Visão geral do MPTCP e suporte a produtos

Contents

Introduction

Este documento fornece uma visão geral do Multipath TCP (MPTCP), seu impacto na inspeção de fluxo e os produtos da Cisco que são e não são afetados por ele.

Visão geral do MPTCP

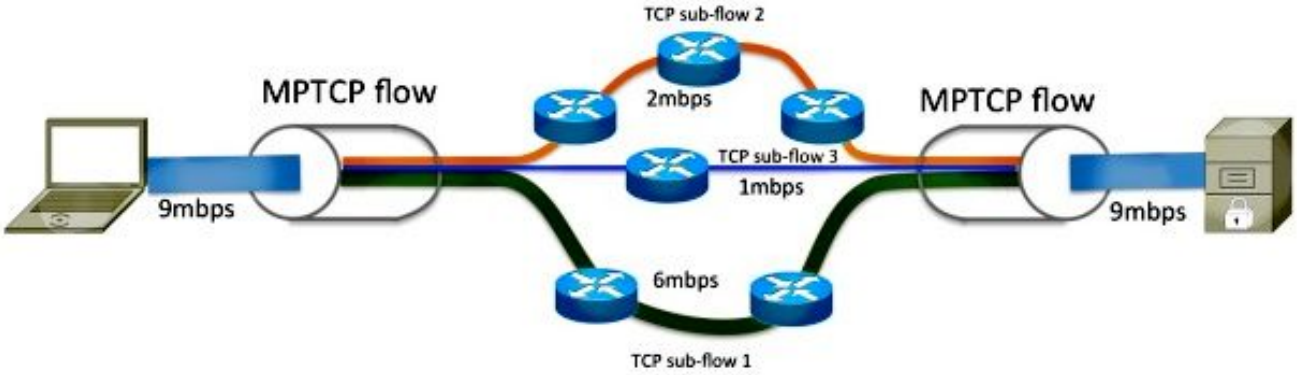
Informações de Apoio

Os hosts conectados à Internet ou em um ambiente de data center são frequentemente conectados por vários caminhos. No entanto, quando o TCP é usado para transporte de dados, a comunicação é restrita a um único caminho de rede. É possível que alguns caminhos entre os dois hosts estejam congestionados, enquanto os caminhos alternativos são subutilizados. Um uso mais eficiente dos recursos de rede é possível se esses vários caminhos forem usados simultaneamente. Além disso, o uso de várias conexões melhora a experiência do usuário, pois ele fornece maior throughput e melhor resiliência contra falhas de rede.

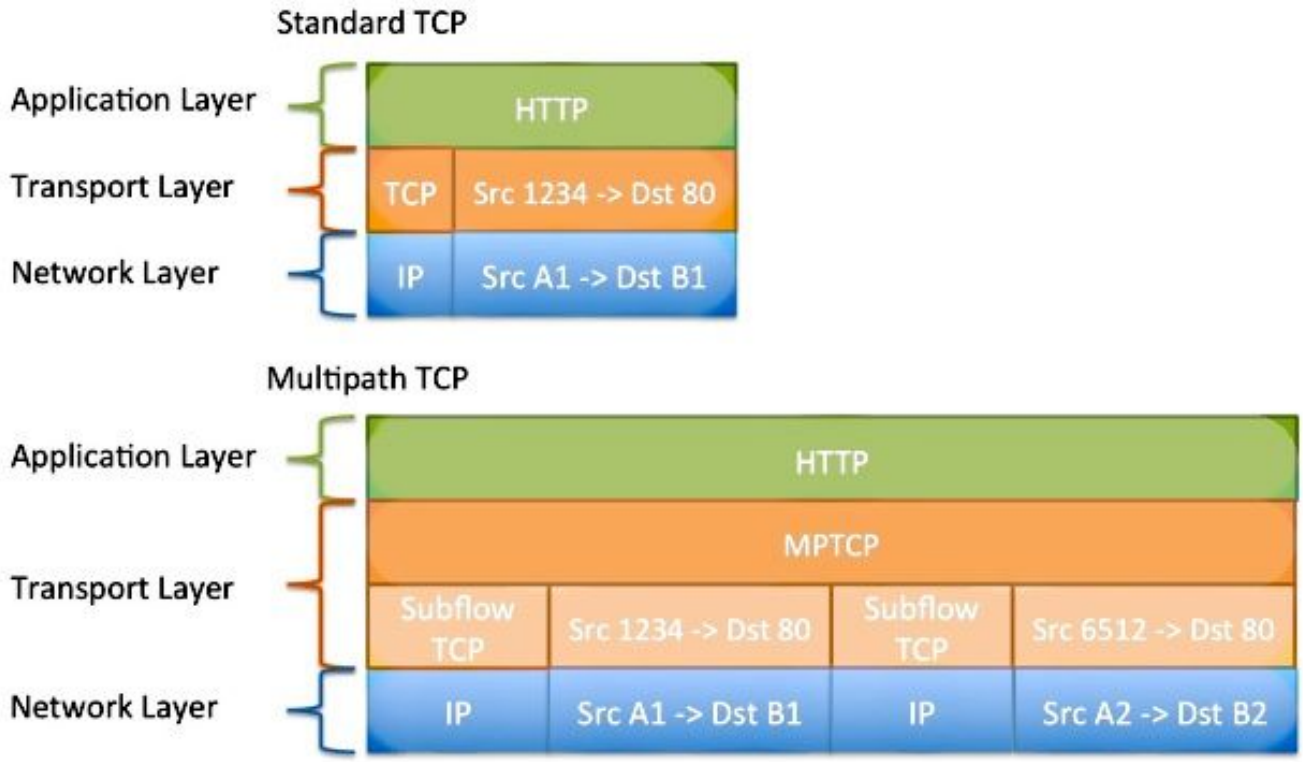
O MPTCP é um conjunto de extensões do TCP regular que permite que um único fluxo de dados seja separado e transportado através de várias conexões. Consulte o RFC6824: Extensões TCP para Operação Multipath com Vários Endereços para obter mais informações.

Como mostrado neste diagrama, o MPTCP é capaz de separar o fluxo de 9mbps em três

subfluxos diferentes no nó do remetente, que é subsequentemente agregado de volta ao fluxo de dados original no nó receptor.



Os dados que entram na conexão MPTCP atuam exatamente como fazem através de uma conexão TCP regular; os dados transmitidos garantiram uma entrega em ordem. Como o MPTCP ajusta a pilha de rede e opera dentro da camada de transporte, ele é usado de forma transparente pelo aplicativo.



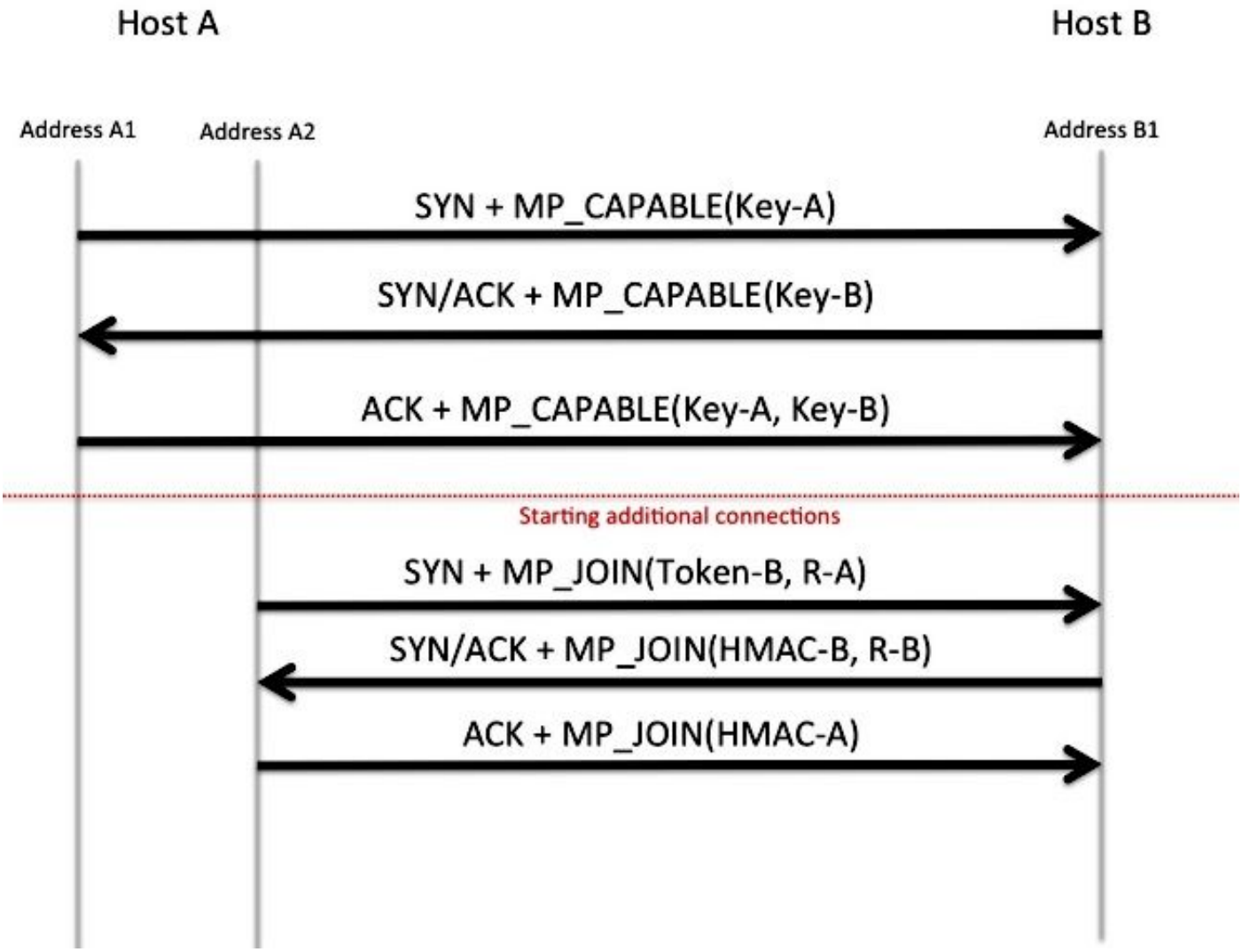
Estabelecimento de sessão

O MPTCP usa as opções de TCP para negociar e orquestrar a separação e a remontagem de dados sobre os vários subfluxos. **A opção 30 do TCP** é reservada pela Internet Assigned Numbers Authority (IANA) para uso exclusivo do MPTCP. Consulte Parâmetros TCP (Transmission Control Protocol) para obter mais informações. No estabelecimento de uma sessão TCP regular, uma opção **MP_CAPABLE** é incluída no pacote de sincronização inicial (SYN). Se o respondente suportar e escolher negociar o MPTCP, ele também responde com a opção **MP_CAPABLE** no pacote SYN-accept (ACK). As chaves trocadas dentro desse handshake serão usadas no futuro para autenticar a junção e a remoção de outras sessões TCP neste fluxo

MPTCP.

Unir Subfluxos Adicionais

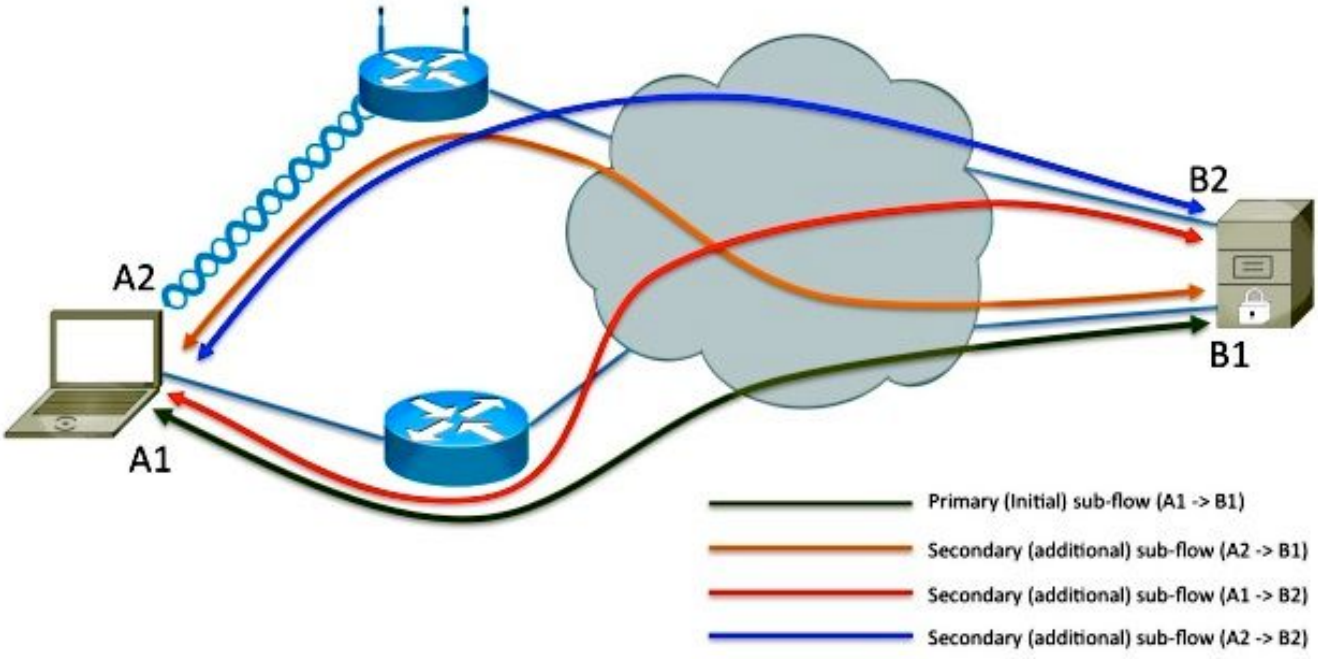
Quando considerado necessário, o **Host-A** pode iniciar subfluxos adicionais originados de uma interface ou endereço diferente para o **Host-B**. Assim como no sub-fluxo inicial, as opções de TCP são usadas para indicar o desejo de mesclar esse sub-fluxo com o outro sub-fluxo. As chaves que são trocadas no estabelecimento de sub-fluxo inicial (juntamente com um algoritmo de hash) são usadas pelo **Host-B** para confirmar se a solicitação de junção é realmente enviada pelo **Host-A**. O sub-fluxo secundário de 4 tuplas (IP origem, IP destino, porta origem e porta destino) é diferente do sub-fluxo principal; esse fluxo pode seguir um caminho diferente pela rede.



Adicionar endereço

O Host-A tem várias interfaces e é possível que o **Host-B** tenha várias conexões de rede. **O Host-B** aprende sobre os endereços A1 e A2 implicitamente como resultado de subfluxos de origem do **Host-A** de cada um de seus endereços destinados a B1. É possível que o **Host-B** anuncie seu endereço adicional (B2) ao **Host-A** para que outros subfluxos sejam feitos para B2. Isso é concluído por meio da **opção 30 do TCP**. Como mostrado neste diagrama, o **Host-B** anuncia seu endereço secundário (B2) ao **Host-A**, e dois subfluxos adicionais são criados. Como o MPTCP opera acima da camada de rede da pilha Open System Interconnection (OSI), os endereços IP anunciados podem ser IPv4, IPv6 ou ambos. É possível que alguns dos subfluxos sejam transportados pelo IPv4 simultaneamente, à medida que outros subfluxos são transportados pelo

IPv6.



Segmentação, multipath e remontagem

Um fluxo de dados fornecido ao MPTCP pelo aplicativo deve ser segmentado e distribuído pelos vários subfluxos pelo remetente. Em seguida, ele deve ser remontado no fluxo de dados único antes de ser entregue de volta ao aplicativo.

O MPTCP inspeciona o desempenho e a latência de cada subfluxo e ajusta dinamicamente a distribuição de dados para obter o maior throughput agregado. Durante a transferência de dados, a opção de cabeçalho TCP inclui informações sobre os números de sequência/confirmação MPTCP, a sequência de subfluxo/número de confirmação atual e uma soma de verificação.

Impacto na inspeção do fluxo

Muitos dispositivos de segurança podem zerar ou substituir opções TCP desconhecidas por um valor Sem opção (NOOP). Se o dispositivo de rede fizer isso com o pacote TCP SYN no sub-fluxo inicial, o anúncio **MP_CAPABLE** será removido. Como resultado, parece ao servidor que o cliente não suporta MPTCP e que ele reverte para a operação TCP normal.

Se a opção for preservada e o MPTCP for capaz de estabelecer vários subfluxos, a análise de pacotes em linha por dispositivos de rede pode não funcionar de forma confiável. Isso porque apenas partes do fluxo de dados são transportadas para cada subfluxo. O efeito da inspeção de protocolo sobre o MPTCP pode variar de nada a interrupção total do serviço. O efeito varia com base no que e na quantidade de dados inspecionados. A análise de pacotes pode incluir firewall Application Layer Gateway (ALG ou fixup), Network Address Translation (NAT) ALG, Application Visibility and Control (AVC), Network Based Application Recognition (NBAR) ou Intrusion Detection Services (IDS/IPS). Se a inspeção de aplicativos for necessária em seu ambiente, é recomendável que a limpeza da **opção 30 do TCP** seja habilitada.

Se o fluxo não puder ser inspecionado devido à criptografia ou se o protocolo for desconhecido, o dispositivo em linha não deverá ter impacto no fluxo de MPTCP.

Produtos Cisco afetados pelo MPTCP

Esses produtos são afetados pelo MPTCP:

- ASA (Adaptive Security Appliance)
- Defesa contra ameaças do Cisco Firepower
- Sistema de prevenção de intrusão (IPS)
- Cisco IOS-XE e IOS®
- Application Control Engine (ACE)

Cada produto é descrito em detalhes nas seções subsequentes deste documento.

ASA

Operações TCP

Por padrão, o firewall Cisco ASA substitui as opções TCP não suportadas, que incluem a **opção 30 MPTCP**, pela opção NOOP (opção 1). Para permitir a opção MPTCP, use esta configuração:

1. Defina a política para permitir a **opção 30 do TCP** (usada pelo MPTCP) através do dispositivo:

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

2. Defina a seleção de tráfego:

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

3. Defina um mapa do tráfego para a ação:

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

4. Ative-o na caixa ou por interface:

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

Inspeção de protocolo

O ASA suporta a inspeção de muitos protocolos. O efeito que o motor de inspeção pode ter sobre a aplicação varia. Recomenda-se que, se a inspeção for necessária, o mapa TCP descrito anteriormente NÃO seja aplicado.

Defesa contra ameaças do Cisco Firepower

Operações TCP

Como o FTD executa uma inspeção profunda de pacotes para serviços de IPS/IDS, não é recomendável modificar o mapa tcp para permitir a opção de TCP através do .

Cisco IOS Firewall

Controle de acesso baseado em contexto (CBAC)

O CBAC não remove as opções TCP do fluxo TCP. O MPTCP cria uma conexão através do firewall.

Firewall baseado em zona (ZBFW)

O Cisco IOS e o IOS-XE ZBFW não removem as opções TCP do fluxo TCP. O MPTCP cria uma conexão através do firewall.

ACE

Por padrão, o dispositivo ACE retira as opções TCP das conexões TCP. A conexão MPTCP retorna às operações TCP normais.

O dispositivo ACE pode ser configurado para permitir as opções de TCP por meio do comando **tcp-options**, conforme descrito na seção Configuração de Como o ACE lida com as Opções TCP do Guia de Segurança vA5(1.0), Cisco ACE Application Control Engine. No entanto, isso nem sempre é recomendado, pois os subfluxos secundários podem ser balanceados para servidores reais diferentes e a junção falha.

Produtos da Cisco não afetados pelo MPTCP

Geralmente, qualquer dispositivo que não inspeciona fluxos TCP ou informações da Camada 7 também não altera as opções de TCP e, como resultado, deve ser transparente ao MPTCP. Esses dispositivos podem incluir:

- ASRs Cisco 5000 Series (Inicial)
- Serviços de aplicações de área ampla (WAAS)
- NAT de nível de operadora (CGN - Carrier-Grade Services Engine) (CGSE - Carrier-Grade Services Engine) no Sistema de roteamento de operadora (CRS - Carrier Routing System)-1)
- Todos os produtos de switch Ethernet
- Todos os produtos de roteador (a menos que a funcionalidade de firewall ou NAT esteja habilitada; consulte a seção Produtos Cisco afetados pelo MPTCP anteriormente no documento para obter mais detalhes)