FlexVPN-handleiding in redundant hubontwerp met FlexVPN-clientblokconfiguratievoorbeeld

Inhoud

Inleiding

Dit document beschrijft hoe u een gesproken netwerk in een FlexVPN-netwerk kunt configureren met gebruik van het FlexVPN-clientconfiguratieblok in een scenario waarin meerdere knooppunten beschikbaar zijn.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- FlexVPN
- Cisco-routingprotocollen

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco G2 Series geïntegreerde services router (ISR)
- Cisco IOS versie 15.2M

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 de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Voor overtollige doeleinden, zou een gesproken kunnen met meerdere knooppunten moeten verbinden. Redundantie van de spaakzijde maakt continu gebruik mogelijk zonder één enkel punt van falen op de hub.

De twee meest gebruikelijke FlexVPN redundante hub ontwerpen die de spaakconfiguratie gebruiken zijn:

- **Dubbele wolkenbenadering**, waarbij een gesproken wordt heeft twee aparte tunnels die te allen tijde actief zijn op beide hubs.
- **Failover-benadering**, waarbij een spits een actieve tunnel heeft met één hub op een bepaald moment in de tijd.

Beide benaderingen hebben een unieke reeks voor- en nadelen.

benaderen	Pros	Cons
Dubbele cloud	• Sneller herstel in een mislukking, gebaseerd op het routeren van protocol timers • Meer mogelijkheden om verkeer tussen knooppunten te verdelen aangezien de verbindingen met beide knooppunten actief zijn	• Spoke onderhoudt sessie aan beide knooppunten tegelijkertijd, wat middelen beide knooppunten consumeert
failover	• Eenvoudige configuratie - ingebouwd in FlexVPN • Vertrouwt niet op het routingprotocol in een mislukking	• Lagere terugwinningstijd - gebaseerd op Dead Peer Detection (DPD) of (optionee object tracking • Al het verkeer is gedwongen om tegelijk naar één hub te reizen

In dit document wordt de tweede aanpak beschreven.

Configureren

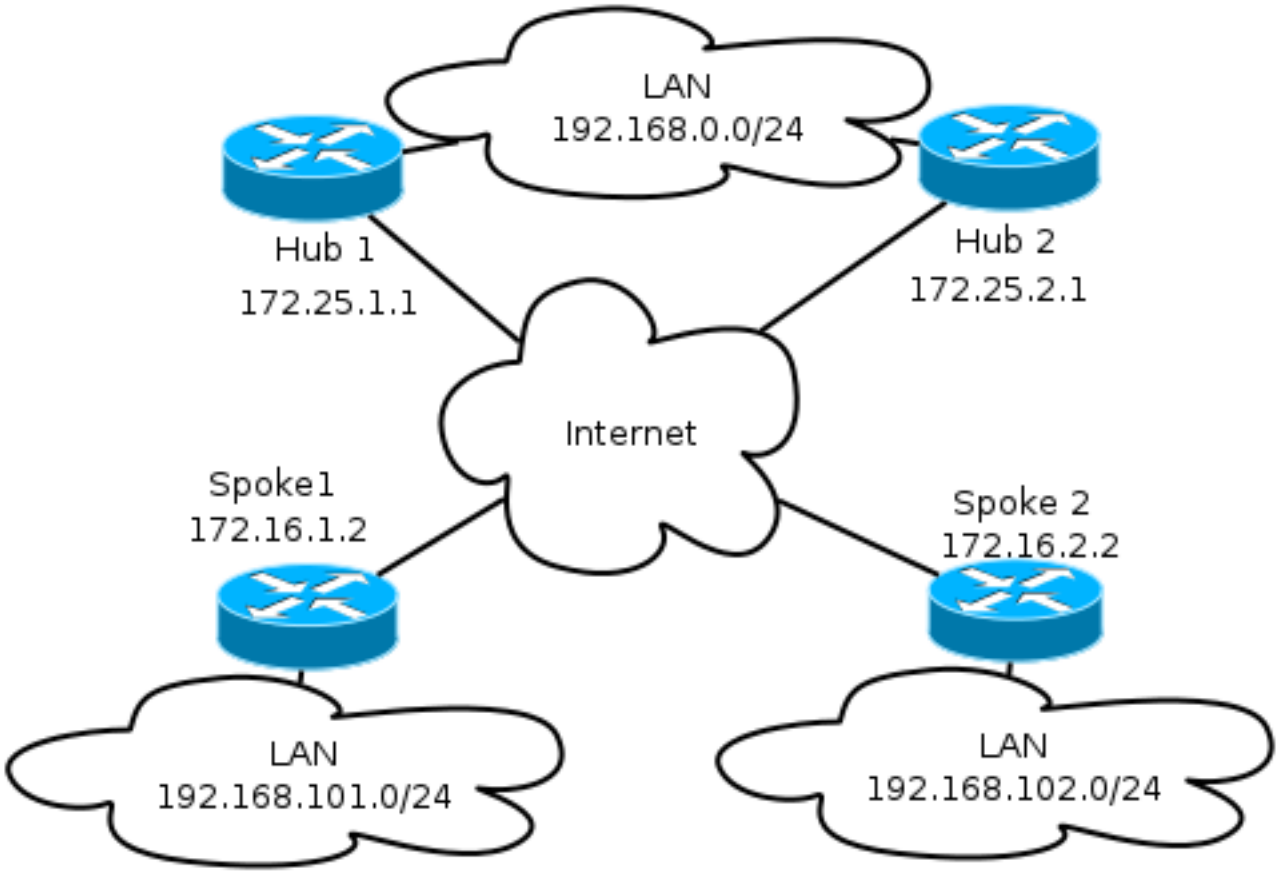
Opmerking: Gebruik de Command Lookup Tool (alleen voor geregistreerde gebruikers) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagrammen

Deze diagrammen tonen zowel het vervoer als de topologie van de bekleding.

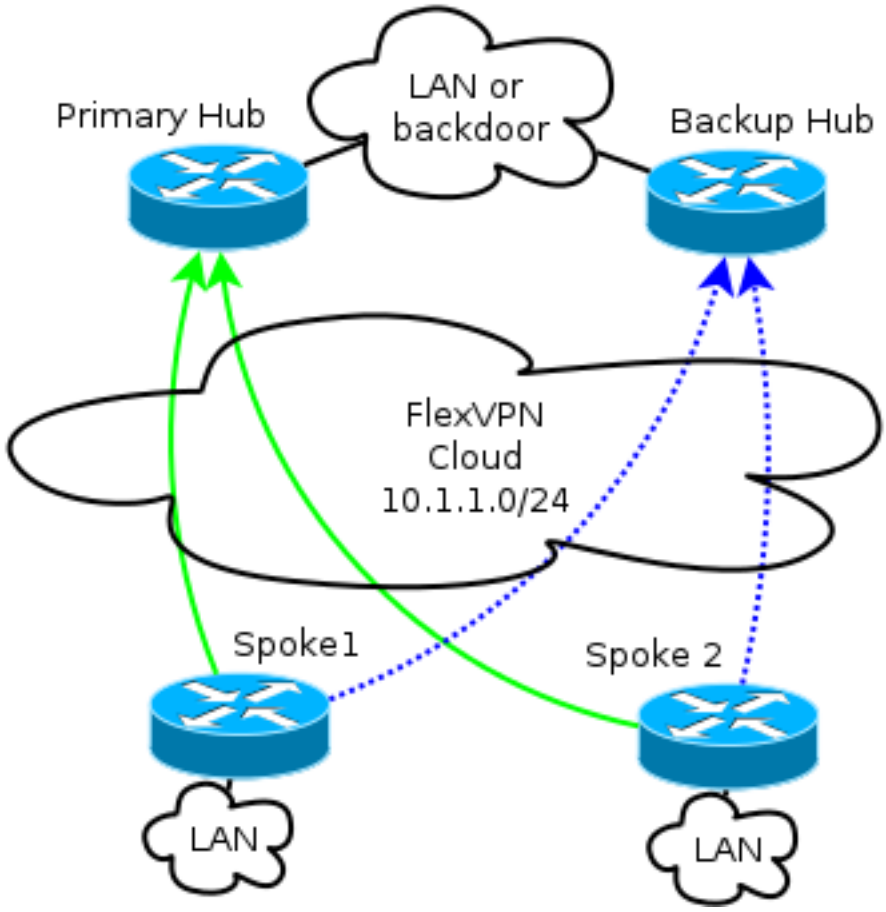
transportnetwerk

Dit diagram illustreert het basisnetwerk van het transport dat typisch in FlexVPN netwerken wordt gebruikt.



Overlay-netwerk

Dit diagram illustreert het overlay netwerk met logische connectiviteit die toont hoe de failover zou moeten werken. Tijdens normaal gebruik onderhouden Spoke 1 en Spoke 2 alleen een relatie met één hub.



Opmerking: In het diagram tonen de solide groene lijnen de verbinding en de richting van de primaire de Vertaling van Internet Belangrijkste Versie 2 (IKEv2)/Flex sessies, en de gestippelde blauwe lijnen wijzen op de reserveverbinding als de van Internet Key Exchange (IKE) zitting op de primaire hub faalde.

De **24** adressering vertegenwoordigt het aantal adressen dat voor deze cloud is toegewezen en niet de eigenlijke interface-adressering. Dit komt doordat het FlexVPN-knooppunt doorgaans een dynamisch IP-adres toewijst voor de inkomende interface en is gebaseerd op routes die dynamisch via routeopdrachten in het FlexVPN-vergunningsblok zijn ingevoegd.

Basisconfiguratie van slangen en hub

De basisconfiguratie van de hub en het spraakvenster is gebaseerd op migratiedocumenten van Dynamic Multipoint VPN (DMVPN) naar FlexVPN. Deze configuratie wordt beschreven in de [FlexVPN-migratie: Harde beweging van DMVPN naar FlexVPN op hetzelfde](#) artikel [Apparaten](#).

Aanpassing van de Spoelconfiguratie

Spraakconfiguratie - Clientconfiguratie

De configuratie van de slang moet worden uitgebreid door de configuratie van de client.

In de basisconfiguratie worden meerdere peers gespecificeerd. De peer met de hoogste voorkeur

(het laagste aantal) wordt overwogen vóór anderen.

```
crypto ikev2 client flexvpn Flex_Client
peer 1 172.25.1.1
peer 2 172.25.2.1
client connect Tunnel1
```

De tunnelconfiguratie moet veranderen om de tunnelbestemming dynamisch te laten kiezen, op basis van het FlexVPN-clientconfiguratie blok.

```
interface Tunnel1
 tunnel destination dynamic
```

Het is belangrijk om te onthouden dat het FlexVPN-clientconfiguratieblok aan een interface is gekoppeld en niet aan IKEv2 of het IPsec-profiel (Internet Protocol Security).

Het configuratieblok van de client biedt meerdere opties om de overvaltijd en de bewerkingen aan te passen, waaronder het volgen van objecten, back-up van bellen en de functies van back-upgroepen.

Met basisconfiguratie maakt de spaak gebruik van DPD's om te zien of een speld niet reageert. Het veroorzaakt een verandering zodra de peer dood is verklaard. De optie om DPD te gebruiken is geen snelle, vanwege de manier waarop DPD werkt. Een beheerder zou de configuratie kunnen willen verbeteren met object tracking of vergelijkbare verbeteringen.

Raadpleeg voor meer informatie het hoofdstuk van de **FlexVPN-clientconfiguratie** van de Cisco IOS-configuratiegids, die aan het einde van dit document is gekoppeld in de **Verwante informatie**.

Volledig bereik configuratie - referentie

```
crypto logging session

crypto ikev2 keyring Flex_key
 peer Spokes
 address 0.0.0.0 0.0.0.0
 pre-shared-key local cisco
 pre-shared-key remote cisco

crypto ikev2 profile Flex_IKEv2
 match identity remote address 0.0.0.0
 authentication remote pre-share
 authentication local pre-share
 keyring local Flex_key
 aaa authorization group psk list default default
 virtual-template 1

crypto ikev2 dpd 30 5 on-demand

crypto ikev2 client flexvpn Flex_Client
 peer 1 172.25.1.1
 peer 2 172.25.2.1
 client connect Tunnel1

crypto ipsec transform-set IKEv2 esp-gcm
 mode transport
```

```
crypto ipsec profile default
 set ikev2-profile Flex_IKEv2

interface Tunnel1
 description FlexVPN tunnel
 ip address negotiated
 ip mtu 1400
 ip nhrp network-id 2
 ip nhrp shortcut virtual-template 1
 ip nhrp redirect
 ip tcp adjust-mss 1360
 delay 2000
 tunnel source Ethernet0/0
 tunnel destination dynamic
 tunnel path-mtu-discovery
 tunnel protection ipsec profile default
```

Hub-configuratie

Hoewel de meerderheid van de configuratie van de hub hetzelfde blijft, moeten verschillende aspecten worden aangepakt. De meesten van hen hebben te maken met een situatie waarin één of meer woordjes verbonden zijn met één hub, terwijl anderen in relatie blijven met een ander knooppunt.

Spoeladressen

Omdat de woords IP adressen van knooppunten verkrijgen, is het normaal gewenst dat de knooppunten adressen van verschillende subnetten of een verschillend deel van een ubnet toewijzen.

Bijvoorbeeld:

Hub1

```
ip local pool FlexSpokes 10.1.1.100 10.1.1.175
```

Hub2

```
ip local pool FlexSpokes 10.1.1.176 10.1.1.254
```

Dit voorkomt overlap, zelfs als de adressen niet buiten de FlexVPN-cloud worden gelegd, wat de probleemoplossing kan belemmeren.

Adres hub Overlay

Beide hubs kunnen hetzelfde IP-adres behouden op een virtuele-sjabloon-interface; dit kan echter in sommige gevallen gevolgen hebben voor de oplossing van problemen . Deze ontwerpkeuze maakt het gemakkelijker om in te zetten en te plannen, aangezien de sprak slechts één peer adres voor Border Gateway Protocol (BGP) moet hebben.

In sommige gevallen is dit misschien niet gewenst of nodig.

Routing

Het is noodzakelijk voor knooppunten om informatie uit te wisselen over de spaken die verbonden zijn.

Hubs moeten in staat zijn de specifieke routes van de door hen verbonden voorzieningen te ruilen en nog steeds een samenvatting te geven aan de woordvoerders.

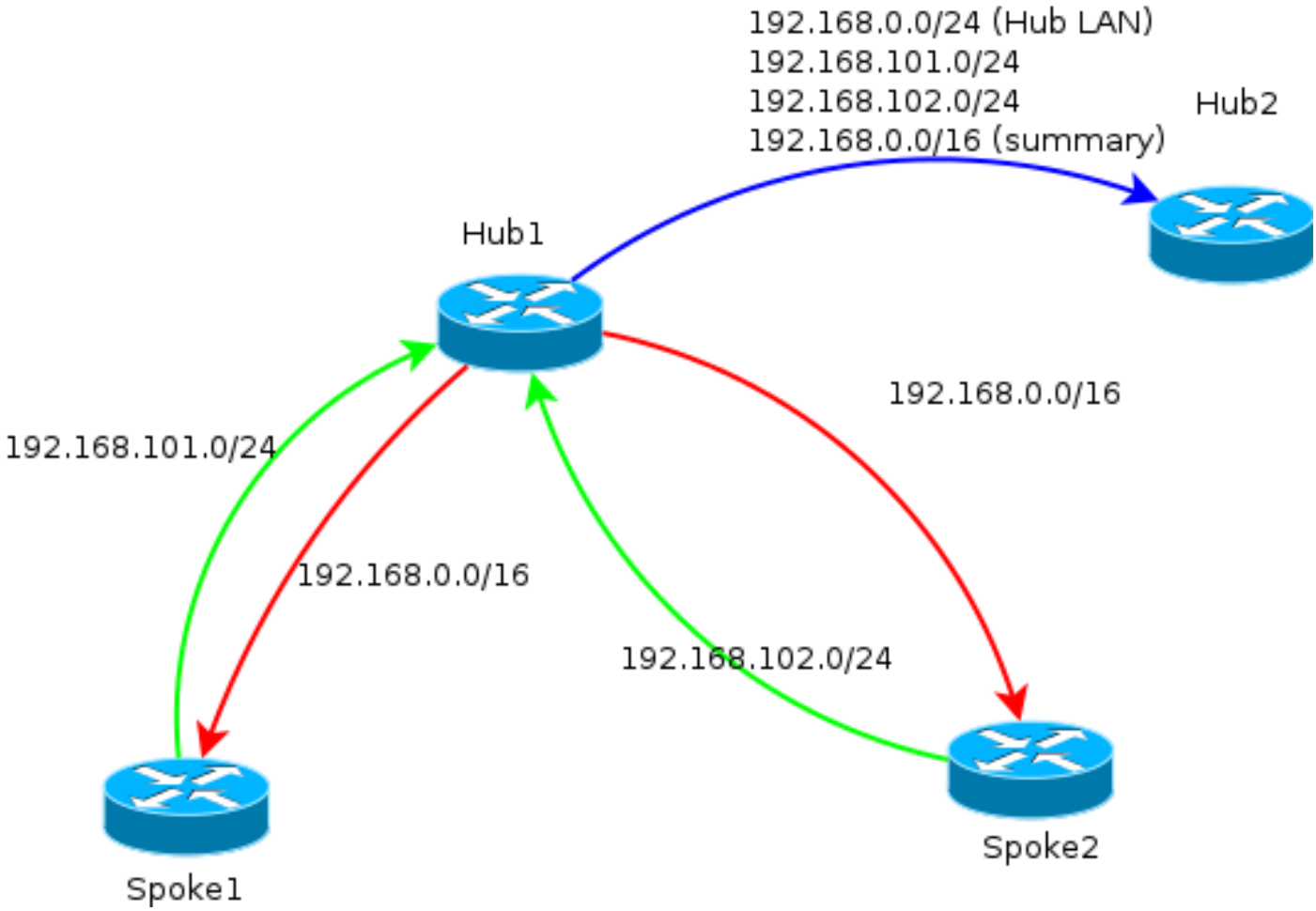
Aangezien Cisco u aanbeveelt iBGP met FlexVPN en DMVPN te gebruiken, wordt alleen dat Routing Protocol weergegeven.

```
bgp log-neighbor-changes
bgp listen range 10.1.1.0/24 peer-group Spokes
network 192.168.0.0
neighbor Spokes peer-group
neighbor Spokes remote-as 65001
neighbor 192.168.0.2 remote-as 65001
neighbor 192.168.0.2 route-reflector-client
neighbor 192.168.0.2 next-hop-self all
neighbor 192.168.0.2 unsuppress-map ALL

access-list 1 permit any

route-map ALL permit 10
match ip address 1
```

Dankzij deze configuratie kan:

- Dynamische luisteraar van adressen toegewezen aan woordvoerders
- Reclamenetwerk van 192.168.0.0/24
- Reclameressummiere route van 192.168.0.0/16 naar alle spokes. De geaggregeerde adresconfiguratie creëert een statische route voor dat prefix via nul interface, dat een verworpen route is die wordt gebruikt om routing lijnen te voorkomen.
- Doorsturen van specifieke prefixes naar de andere hub
- Routereflector client om ervoor te zorgen dat de knooppunten informatie die van spaken tussen elkaar geleerd is, uitwisselen

Dit diagram vertegenwoordigt de prefix uitwisseling in BGP in deze opstelling, vanuit het perspectief van één van de knooppunten.



Opmerking: In dit diagram representeert de groene lijn informatie die door spaken aan de hub wordt verstrekt, vertegenwoordigt de rode lijn informatie die door elke hub aan de spaken wordt verstrekt (slechts een samenvatting), en de blauwe lijn vertegenwoordigt de prefixes die tussen knooppunten worden uitgewisseld.

Gebruik van netwerkoverzichten

In sommige scenario's kunnen bedragen niet van toepassing of gewenst zijn. Gebruik voorzichtigheid wanneer u de bestemming IP in prefixes aanwijst, omdat iBGP de volgende hop standaard niet overtreft.

Samenvattingen worden aanbevolen in netwerken die de status vaak wijzigen. De instabiele internetverbindingen zouden bijvoorbeeld samenvattingen kunnen vereisen om: het verwijderen en toevoegen van prefixes voorkomen, het aantal updates beperken en de meeste instellingen in staat stellen hun schaalgrootte goed te vergroten.

Spoke-to-Spoke tunnels

In het scenario en de configuratie die in de vorige sectie zijn vermeld, kunnen woordvoerders op verschillende knooppunten geen directe gesproken-aan-gesproken tunnels inrichten. Het verkeer tussen spaken verbonden met verschillende hubs stroomt over de centrale apparaten.

Hier is een eenvoudige omweg. Nochtans, vereist het dat het Next Hopprotocol (NHRP) met

dezelfde netwerk-ID tussen knooppunten wordt geactiveerd. Dit kan bijvoorbeeld worden bereikt, als u een point-to-point Generic Routing Encapsulation (GRE) tussen hubs maakt. Dan is IPsec niet vereist.

Verifiëren

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met show. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

De **show crypto ikev2 sa** opdracht geeft u op de hoogte van waar de sprak momenteel verbonden is.

De opdracht **Show crypto ikev2 client-flexVPN** stelt een beheerder in staat om de huidige status van de FlexVPN client-handeling te begrijpen.

```
Spoke2# show crypto ikev2 client flexvpn

Profile : Flex_Client
Current state:ACTIVE
Peer : 172.25.1.1
Source : Ethernet0/0
ivrf : IP DEFAULT
fvrf : IP DEFAULT
Backup group: Default
Tunnel interface : Tunnel1
Assigned IP address: 10.1.1.111
```

Een succesvolle failover met de configuratie van de **show logging** logt deze uitvoer op het gebruikte apparaat in:

```
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is DOWN.  Peer 172.25.1.1:500
Id: 172.25.1.1
%FLEXVPN-6-FLEXVPN_CONNECTION_DOWN: FlexVPN(Flex_Client) Client_public_addr =
172.16.2.2 Server_public_addr = 172.25.1.1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to down
%LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, changed state to up
%CRYPTO-5-IKEV2_SESSION_STATUS: Crypto tunnel v2 is UP.  Peer 172.25.2.1:500
Id: 172.25.2.1
%FLEXVPN-6-FLEXVPN_CONNECTION_UP: FlexVPN(Flex_Client) Client_public_addr =
172.16.2.2 Server_public_addr = 172.25.2.1 Assigned_Tunnel_v4_addr = 10.1.1.177
```

In deze output detecteert de sprak de verbinding van **hub 172.25.1.1**, het Flex_Client-configuratieblok defect en dwingt een verbinding naar **172.25.2.1** waar een tunnel omhoog komt, en een toespraak krijgt een IP toegewezen van **10.1.177**.

Problemen oplossen

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met show. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

> **Opmerking:** Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met **debug opgeeft.**

Hier zijn de relevante debug-opdrachten:

- **debug van crypto ikev2**
- **straal deken**

Gerelateerde informatie

- Configuratie-gids voor FlexVPN en Internet Key Exchange, versie 2, Cisco IOS release 15 M&T
- Technische ondersteuning en documentatie – Cisco Systems