Overzicht van MPTCP- en productondersteuning

Inhoud

Inleiding

Dit document biedt een overzicht van Multipath TCP (MPTCP), de impact op flow-inspectie en de Cisco producten die wel en niet door deze worden beïnvloed.

MPTCP-Overzicht

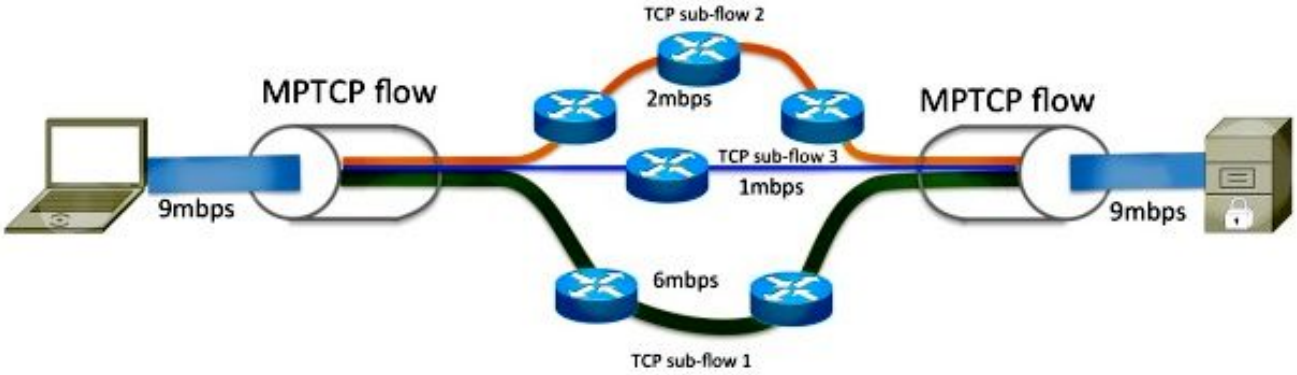
Achtergrondinformatie

De hosts die met internet of binnen een datacenteromgeving zijn verbonden, worden vaak door meerdere paden verbonden. Wanneer TCP echter wordt gebruikt voor gegevenstransport, is communicatie beperkt tot één netwerkpad. Het is mogelijk dat sommige paden tussen de twee hosts overvol zijn, terwijl alternatieve paden onderbenut zijn. Een efficiënter gebruik van netwerkbronnen is mogelijk als deze meerdere paden tegelijkertijd worden gebruikt. Bovendien vergroot het gebruik van meerdere verbindingen de gebruikerservaring, omdat het een hogere doorvoersnelheid en een betere veerkracht tegen netwerkstoringen biedt.

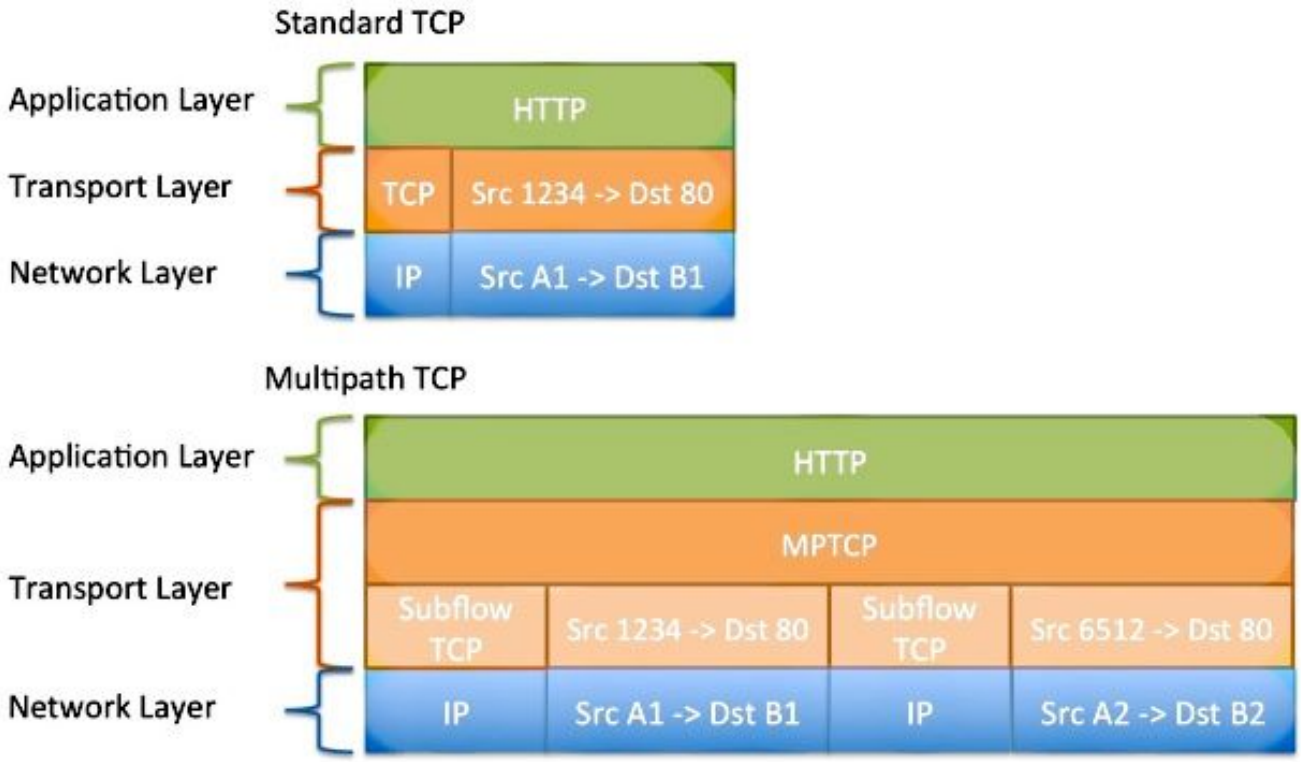
MPTCP is een set van extensies van reguliere TCP die een enkele gegevensstroom scheiden en over meerdere verbindingen meebrengen. Raadpleeg RFC6824: TCP-uitbreidingen voor Multipath-bediening met meerdere adressen voor meer informatie.

Zoals in dit diagram wordt getoond, kan MPTCP de 9mbps-stroom in drie verschillende

substromen op het sender-knooppunt scheiden, die vervolgens wordt geaggregeerd naar de oorspronkelijke gegevensstroom op het ontvangende knooppunt.



De gegevens die de MPTCP-verbinding invoeren, werken precies zoals ze via een reguliere TCP-verbinding doen; de verstrekte gegevens hebben gezorgd voor een levering in bestelling. Aangezien MPTCP de netwerkstack aanpast en binnen de transportlaag werkt, wordt deze door de toepassing op transparante wijze gebruikt.



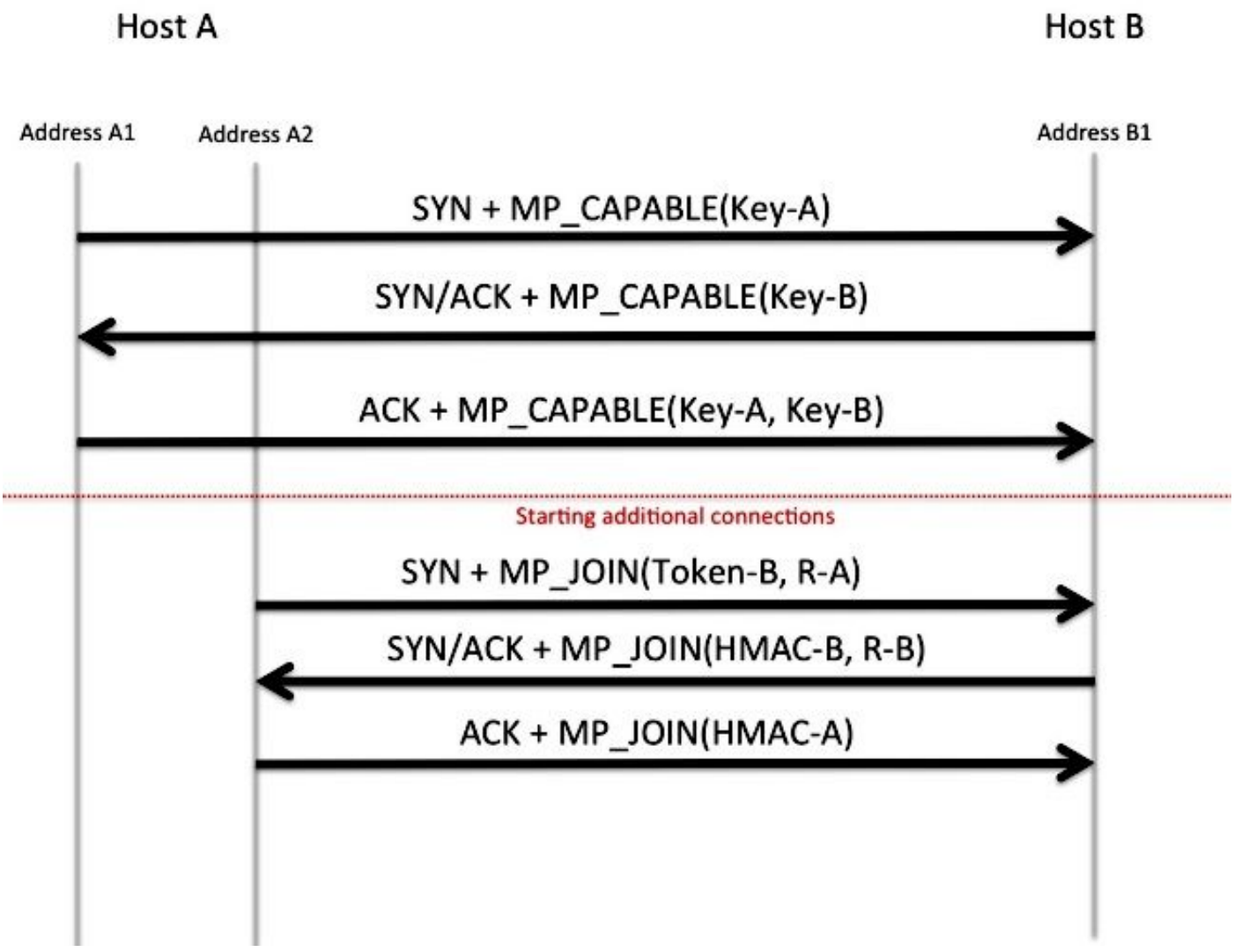
Sessiebedrijf

MPTCP gebruikt TCP-opties om te onderhandelen en de scheiding en hermontage van gegevens over de meerdere substromen te orkestreren. **TCP-optie 30** is voorbehouden aan de Internet Assigned Numbers Authority (IANA) voor exclusief gebruik door MPTCP. Raadpleeg [TCP-parameters (Transmission Control Protocol)] voor meer informatie. In de vestiging van een regelmatige TCP sessie, is een **MP_CAPABLE** optie in het eerste synchrone (SYN) pakket opgenomen. Als de responder zich ondersteunt en kiest om over MPTCP te onderhandelen, reageert hij ook met de **MP_CAPABLE** optie in het SYN-recognition (ACK) pakje. De toetsen die binnen deze handdruk worden uitgewisseld, worden in de toekomst gebruikt om de verbinding en

verwijdering van andere TCP-sessies naar deze MPTCP-flow te authentiseren.

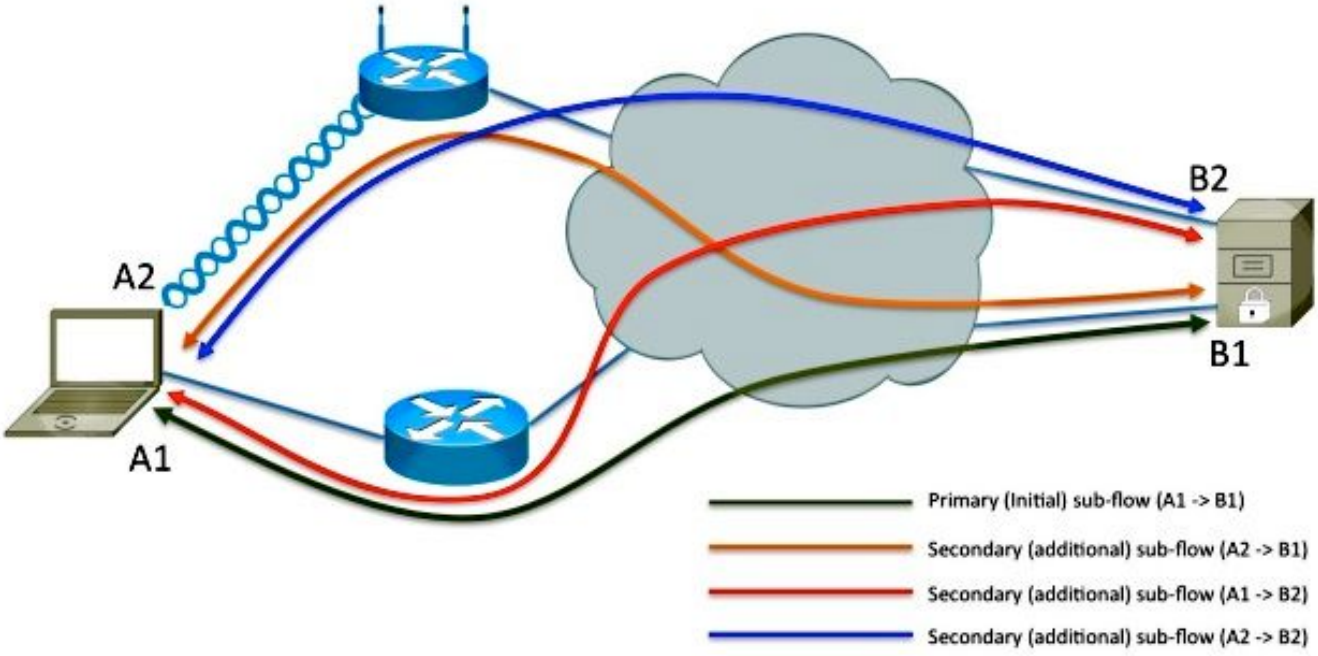
Extra substromen samenvoegen

Indien nodig kan **Host-A** aanvullende substromen initiëren, afkomstig van een andere interface of adres naar **Host-B**. Net als bij de eerste sub-flow worden TCP-opties gebruikt om aan te geven dat deze sub-flow met de andere sub-flow wil samenvoegen. De toetsen die binnen de initiële sub-flow vestiging (samen met een hashing algoritme) worden uitgewisseld, worden door **Host-B** gebruikt om te bevestigen dat het aansluitende verzoek inderdaad door **Host-A** wordt verzonden. De secundaire sub-flow 4-tuple (bron IP, bestemming IP, bronpoort en doelpoort) is anders dan die van de primaire sub-flow; deze stroom zou een ander pad door het netwerk kunnen leiden .



Adres toevoegen

Host-A heeft meerdere interfaces, en het is mogelijk dat **Host-B** meerdere netwerkverbindingen heeft. **Host-B** leert over de adressen A1 en A2 impliciet als resultaat van **Host-A**-bronsubstromen vanuit elk van zijn adressen bestemd voor B1. Het is mogelijk dat **Host-B** zijn aanvullende adres (B2) naar **Host-A** adverteert zodat andere substromen naar B2 worden uitgevoerd. Dit wordt voltooid via **TCP optie 30** 2. Zoals in dit diagram wordt getoond, adverteert Host-B zijn secundaire adres (B2) aan Host-A, en worden er twee extra substromen gecreëerd. Omdat MPTCP boven de netwerklaag van de OSI-stack (Open System Interconnect) werkt, kunnen de IP-adressen die worden geadverteerd IPv4, IPv6 of beide zijn. Het is mogelijk dat een deel van de substromen gelijktijdig per IPv4 wordt vervoerd, aangezien andere substromen per IPv6 worden vervoerd.



Segmentering, multipath en reassemblering

Een gegevensstroom die door de toepassing aan MPTCP wordt gegeven, moet door de zender worden gesegmenteerd en verdeeld over de meerdere sub-stromen. Het moet vervolgens opnieuw worden geassembleerd in de enkele gegevensstroom voordat het terug naar de toepassing wordt geleverd.

MPTCP inspecteert de prestaties en de latentie van elke substroom en past dynamisch de distributie van gegevens aan om de hoogste geaggregeerde doorvoersnelheid te bereiken. Tijdens gegevensoverdracht omvat de TCP headeroptie informatie over de MPTCP sequentie/ontvangstnummers, de huidige sub-flow sequentie/erkenningsnummer en een checksum.

Gevolgen voor de stroominspectie

Veel beveiligingsapparaten kunnen de onbekende TCP-opties nul-uitbellen of vervangen door een NOOP-waarde (No Option). Als het netwerkapparaat dit aan het TCP SYN-pakket op de eerste sub-flow doet, wordt de **MP_CAPABLE** advertentie verwijderd. Als resultaat hiervan, lijkt het op de server dat de client geen MPTCP ondersteunt en keert deze terug naar de normale TCP handeling.

Als de optie geconserveerd is en MPTCP meerdere sub-stromen kan inline pakketanalyse door netwerkapparaten niet betrouwbaar functioneren. Dit komt doordat slechts een deel van de gegevensstroom naar elke substroom wordt overgebracht. Het effect van protocolinspectie op MPTCP kan van niets tot volledige verstoring van de service variëren. Het effect varieert afhankelijk van wat en hoeveel gegevens worden geïnspecteerd. Packet-analyse kan betrekking hebben op Firewalltoepassingsgateway (ALG of fixup), Network-adresomzetting (NAT) ALG, Application Visibility and Control (AVC), Network-Based Application Recognition (NBAR) of inbraakdetectieservice (IDS/IPS). Als de toepassing inspectie in uw omgeving vereist is, wordt aanbevolen om **TCP optie 30** op te ruimen.

Als de stroom niet kan worden geïnspecteerd vanwege encryptie of als het protocol onbekend is,

dan zou het inline apparaat geen impact moeten hebben op de MPTCP-stroom.

Cisco-producten die door MPTCP zijn beïnvloed

Deze producten hebben invloed op MPTCP:

- Adaptieve security applicatie (ASA)
- Cisco Firepower Threat Defense
- Inbraakpreventiesysteem (IPS)
- Cisco IOS-XE en IOS®
- Application Control Engine

Elk product wordt in latere secties van dit document uitvoerig beschreven.

ASA

TCP-bewerkingen

Standaard vervangt de Cisco ASA-firewall niet-ondersteunde TCP-opties, die de **MPTCP-optie 30** omvatten, met de NOOP-optie (optie 1). Gebruik deze configuratie om de MPTCP-optie toe te staan:

1. Defineert het beleid om **TCP optie 30** toe te staan (gebruikt door MPTCP) door het apparaat:

```
tcp-map my-mptcp
   tcp-options range 30 30 allow
```

2. Bepaal de selectie van het verkeer:

```
class-map my-tcpnorm
   match any
```

3. Defineert een kaart van verkeer naar actie:

```
policy-map my-policy-map
   class my-tcpnorm
       set connection advanced-options my-mptcp
```

4. Activeert het in het vak of per interface:

```
service-policy my-policy-map global
```

Protocolinspectie

De ASA ondersteunt inspectie van vele protocollen. Het effect dat de inspectiemotor op de toepassing kan hebben, varieert. Aanbevolen wordt, als inspectie vereist is, de eerder beschreven TCP-map NIET toe te passen.

Cisco Firepower Threat Defense

TCP-bewerkingen

Aangezien de FTD diepe pakketinspectie voor IPS/IDS services uitvoert wordt het niet aanbevolen

om de TCP-optie te wijzigen in de TCP-kaart om deze mogelijk te maken.

Cisco IOS Firewall

Context-gebaseerde toegangscontrole (CBAC)

CBAC verwijdert de TCP-opties niet uit de TCP-stream. MPTCP bouwt een verbinding door de firewall.

Zone-gebaseerde firewall (ZBFW)

Cisco IOS en IOS-XE ZBFW verwijderen de TCP-opties niet uit de TCP-stream. MPTCP bouwt een verbinding door de firewall.

ACE

Standaard wordt het ACE-apparaat de TCP-opties uit de TCP-verbindingen verwijderd. De MPTCP-verbinding wordt teruggebracht naar reguliere TCP-bewerkingen.

Het ACE-apparaat kan worden geconfigureerd om de TCP-opties in te schakelen via de opdracht **TCP-opties**, zoals beschreven in de configureren hoe ACE TCP-opties hanteert in het gedeelte Security Guide vA5(1.0), Cisco ACE Application Control Engine. Dit wordt echter niet altijd aanbevolen, omdat de secundaire sub-stromen in evenwicht kunnen zijn met verschillende real-servers en de aansluiting mislukt.

Cisco-producten die niet door MPTCP zijn beïnvloed

Over het algemeen verandert elk apparaat dat TCP stromen of Layer 7 informatie niet inspecteert ook de TCP opties niet en zou dientengevolge transparant moeten zijn om MPTCP te controleren. Deze apparaten kunnen het volgende omvatten:

- Cisco 5000 Series ASR's (start)
- Wide Area Application Services (WAAS)
- Carrier-Grade NAT (CGN) (Carrier-Grade Services Engine (CGSE) blade in Carrier Routing System (CRS)-1
- Alle Ethernet-switchproducten
- Alle routerproducten (tenzij firewall of NAT-functionaliteit is ingeschakeld); zie Cisco-producten die door MPTCP zijn beïnvloed eerder in het document voor meer informatie)