MPTCP- und Produkt-Support - Übersicht

Inhalt

Einführung

Dieses Dokument bietet eine Übersicht über Multipath TCP (MPTCP), seine Auswirkungen auf die Flow Inspection und die Cisco Produkte, die davon betroffen sind und nicht davon betroffen sind.

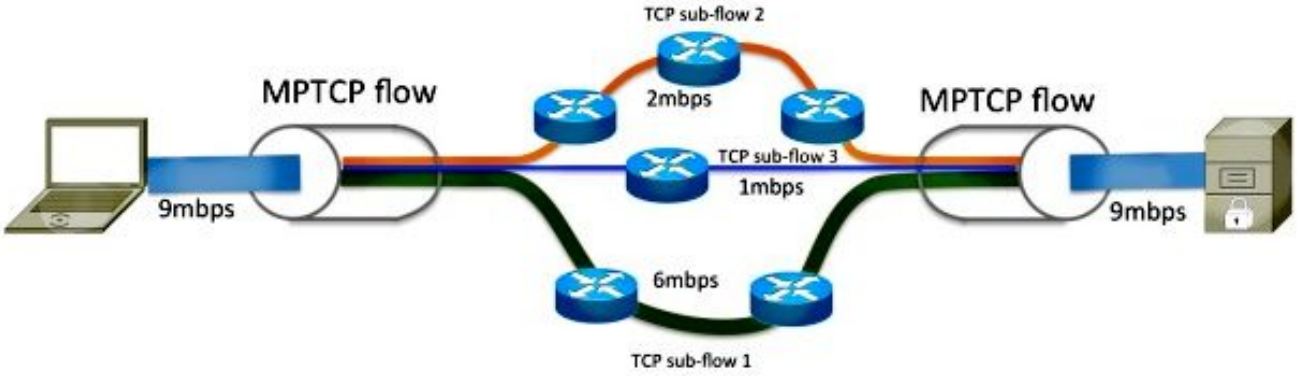
MPTCP - Übersicht

Hintergrundinformationen

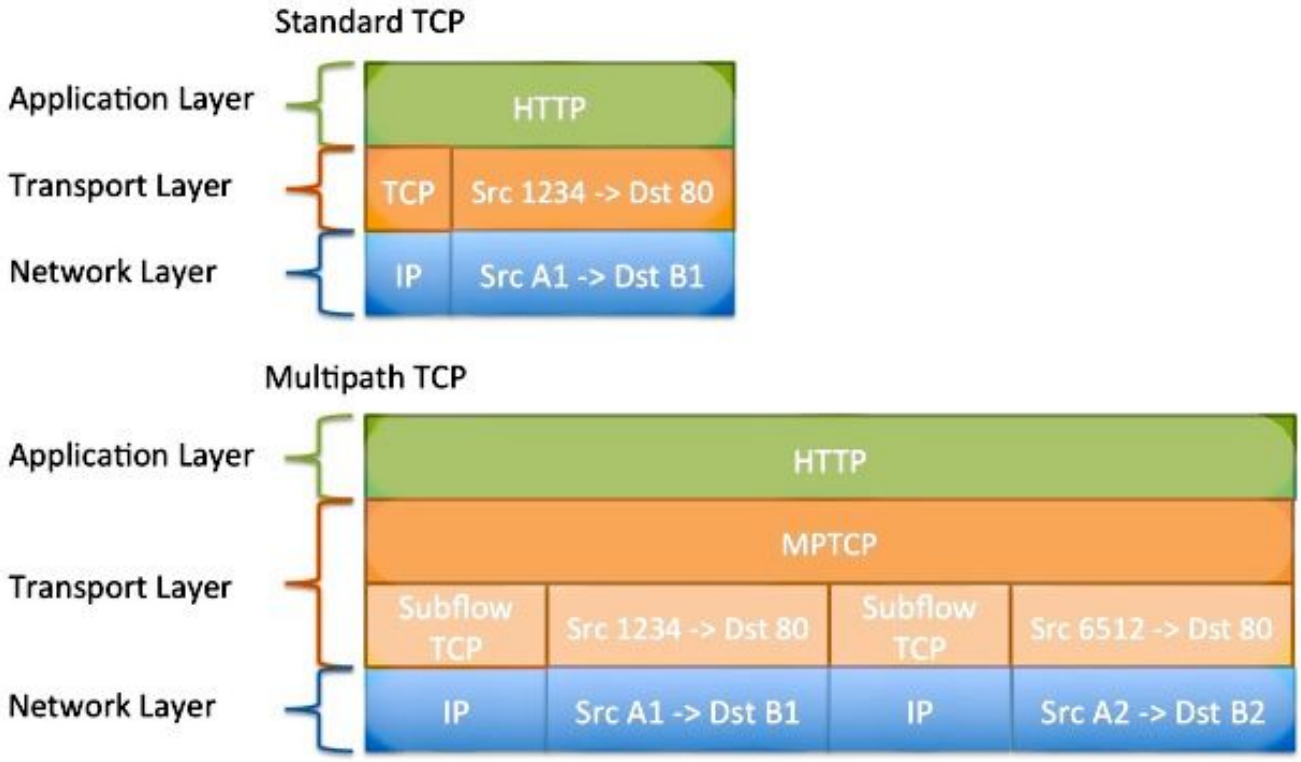
Hosts, die mit dem Internet oder in einer Rechenzentrumsumgebung verbunden sind, sind häufig über mehrere Pfade verbunden. Wenn TCP jedoch für die Datenübertragung verwendet wird, ist die Kommunikation auf einen einzelnen Netzwerkpfad beschränkt. Es ist möglich, dass einige Pfade zwischen den beiden Hosts überlastet sind, während alternative Pfade nicht ausgelastet sind. Eine effizientere Nutzung von Netzwerkressourcen ist möglich, wenn diese mehrere Pfade gleichzeitig verwendet werden. Darüber hinaus wird durch die Verwendung mehrerer Verbindungen das Anwendererlebnis verbessert, da der Durchsatz erhöht und die Ausfallsicherheit bei Netzwerkausfällen verbessert wird.

MPTCP ist ein Satz von Erweiterungen für reguläre TCP-Verbindungen, die die Trennung und Übertragung eines einzelnen Datenflusses über mehrere Verbindungen ermöglichen. Siehe RFC6824: TCP-Erweiterungen für Multipath-Betrieb mit mehreren Adressen für weitere Informationen.

Wie in diesem Diagramm gezeigt, kann MPTCP den Datenfluss von 9 Mbit/s in drei verschiedene Subflüsse auf dem Senderknoten aufteilen, die anschließend wieder in den ursprünglichen Datenfluss auf dem empfangenden Knoten aggregiert werden.



Die Daten, die in die MPTCP-Verbindung eingegeben werden, funktionieren genau wie über eine reguläre TCP-Verbindung. die übermittelten Daten garantierten eine ordnungsgemäße Zustellung. Da MPTCP den Netzwerk-Stack anpasst und innerhalb der Transportschicht arbeitet, wird es von der Anwendung transparent verwendet.



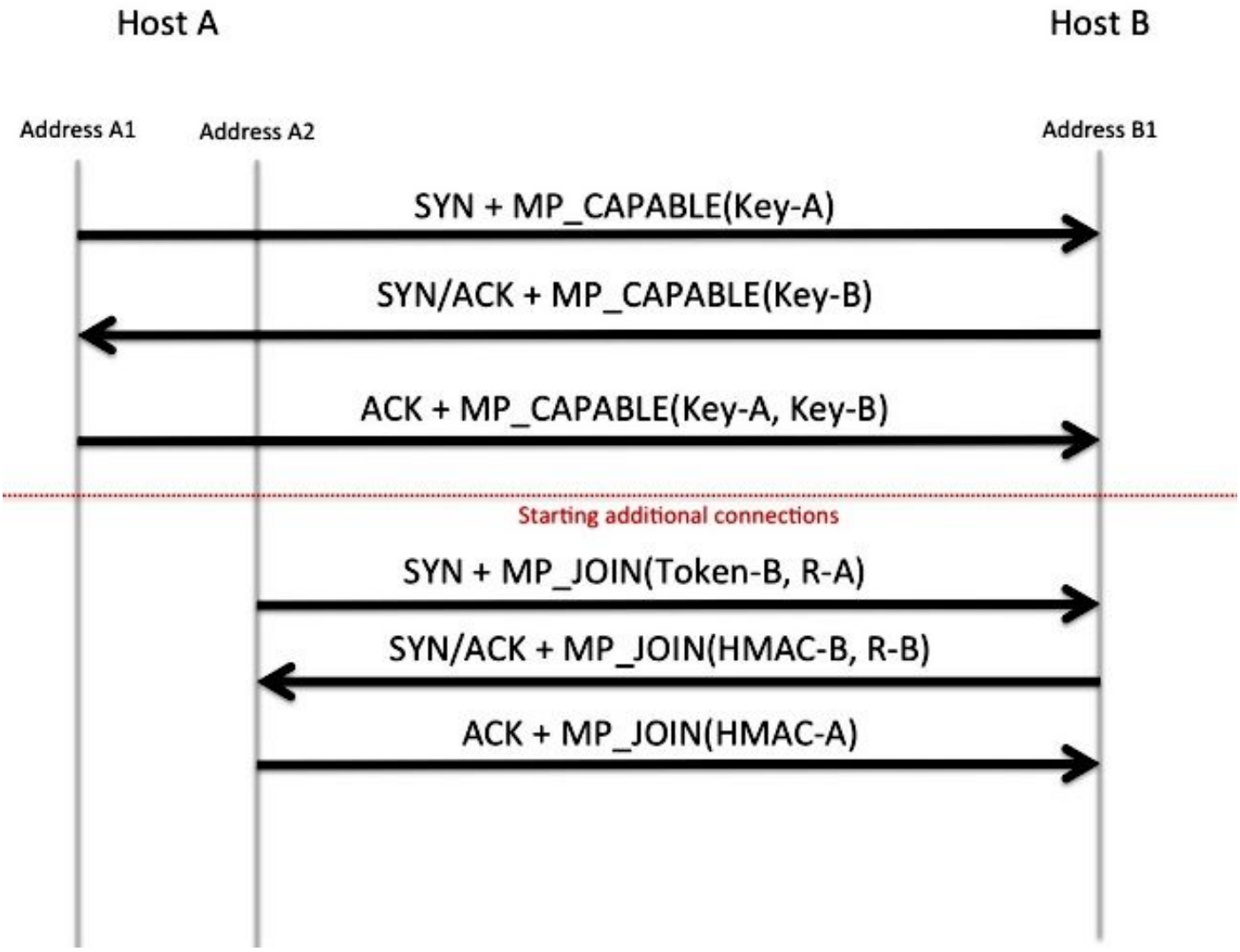
Sitzungsaufbau

MPTCP nutzt TCP-Optionen, um die Trennung und Reassemblierung von Daten über die verschiedenen Subflows zu verhandeln und zu orchestrieren. **Die TCP-Option 30** ist der Internet Assigned Numbers Authority (IANA) zur ausschließlichen Verwendung durch MPTCP vorbehalten. Weitere Informationen finden Sie unter Transmission Control Protocol (TCP)-Parameter. Beim Einrichten einer regulären TCP-Sitzung ist eine **MP_CAPABLE**-Option im ersten SYN-Paket (Synchronize) enthalten. Wenn der Responder MPTCP unterstützt und verhandelt, antwortet er auch mit der **MP_CAPABLE-**Option im SYN-Bestätigungs-Paket (ACK). Die in diesem Handshake

ausgetauschten Schlüssel werden zukünftig verwendet, um das Hinzufügen und Entfernen anderer TCP-Sitzungen in diesem MPTCP-Fluss zu authentifizieren.

Zusätzliche Sub-Flows beitreten

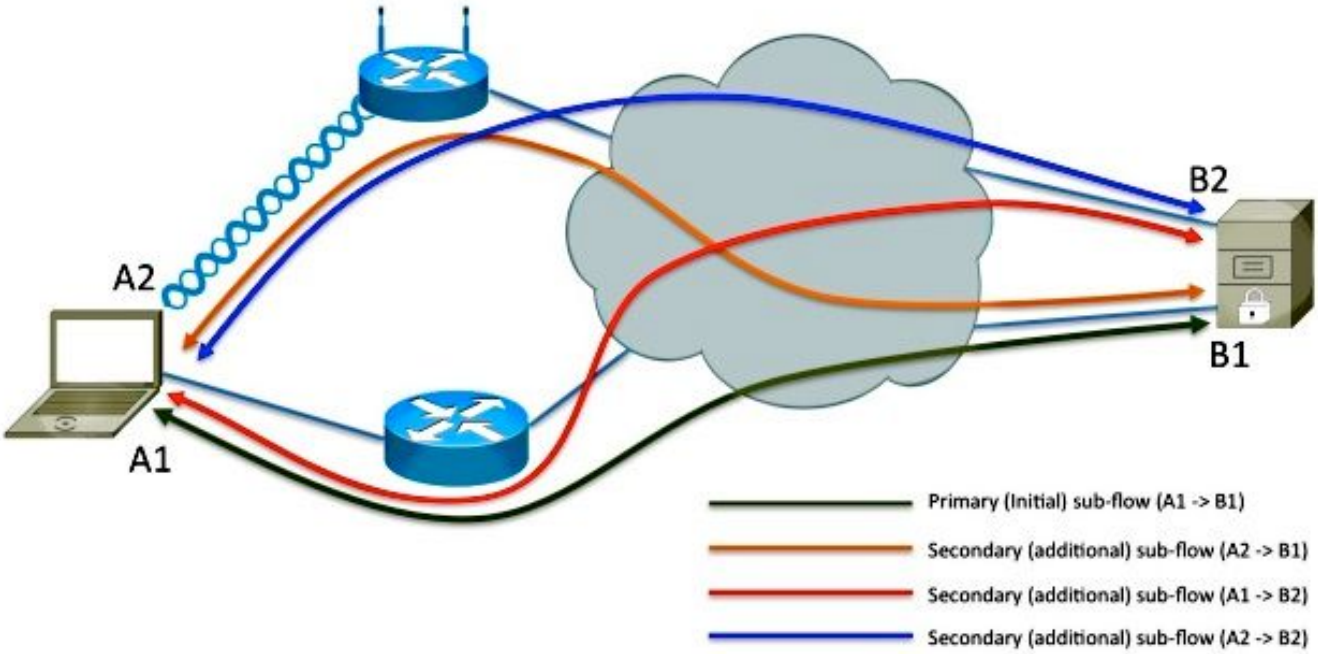
Wenn dies für notwendig erachtet wird, kann **Host-A** zusätzliche Subflows initiieren, die von einer anderen Schnittstelle oder Adresse an **Host-B** stammen. Wie beim ersten Subflow werden auch hier TCP-Optionen verwendet, um anzugeben, ob dieser Substrom mit dem anderen Subflow zusammengeführt werden soll. Die Schlüssel, die innerhalb der anfänglichen Sub-Flow-Einrichtung ausgetauscht werden (zusammen mit einem Hashing-Algorithmus), werden von **Host-B** verwendet, um zu bestätigen, dass die Join-Anforderung tatsächlich von **Host-A** gesendet wird. Der sekundäre Sub-Flow 4-Tupel (Quell-IP, Ziel-IP, Quell-Port und Ziel-Port) unterscheidet sich von dem des primären Subflusses. Dieser Datenfluss kann einen anderen Pfad durch das Netzwerk annehmen.



Adresse hinzufügen

Host-A hat mehrere Schnittstellen, und es ist möglich, dass **Host-B** über mehrere Netzwerkverbindungen verfügt. **Host-B** erfährt implizit durch **Host-A-**Sourcing-Subströme von jeder Adresse, die für B1 bestimmt ist, von den Adressen A1 und A2. Es ist möglich, dass **Host-B** seine zusätzliche Adresse (B2) an **Host-A** meldet, sodass andere Sub-Flows an B2 gesendet werden. Dies wird über die **TCP-Option 30** abgeschlossen. Wie in diesem Diagramm gezeigt, kündigt **Host-B** seine sekundäre Adresse (B2) an **Host-A**, und es werden zwei zusätzliche

Unterflüsse erstellt. Da MPTCP über der Netzwerkebene des OSI-Stacks (Open System Interconnection) betrieben wird, können die angegebenen IP-Adressen IPv4, IPv6 oder beides sein. Es ist möglich, dass ein Teil der Subströme gleichzeitig über IPv4 transportiert wird, während andere Subströme über IPv6 transportiert werden.



Segmentierung, Multipath und Reassemblierung

Ein von der Anwendung an MPTCP übergebener Datenstrom muss segmentiert und durch den Absender auf mehrere Subflüsse verteilt werden. Anschließend muss sie in einem einzigen Datenstrom ream wieder zusammengesetzt werden, bevor sie an die Anwendung zurückgesendet wird.

MPTCP überprüft die Leistung und Latenz jedes Subflusses und passt die Datenverteilung dynamisch an, um den höchsten aggregierten Durchsatz zu erzielen. Während der Datenübertragung enthält die TCP-Kopfzeilenoption Informationen über die MPTCP-Sequenz/Bestätigungsnummer, die aktuelle Folge-/Bestätigungsnummer des Unterflusses und eine Prüfsumme.

Auswirkungen auf Flow Inspection

Viele Sicherheitsgeräte können unbekannte TCP-Optionen durch einen NOOP-Wert (No Option) ersetzen. Wenn das Netzwerkgerät dies mit dem TCP-SYN-Paket auf dem ursprünglichen Subflow durchführt, wird das **MP_CAPABLE-**Advertisement entfernt. Daraus ergibt sich, dass der Client MPTCP nicht unterstützt und zum normalen TCP-Betrieb zurückkehrt.

Wenn die Option erhalten bleibt und MPTCP mehrere Sub-Flows erstellen kann, funktioniert die In-Line-Paketanalyse durch Netzwerkgeräte möglicherweise nicht zuverlässig. Der Grund hierfür ist, dass nur Teile des Datenflusses auf jeden Unterfluss übertragen werden. Die Auswirkungen der Protokollüberprüfung auf MPTCP können von nichts bis hin zu einer vollständigen Dienstunterbrechung variieren. Die Auswirkungen variieren je nach Art und Umfang der zu untersuchenden Daten. Die Paketanalyse kann Firewall Application Layer Gateway (ALG oder Fixup), Network Address Translation (NAT) ALG, Application Visibility and Control (AVC), Network

Based Application Recognition (NBAR) oder Intrusion Detection Services (IDS/IPS) umfassen. Wenn in Ihrer Umgebung eine Anwendungsprüfung erforderlich ist, wird empfohlen, die **TCP-Option 30** zu deaktivieren.

Wenn der Datenfluss aufgrund von Verschlüsselung nicht überprüft werden kann oder das Protokoll unbekannt ist, sollte das Inline-Gerät keine Auswirkungen auf den MPTCP-Datenfluss haben.

Von MPTCP betroffene Cisco Produkte

Diese Produkte sind von MPTCP betroffen:

- Adaptive Security Appliance (ASA)
- Cisco FirePOWER Threat Defense
- Intrusion Prevention System (IPS)
- Cisco IOS-XE und IOS®
- Application Control Engine (ACE)

Jedes Produkt wird in den nachfolgenden Abschnitten dieses Dokuments detailliert beschrieben.

ASA

TCP-Prozesse

Standardmäßig ersetzt die Cisco ASA-Firewall nicht unterstützte TCP-Optionen, darunter die **MPTCP-Option 30**, durch die NOOP-Option (Option 1). Um die MPTCP-Option zuzulassen, verwenden Sie die folgende Konfiguration:

1. Definieren Sie die Richtlinie, um die **TCP-Option 30** (von MPTCP verwendet) über das Gerät zuzulassen:

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

2. Definieren Sie die Datenverkehrsauswahl:

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

3. Erstellen einer Zuordnung von Datenverkehr zu Aktion:

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

4. Aktivieren Sie sie auf dem Gerät oder pro Schnittstelle:

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

Protokollüberprüfung

Die ASA unterstützt die Inspektion einer Vielzahl von Protokollen. Die Auswirkungen der Prüfungs-Engine auf die Anwendung variieren. Wenn eine Überprüfung erforderlich ist, sollte die zuvor beschriebene TCP-Map NICHT angewendet werden.

Cisco FirePOWER Threat Defense

TCP-Prozesse

Da die FTD Deep Packet Inspection für IPS/IDS-Services durchführt, wird nicht empfohlen, die TCP-Map zu ändern, um die TCP-Option durch zuzulassen.

Cisco IOS-Firewall

Kontextbasierte Zugriffskontrolle (CBAC)

CBAC entfernt die TCP-Optionen nicht aus dem TCP-Stream. MPTCP erstellt eine Verbindung über die Firewall.

Zonenbasierte Firewall (ZBFW)

Cisco IOS und IOS-XE ZBFW entfernen die TCP-Optionen nicht aus dem TCP-Stream. MPTCP erstellt eine Verbindung über die Firewall.

ACE

Standardmäßig entfernt das ACE-Gerät TCP-Optionen aus den TCP-Verbindungen. Die MPTCP-Verbindung greift auf reguläre TCP-Vorgänge zurück.

Das ACE-Gerät kann so konfiguriert werden, dass die TCP-Optionen über den Befehl **tcp-options** zugelassen werden, wie im Abschnitt Konfigurieren der Vorgehensweise des ACE bei TCP-Optionen im Abschnitt Sicherheitsleitfaden vA5(1.0), Cisco ACE Application Control Engine, beschrieben. Dies wird jedoch nicht immer empfohlen, da die sekundären Sub-Flows auf verschiedene Realserver verteilt werden können und die Verknüpfung fehlschlägt.

Nicht von MPTCP betroffene Cisco Produkte

Im Allgemeinen ändert jedes Gerät, das keine TCP-Flüsse oder Layer-7-Informationen überprüft, auch keine TCP-Optionen und sollte daher für MPTCP transparent sein. Diese Geräte können Folgendes umfassen:

- Cisco ASRs der Serie 5000 (Starent)
- Wide Area Application Services (WAAS)
- Carrier-Grade NAT (CGN)-Blade (Carrier-Grade Services Engine (CGSE) im Carrier Routing System (CRS)-1
- Alle Ethernet-Switch-Produkte
- Alle Routerprodukte (außer Firewall- oder NAT-Funktionen sind aktiviert) Weitere Informationen finden Sie im Abschnitt zu den Cisco Produkten, die vom MPTCP betroffen sind (siehe Abschnitt weiter oben im Dokument).