Problemen oplossen met EIGRP op FTD-apparaten beheerd door FMC

Inhoud

Inleiding

In dit document wordt beschreven hoe de EIGRP-configuratie kan worden geverifieerd en opgelost op FTD die wordt beheerd door FMC.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Cisco Secure Firewall Management Center (FMC)
- Cisco Secure Firewall Threat Defense (FTD)

Gebruikte componenten

- FTDv in versie 7.4.2.
- FMCv in versie 7.4.2.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

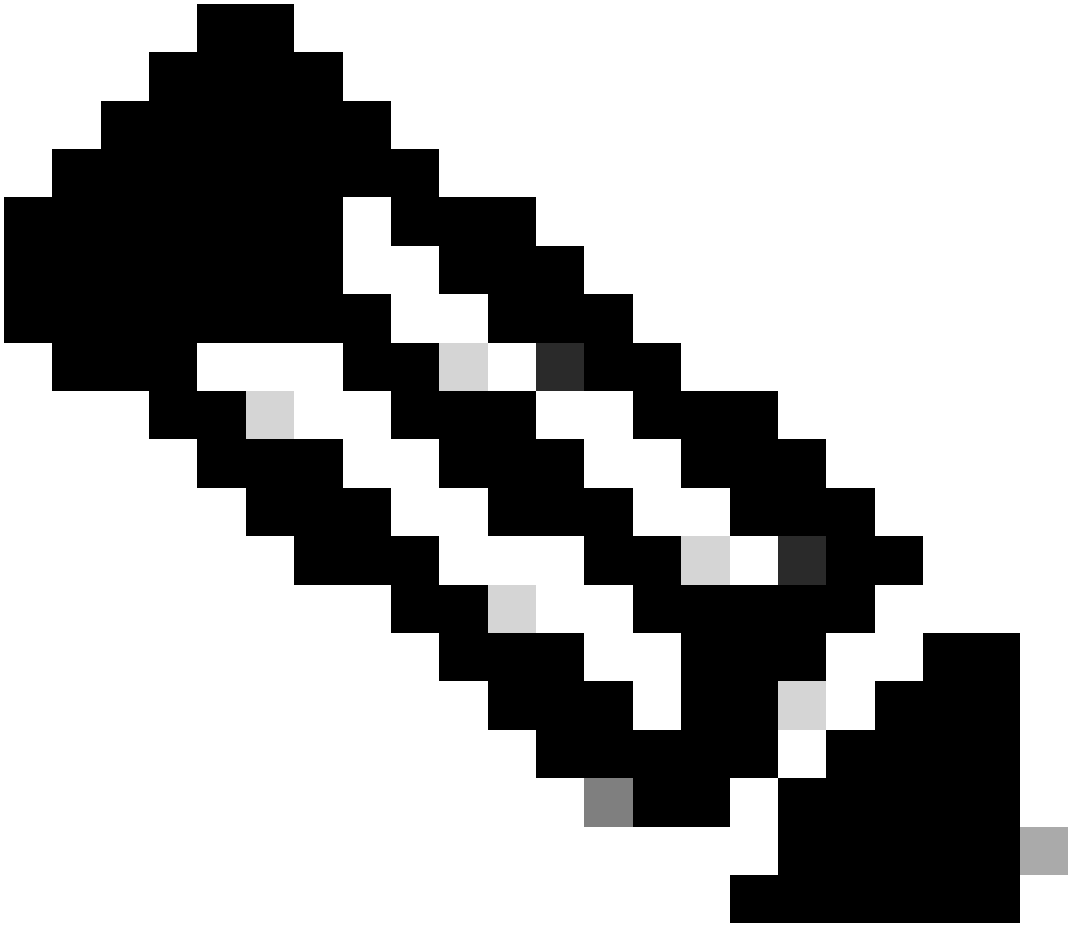
Achtergrondinformatie

EIGRP is een geavanceerd routeringsprotocol voor afstandsvectoren dat functies van zowel afstandsvectoren als linkstatusprotocollen combineert. Het biedt snelle convergentie door routeringsinformatie van buren te behouden, waardoor snelle aanpassing aan alternatieve routes mogelijk is. EIGRP is efficiënt en maakt gebruik van gedeeltelijke, getriggerde updates voor route- of metrische wijzigingen in plaats van periodieke volledige updates.
Voor communicatie werkt EIGRP direct op de IP-laag (Protocol 88) en gebruikt het Reliable Transport Protocol (RTP) voor gegarandeerde, bestelde pakketbezorging. Het ondersteunt zowel multicast als unicast, met hello-berichten die specifiek multicast-adressen 224.0.0.10 of FF02::A gebruiken.
De werking van EIGRP is hoofdzakelijk gebaseerd op de informatie die is opgeslagen in drie tabellen:

- Buurttabel: Deze tabel houdt een register bij van direct aangesloten EIGRP-apparaten waarmee een nabijheid met succes is vastgesteld.
- Topologietabel: deze tabel slaat alle aangeleerde routes op die door buren worden geadverteerd, inclusief alle haalbare paden naar een specifieke bestemming en de bijbehorende statistieken, zodat de kwaliteit en het aantal beschikbare paden kunnen worden geëvalueerd.
- Routeertabel: Deze tabel bevat het beste pad voor elke bestemming, bekend als de 'Opvolger'. Deze opvolger route is degene die actief wordt gebruikt voor het doorsturen van verkeer en wordt vervolgens geadverteerd aan andere EIGRP buren.

EIGRP gebruikt metrische gewichten, bekend als K-waarden, in routing en metrische berekeningen om het optimale pad naar een bestemming te bepalen. Deze metrische waarde is afgeleid van een formule die gebruik maakt van parameters:

- bandbreedte
- vertragingstijd
- betrouwbaarheid
- laden
- MTU

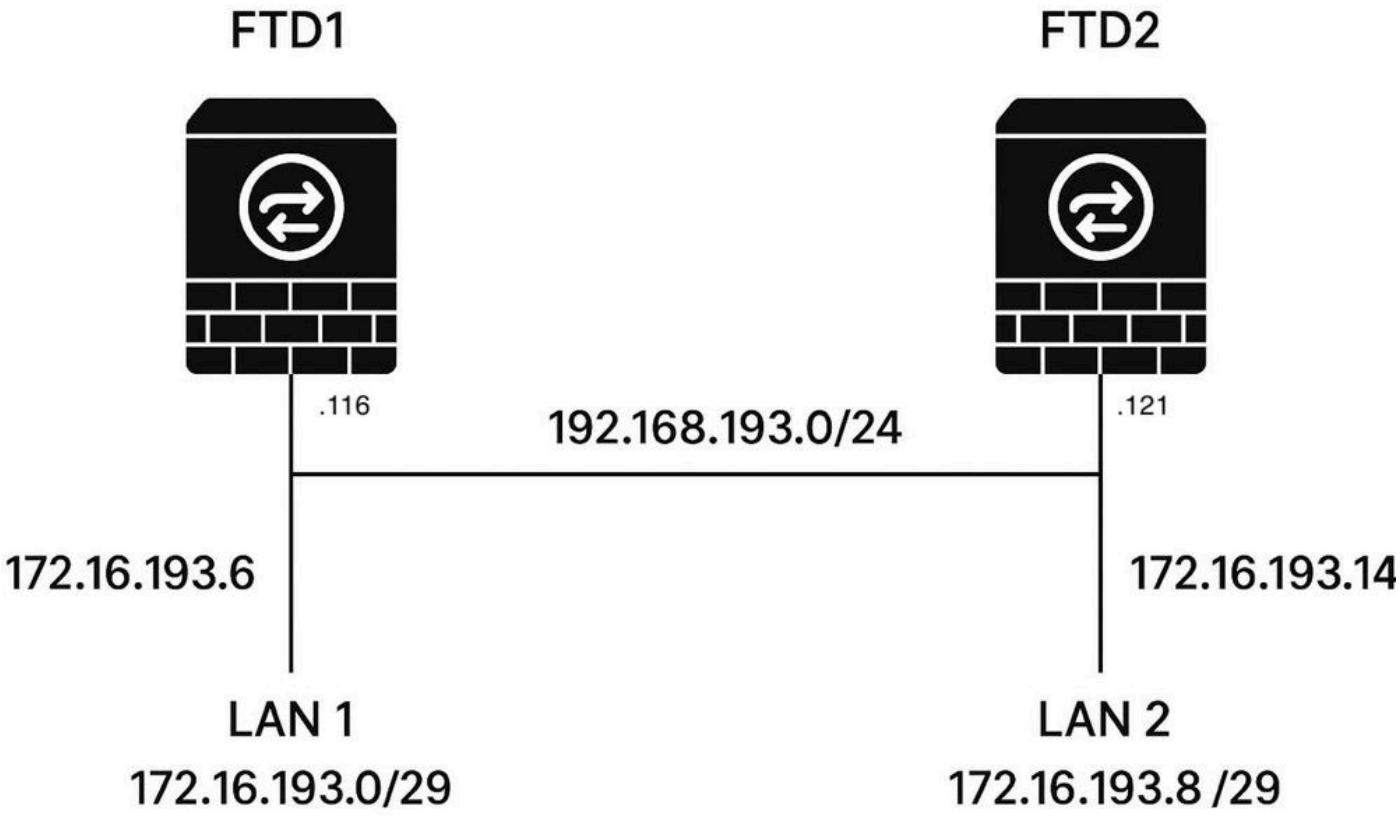


Opmerking: In het geval van een metrische band tussen meerdere paden, wordt de Maximum Transmission Unit (MTU) gebruikt als een tie-breaker, met een hogere MTU-waarde de voorkeur.

- Opvolger Route: Dit wordt gedefinieerd als het beste pad naar een specifieke bestemming. Het is de route die uiteindelijk in de routeringstafel wordt geïnstalleerd.
- Feasible Distance (FD): Dit is de best berekende metriek om een bepaald subnet te bereiken vanuit het perspectief van de lokale router.
- Gerapporteerde afstand (RD) / geadverteerde afstand (AD): Dit is de afstand (metriek) tot een specifiek subnet zoals gerapporteerd door een buur. Om een pad als een haalbare opvolger te kunnen beschouwen, moet de gerapporteerde afstand tot de buur kleiner zijn dan de lokale router haalbare afstand tot dezelfde bestemming.
- Feasible Successor (FS): Dit is een back-uppad naar een bestemming, dat een alternatieve route biedt voor het geval de primaire opvolgerroute mislukt. Een pad kwalificeert als een

haalbare opvolger als de gerapporteerde afstand (van de reclameburger) strikt kleiner is dan de haalbare afstand van de huidige opvolgerroute naar dezelfde bestemming.

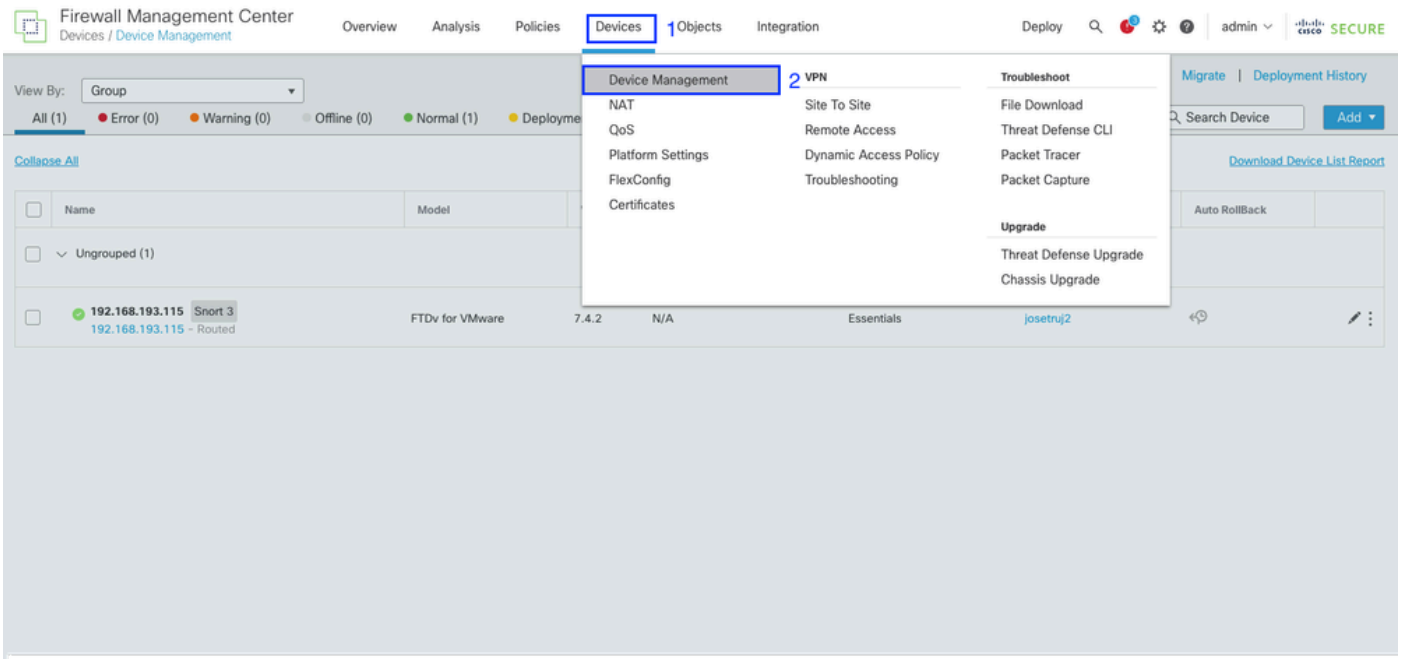
Netwerkdiagram



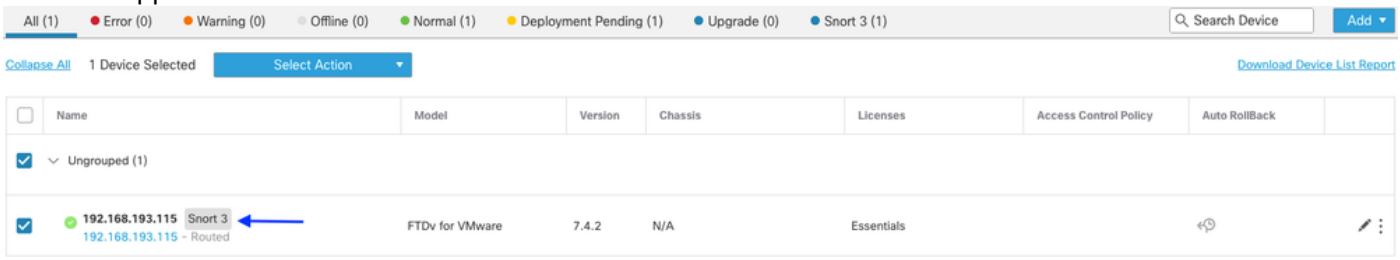
Netwerkdiagram

Basisconfiguratie

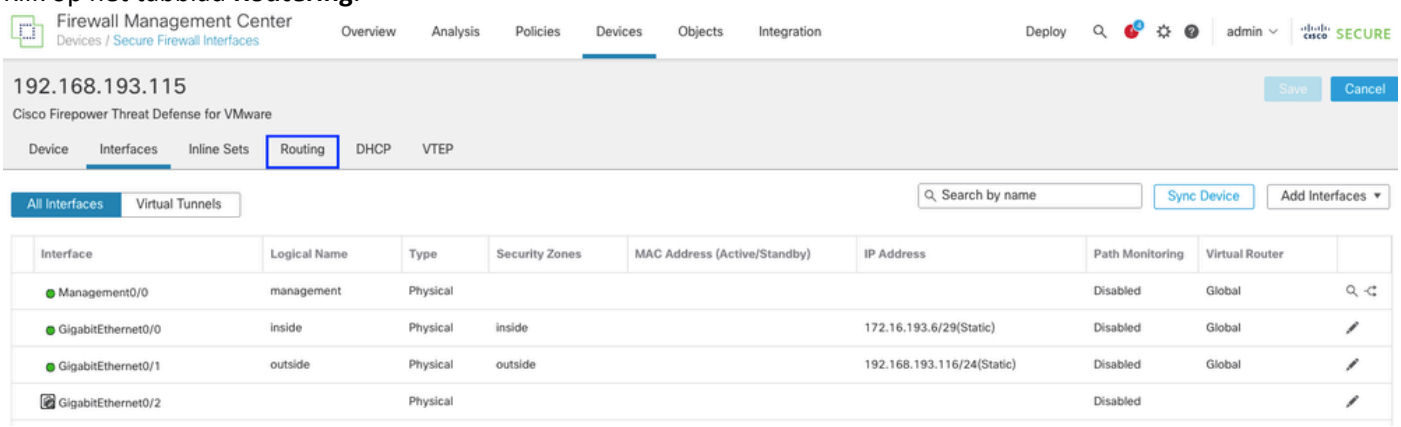
Navigeer naar **Apparaten > Apparaatbeheer**:



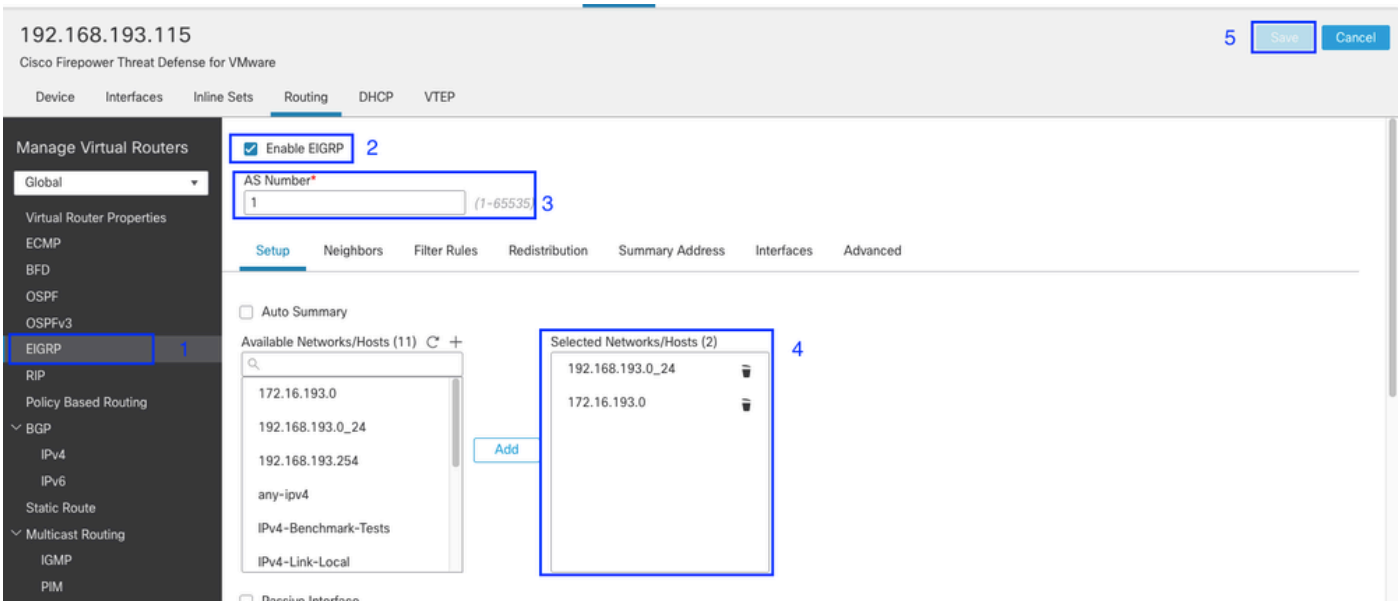
Selecteer apparaat:



Klik op het tabblad **Routering**.



Klik op **EIGRP** in het linkermenu.
Klik op **EIGRP inschakelen**.
Wijs het **AS-nummer toe** (1-65535).
Selecteer één **netwerk/host**. U kunt een eerder gemaakt object selecteren in de lijst 'Beschikbaar netwerk/host' of u kunt een nieuw object maken door op de plusknop (**+**) te klikken.
Klik op Save (Opslaan).



validering

Hier zijn de minimumvereisten voor de aangrenzende EIGRP-buren:

- Het AS-nummer moet overeenkomen.
- De interface moet actief en bereikbaar zijn.
- Als een best practice moeten Hello and Hold-timers overeenkomen.
- K-waarden moeten overeenkomen.
- Geen toegangslijsten mogen EIGRP-verkeer blokkeren.

Validatie met CLI

- Router EIGRP uitvoeren weergeven
- EIGRP-buren weergeven
- EIGRP-topologie weergeven
- EIGRP-interfaces weergeven
- Route EIGRP weergeven
- EIGRP-verkeer weergeven
- Foutopsporings-IP-eIGRP-buurman
- Foutopsporingspakketten

Firepower# Router EIGRP uitvoeren

Router EIGRP 1

Geen standaardinformatie in

Geen standaardinformatie-uitgang

Geen EIGRP log-buur-waarschuwingen

Geen wijzigingen in EIGRP-log-buurman

Netwerk 192.168.193.0 255.255.255.0

```
 Netwerk 172.16.193.8 255.255.255.248
Vuurkracht#
Firepower# EIGRP-buren weergeven
EIGRP-IPv4-buren voor AS(1)
H Adres Interface Hold Uptime SRTT RTO Q Seq
                                   sec) ms) Cnt Num
0 192.168.193.121 buiten 14 21:45:04 40 240 0 30
Firepower# Toon EIGRP-topologie
EIGRP-IPv4-topologietabel voor AS(1)/ID(192.168.193.121)
codes: p-passief, a-actief, u-update, q-query, r-antwoord,
      r - antwoordstatus, s - sia Status
P 192.168.193.0 255.255.255.0, 1 opvolgers, FD is 512
       Verbonden via, buiten
P 172.16.193.0 255.255.255.248, 1 opvolgers, FD is 768
       Via 192 168 193 116 (768/512), buiten
P 172.16.193.8 255.255.255.248, 1 opvolgers, FD is 512
       Verbonden via, binnen
Firepower# EIGRP-interfaces weergeven
EIGRP-IPv4-interfaces voor AS(1)
                    XMIT Queue Mean Pacing Time Multicast in behandeling
Interface Peers VN/Betrouwbare SRTT UN/Betrouwbare Flow Timer Routes
Buiten 1 0 / 0 10 0 / 1 50 0
binnenzijde 0 0 / 0 0 / 1 0 0
Vuurkracht#

Firepower# Routebeschrijving weergeven
Codes: L - lokaal, C - aangesloten, S - statisch, R - RIP, M - mobiel, B - BGP
```

D-EIGRP, EX-EIGRP extern, O-OSPF, IA-OSPF interarea

N1 - OSPF NSSA extern type 1, N2 - OSPF NSSA extern type 2

E1 - OSPF extern type 1, E2 - OSPF extern type 2, V - VPN

i - IS-IS, su - IS-IS samenvatting, L1 - IS-IS niveau-1, L2 - IS-IS niveau-2

ia - IS-IS interarea, * - candidate default, U - statische route per gebruiker

o - ODR, P - periodiek gedownloade statische route, + - gerepliceerde route

SI - Statisch InterVRF, BI - BGP InterVRF

Gateway of last resort is 192.168.193.254 naar netwerk 0.0.0.0

D 172.16.193.0 255.255.255.248

[90/768] via 192.168.193.116, 02:32:58, buiten

Firepower# Route weergeven

Codes: L - lokaal, C - aangesloten, S - statisch, R - RIP, M - mobiel, B - BGP

D-EIGRP, EX-EIGRP extern, O-OSPF, IA-OSPF interarea

N1 - OSPF NSSA extern type 1, N2 - OSPF NSSA extern type 2

E1 - OSPF extern type 1, E2 - OSPF extern type 2, V - VPN

i - IS-IS, su - IS-IS samenvatting, L1 - IS-IS niveau-1, L2 - IS-IS niveau-2

ia - IS-IS interarea, * - candidate default, U - statische route per gebruiker

o - ODR, P - periodiek gedownloade statische route, + - gerepliceerde route

SI - Statisch InterVRF, BI - BGP InterVRF

Gateway of last resort is 192.168.193.254 naar netwerk 0.0.0.0

S* 0.0.0.0.0.0.0.0 [1/0] via 192.168.193.254, buiten

D 172.16.193.0 255.255.255.248

[90/768] via 192.168.193.116, 02:33:41, buiten

C 172.16.193.8 255.255.255.248 is direct aangesloten, binnenin

L 172.16.193.14 255.255.255.255 is direct aangesloten, binnen

C 192.168.193.0 255.255.255.0 is direct aangesloten, buiten

L 192.168.193.121 255.255.255.255 is direct aangesloten, buiten

Vuurkracht#

Firepower# Toon eIGRP-verkeer

EIGRP-IPv4-verkeersstatistieken voor AS(1)

  Hulp verzonden/ontvangen: 4006/4001

  Verzonden/ontvangen updates: 4/4

  Verzonden/ontvangen vragen: 0/0

  Verzonden/ontvangen antwoorden: 0/0

  Acks verzonden/ontvangen: 3/2

  SIA-Query's verzonden/ontvangen: 0/0

  SIA-Antwoorden verzonden/ontvangen: 0/0

  Hello Process ID: 2503149568

  PDM Process ID: 2503150496

  Socket Queue:

  Invoerwachtrij: 0/2000/2/0 (stroom/max/hoogste/druppels)

Vuurkracht#

Problemen oplossen

Scenario 1 - Debug IP EIGRP Neighbor

Debug-opdrachten kunnen worden gebruikt om wijzigingen in buurstaten te observeren.

Firepower# debug IP-eIGRP-buurman

Vuurkracht#

EIGRP: Holdtime verlopen

Aflopend: Peer 192.168.193.121 totaal=0 stub 0, iidb-stub=0 iid-all=0

EIGRP: Fout bij handle-delokalisatie [0]

EIGRP: Buurman 192.168.193.121 ging naar buiten

Voer de opdracht buren weergeven uit om de buurstatus tussen de FTD's te valideren.

Firepower# EIGRP-buren weergeven

EIGRP-IPv4-buren voor AS(1)

Controleer de status van de interfaces met de opdracht ip brief van de interface tonen. U kunt zien dat de GigabitEthernet0/1-interface administratief niet werkt.

Firepower# Toon interface IP-overzicht

Interface IP-adres OK? Methode Status Protocol

Gigabit Ethernet0/0 172.16.193.14 JA CONFIGURATIE omhoog

Gigabit Ethernet0/1 192.168.193.121 JA CONFIG administratief omlaag

Gigabit Ethernet0/2 192.168.194.24 JA handleiding omhoog

Interne controle0/0 127.0.1.1 JA niet ingesteld

Internal-Control0/1 unassigned YES unset up

Internal-Data0/0 unassigned YES unset up

Internal-Data0/0 unassigned YES unset up

Intern-gegevens0/1 169.254.1.1 JA niet ingesteld

Internal-Data0/2 unassigned YES unset up

Beheer0/0 203.0.113.130 JA niet ingesteld

Scenario 2 - Authenticatie

De FTD ondersteunt het MD5-hash-algoritme om EIGRP-pakketten te verifiëren. Standaard is deze verificatie uitgeschakeld.

Om het MD5-hashalgoritme in te schakelen, vinkt u het selectievakje 'MD5-verificatie' aan. Het is van cruciaal belang dat de authenticatie-instellingen op beide apparaten overeenkomen; indien ingeschakeld op het ene apparaat, maar niet op het andere, kan er zich geen naaste omgeving tussen hen vormen.

Controleer deze configuratie met foutopsporingspakketten.

Firepower#-foutopsporingspakketten

(UPDATE, VERZOEK, QUERY, ANTWOORD, HALLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY) EIGRP-pakketdebugging is ingeschakeld

Vuurkracht#

EIGRP: buiten: genegeerd pakket van 192.168.193.121, opcode = 5 (verificatie uit of sleutelhanger ontbreekt)

EIGRP: Ontvangen HALLO op buiten nbr 172.16.193.14

AS 1, vlaggen 0x0: (NULL), Seq 0/0 interfaceQ 0/0

EIGRP: HALLO aan de buitenkant

AS 1, Flags 0x0: (NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP: HALLO aan de binnenkant

AS 1, Flags 0x0: (NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP: buiten: genegeerd pakket van 192.168.193.121, opcode = 5 (verificatie uit of sleutelhanger ontbreekt)

EIGRP: Ontvangen HALLO op buiten nbr 172.16.193.14

AS 1, vlaggen 0x0: (NULL), Seq 0/0 interfaceQ 0/0

EIGRP: HALLO aan de binnenkant

AS 1, Flags 0x0: (NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP: HALLO aan de buitenkant

AS 1, Flags 0x0: (NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP: buiten: genegeerd pakket van 192.168.193.121, opcode = 5 (verificatie uit of sleutelhanger ontbreekt).

U kunt een bericht waarnemen dat aangeeft dat de verificatie is uitgeschakeld of dat de sleutelhanger ontbreekt. In dit scenario treedt dit meestal op wanneer verificatie is ingeschakeld op de ene peer, maar niet op de andere.

EIGRP: buiten: genegeerd pakket van 192.168.193.121, opcode = 5 (verificatie uit of sleutelhanger ontbreekt).

Verifiëren met show run interface <EIGRP interface>.

Firepower1# toont run-interface GigabitEthernet0/1

Ja!

Gigabit Ethernet-interface0/1

Naam buiten

veiligheidsniveau 0

IP-adres 192.168.193.121 255.255.255.0

Verificatiesleutel EIGRP 1 ***** Key-ID 10

Verificatiemodus EIGRP 1 MD5

Firepower2# toont run-interface GigabitEthernet0/1

Ja!

Gigabit Ethernet-interface0/1

Naam buiten

veiligheidsniveau 0

IP-adres 192.168.193.116 255.255.255.0

Scenario 3 - Passieve interfaces

Wanneer EIGRP is geconfigureerd, worden EIGRP-hello-pakketten meestal verzonden en ontvangen op interfaces waar het netwerk is ingeschakeld.

Als een interface echter als passief is geconfigureerd, onderdrukt EIGRP de uitwisseling van hello-pakketten tussen twee routers op die interface, wat resulteert in het verlies van de nabijheid van de buren. Bijgevolg voorkomt deze actie niet alleen dat de router reclame maakt voor het routeren van updates uit die interface, maar voorkomt het ook dat het routeringsupdates van die interface ontvangt.

Voer de opdracht buren weergeven uit om de buurstatus tussen de FTD's te valideren.

Firepower# Toon eIGRP-buren

EIGRP-IPv4-buren voor AS(1)

U kunt de EIGRP-pakketten die worden verzonden en de interfaces waar ze doorheen worden verzonden verifiëren met behulp van de opdracht debug eigrp-pakketten.

FTD 1

Vuurkracht1#

(UPDATE, VERZOEK, QUERY, ANTWOORD, HALLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY) EIGRP-pakketdebugging is ingeschakeld

Vuurkracht#

EIGRP: HALLO aan de buitenkant

AS 1, Flags 0x0: (NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP: HALLO aan de binnenkant

AS 1, Flags 0x0: (NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP: HALLO aan de buitenkant

AS 1, Flags 0x0: (NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP: HALLO aan de binnenkant

AS 1, Flags 0x0: (NULL), Seq 0/0 interfaceQ 0/0 iidbQ un/rely 0/0

EIGRP: HALLO aan de buitenkant

FTD 2

Firepower2#-foutopsporingspakketten

(UPDATE, VERZOEK, QUERY, ANTWOORD, HALLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY) EIGRP-pakketdebugging is ingeschakeld

Firepower2#

In dit scenario stuurt FTD 2 geen EIGRP-hello-berichten omdat de binnen- en buiteninterfaces als passief zijn geconfigureerd. Controleer dit met de opdracht routercontrole uitvoeren.

Firepower2# geeft routercontrole weer

Router EIGRP 1

Geen standaardinformatie in

Geen standaardinformatie-uitgang

Geen EIGRP log-buur-waarschuwingen

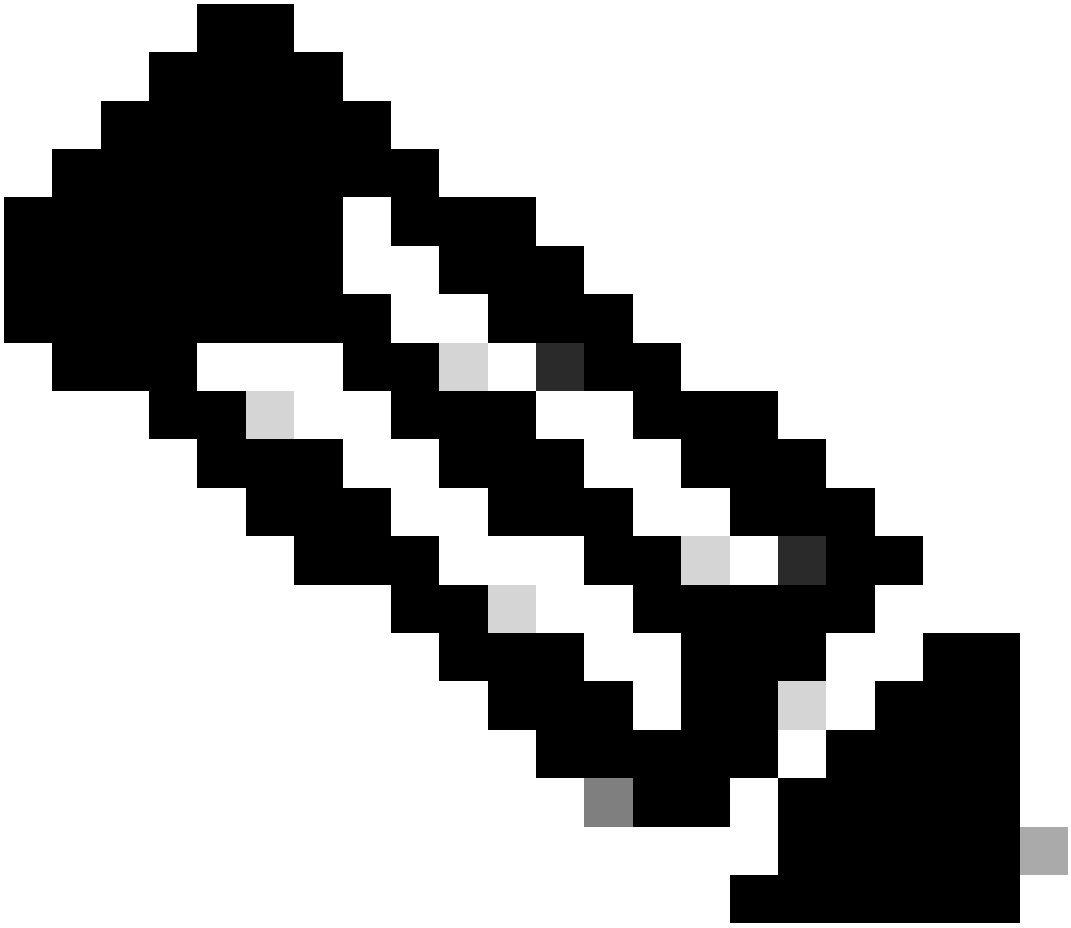
Geen wijzigingen in EIGRP-log-buurman

Netwerk 192.168.193.0 255.255.255.0

Netwerk 172.16.193.8 255.255.255.248

passieve interface buiten

passieve interface binnenin



Opmerking: om alle geconfigureerde debug processen te stoppen, gebruik je de undebug all opdracht.

Gerelateerde informatie

- EIGRP op FTD-apparaten
- EIGRP configureren voor FTD
- EIGRP samengestelde kosten Metrics

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.