Panoramica di MPTCP e del supporto prodotti

Sommario

Introduzione

Questo documento offre una panoramica di Multipath TCP (MPTCP), il suo impatto sull'ispezione del flusso e i prodotti Cisco che sono o non sono interessati da esso.

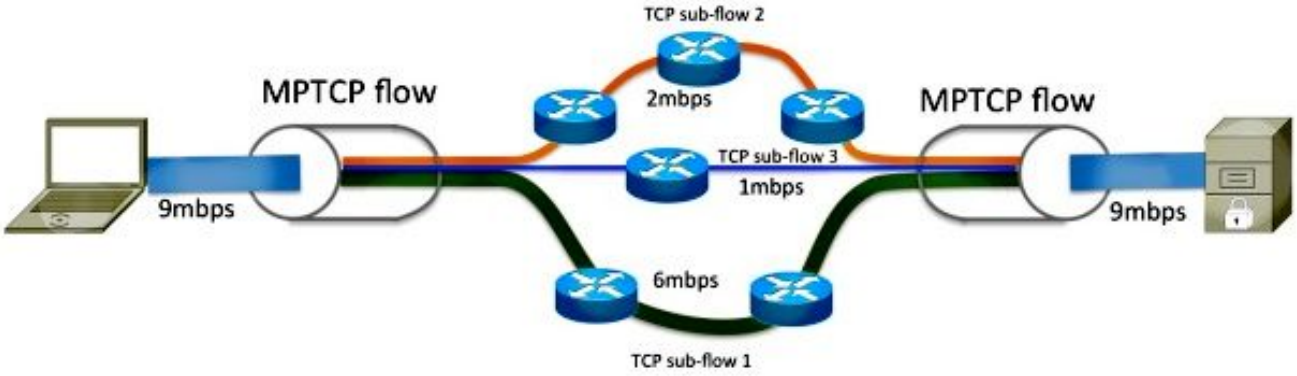
Panoramica di MPTCP

Premesse

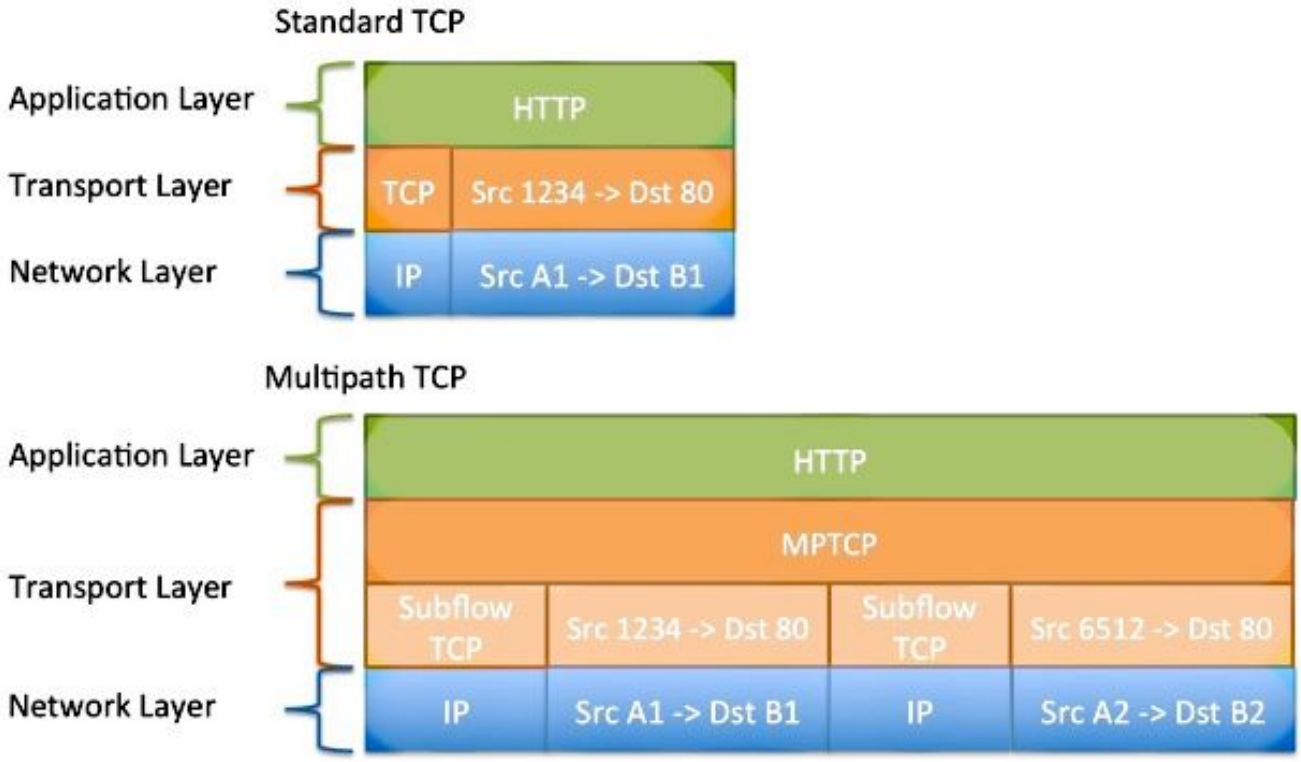
Gli host connessi a Internet o all'interno di un ambiente di data center sono spesso connessi da più percorsi. Tuttavia, quando si utilizza TCP per il trasporto dei dati, la comunicazione è limitata a un singolo percorso di rete. È possibile che alcuni percorsi tra i due host siano congestionati, mentre i percorsi alternativi sono sottoutilizzati. Un utilizzo più efficiente delle risorse di rete è possibile se questi percorsi multipli vengono utilizzati contemporaneamente. Inoltre, l'utilizzo di più connessioni migliora l'esperienza dell'utente, in quanto fornisce un throughput più elevato e una migliore resilienza contro gli errori di rete.

Il protocollo MPTCP è un insieme di estensioni del protocollo TCP standard che consente di separare e trasportare un singolo flusso di dati su più connessioni. Per ulteriori informazioni, fare riferimento alla RFC6824: estensioni TCP per operazioni a percorsi multipli con più indirizzi per ulteriori informazioni.

Come mostrato in questo diagramma, MPTCP è in grado di separare il flusso di 9mbps in tre diversi sotto-flussi sul nodo mittente, che vengono successivamente aggregati nuovamente nel flusso di dati originale sul nodo ricevente.



I dati che entrano nella connessione MPTCP funzionano esattamente come avviene attraverso una normale connessione TCP; i dati trasmessi hanno garantito una consegna in ordine. Poiché MPTCP regola lo stack di rete e funziona all'interno del livello di trasporto, viene utilizzato in modo trasparente dall'applicazione.



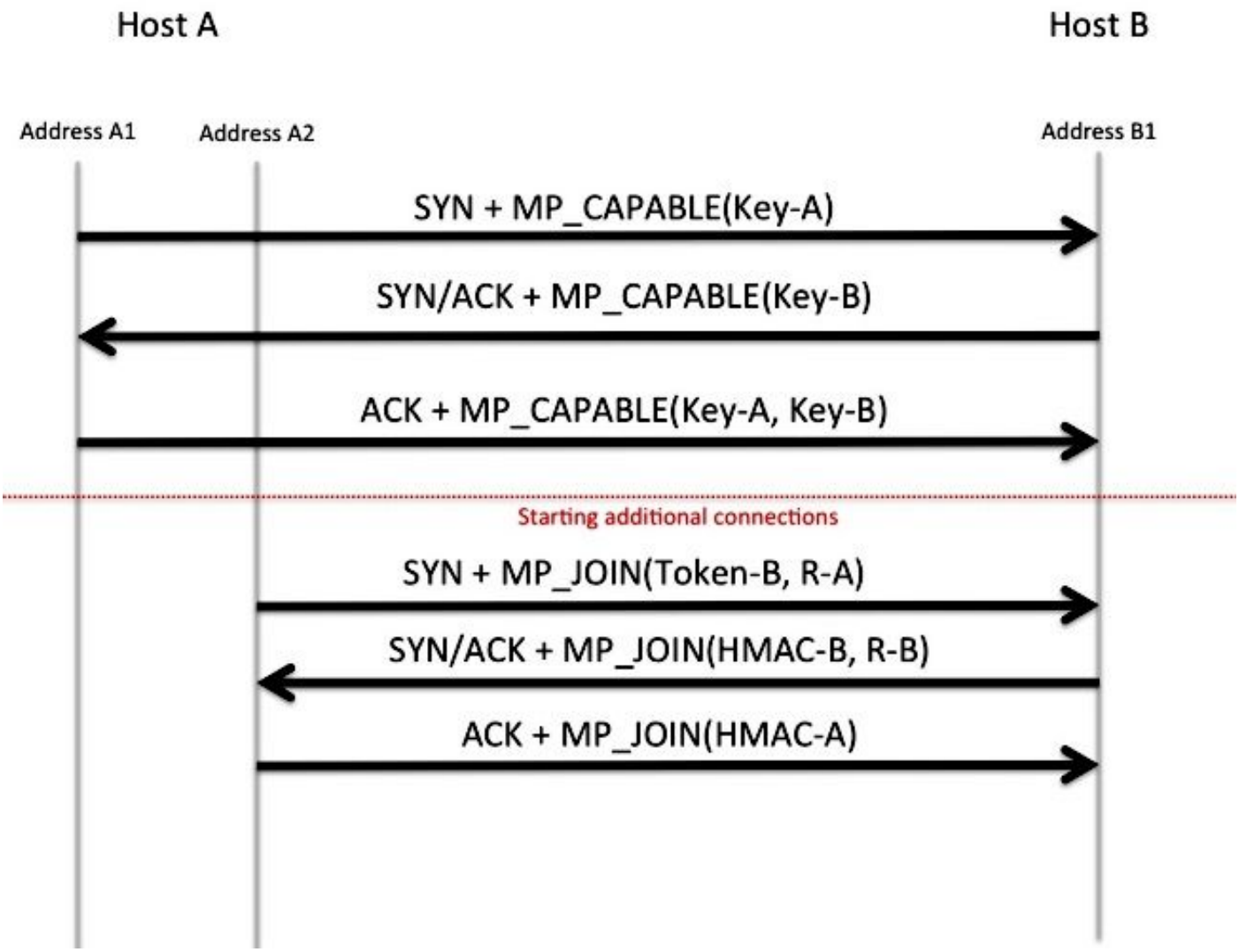
Definizione della sessione

MPTCP utilizza le opzioni TCP per negoziare e orchestrare la separazione e il riassemblaggio dei dati su più sottoflussi. **L'opzione TCP 30** è riservata dalla Internet Assigned Numbers Authority (IANA) all'uso esclusivo da parte di MPTCP. Per ulteriori informazioni, fare riferimento a Parametri TCP (Transmission Control Protocol). Quando si stabilisce una sessione TCP regolare, nel pacchetto SYN (Sincronizzazione iniziale) è inclusa l'opzione **MP_CAPABLE**. Se il responder supporta e sceglie di negoziare MPTCP, risponde anche con l'opzione **MP_CAPABLE** nel pacchetto di conferma SYN (ACK). Le chiavi scambiate in questo handshake vengono utilizzate in

futuro per autenticare l'unione e la rimozione di altre sessioni TCP in questo flusso MPTCP.

Unisci flussi secondari aggiuntivi

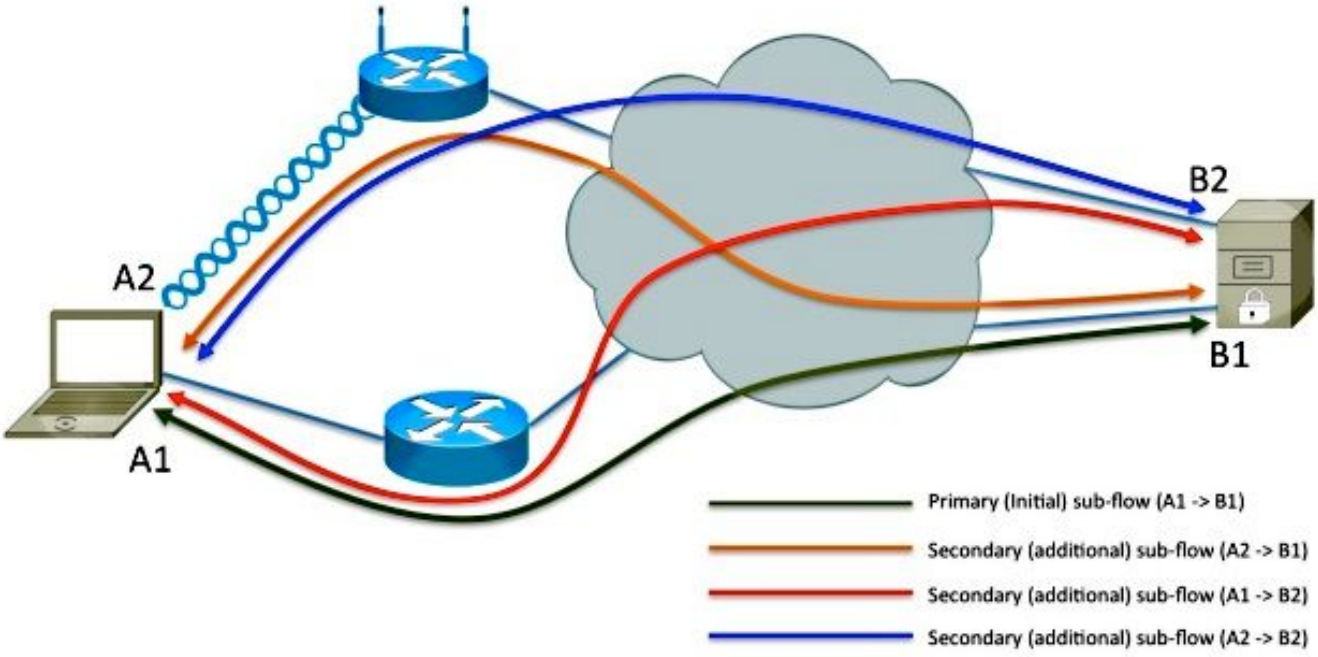
Quando ritenuto necessario, l'**host A** potrebbe avviare altri flussi secondari provenienti da un'interfaccia o da un indirizzo diverso verso l'**host B**. Come per il flusso secondario iniziale, vengono usate le opzioni TCP per indicare che si desidera unire questo flusso secondario con l'altro flusso secondario. Le chiavi scambiate all'interno della definizione del sottoflusso iniziale (insieme a un algoritmo di hashing) vengono utilizzate dall'**host B** per confermare che la richiesta di join è stata effettivamente inviata dall'**host A**. il flusso secondario a 4 tuple (IP di origine, IP di destinazione, porta di origine e porta di destinazione) è diverso da quello del flusso secondario primario; questo flusso potrebbe avere un percorso diverso nella rete.



Aggiungi indirizzo

L'host A dispone di più interfacce ed è possibile che l'**host B** disponga di più connessioni di rete. **L'host B apprende gli indirizzi A1 e A2 in modo implicito come risultato dei flussi secondari di determinazione origine dell'host A da ciascuno dei propri indirizzi destinati a B1. È possibile che l'host B annunci il proprio indirizzo aggiuntivo (B2) all'host A in modo che altri flussi secondari vengano eseguiti a B2. Questa operazione viene completata tramite l'opzione TCP 30**. Come mostrato nel diagramma, l'**host B** annuncia il proprio indirizzo secondario (B2) all'**host A** e vengono creati due flussi secondari aggiuntivi. Poiché MPTCP opera al di sopra del livello Rete dello stack OSI (Open System Interconnection), gli indirizzi IP annunciati possono essere IPv4, IPv6 o

entrambi. È possibile che alcuni flussi secondari vengano trasportati contemporaneamente da IPv4, mentre altri flussi secondari vengono trasportati da IPv6.



Segmentazione, percorsi multipli e riassemblaggio

Un flusso di dati fornito a MPTCP dall'applicazione deve essere segmentato e distribuito tra più flussi secondari dal mittente. Deve quindi essere ricomposto nel singolo flusso di dati prima di essere restituito all'applicazione.

MPTCP controlla le prestazioni e la latenza di ogni sottoflusso e regola dinamicamente la distribuzione dei dati per ottenere il massimo throughput aggregato. Durante il trasferimento dei dati, l'opzione dell'intestazione TCP include informazioni sui numeri di sequenza/conferma MPTCP, il numero di sequenza/conferma del flusso secondario corrente e un checksum.

Impatto sull'ispezione del flusso

Molti dispositivi di sicurezza potrebbero azzerare o sostituire le opzioni TCP sconosciute con un valore No Option (NOOP). Se il dispositivo di rete esegue questa operazione sul pacchetto TCP SYN nel flusso secondario iniziale, viene rimosso l'annuncio **MP_CAPABLE**. Di conseguenza, il server ritiene che il client non supporti MPTCP e ripristina il normale funzionamento di TCP.

Se l'opzione viene mantenuta e MPTCP è in grado di stabilire più flussi secondari, l'analisi dei pacchetti in linea da parte dei dispositivi di rete potrebbe non funzionare in modo affidabile. Infatti, a ciascun flusso secondario vengono trasferite solo parti del flusso di dati. L'effetto dell'ispezione del protocollo su MPTCP potrebbe variare da niente a totale interruzione del servizio. L'effetto varia in base a quali dati vengono ispezionati e a quanto. L'analisi dei pacchetti può includere il gateway di livello applicazione del firewall (ALG o correzione), l'ALG NAT (Network Address Translation), l'AVC (Application Visibility and Control), il NBAR (Network Based Application Recognition) o i servizi di rilevamento intrusioni (IDS/IPS). Se nell'ambiente è richiesta l'ispezione dell'applicazione, si consiglia di abilitare la cancellazione dell'**opzione TCP 30**.

Se il flusso non può essere ispezionato a causa della crittografia o se il protocollo è sconosciuto, il

dispositivo in linea non dovrebbe avere alcun impatto sul flusso MPTCP.

Prodotti Cisco interessati da MPTCP

Questi prodotti sono interessati da MPTCP:

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

Ciascun prodotto è descritto in dettaglio nelle sezioni seguenti del presente documento.

ASA

Operazioni TCP

Per impostazione predefinita, il firewall Cisco ASA sostituisce le opzioni TCP non supportate, tra cui l'opzione **MPTCP 30**, con l'opzione NOOP (opzione 1). Per autorizzare l'opzione MPTCP, utilizzare questa configurazione:

1. Definire il criterio per consentire l'**opzione TCP 30** (utilizzata da MPTCP) tramite il dispositivo:

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

2. Definire la selezione del traffico:

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

3. Definire una mappa dal traffico all'azione:

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

4. Attivarlo sulla confezione o per interfaccia:

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

Ispezione protocollo

L'ASA supporta l'ispezione di molti protocolli. L'effetto che il motore di ispezione potrebbe avere sull'applicazione varia. Se è richiesta un'ispezione, si consiglia di NON applicare la mappa TCP descritta in precedenza.

Cisco Firepower Threat Defense

Operazioni TCP

Poiché l'FTD esegue l'ispezione approfondita dei pacchetti per i servizi IPS/IDS, non è

consigliabile modificare la mappa tcp per consentire l'accesso all'opzione TCP.

Cisco IOS Firewall

Controllo degli accessi basato sul contesto (CBAC)

La funzione CBAC non rimuove le opzioni TCP dal flusso TCP. MPTCP crea una connessione attraverso il firewall.

Zone-Based Firewall (ZBFW)

Cisco IOS e IOS-XE ZBFW non rimuovono le opzioni TCP dal flusso TCP. MPTCP crea una connessione attraverso il firewall.

ASSO

Per impostazione predefinita, il dispositivo ACE rimuove le opzioni TCP dalle connessioni TCP. La connessione MPTCP torna alle normali operazioni TCP.

Il dispositivo ACE potrebbe essere configurato in modo da consentire le opzioni TCP tramite il comando **tcp-options**, come descritto nella sezione Configurazione della modalità di gestione delle opzioni TCP della Security Guide vA5(1.0), Cisco ACE Application Control Engine. Tuttavia, questa operazione non è sempre consigliata, in quanto i flussi secondari potrebbero essere bilanciati su server reali diversi e il join non riesce.

Prodotti Cisco non interessati da MPTCP

In genere, anche i dispositivi che non ispezionano i flussi TCP o le informazioni di livello 7 non modificano le opzioni TCP e, di conseguenza, devono essere trasparenti per MPTCP. Tali dispositivi possono includere:

- Cisco serie 5000 ASR (Starent)
- WAAS (Wide Area Application Services)
- CGN (Carrier-Grade NAT) [blade Carrier-Grade Services Engine (CGSE) in Carrier Routing System (CRS)-1]
- Tutti i prodotti di switch Ethernet
- Tutti i prodotti router (a meno che la funzionalità firewall o NAT non sia abilitata; per ulteriori informazioni, vedere la sezione Prodotti Cisco interessati da MPTCP più indietro nel documento)