Présentation de l'assistance produit et MPTCP

Contenu

Introduction

Ce document fournit une vue d'ensemble du protocole TCP multichemin (MPTCP), de son impact sur l'inspection de flux et des produits Cisco qui sont et ne sont pas affectés par ce protocole.

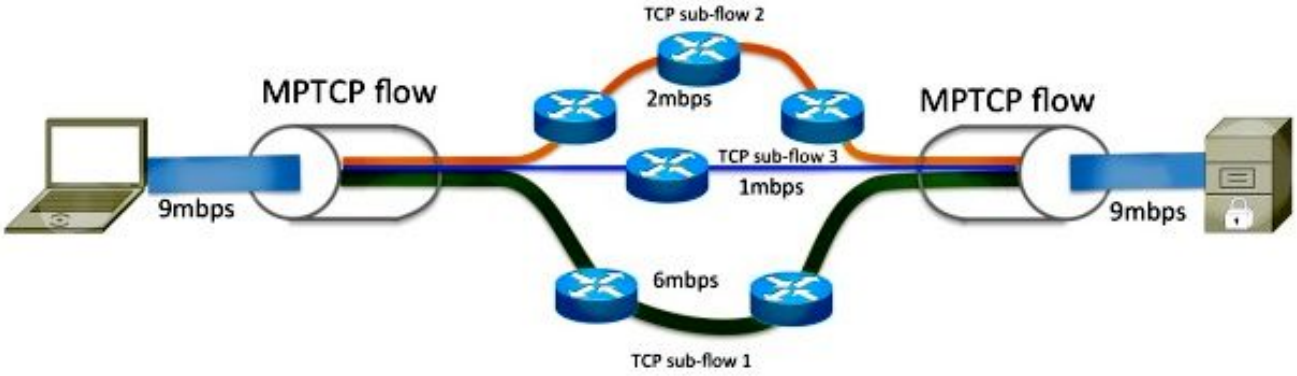
Présentation du protocole MPTCP

Informations générales

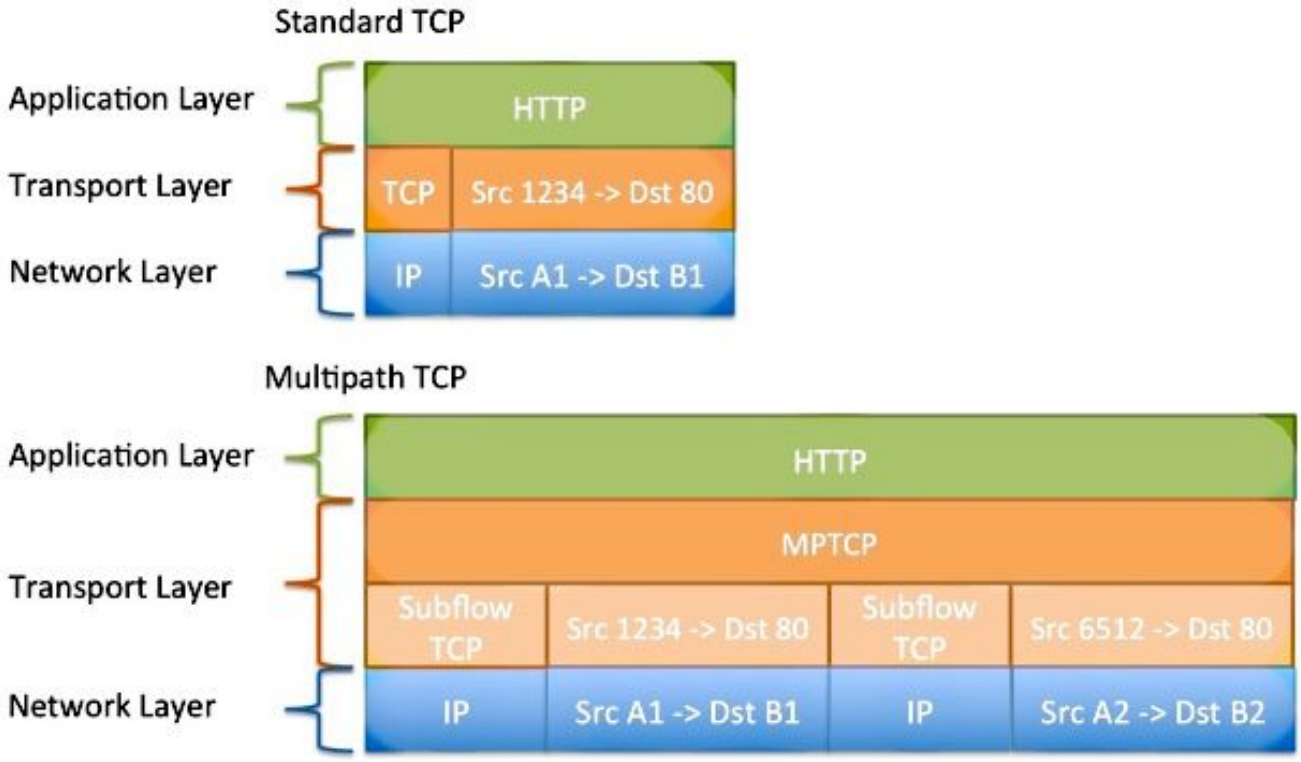
Les hôtes connectés à Internet ou dans un environnement de data center sont souvent connectés par plusieurs chemins. Cependant, lorsque le protocole TCP est utilisé pour le transport de données, la communication est limitée à un seul chemin réseau. Il est possible que certains chemins entre les deux hôtes soient congestionnés, alors que d'autres chemins sont sous-utilisés. Une utilisation plus efficace des ressources réseau est possible si ces chemins multiples sont utilisés simultanément. En outre, l'utilisation de plusieurs connexions améliore l'expérience utilisateur, car elle offre un débit plus élevé et une résilience améliorée contre les pannes de réseau.

Le protocole MPTCP est un ensemble d'extensions du protocole TCP standard qui permet de séparer un flux de données unique et de le transporter sur plusieurs connexions. Reportez-vous à RFC6824 : Extensions TCP pour le fonctionnement à chemins multiples avec plusieurs adresses pour plus d'informations.

Comme l'illustre ce schéma, MPTCP est capable de séparer le flux de 9 Mbits/s en trois sous-flux différents sur le noeud expéditeur, qui est ensuite agrégé de nouveau dans le flux de données d'origine sur le noeud récepteur.



Les données qui entrent dans la connexion MPTCP agissent exactement comme par le biais d'une connexion TCP régulière ; les données transmises ont garanti une livraison dans l'ordre. Puisque MPTCP ajuste la pile réseau et fonctionne au sein de la couche transport, il est utilisé de manière transparente par l'application.



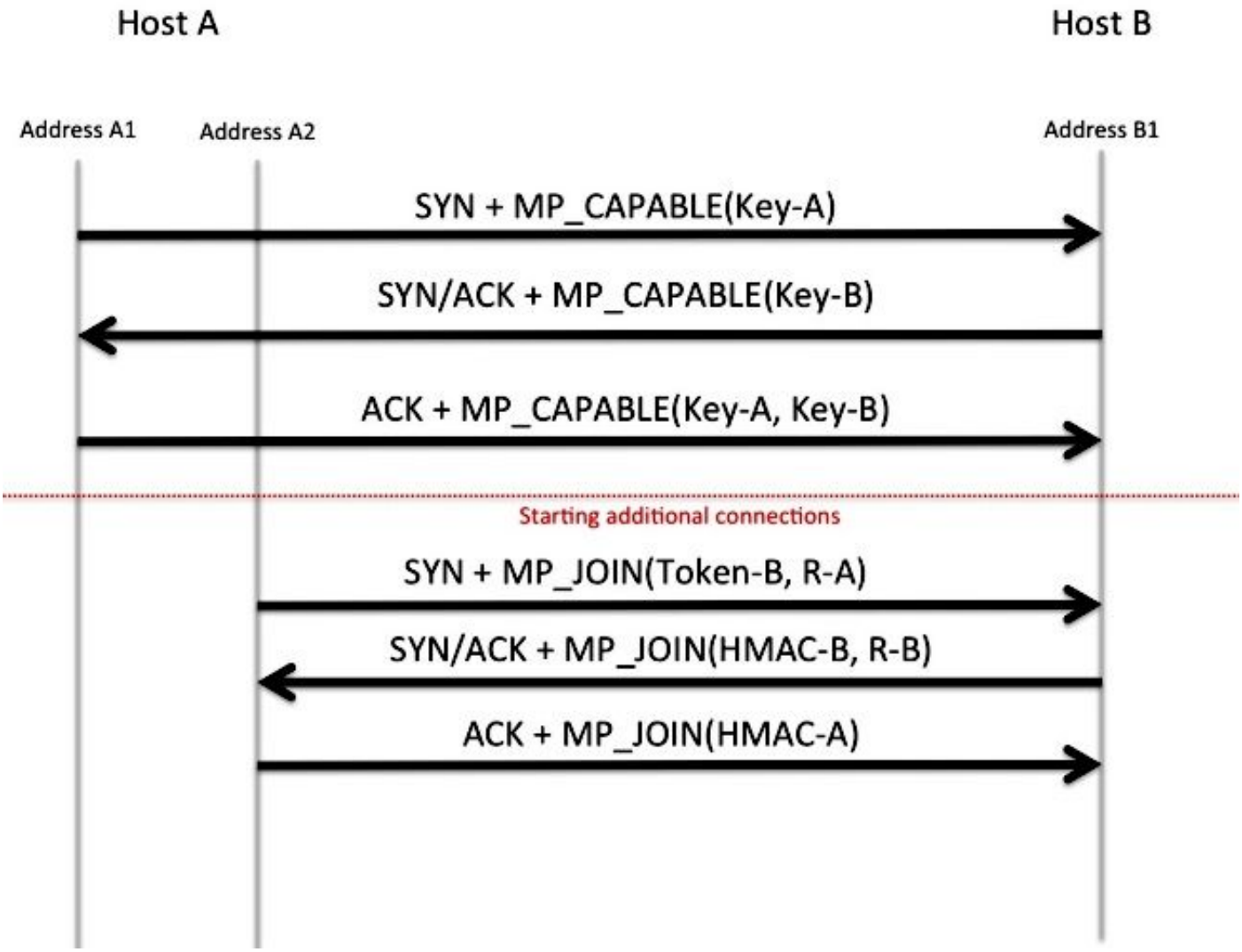
Établissement de la session

MPTCP utilise des options TCP afin de négocier et d'orchestrer la séparation et le réassemblage des données sur les sous-flux multiples. **L'option TCP 30** est réservée par l'IANA (Internet Assigned Numbers Authority) pour une utilisation exclusive par MPTCP. Référez-vous à Paramètres TCP (Transmission Control Protocol) pour plus d'informations. Lors de l'établissement d'une session TCP régulière, une option **MP_CAPABLE** est incluse dans le paquet SYN (Synchronize initial). Si le répondeur prend en charge et choisit de négocier MPTCP, il répond également avec l'option **MP_CAPABLE** dans le paquet SYN-accuse (ACK). Les clés échangées

dans cette connexion seront utilisées ultérieurement afin d'authentifier la jointure et la suppression d'autres sessions TCP dans ce flux MPTCP.

Joindre des sous-flux supplémentaires

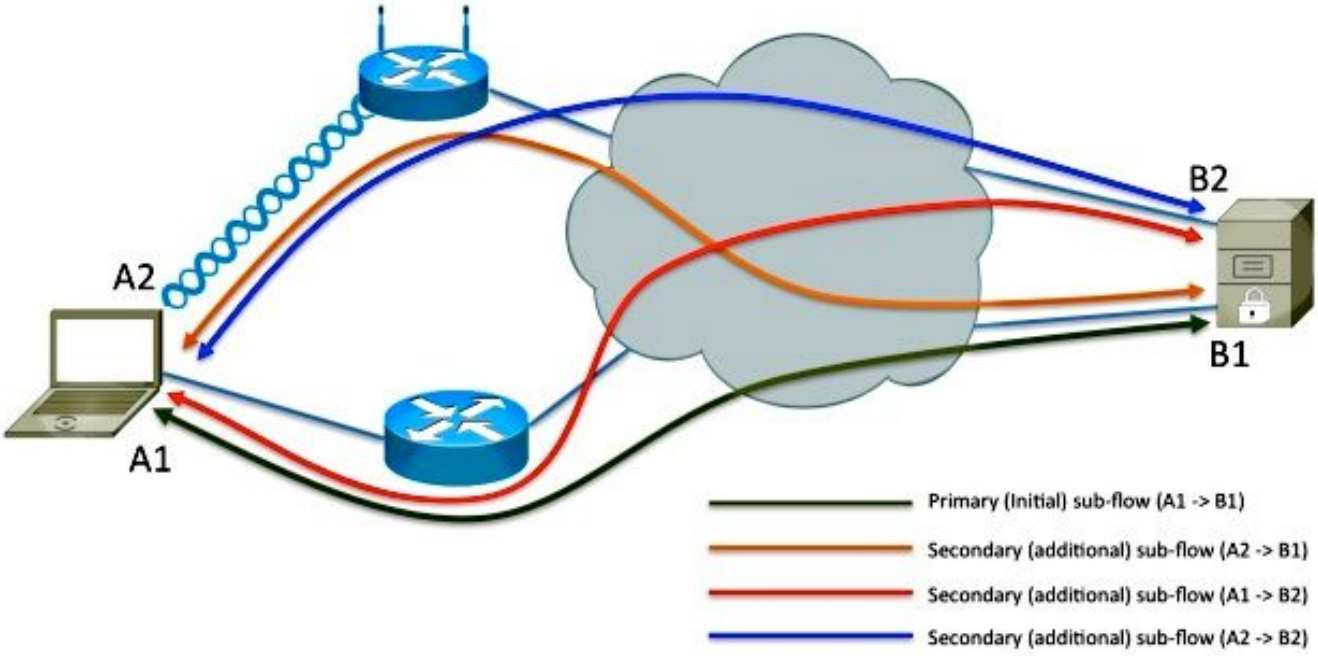
Lorsque cela est jugé nécessaire, **l'hôte A** peut initier des sous-flux supplémentaires provenant d'une autre interface ou adresse vers **l'hôte B**. Comme pour le sous-flux initial, les options TCP sont utilisées afin d'indiquer le désir de fusionner ce sous-flux avec l'autre sous-flux. Les clés échangées dans l'établissement initial du sous-flux (avec un algorithme de hachage) sont utilisées par **Host-B** afin de confirmer que la demande de jointure est effectivement envoyée par **Host-A**. Le sous-flux secondaire 4-tuple (IP source, IP de destination, port source et port de destination) est différent de celui du sous-flux principal ; ce flux peut emprunter un chemin différent à travers le réseau.



Ajouter une adresse

L'hôte A a plusieurs interfaces et il est possible que **l'hôte B** ait plusieurs connexions réseau. **L'hôte B** apprend implicitement les adresses A1 et A2 en raison des sous-flux d'approvisionnement de **l'hôte A** à partir de chacune de ses adresses destinées à B1. Il est possible que **Host-B** annonce son adresse supplémentaire (B2) à **Host-A** afin que d'autres sous-flux soient effectués vers B2. Ceci est effectué via l'**option TCP 30**. Comme le montre ce diagramme, **l'hôte B** annonce son adresse secondaire (B2) à **l'hôte A**, et deux sous-flux supplémentaires sont créés. Étant donné que MPTCP fonctionne au-dessus de la couche réseau

de la pile OSI (Open System Interconnection), les adresses IP annoncées peuvent être IPv4, IPv6 ou les deux. Il est possible que certains des sous-flux soient transportés par IPv4 simultanément lorsque d'autres sous-flux sont transportés par IPv6.



Segmentation, multichemin et réassemblage

Un flux de données donné à MPTCP par l'application doit être segmenté et distribué par l'expéditeur sur les différents sous-flux. Il doit ensuite être réassemblé dans le flux de données unique avant d'être remis à l'application.

Le protocole MPTCP inspecte les performances et la latence de chaque sous-flux et ajuste dynamiquement la distribution des données afin d'obtenir le débit agrégé le plus élevé. Lors du transfert de données, l'option d'en-tête TCP inclut des informations sur les numéros de séquence/accusé de réception MPTCP, le numéro de séquence/accusé de réception de sous-flux actuel et une somme de contrôle.

Impact sur l'inspection des flux

De nombreux périphériques de sécurité peuvent supprimer ou remplacer les options TCP inconnues par une valeur NOOP (No Option). Si le périphérique réseau fait cela au paquet SYN TCP sur le sous-flux initial, l'annonce **MP_CAPABLE** est supprimée. Par conséquent, il apparaît au serveur que le client ne prend pas en charge le protocole MPTCP et qu'il revient à un fonctionnement TCP normal.

Si l'option est conservée et que MPTCP est capable d'établir plusieurs sous-flux, l'analyse des paquets en ligne par les périphériques réseau risque de ne pas fonctionner de manière fiable. En effet, seules des parties du flux de données sont transportées vers chaque sous-flux. L'effet de l'inspection de protocole sur le protocole MPTCP peut varier de rien à toute interruption de service. L'effet varie selon le type et la quantité de données inspectées. L'analyse des paquets peut inclure la passerelle de couche application (ALG ou fixup) du pare-feu, la traduction d'adresses réseau (NAT) ALG, la visibilité et le contrôle des applications (AVC), la reconnaissance des applications réseau (NBAR) ou les services de détection des intrusions (IDS/IPS). Si

l'inspection des applications est requise dans votre environnement, il est recommandé d'activer la suppression de l'**option TCP 30**.

Si le flux ne peut pas être inspecté en raison du chiffrement ou si le protocole est inconnu, alors le périphérique en ligne ne devrait avoir aucun impact sur le flux MPTCP.

Produits Cisco affectés par MPTCP

Ces produits sont affectés par MPTCP :

- Appareil de sécurité adaptatif (ASA)
- Cisco Firepower Threat Defense
- Système de prévention des intrusions (IPS)
- Cisco IOS-XE et IOS®
- Moteur de contrôle des applications (ACE)

Chaque produit est décrit en détail dans les sections suivantes de ce document.

ASA

Opérations TCP

Par défaut, le pare-feu Cisco ASA remplace les options TCP non prises en charge, qui incluent l'**option MPTCP 30**, par l'option NOOP (option 1). Afin d'autoriser l'option MPTCP, utilisez cette configuration :

1. Définissez la stratégie afin d'autoriser l'**option TCP 30** (utilisée par MPTCP) via le périphérique :

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

2. Définissez la sélection du trafic :

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

3. Définissez une carte du trafic à l'action :

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

4. Activez-le sur la boîte ou par interface :

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

Inspection du protocole

L'ASA prend en charge l'inspection de nombreux protocoles. L'effet que le moteur d'inspection peut avoir sur l'application varie. Il est recommandé que, si une inspection est requise, la carte TCP décrite précédemment ne soit PAS appliquée.

Cisco Firepower Threat Defense

Opérations TCP

Étant donné que le FTD effectue une inspection approfondie des paquets pour les services IPS/IDS, il n'est pas recommandé de modifier le tcp-map pour autoriser l'option TCP à passer.

Cisco IOS Firewall

Contrôle d'accès basé sur le contexte (CBAC)

CBAC ne supprime pas les options TCP du flux TCP. Le protocole MPTCP établit une connexion via le pare-feu.

Pare-feu basé sur une zone (ZBFW)

Cisco IOS et IOS-XE ZBFW ne suppriment pas les options TCP du flux TCP. Le protocole MPTCP établit une connexion via le pare-feu.

ACE

Par défaut, le périphérique ACE supprime les options TCP des connexions TCP. La connexion MPTCP revient aux opérations TCP régulières.

Le périphérique ACE peut être configuré pour autoriser les options TCP via la commande **tcp-options**, comme décrit dans la section Configuration du traitement des options TCP par ACE du Guide de sécurité vA5(1.0), Cisco ACE Application Control Engine. Cependant, cela n'est pas toujours recommandé, car les sous-flux secondaires peuvent être équilibrés avec différents serveurs réels et la jointure échoue.

Produits Cisco non affectés par MPTCP

En règle générale, tout périphérique qui n'inspecte pas les flux TCP ou les informations de couche 7 ne modifie pas les options TCP et doit donc être transparent pour MPTCP. Ces périphériques peuvent inclure :

- Gamme Cisco 5000 ASR (Starent)
- Services d’applications de réseau étendu (WAAS)
- NAT de niveau opérateur (CGN) (lame CGSE (Carrier-Grade Services Engine) dans CRS-1 (Carrier Routing System)
- Tous les produits de commutation Ethernet
- Tous les produits de routeur (sauf si la fonctionnalité de pare-feu ou NAT est activée); pour plus d'informations, reportez-vous à la section Produits Cisco affectés par le protocole MPTCP ci-dessus).