MPTCP 및 제품 지원 개요

목차

소개

이 문서에서는 MPTCP(Multipath TCP)의 개요, 플로우 검사에 미치는 영향, 영향을 받지 않고 영향을 받는 Cisco 제품에 대해 설명합니다.

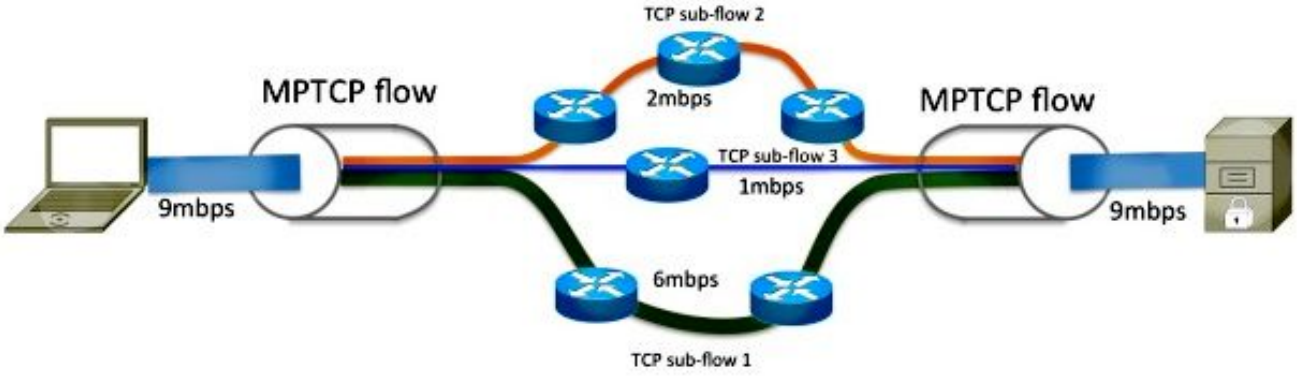
MPTCP 개요

배경 정보

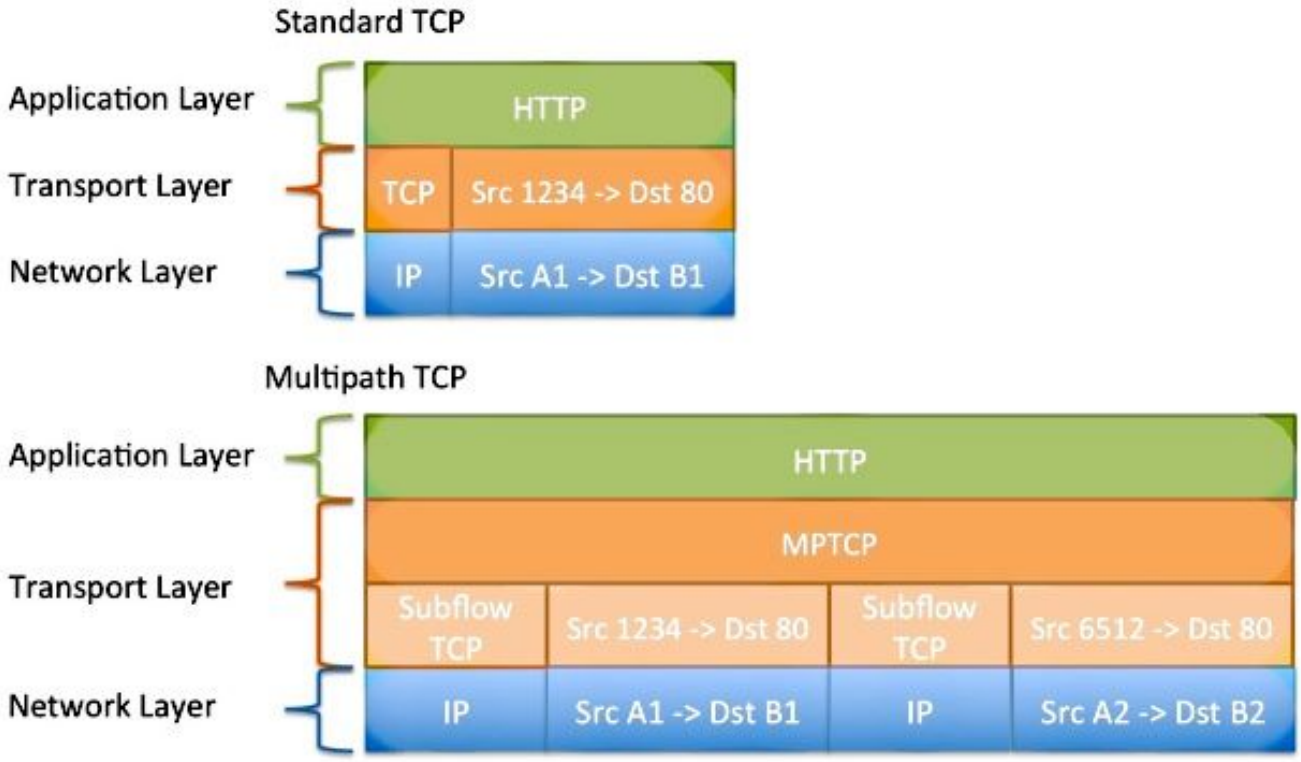
인터넷이나 데이터 센터 환경 내에 연결된 호스트는 여러 경로로 연결되는 경우가 많습니다.그러나 TCP를 데이터 전송에 사용할 경우 통신이 단일 네트워크 경로로 제한됩니다.두 호스트 간의 일부 경로가 혼잡한 반면 대체 경로는 활용도가 낮을 수 있습니다.이러한 다중 경로를 동시에 사용할 경우 네트워크 리소스를 보다 효율적으로 사용할 수 있습니다.또한 다중 연결을 사용하면 처리량이 향상되고 네트워크 장애에 대한 탄력성이 개선되므로 사용자 환경이 향상됩니다.

MPTCP는 단일 데이터 흐름을 분리하고 여러 연결에서 전달할 수 있도록 하는 일반 TCP의 확장 집합입니다.RFC6824[를 참조하십시오.자세한 내용은 다중 주소가 있는 다중 경로 작업을 위한 TCP](#) 확장.

이 다이어그램에 표시된 것처럼 MPTCP는 9mbps 플로우를 발신자 노드의 세 가지 다른 하위 플로우로 분리할 수 있으며, 이 하위 플로우는 이후에 수신 노드의 원래 데이터 플로우로 다시 집계됩니다.



MPTCP 연결을 입력하는 데이터는 일반 TCP 연결을 통해 정확히 동작합니다.전송된 데이터는 주문 배송을 보장합니다.MPTCP는 네트워크 스택을 조정하고 전송 레이어 내에서 작동하므로 애플리케이션에 의해 투명하게 사용됩니다.



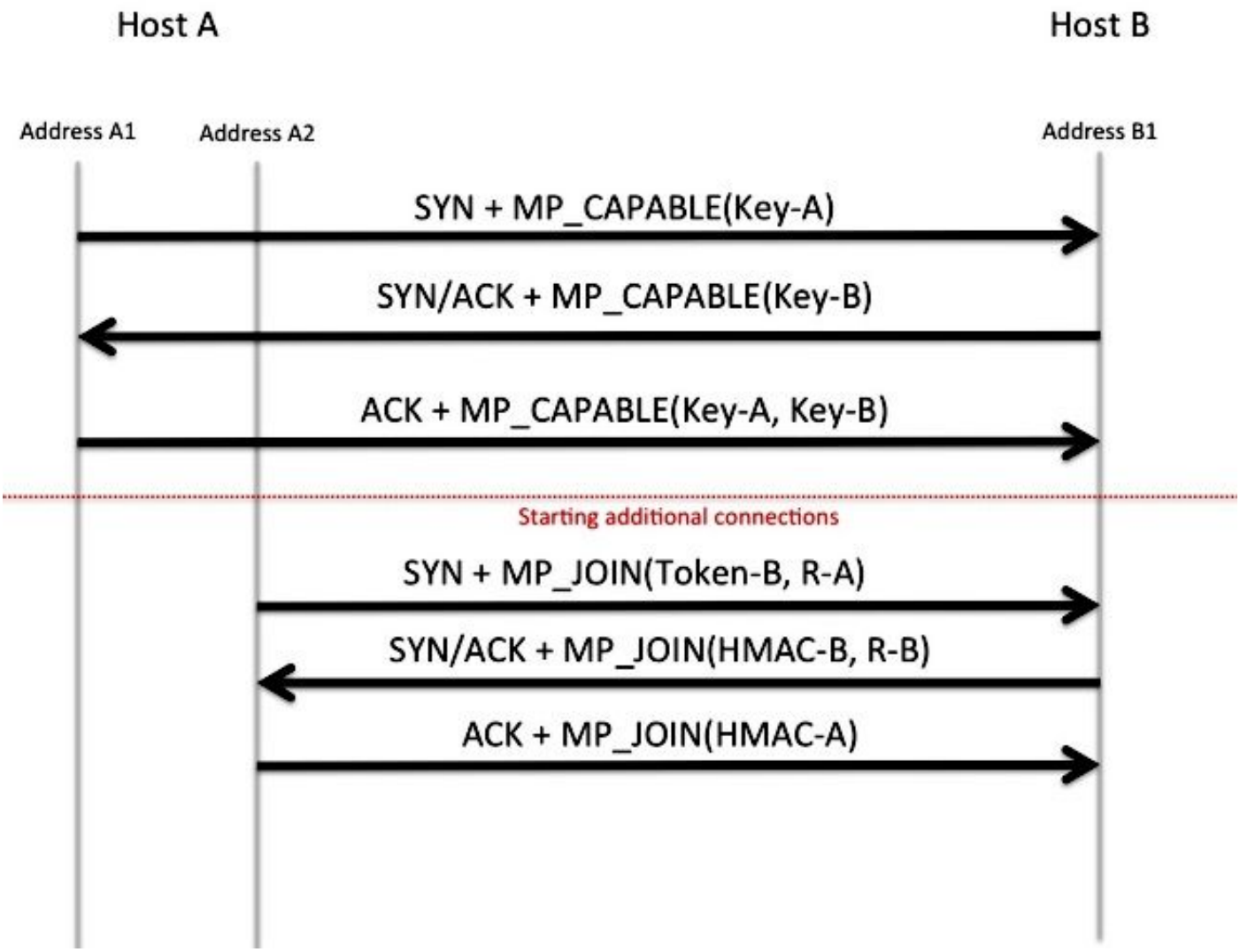
세션 설정

MPTCP는 TCP 옵션을 사용하여 여러 하위 플로우를 통해 데이터의 분리 및 리어셈블리를 협상하고 오케스트레이션합니다.**TCP 옵션 30**은 IANA(Internet Assigned Numbers Authority)에서 MPTCP에 단독으로 사용하도록 예약되어 있습니다.자세한 내용은 TCP(Transmission Control Protocol) 매개변수를 참조하십시오.일반 TCP 세션을 설정할 때 **MP_CAPABLE** 옵션이 초기 동기화(SYN) 패킷에 포함됩니다.응답자가 MPTCP를 지원하고 협상하도록 선택한 경우 SYN 승인(ACK) 패킷의 **MP_CAPABLE** 옵션으로 응답합니다.이 핸드셰이크 내에서 교환되는 키는 나중에 이 MPTCP 흐름에 다른 TCP 세션을 연결하고 제거하는 것을 인증하기 위해 사용됩니다.

추가 하위 플로우 참가

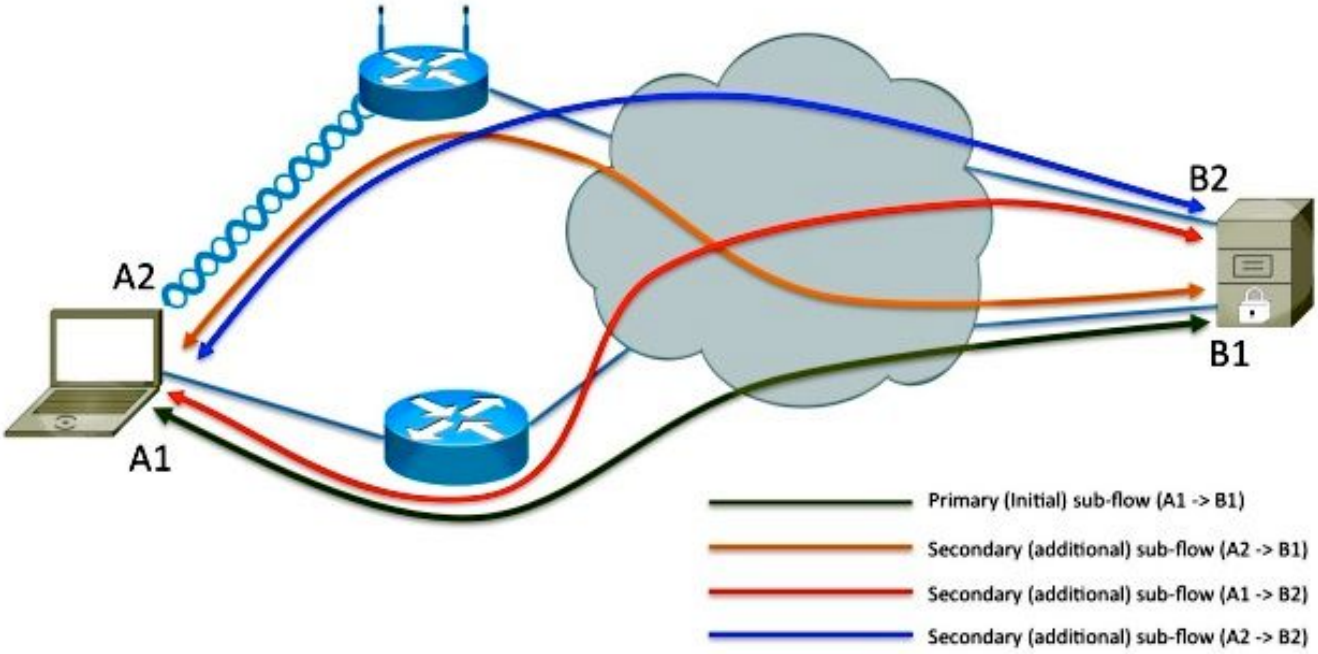
필요한 경우 **Host-A는** 다른 인터페이스 또는 주소에서 **Host-B**로 소싱된 추가 하위 플로우를 시작할 수 있습니다.초기 하위 흐름과 마찬가지로, 이 하위 흐름을 다른 하위 흐름과 병합하려는 의사를 나

타내기 위해 TCP 옵션이 사용됩니다.초기 하위 플로우 설정(해싱 알고리즘 포함) 내에서 교환되는 키는 조인 요청이 **Host-A**에 의해 실제로 전송되는지 확인하기 위해 **Host-B**에서 사용됩니다.보조 하위 플로우 4-튜플(소스 IP, 대상 IP, 소스 포트 및 대상 포트)이 기본 하위 흐름의 것과 다릅니다.이 흐름은 네트워크를 통해 다른 경로를 사용할 수 있습니다.



주소 추가

Host-A에는 여러 인터페이스가 있으며 **Host-B에** 여러 네트워크 연결이 있을 수 있습니다.**호스트-B**는 **Host-A** 소싱 하위 플로우의 결과로 암시적으로 주소 A1 및 A2에 대해 학습합니다. **Host-B는** 추가 주소(B2)를 **Host-A에** 광고하여 다른 하위 플로우가 B2로 생성되도록 할 수 있습니다. 이 작업은 **TCP 옵션 30을 통해** 완료됩니다. 이 다이어그램에 표시된 대로 호스트-B에는**를 광고합니다. 보조 주소(B2)를 Host-A로 이동하고 두 개의 추가 하위 플로우가 생성됩니다.**MPTCP는 OSI(Open System Interconnection) 스택의 네트워크 레이어 위에서 작동하므로 광고되는 IP 주소는 IPv4, IPv6 또는 둘 다일 수 있습니다.다른 하위 플로우가 IPv6에 의해 전송될 때 일부 하위 플로우는 IPv4를 통해 동시에 전송될 수 있습니다.



세그멘테이션, 다중 경로 및 리어셈블리

애플리케이션이 MPTCP에 제공하는 데이터 스트림은 발신자가 여러 하위 플로우에 걸쳐 분할하고 분배해야 합니다.그런 다음 단일 데이터 스트림으로 리어셈블한 후 애플리케이션에 다시 전달해야 합니다.

MPTCP는 각 하위 흐름의 성능 및 레이턴시를 검사하고, 최고 수준의 집계 처리량을 얻기 위해 데이터 배포를 동적으로 조정합니다.데이터 전송 중에 TCP 헤더 옵션에는 MPTCP 시퀀스/승인 번호, 현재 하위 플로우 시퀀스/승인 번호 및 체크섬이 포함됩니다.

플로우 검사에 미치는 영향

대부분의 보안 디바이스는 제로 아웃되거나 알 수 없는 TCP 옵션을 NOOP(No Option) 값으로 대체할 수 있습니다.네트워크 디바이스가 초기 하위 플로우의 TCP SYN 패킷에 이 작업을 수행하면 **MP_CAPABLE** 광고가 제거됩니다.따라서 클라이언트가 MPTCP를 지원하지 않는 것으로 서버에 나타나며 정상 TCP 작업으로 돌아갑니다.

옵션이 유지되고 MPTCP가 여러 하위 플로우를 설정할 수 있는 경우 네트워크 디바이스에 의한 인라인 패킷 분석이 안정적으로 작동하지 않을 수 있습니다.이는 데이터 흐름의 일부만 각 하위 플로우에 전달되기 때문입니다.MPTCP에 대한 프로토콜 검사의 효과는 무에서 전체 서비스 중단에 따라 달라질 수 있습니다.이 효과는 검사 대상 및 데이터 양에 따라 달라집니다.패킷 분석에는 방화벽 ALG(Application Layer Gateway), NAT(Network Address Translation) ALG, AVC(Application Visibility and Control), NBAR(Network Based Application Recognition) 또는 IDS/IPS(Intrusion Detection Services)가 포함될 수 있습니다. 사용자 환경에서 애플리케이션 검사가 필요한 경우 **TCP 옵션 30**을 지우는 **것이** 좋습니다.

암호화 때문에 플로우를 검사할 수 없거나 프로토콜을 알 수 없는 경우 인라인 디바이스는 MPTCP 플로우에 영향을 미치지 않아야 합니다.

MPTCP의 영향을 받는 Cisco 제품

이러한 제품은 MPTCP의 영향을 받습니다.

- ASA(Adaptive Security Appliance)
- Cisco Firepower 위협 방어
- IPS(Intrusion Prevention System)
- Cisco IOS-XE 및 IOS®
- ACE(Application Control Engine)

각 제품은 본 문서의 다음 섹션에서 자세히 설명합니다.

ASA

TCP 작업

기본적으로 Cisco ASA 방화벽은 지원되지 않는 TCP 옵션(MPTCP **옵션 30** 포함)을 NOOP 옵션(옵션 1)으로 대체합니다. MPTCP 옵션을 허용하려면 다음 컨피그레이션을 사용합니다.

1. 디바이스를 통해 **TCP 옵션 30**(MPTCP에서 사용)을 허용하려면 정책을 정의합니다.

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

2. 트래픽 선택을 정의합니다.

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

3. 트래픽에서 동작까지의 맵을 정의합니다.

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

4. 박스 또는 인터페이스별로 활성화합니다.

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

프로토콜 검사

ASA는 여러 프로토콜의 검사를 지원합니다.검사 엔진이 애플리케이션에 미칠 수 있는 효과는 다릅니다.검사가 필요한 경우 이전에 설명한 TCP 맵이 적용되지 않는 것이 좋습니다.

Cisco Firepower 위협 방어

TCP 작업

FTD는 IPS/IDS 서비스에 대한 심층 패킷 검사를 수행하므로 TCP 옵션을 통과하도록 tcp-map을 수정하지 않는 것이 좋습니다.

Cisco IOS Firewall

CBAC(Context-Based Access Control)

CBAC는 TCP 스트림에서 TCP 옵션을 제거하지 않습니다.MPTCP는 방화벽을 통해 연결을 구축합니다.

ZBFW(Zone-Based Firewall)

Cisco IOS 및 IOS-XE ZBFW는 TCP 스트림에서 TCP 옵션을 제거하지 않습니다.MPTCP는 방화벽을 통해 연결을 구축합니다.

ACE

기본적으로 ACE 디바이스는 TCP 연결에서 TCP 옵션을 제거합니다.MPTCP 연결은 일반 TCP 작업으로 돌아갑니다.

ACE 디바이스는 Security Guide vA5(1.0), Cisco ACE Application Control Engine의 Configuring How the ACE Handles TCP Options 섹션에 설명된 대로 tcp-**options** 명령을 통해 TCP 옵션을 허용하도록 구성할 수 있습니다.그러나 보조 하위 플로우가 다른 실제 서버로 균형 조정될 수 있으며 조인이 실패하기 때문에 항상 권장되지는 않습니다.

MPTCP의 영향을 받지 않는 Cisco 제품

일반적으로 TCP 흐름 또는 레이어 7 정보를 검사하지 않는 모든 디바이스는 TCP 옵션도 변경하지 않으므로 MPTCP에 투명해야 합니다.이러한 디바이스에는 다음이 포함될 수 있습니다.

- Cisco 5000 Series ASR(투명)
- WAAS(Wide Area Application Services)
- CGN(Carrier-Grade NAT)(CRS(Carrier Routing System)-1의 CGSE(Carrier-Grade Services Engine) 블레이드
- 모든 이더넷 스위치 제품
- 모든 라우터 제품(방화벽 또는 NAT 기능이 활성화되지 않은 경우 제외)자세한 내용은 문서의 앞부분에서 Cisco Products Impacted by MPTCP 섹션을 참조하십시오.)