routen definieren, die administrativen Distanzen für interne und externe EIGRP-Routen ändern, eine statische Router-ID konfigurieren und die Protokollierung von Adjacency-Änderungen aktivieren oder deaktivieren. In diesem Beispiel wird die EIGRP-Router-ID statisch mit der IP-Adresse der internen Schnittstelle (10.10.10.1) konfiguriert. Zusätzlich ist **die automatische Zusammenfassung** ebenfalls deaktiviert. Alle anderen Optionen sind mit ihren Standardwerten konfiguriert.



5. Nachdem Sie die vorherigen Schritte ausgeführt haben, definieren Sie auf der Registerkarte **Setup > Networks (Setup > Netzwerke)** die Netzwerke und Schnittstellen, die am EIGRP-Routing teilnehmen. Klicken Sie auf **Hinzufügen**, wie in diesem Screenshot gezeigt.



6. Dieser Bildschirm wird angezeigt. In diesem Beispiel wird nur das interne Netzwerk (10.10.10.0/24) hinzugefügt, da EIGRP nur für die interne Schnittstelle aktiviert ist.



Nur Schnittstellen mit einer IP-Adresse, die zu den definierten Netzwerken gehört, nehmen am EIGRP-Routing-Prozess teil. Wenn Sie eine Schnittstelle haben, die Sie nicht am EIGRP-Routing teilnehmen möchten, die aber an ein Netzwerk angeschlossen ist, das Sie weitergeben möchten, konfigurieren Sie einen Netzwerkeintrag auf der Registerkarte **Setup > Networks** (**Setup > Netzwerke**), der das Netzwerk abdeckt, an das die Schnittstelle angeschlossen ist, und konfigurieren Sie diese Schnittstelle dann als passive Schnittstelle, sodass die Schnittstelle keine EIGRP-Updates senden oder empfangen kann.

Hinweis: Als passiv konfigurierte Schnittstellen senden oder empfangen keine EIGRP-Updates.

7. Sie können optional im Bereich Filterregeln Routenfilter definieren. Die Routenfilterung bietet mehr Kontrolle über die Routen, die in EIGRP-Updates gesendet oder empfangen werden dürfen.

8. Optional können Sie die Routen-Neuverteilung konfigurieren. Die Cisco ASA kann die durch Routing Information Protocol (RIP) und Open Shortest Path First (OSPF) erkannten Routen über den EIGRP-Routing-Prozess neu verteilen. Sie können statische und verbundene Routen auch über den EIGRP-Routing-Prozess neu verteilen. Statische oder verbundene Routen müssen nicht neu verteilt werden, wenn sie im Bereich eines auf der Registerkarte **Setup > Networks** konfigurierten Netzwerks liegen. Definieren Sie die Neuverteilung von Routen im Bereich "Neuverteilung".

9. EIGRP-Hello-Pakete werden als Multicast-Pakete gesendet. Wenn sich ein EIGRP-Nachbar in einem Nicht-Broadcast-Netzwerk befindet, müssen Sie diesen Nachbar manuell definieren. Wenn Sie einen EIGRP-Nachbarn manuell definieren, werden Hello-Pakete als Unicast-Nachrichten an diesen Nachbarn gesendet. Um statische EIGRP-Nachbarn zu definieren, gehen Sie zum Fenster **Static Neighbor** (Statischer Nachbar).

10. Standardmäßig werden Standardrouten gesendet und akzeptiert. Um das Senden und Empfangen von Standard-Routeninformationen zu beschränken oder zu deaktivieren, öffnen Sie den Bereich **Configuration > Device Setup > Routing > EIGRP > Default Information (Konfiguration > Geräteeinrichtung > Routing > EIGRP > Standardinformationen**). Im Bereich "Standardinformationen" wird eine Regeltabelle angezeigt, die das Senden und Empfangen von Standard-Routeninformationen in EIGRP-Updates steuert.

    Hinweis: Sie können für jeden EIGRP-Routing-Prozess eine "*in*"- und eine "*out*"-Regel verwenden. (Derzeit wird nur ein Prozess unterstützt.)

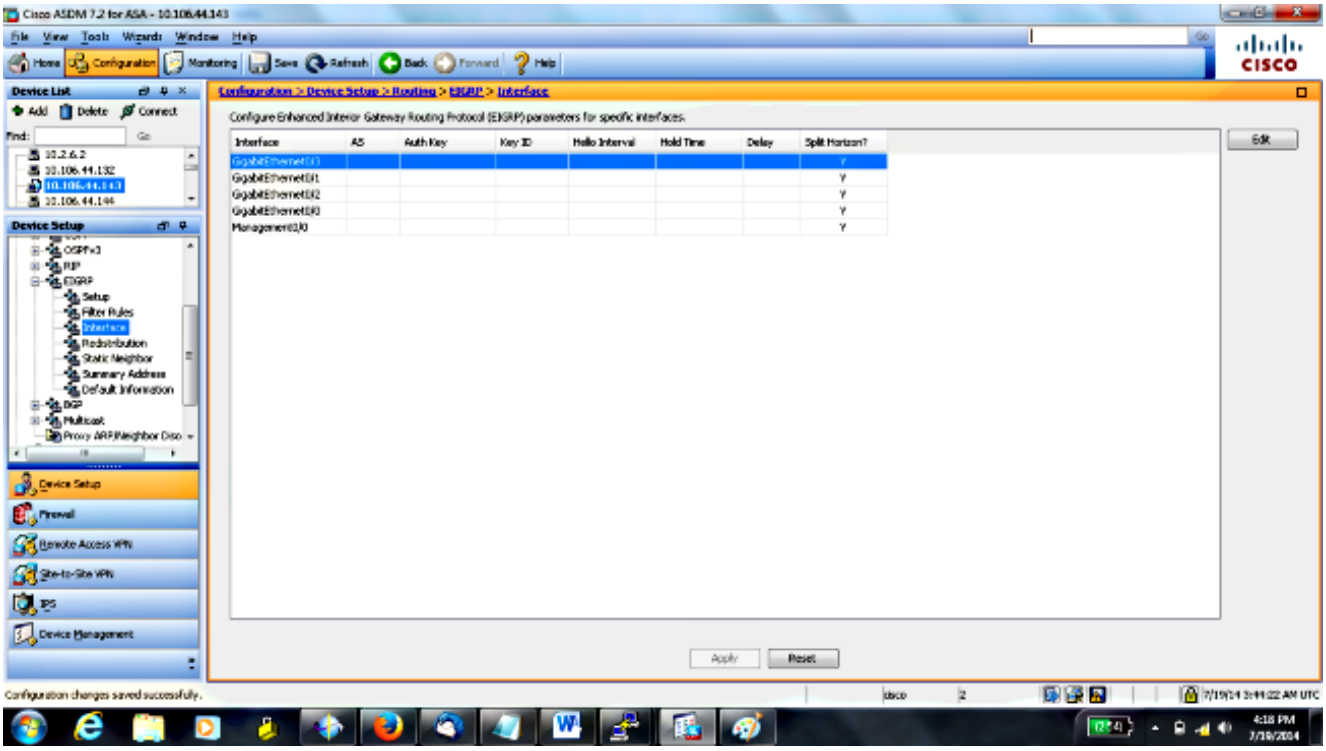
Konfigurieren der EIGRP-Authentifizierung

Die Cisco ASA unterstützt die MD5-Authentifizierung von Routing-Updates über das EIGRP-Routing-Protokoll. Der MD5-verschlüsselte Digest in jedem EIGRP-Paket verhindert die Einführung von nicht autorisierten oder falschen Routing-Nachrichten aus nicht genehmigten Quellen. Durch das Hinzufügen einer Authentifizierung zu Ihren EIGRP-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 keine solche Authentifizierung konfiguriert ist und jemand ein anderes Routing-Gerät mit anderen oder gegenteiligen Routing-Informationen zum Netzwerk einführt, können die Routing-Tabellen auf Ihren Routern oder der Cisco ASA beschädigt werden und ein Denial-of-Service-Angriff durchgeführt werden. Wenn Sie den EIGRP-Nachrichten, die zwischen Ihren Routing-Geräten gesendet werden (einschließlich der ASA), Authentifizierung hinzufügen, werden nicht autorisierte Ergänzungen von EIGRP-Routern in Ihrer Routing-Topologie verhindert.

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

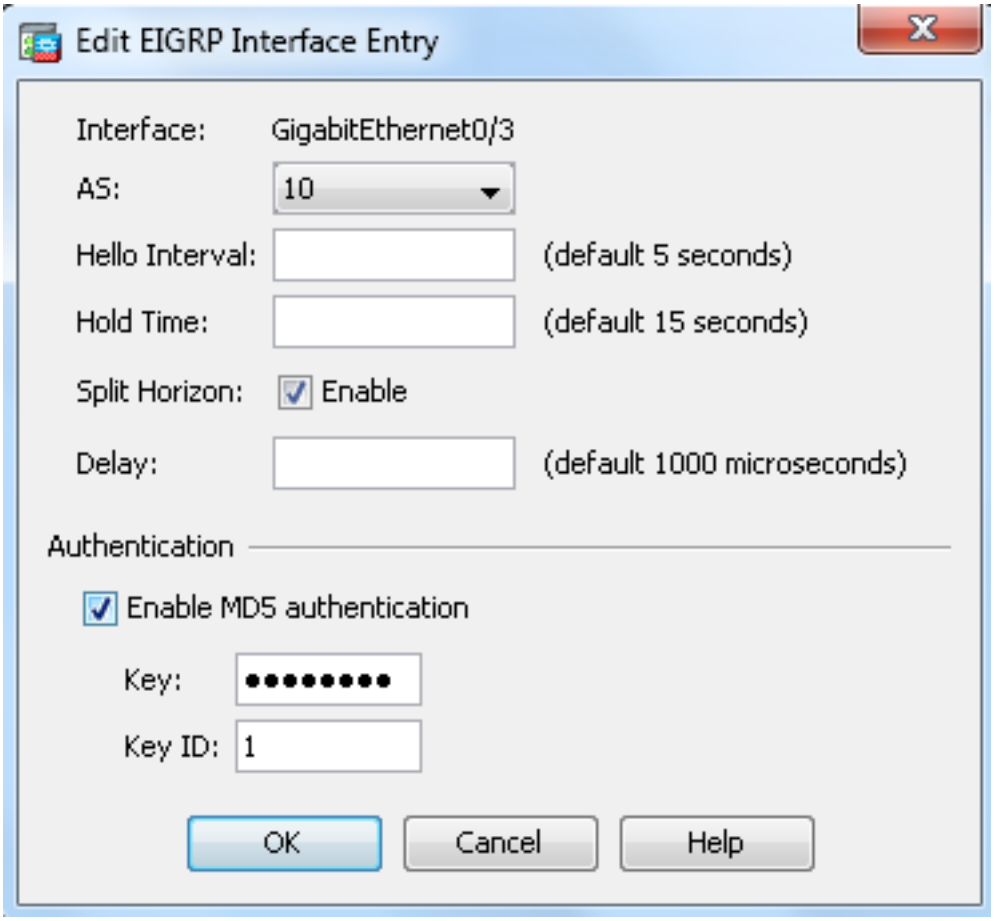
Führen Sie diese Schritte aus, um die EIGRP MD5-Authentifizierung auf der Cisco ASA zu aktivieren.

1. Navigieren Sie im ASDM zu **Configuration > Device Setup > Routing > EIGRP > Interface (Konfiguration > Geräteeinrichtung > Routing > EIGRP > Schnittstelle)**, wie gezeigt.



2. In diesem Fall ist EIGRP auf der internen Schnittstelle aktiviert (GigabitEthernet 0/1). Wählen Sie die **GigabitEthernet 0/1**-Schnittstelle aus, und klicken Sie auf **Bearbeiten**.

3. Wählen Sie unter Authentication (Authentifizierung) die Option **Enable MD5 authentication (MD5-Authentifizierung aktivieren)**. Fügen Sie hier weitere Informationen zu den Authentifizierungsparametern hinzu. In diesem Fall ist der vorinstallierte Schlüssel **cisco123** und die Schlüssel-ID **1**.



EIGRP-Routenfilterung

Mit EIGRP können Sie Routing-Updates steuern, die gesendet und empfangen werden. In diesem Beispiel blockieren Sie Routing-Updates auf der ASA für das Netzwerkpräfix 192.168.10.0/24, das sich hinter R1 befindet. Für die Routenfilterung können Sie nur die **STANDARD-ACL** verwenden.

```
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
```

Überprüfen

```
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
```

Konfigurationen

Cisco ASA CLI-Konfiguration

Dies ist die Cisco ASA CLI-Konfiguration.

```
!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
```

CLI-Konfiguration des Cisco IOS Routers (R1)

Dies ist die CLI-Konfiguration von R1 (interner Router).

```
!!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
!
!
```

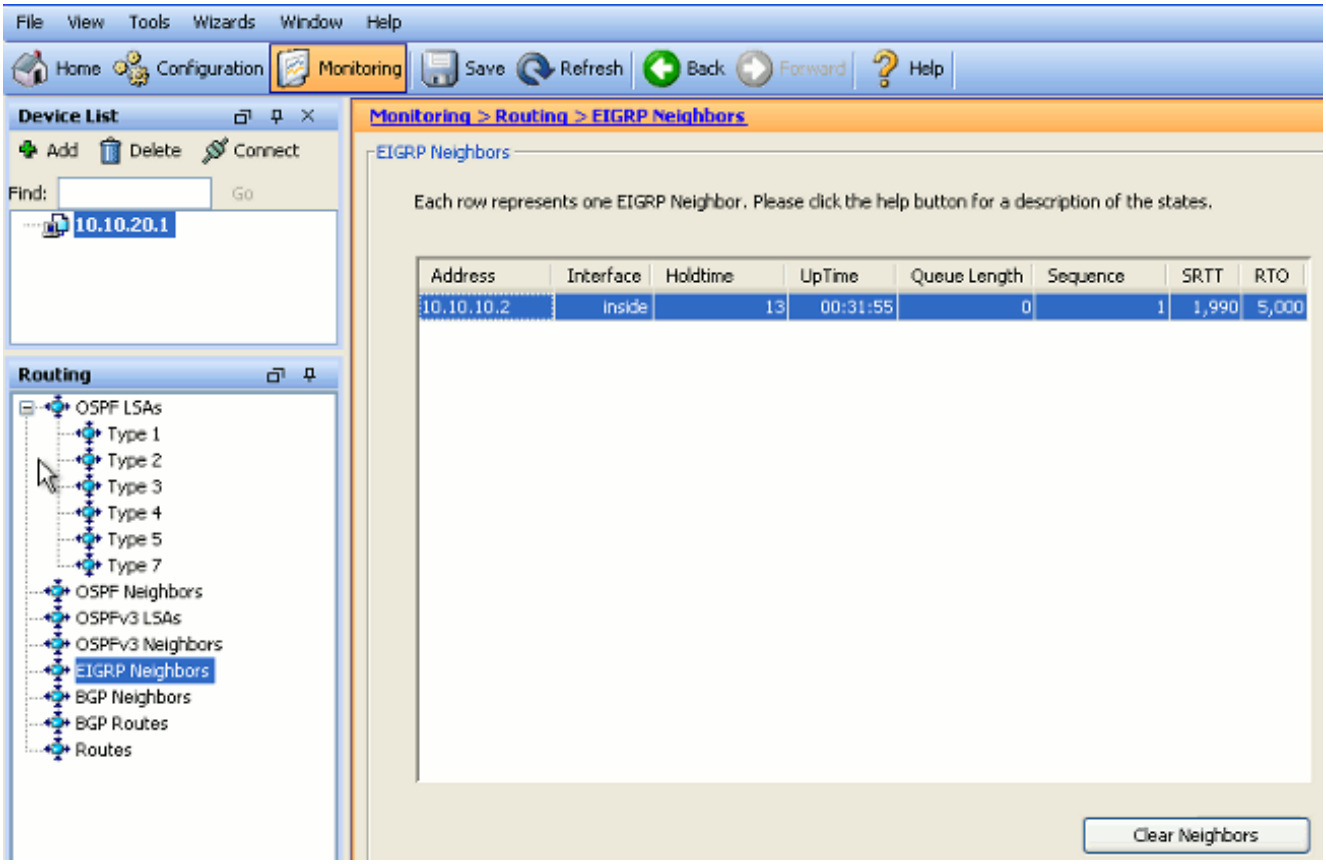
```
! EIGRP Configuration

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
```

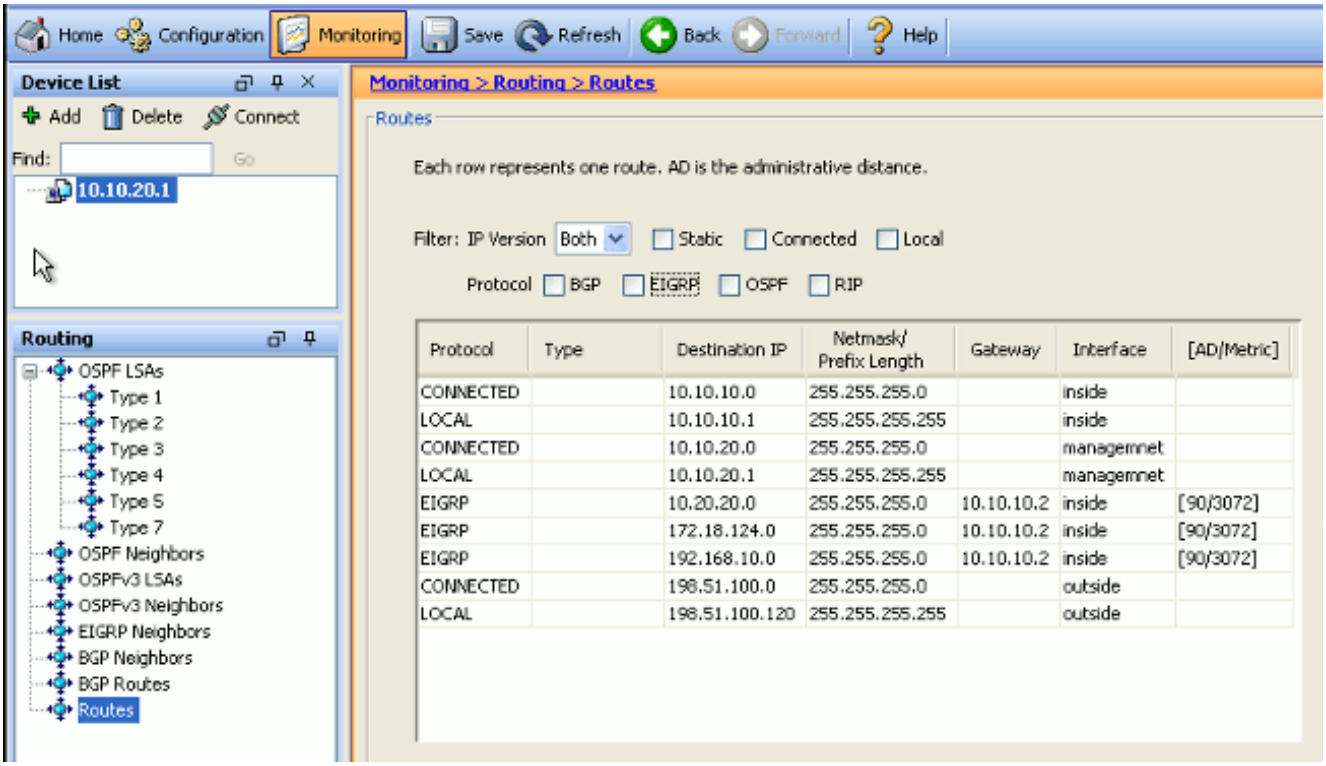
Überprüfen

Führen Sie diese Schritte aus, um Ihre Konfiguration zu überprüfen.

1. Auf dem ASDM können Sie zu **Monitoring > Routing > EIGRP Neighbor** navigieren, um die einzelnen EIGRP-Nachbarn anzuzeigen. Dieser Screenshot zeigt den internen Router (R1) als aktiven Nachbarn. Sie können auch die Schnittstelle sehen, in der sich dieser Nachbar befindet, die Haltezeit und wie lange die Nachbarbeziehung aktiv ist (UpTime).



2. Darüber hinaus können Sie die Routing-Tabelle überprüfen, wenn Sie zu **Monitoring > Routing > Routes** navigieren. In diesem Screenshot sehen Sie, dass die Netzwerke **192.168.10.0/24, 172.18.124.0/24** und **10.20.20.0/24** durch R1 (**10.10.10.2**) erlernt werden.



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 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
```

Mit ASA Version 9.2.1 und höher können Sie den Befehl **show route eigrp** verwenden, um nur EIGRP-Routen anzuzeigen.

```
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. Sie können auch den Befehl **show eigrp topology** verwenden, um Informationen über die erlernten Netzwerke und die EIGRP-Topologie abzurufen.

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

```
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
```

Paketfluss

Dies ist der Paketfluss.

1. Die ASA wird über die Verbindung aktiviert und sendet ein mCast Hello-Paket über alle EIGRP-konfigurierten Schnittstellen.

2. R1 empfängt ein Hello-Paket und sendet ein mCast Hello-Paket.

```
13 5.572557   10.10.10.1   224.0.0.10   EIGRP   86 0x3b1a (15130)   Hello
14 5.573335   10.10.10.2   224.0.0.10   EIGRP   86 0x2321 (8993)    Hello
15 5.575212   10.10.10.1   10.10.10.2   EIGRP   54 0x0589 (1417)    Update
16 5.581712   10.10.10.2   10.10.10.1   EIGRP   54 0x19d9 (6617)    Update
17 5.585145   10.10.10.1   10.10.10.2   EIGRP   54 0x755e (30046)   Hello (Ack)
18 5.585373   10.10.10.1   10.10.10.2   EIGRP   96 0x1c93 (7315)    Update
19 5.591919   10.10.10.2   10.10.10.1   EIGRP   54 0x6695 (26261)   Hello (Ack)
20 5.591950   10.10.10.2   10.10.10.1   EIGRP   180 0x7925 (31013)  Update
21 5.595200   10.10.10.1   10.10.10.2   EIGRP   96 0x62e8 (25320)   Update
22 5.601913   10.10.10.2   10.10.10.1   EIGRP   54 0x08a7 (2215)    Hello (Ack)
23 5.601944   10.10.10.2   10.10.10.1   EIGRP   96 0x31c5 (12741)   Update
```

3. Die ASA empfängt das Hello-Paket und sendet ein Update-Paket mit einem anfänglichen Bitsatz, was anzeigt, dass es sich um den Initialisierungsprozess handelt.

4. R1 empfängt ein Update-Paket und sendet ein Update-Paket mit einem anfänglichen Bitsatz, was anzeigt, dass es sich um den Initialisierungsprozess handelt.

```
⊞ Frame 15: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
⊞ Ethernet II, Src: Cisco_25:32:e2 (00:21:a0:25:32:e2), Dst: Cisco_1f:25:e3 (6c:41:6a:1f:25:e3)
⊞ Internet Protocol Version 4, Src: 10.10.10.1 (10.10.10.1), Dst: 10.10.10.2 (10.10.10.2)
⊟ Cisco EIGRP
    Version: 2
    Opcode: Update (1)
    Checksum: 0xfdc4 [correct]
  ⊟ Flags: 0x00000001, Init
      .... .... .... .... .... .... .... ...1 = Init: Set
      .... .... .... .... .... .... .... ..0. = Conditional Receive: Not set
      .... .... .... .... .... .... .... .0.. = Restart: Not set
      .... .... .... .... .... .... .... 0... = End Of Table: Not set
    Sequence: 47
    Acknowledge: 0
    Virtual Router ID: 0 (Address-Family)
    Autonomous System: 10
```

5. Nachdem sowohl ASA als auch R1 Hellos ausgetauscht haben und die Nachbarbeziehung hergestellt ist, antworten sowohl ASA als auch R1 mit einem ACK-Paket, was anzeigt, dass die Aktualisierungsinformationen empfangen wurden.

6. ASA sendet seine Routing-Informationen in einem Update-Paket an R1.

7. R1 fügt die Aktualisierungspaketinformationen in die Topologietabelle ein. Die Topologietabelle enthält alle Ziele, die von Nachbarn angekündigt werden. Es ist so organisiert, dass jedes Ziel aufgelistet ist, zusammen mit allen Nachbarn, die zum Ziel reisen können, und den zugehörigen Metriken.

8. R1 sendet dann ein Update-Paket an die ASA.

```
⊞ Frame 20: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits)
⊞ Ethernet II, Src: Cisco_1f:25:e3 (6c:41:6a:1f:25:e3), Dst: Cisco_25:32:e2 (00:21:a0:25:32:e2)
⊞ Internet Protocol Version 4, Src: 10.10.10.2 (10.10.10.2), Dst: 10.10.10.1 (10.10.10.1)
⊟ Cisco EIGRP
    Version: 2
    Opcode: Update (1)
    Checksum: 0xd032 [correct]
  ⊞ Flags: 0x00000000
    Sequence: 21
    Acknowledge: 48
    Virtual Router ID: 0 (Address-Family)
    Autonomous System: 10
  ⊞ Internal Route(MTR)  =  10.20.20.0/24
  ⊞ Internal Route(MTR)  =  172.18.124.0/24
  ⊞ Internal Route(MTR)  =  192.168.10.0/24
```

Unicast

Routing update received

9. Sobald das Update-Paket empfangen wurde, sendet die ASA ein ACK-Paket an R1. Nachdem die ASA und R1 die Update-Pakete erfolgreich voneinander empfangen haben, sind sie bereit, die Nachfolgerouten (am besten) und die umsetzbaren Nachfolgerouten (Backup) in der Topologietabelle auszuwählen und die Nachfolgerouten zur Routing-Tabelle anzubieten.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zum **Debuggen** und **Anzeigen** von Befehlen, die zur Behebung von EIGRP-Problemen nützlich sein können.

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**: Weitere Informationen zu Debug-Befehlen vor der Verwendung von **Debug-**Befehlen finden Sie unter Wichtige Informationen. Um Debuginformationen auf dem finiten System des Diffusing Update Algorithm (DUAL) anzuzeigen, verwenden Sie den Befehl **debug eigrp fsm** im privilegierten EXEC-Modus. Mit diesem Befehl können Sie die mögliche Nachfolgeaktivität von EIGRP beobachten und feststellen, ob Routen-Updates vom Routing-Prozess installiert und gelöscht werden.

Dies ist die Ausgabe des Befehls **debug** im erfolgreichen Peering mit R1. Sie können die verschiedenen Routen sehen, die erfolgreich auf dem System installiert wurden.

```
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
```

Sie können auch den Befehl **debug eigrp neighbor** verwenden. Dies ist die Ausgabe dieses **Debugbefehls**, wenn die Cisco ASA erfolgreich eine neue Nachbarbeziehung mit R1 erstellt hat.

```
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 ()
```

Sie können auch die Debug-EIGRP-Pakete für detaillierte EIGRP-Nachrichtenaustauschinformationen zwischen der Cisco ASA und ihren Peers verwenden. In diesem Beispiel wurde der Authentifizierungsschlüssel auf dem Router (R1) geändert, und die Debug-Ausgabe zeigt Ihnen, dass das Problem eine Authentifizierungsungleichheit ist.

```
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)
```

EIGRP-Nachbarschaft geht mit Syslogs ASA-5-336010 zurück

Die ASA verwirft die EIGRP-Nachbarschaft, wenn Änderungen in der EIGRP-Verteilerliste vorgenommen werden. Diese Syslog-Meldung wird angezeigt.

```
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
```

Bei dieser Konfiguration wird bei jedem **Hinzufügen eines neuen ACL-Eintrags** in der ACL die **EIGRP-Netzwerkliste** EIGRP-Nachbarschaft zurückgesetzt.

```
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
```

Sie können feststellen, dass die Nachbarbeziehung mit dem benachbarten Gerät besteht.

```
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
```

Jetzt können Sie **access-list Eigrp-network-list standard deny 172.18.24.0 255.255.255.0** hinzufügen.

```
%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 172.18.24.0.0 255.255.255.0'
%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
```

Diese Protokolle können in **debug eigrp fsm** gesehen werden.

```
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
```

Dieses Verhalten wird in allen neuen ASA-Versionen von 8.4 und 8.6 bis 9.1 erwartet. Dasselbe wurde auch bei Routern beobachtet, die Codezüge 12,4 bis 15,1 betreiben. Dieses Verhalten wird jedoch in ASA Version 8.2 und früheren ASA-Softwareversionen nicht beobachtet, da Änderungen an einer ACL die EIGRP-Adjacencies nicht zurücksetzen.

Da EIGRP beim ersten Einschalten des Nachbarn die vollständige Topologietabelle an einen Nachbarn sendet und dann nur die Änderungen sendet, würde es beim Konfigurieren einer Verteilerliste mit der ereignisgesteuerten Natur von EIGRP schwierig, die Änderungen ohne vollständige Rücksetzung der Nachbarbeziehung anzuwenden. Die Router müssen jede Route verfolgen, die an einen Nachbarn gesendet und von diesem empfangen wird, um zu erfahren, welche Route sich geändert hat (d. h. welche Route geändert wurde, ob gesendet/akzeptiert wird oder nicht), um die in der aktuellen Verteilerliste festgelegten Änderungen anzuwenden. Es ist viel einfacher, die Nachbarschaft zwischen Nachbarn einfach abzureißen und wiederherzustellen.

Wenn eine Adjacency beendet und wiederhergestellt wird, werden alle erlernten Routen zwischen bestimmten Nachbarn einfach vergessen, und die gesamte Synchronisierung zwischen den Nachbarn wird neu durchgeführt - mit der neuen Verteilerliste.

Die meisten EIGRP-Techniken, die Sie zur Fehlerbehebung bei Cisco IOS-Routern verwenden, können auf die Cisco ASA angewendet werden. Verwenden Sie zur Fehlerbehebung für EIGRP das Hauptdiagramm zur Fehlerbehebung. an das Feld **Main** (**Hauptmenü)** anschließen.