Threat Defense Service 정책

특정 트래픽 클래스에 서비스를 적용하기 위해 Firepower Threat Defense Service 정책을 사용할 수 있습니다. 예를 들어 모든 TCP 애플리케이션에 적용되는 것과 반대로, 특정 TCP 애플리케이션과 관련된 시간 제한 구성을 만드는 서비스 정책을 사용할 수 있습니다. 서비스 정책은 인터페이스에 적용되거나 전역으로 적용되는 여러 작업 또는 규칙으로 구성됩니다.

Firepower Threat Defense Service 정책 정보

특정 트래픽 클래스에 서비스를 적용하기 위해 Firepower Threat Defense Service 정책을 사용할 수 있습니다. 서비스 정책을 사용하면 디바이스 또는 특정 인터페이스에 진입하는 모든 연결에 동일한 서비스를 적용하는 데 제한이 없습니다.

트래픽 클래스는 인터페이스와 확장 ACL(액세스 제어 목록)의 조합입니다. ACL "허용" 규칙은 클래스에 속한 연결을 확인합니다. ACL의 "거부" 트래픽에는 서비스가 적용되지 않았으며 이러한 연결은 실제로 삭제되지 않습니다. IP 주소와 TCP/UDP 포트를 사용하여 필요에 따라 일치하는 연결을 식별할 수 있습니다.

두 가지 유형의 트래픽 클래스는 다음과 같습니다.

- 인터페이스 기반 규칙 - 서비스 정책 규칙에 보안 영역 또는 인터페이스 그룹을 지정하는 경우 이 규칙은 인터페이스 개체의 일부인 인터페이스를 통과하는 ACL "허용" 트래픽에 적용됩니다.

  지정된 기능의 경우 인그레스 인터페이스에 적용된 인터페이스 기반 규칙이 항상 전역 규칙보다 우선합니다. 즉, 인그레스 인터페이스 기반 규칙이 연결에 적용되는 경우 일치하는 전역 규칙은 무시됩니다. 인그레스 인터페이스 또는 전역 규칙이 적용되지 않으면 이그레스 인터페이스의 인터페이스 서비스 규칙이 적용됩니다.

- 전역 규칙 - 이 규칙은 모든 인터페이스에 적용됩니다. 인터페이스 기반 규칙이 연결에 적용되지 않으면 전역 규칙이 검사되며 ACL에서 "허용"하는 모든 연결에 적용됩니다. 아무 것도 적용되지 않는 경우 서비스의 적용 없이 연결이 진행됩니다.

지정된 연결은 지정된 기능에 대해 인터페이스 기반 또는 전역 중 하나의 트래픽 클래스만 일치시킬 수 있습니다. 지정된 인터페이스 개체/트래픽 흐름 조합에 대한 규칙이 적어도 하나는 있어야 합니다.

서비스 정책 규칙은 액세스 제어 규칙 이후에 적용됩니다. 이러한 서비스는 허용된 연결에 대해서만 구성됩니다.

서비스 정책과 **FlexConfig** 및 기타 기능의 관계

버전 6.3(0) 이전에는 TCP_Embryonic_Conn_Limit 및 TCP_Embryonic_Conn_Timeout 사전 정의된 FlexConfig 개체를 사용하여 연결 관련 서비스 규칙을 구성할 수 있었습니다. Firepower Threat Defense Service 정책을 사용하여 이러한 개체를 제거하고 규칙을 다시 실행해야 합니다. 이러한 연결 관련 기능(**set connection** 명령)을 구현하기 위해 사용자 정의 FlexConfig 개체를 생성한 경우 해당 개체를 제거하고 서비스 정책을 통해 기능을 구현해야 합니다.

연결 관련 서비스 정책 기능은 다른 서비스 규칙 구현 기능과는 별도의 기능 그룹으로 처리되므로 중복되는 트래픽 클래스 문제가 발생하지 않아야 합니다. 하지만 다음과 같이 구성할 때 주의를 기울여야 합니다.

- QoS 정책 규칙은 서비스 정책 CLI를 사용하여 구현됩니다. 이러한 규칙은 연결 기반 서비스 정책 규칙보다 먼저 적용됩니다. 하지만 QoS 및 연결 설정은 동일하거나 중복되는 트래픽 클래스에 적용될 수 있습니다.
- FlexConfig 정책을 사용하여 사용자 정의 애플리케이션 검사 및 NetFlow를 구현할 수 있습니다. **show running-config** 명령을 사용하여 **policy-map**, **class-map**, **service-policy** 명령을 포함하여 서비스 규칙을 이미 구성하는 CLI를 검사하십시오. Netflow 및 애플리케이션 검사는 QoS 및 연결 설정과 호환되지만 FlexConfig를 구현하기 전에 기존 구성을 이해해야 합니다. 연결 설정은 애플리케이션 검사 및 Netflow 전에 적용됩니다.

참고 Firepower Threat Defense Service 정책에서 생성된 트래픽 클래스의 이름은 **class_map_***ACLname*입니다. 여기서 *ACLname*은 서비스 정책 규칙에 사용된 확장 ACL 개체의 이름입니다.

연결 설정이란**?**

연결 설정은 Firepower Threat Defense 디바이스를 통한 TCP 흐름 등 트래픽 연결 관리에 관련된 다양한 기능으로 구성되어 있습니다. 일부 기능은 특정 서비스 제공을 구성하는 구성 요소로 이름이 지정되어 있습니다.

연결 설정은 다음과 같습니다.

- **Global timeouts for various protocols(**다양한 프로토콜을 위한 전역 시간 제한**)** - 모든 전역 시간 제한에는 기본값이 있으므로 예기치 않은 연결 손실이 발생한 경우에만 전역 시간 제한을 변경

해야 합니다. Firepower Threat Defense Platform 정책에서 전역 시간 초과를 구성합니다. **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택합니다.

- **Connection timeouts per traffic class(**트래픽 클래스당 연결 시간 제한**)** - 서비스 정책을 사용하여 특정 트래픽 유형에 전역 시간 제한을 재정의할 수 있습니다. 트래픽 클래스 시간 제한에는 모두 기본값이 있으므로 따로 설정하지 않아도 됩니다.
- **Connection limits and TCP Intercept(**연결 제한 및 **TCP** 가로채기**)** - 기본적으로 Firepower Threat Defense 디바이스를 통과하거나 이동할 수 있는 연결 수에는 제한이 없습니다. DoS(서비스 거부) 공격으로부터 서버를 보호하기 위해 서비스 정책 규칙을 사용하여 특정 트래픽 클래스에 제한을 설정할 수 있습니다. 특히 TCP 핸드셰이크를 완료하지 않은 원시 연결에 제한을 설정하면 SYN 플러딩 공격을 방지할 수 있습니다. 원시 연결 시간 제한이 초과되면 TCP 가로채기 구성 요소가 프록시 연결에 개입하여 공격을 제한합니다.
- **Dead Connection Detection (DCD)(**끊어진 연결 탐지**(DCD))** - 유효하지만 종종 유휴 상태가 되는 지속 연결이 있고 이러한 연결이 유휴 시간 제한 설정을 초과해 닫히는 경우, DCD(Dead Connection Detection)를 활성화하여 유휴 타이머를 재설정함으로써 유휴 상태지만 유효한 연결을 식별하고 유지할 수 있습니다. 유휴 시간이 초과되면 DCD가 연결의 양쪽을 프로브하여 양쪽 연결 모두 연결이 유효한 것에 동의하는지 확인합니다. **show service-policy** 명령 출력은 DCD의 작업 양을 표시하는 카운터를 포함합니다. **show conn detail** 명령을 사용하여 이니시에이터 및 응답자 관련 정보와 프로브 전송 빈도를 확인할 수 있습니다.
- **TCP sequence randomization(TCP** 시퀀스 임의 설정**)** - 각 TCP 연결에는 각각 클라이언트와 서버에서 생성된 두 개의 ISN(초기 시퀀스 번호)이 있습니다. 기본적으로 Firepower Threat Defense 디바이스는 인바운드와 아웃바운드 두 방향 모두로 전달되는 TCP SYN의 ISN을 임의로 설정합니다. ISN을 임의로 설정하면 공격자가 새 연결을 위한 다음 ISN을 예측하지 못하며 잠재적으로 새 세션의 가로채기가 방지됩니다. 원하는 경우 트래픽 클래스별 임의 설정을 비활성화할 수 있습니다.
- **TCP Normalization(TCP** 정규화**)** - TCP 노멀라이저는 비정상 패킷을 방지합니다. 트래픽 클래스에서 일부 패킷 이상 유형을 처리하는 방식을 구성할 수 있습니다. FlexConfig 정책을 사용하여 TCP 정규화를 구성할 수 있습니다.
- **TCP State Bypass(TCP** 상태 우회**)** - 네트워크에서 비대칭 라우팅을 사용하는 경우 TCP 상태 검사를 우회할 수 있습니다.

서비스 정책을 위한 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할

관리자

액세스 관리자

Network Admin(네트워크 관리자)

서비스 정책 가이드라인 및 제한 사항

- 서비스 정책은 라우팅 모드 또는 투명 모드에서 라우팅된 인터페이스 또는 스위치 인터페이스에만 적용됩니다. 인라인 집합 또는 수동 인터페이스에는 적용되지 않습니다.
- 특정 인터페이스 또는 전역 정책에 대해 최대 25개의 트래픽 클래스를 가질 수 있습니다. 이는 특정 보안 영역 또는 인터페이스 그룹의 전역 정책에 대해 25개를 초과하는 서비스 정책 규칙을 가질 수 없음을 의미합니다. 하지만 인터페이스의 경우 동일한 인터페이스가 보안 영역과 인터페이스 그룹 모두에 나타날 수 있기 때문에 실제로 영역/그룹이 아닌 인터페이스를 기반으로 제한이 있다는 점에 유의하십시오. 따라서 영역/그룹의 멤버 수에 따라 영역/그룹당 25개의 규칙을 가질 수 없습니다.
- 특정 인터페이스 개체/트래픽 흐름 조합에 대한 규칙이 적어도 하나 이상 있을 수 있습니다.
- 서비스 정책 변경 사항을 구성에 적용하면 모든 새 연결에서 새로운 서비스 정책을 사용합니다. 기존 연결에서는 연결 설정 당시에 구성된 정책을 계속 사용합니다. 모든 연결에서 새 정책을 즉시 사용하려면 새 정책을 사용하여 다시 연결할 수 있도록 현재 연결을 해제해야 합니다. SSH 또는 콘솔 CLI 세션에서 **clear conn** 또는 **clear local-host** 명령을 입력합니다.

Firepower Threat Defense Service 정책 설정

특정 트래픽 클래스에 서비스를 적용하기 위해 Firepower Threat Defense Service 정책을 사용할 수 있습니다. 예를 들어 모든 TCP 애플리케이션에 적용되는 것과 반대로, 특정 TCP 애플리케이션과 관련된 시간 제한 구성을 만드는 서비스 정책을 사용할 수 있습니다. 서비스 정책은 인터페이스에 적용되거나 전역으로 적용되는 여러 작업 또는 규칙으로 구성됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**을 선택하고 Firepower Threat Defense Service 정책을 편집하려는 액세스 제어 정책의 수정( )을 클릭합니다.

단계 **2** **Advanced(**고급**)**를 클릭합니다.

단계 **3** **Threat Defense Service Policy(Threat Defense Service** 정책**)** 그룹에서 수정( )을 클릭합니다.

기존 정책을 보여 주는 대화 상자가 열립니다. 정책은 전역 규칙(모든 인터페이스에 적용)과 인터페이스 기반 규칙으로 구분된 규칙의 정렬 목록으로 구성됩니다. 테이블에는 인터페이스 개체 및 확장된 액세스 제어 목록 이름(결합된 규칙에 대한 트래픽 클래스 정의) 및 적용된 서비스가 표시됩니다.

단계 **4** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)**을 클릭하여 새로운 규칙을 추가합니다. 서비스 정책 규칙 구성, 5 페이지의 내용을 참조하십시오.
- 수정( )을 클릭하여 기존 규칙을 수정합니다. 서비스 정책 규칙 구성, 5 페이지의 내용을 참조하십시오.
- 삭제( )을 클릭하여 규칙을 삭제합니다.
- 규칙을 클릭하고 새 위치로 드래그하여 옮깁니다. 인터페이스와 전역 목록 간에 규칙을 드래그할 수는 없지만 대신 규칙을 편집하여 인터페이스/전역 설정을 변경해야 합니다. 연결과 일치하는 목록의 첫 번째 규칙이 연결에 적용됩니다.

단계 **5** 정책 편집이 완료되면 **OK(**확인**)**를 클릭합니다.

단계 **6** **Advanced(**고급**)** 창에서 **Save(**저장**)**를 클릭합니다. 저장을 클릭할 때까지 변경 사항이 저장되지 않습니다.

서비스 정책 규칙 구성

특정 트래픽 클래스에 서비스를 적용하기 위해 서비스 정책 규칙을 구성할 수 있습니다.

시작하기 전에

Objects(개체**)** > **Object Management(**개체 관리**)** > **Access List(**액세스 목록**)** > **Extended(**확장**)**로 이동하고 규칙이 적용되는 트래픽을 정의하는 확장된 액세스 목록을 생성합니다. 이 규칙은 확장된 액세스 목록의 허용 규칙과 일치하는 모든 연결에 적용됩니다. ACL 규칙을 정확하게 정의하여 서비스 정책 규칙이 서비스가 필요한 트래픽에만 적용되도록 하십시오.

인터페이스 기반 규칙을 생성하는 경우 할당된 디바이스에서 인터페이스를 구성하고 보안 영역이나 인터페이스 그룹에 인터페이스를 추가해야 합니다.

프로시저

단계 **1** 아직 Firepower Threat Defense Service Policy(Firepower Threat Defense Service 정책) 대화 상자에 존재하지 않는 경우, **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**을 선택하고 액세스 제어 정책을 편집한 다음 **Advanced(**고급**)**를 클릭하고 **Threat Defense Service Policy(Threat Defense Service** 정책**)**를 편집합니다.

단계 **2** 다음 중 하나를 수행합니다.

- **Add Rule(**규칙 추가**)**을 클릭하여 새로운 규칙을 추가합니다.
- 수정( )을 클릭하여 기존 규칙을 수정합니다.

서비스 정책 규칙 마법사가 열리고 규칙을 구성하는 과정을 단계별로 안내합니다.

단계 **3** **Interface Object(**인터페이스 개체**)** 단계에서 정책을 사용하는 인터페이스를 정의하는 옵션을 선택합니다.

- **Apply Globally(**전역으로 적용**)** - 모든 인터페이스에 적용되는 전역 규칙을 생성하려면 이 옵션을 선택합니다.
- **Select Interface Objects(**인터페이스 개체 선택**)** - 인터페이스 기반 규칙을 생성하려면 이 옵션을 선택합니다. 그런 다음 원하는 인터페이스가 포함된 보안 영역 또는 인터페이스 개체를 선택하고 >를 클릭하여 **Next**selected 목록으로 이동합니다. 서비스 정책 규칙은 선택한 개체에 포함된 각 인터페이스에 구성되며 영역/그룹 자체에는 구성되지 않습니다.

인터페이스 기준이 완료되면 클릭합니다.

단계 **4** **Traffic Flow(**트래픽 흐름**)** 단계에서 규칙이 적용되는 연결을 정의하는 확장 ACL 개체를 선택한 후 **Next(**다음**)**를 클릭합니다.

단계 **5** **Connection Setting(**연결 설정**)** 단계에서 이 트래픽 클래스에 적용할 서비스를 구성합니다.

- **Enable TCP State Bypass(TCP** 상태 우회 활성화**)**(TCP 연결만 해당) - TCP 상태 우회를 구현합니다. TCP 상태 우회가 적용되는 연결은 검사 엔진의 검사 대상이 아니며 모든 TCP 상태 검사 및 TCP 정규화를 우회합니다. 자세한 내용은 비동기 라우팅의 TCP 상태 검사 우회(TCP 상태 우회), 8 페이지의 내용을 참조하십시오.

  참고 문제 해결 목적 또는 비대칭 라우팅을 해결할 수 없는 경우 TCP 상태 우회를 사용합니다. 이 기능은 좁은 범위로 정의된 트래픽 클래스로 제대로 구현되지 않는 경우 많은 수의 연결을 유발할 수 있는 여러 보안 기능을 비활성화합니다.

- **Randomize TCP Sequence Number(TCP** 일련 번호 임의 지정**)**(TCP 연결만 해당) - TCP 시퀀스 번호 임의 설정을 활성화하거나 비활성화합니다. 임의 설정은 기본적으로 활성화되어 있습니다. 자세한 내용은 TCP 시퀀스 임의 설정 비활성화, 12 페이지를 참고하십시오.

- **Enable Decrement TTL(TTL** 감소 활성화**)**(TCP 연결만 해당) - 클래스와 일치하는 패킷의 TTL(time-to-live)을 줄입니다. TTL(time-to-live)을 줄이면 TTL이 1인 패킷이 삭제되지만, 연결이 더 큰 TTL이 있는 패킷을 포함할 수 있다는 가정하에 세션에 대한 연결이 열립니다. OSPF Hello 패킷과 같은 일부 패킷은 TTL 이 1로 전송되어 TTL을 줄이면 예기치 않은 결과가 발생할 수 있습니다.

  참고 Firepower Threat Defense 디바이스를 트레이스라우트(traceroute)에 표시하려면 감소 TTL 옵션을 구성하고 플랫폼 설정 정책에서 ICMP 연결 불가 속도 제한을 설정해야 합니다. Firepower Threat Defense 디바이스가 트레이스라우트(traceroute)에 표시되도록 설정, 17 페이지의 내용을 참조하십시오.

- **Connections(**연결**)** - 전체 클래스에 대해 허용된 연결의 수를 제한합니다. 이러한 옵션을 구성할 수 있습니다.
  - **Maximum TCP and UDP(**최대 **TCP** 및 **UDP)**(TCP/UDP 연결만 해당) - 전체 클래스에 대해 허용되는 최대 동시 연결 수(0~2000000)입니다. TCP의 경우 이 수는 설정된 연결에만 적용됩니다. 기본값은 무제한 연결을 허용하는 0입이다. 클래스에 제한이 적용되므로 하나의 공격 호스트가 모든 연결을 사용하여 클래스에 일치하는 호스트를 남겨 두지 않을 수 있습니다. 이 문제를 개선하기 위해 클라이언트당 제한을 설정합니다.

- **Maximum Embryonic(**최대 원시**)**(TCP 연결만 해당) - 허용되는 최대 동시 원시 TCP 연결 수(TCP 핸드셰이크를 완료하지 않은 TCP 연결 수)입니다(0~2000000). 기본값은 무제한 연결을 허용하는 0입이다. 0이 아닌 제한을 설정하면 TCP 가로채기가 활성화되며, 이렇게 하면 TCP SYN 패킷을 인터페이스에 플러딩하여 시행된 DoS 공격으로부터 내부 시스템을 보호할 수 있습니다. 또한 SYN 플러딩을 방지하려면 클라이언트당 옵션을 설정합니다. 자세한 내용은 SYN 플러딩 DoS 공격(TCP 가로채기)로부터 서버 보호, 14 페이지를 참고하십시오.

- **Connections Per Client(**클라이언트당 연결**)** - 특정 클라이언트(소스 IP 주소)에 허용된 연결에 대한 제한입니다. 이러한 옵션을 구성할 수 있습니다.
  - **Maximum TCP and UDP(**최대 **TCP** 및 **UDP)**(TCP/UDP 연결만 해당) - 클라이언트당 허용되는 최대 동시 연결 수(0~2000000)입니다. TCP의 경우 설정된 연결, 원시(절반이 열림) 연결 및 절반이 닫힌 연결을 포함합니다. 기본값은 무제한 연결을 허용하는 0입이다. 이 옵션은 해당 클래스에 일치하는 각 호스트에 대해 허용되는 동시 연결의 최대 수를 제한합니다.
  - **Maximum Embryonic(**최대 원시**)**(TCP/UDP 연결만 해당) - 클라이언트당 허용되는 최대 동시 원시 TCP 연결 수(0~2000000)입니다. 기본값은 무제한 연결을 허용하는 0입이다. 자세한 내용은 SYN 플러딩 DoS 공격(TCP 가로채기)로부터 서버 보호, 14 페이지를 참고하십시오.

- **Connections Timeout(**연결 시간 초과**)** - 트래픽 클래스에 적용할 시간 초과 설정입니다. 이러한 시간 초과는 플랫폼 설정 정책에 정의된 전역 시간 초과 값보다 우선합니다. 다음을 구성할 수 있습니다.
  - **Embryonic(**원시**)**(TCP 연결만 해당) - TCP 원시(절반이 열림) 연결이 닫힐 때까지의 시간 제한 기간(0:0:5~1193:00:00)입니다. 기본값은 0:0:30입니다.
  - **Half Closed(**절반이 닫힘**)**(TCP 연결만 해당) - 절반이 닫힌 연결이 닫힐 때까지의 유휴 시간 제한 기간(0:0:30~1193:0:0)입니다. 기본값은 0:10:0입니다. 절반이 닫힌 연결은 DCD(Dead Connection Detection)의 영향을 받지 않습니다. 또한 해당 시스템은 절반이 닫힌 연결을 해제할 때 재설정을 보내지 않습니다.
  - **Idle(**유휴**)**(TCP, UDP, ICMP, IP 연결) - 프로토콜의 기존 연결이 닫히기까지의 유휴 시간 제한 기간(0:0:1~1193:0:0)입니다. 기본값이 0:2:0인 TCP State Bypass(TCP 상태 우회) 옵션을 선택하지 않는 경우 기본값은 1:0:0입니다.
  - **Reset Connection Upon Timeout(**시간 초과 시 연결 재설정**)**(TCP 연결만 해당) - 유휴 연결이 제거된 후 양방향 시스템에 TCP RST 패킷을 보낼지 여부입니다.

- **Detect Dead Connections(**끊어진 연결 탐지**)** - DCD(Dead Connection Detection)를 활성화할 것인지 지정합니다. 유휴 연결이 만료되기 전에 시스템에서 종단 호스트에 프로브를 보내 연결이 유효한지 확인합니다. 두 호스트가 모두 응답하면 연결이 유지되고 그렇지 않으면 연결이 해제됩니다. 투명 방화벽 모드에서 작동하는 경우 엔드포인트에 대한 정적 경로를 구성해야 합니다. 오프로드된 연결에서는 DCD를 설정할 수 없으므로 사전 필터 정책에서 빠른 경로를 지정하는 연결에서는 DCD를 설정하지 마십시오.FTD CLI에서 **show conn detail** 명령을 사용하여 이니시에이터와 응답자가 전송한 DCD 프로브 수를 추적합니다.

  다음 옵션을 구성합니다.

- **Detection Timeout(**탐지 시간 초과**)** - DCD 프로브에서 응답이 없을 때 또 다른 프로브를 보내기까지 대기하는 시간을 hh:mm:ss 형식으로 설정합니다(0:0:1~24:0:0). 기본값은 0:0:15입니다.

  클러스터 또는 고가용성 구성에서 작동하는 시스템의 경우, 간격을 1분 미만(0:1:0)으로 설정하지 것은 좋지 않습니다. 연결을 다른 시스템으로 옮겨야 한다면, 이러한 변경은 30초 이상 걸리며 변경이 완료되기 전에 연결이 삭제될 수 있습니다.

- **Detection Retries(**탐지 재시도**)** - 연결이 끊어진 상태임을 선언하기 전 DCD에 대한 연속 실패 재시도 횟수를 설정합니다(1~255). 기본값은 5입니다.

단계 **6** 변경 사항을 저장하려면 **Finish(**마침**)**를 클릭합니다.

규칙은 해당 목록의 맨 아래(Interfaces(인터페이스) 또는 Global(전역))에 추가됩니다. 전역 규칙은 하향식 순서로 연결됩니다. 인터페이스 목록의 규칙은 각 인터페이스 개체의 하향식 순서로 연결됩니다. 광범위한 규칙 위에 좁은 범위로 정의된 트래픽 클래스에 대한 규칙을 적용하여 적절한 서비스가 적용되도록 하십시오. 드래그 앤 드롭을 사용하여 각 목록 내에서 규칙을 이동할 수 있습니다. 규칙 목록 간에는 이동할 수 없습니다.

비동기 라우팅의 TCP 상태 검사 우회(TCP 상태 우회)

특정 연결의 인바운드 및 아웃바운드 흐름이 두 개의 다른 Firepower Threat Defense 디바이스를 통과하는 비동기 라우팅 환경이 네트워크에 있는 경우, 영향을 받는 트래픽에 TCP 상태 우회를 구현해야 합니다.

그러나 TCP 상태 우회는 네트워크의 보안을 약화시키므로 매우 제한된 특정 트래픽 클래스에만 우회를 적용해야 합니다.

다음 주제에서는 이러한 문제와 해결책에 대해 자세하게 설명합니다.

비동기 라우팅 문제

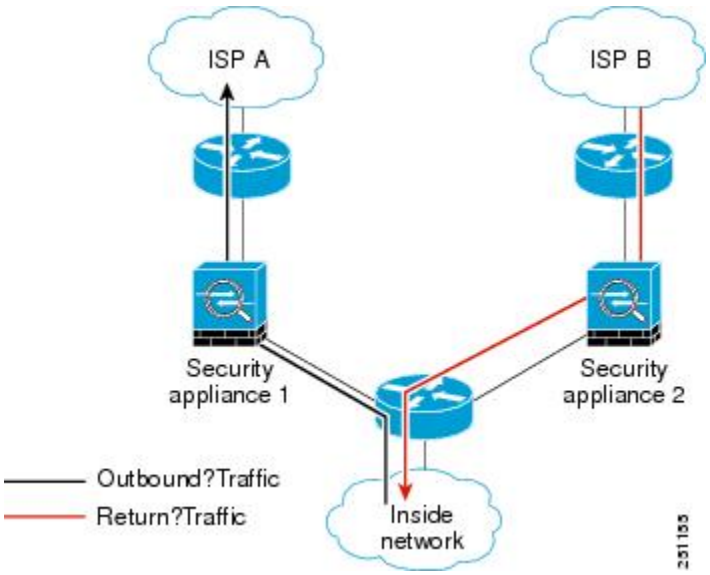
기본적으로 Firepower Threat Defense 디바이스를 통과하는 모든 트래픽은 ASA(Adaptive Security Algorithm)를 사용하여 검사되며, 보안 정책에 따라 통과하도록 허용되거나 삭제됩니다. Firepower Threat Defense 디바이스는 각 패킷의 상태(새 연결인지 설정된 연결인지)를 확인하고 이를 세션 관리 경로(새 연결 SYN 패킷), 빠른 경로(설정된 연결) 또는 제어 평면 경로(고급 검사)에 할당하여 방화벽 성능을 극대화합니다.

빠른 경로에 있는 기존 연결과 일치하는 TCP 패킷은 보안 정책의 모든 사항을 다시 확인하지 않고 Firepower Threat Defense 디바이스를 통과할 수 있습니다. 이 기능은 성능을 극대화합니다. 그러나 SYN 패킷을 사용하여 빠른 경로에서 세션을 설정하는 방법과 빠른 경로에서 발생하는 확인(예: TCP 시퀀스 번호)은 비동기 라우팅 솔루션을 방해할 수 있습니다. 연결의 아웃바운드 및 인바운드 흐름이 모두 동일한 Firepower Threat Defense 디바이스를 통과해야 합니다.

예를 들어, 새로운 연결은 보안 어플라이언스 1로 연결됩니다. SYN 패킷은 세션 관리 경로를 통과하며 연결 항목이 빠른 경로 테이블에 추가됩니다. 이 연결의 후속 패킷이 보안 어플라이언스 1을 통과하는 경우 이러한 패킷은 빠른 경로의 항목과 일치하므로 통과됩니다. 그러나 후속 패킷이 세션 관리

경로를 통과한 SYN 패킷이 없는 Security Appliance 2로 이동하는 경우에는 빠른 경로에 연결을 위한 항목이 없으므로 패킷이 삭제됩니다. 다음 그림에서는 아웃바운드 트래픽이 다른 Firepower Threat Defense 디바이스를 통과한 다음 인바운드 트래픽을 통과하는 비대칭 라우팅 예를 보여줍니다.

그림 *1:* 비대칭 라우팅



업스트림 라우터에서 비동기 라우팅을 구성하고 트래픽이 두 개의 Firepower Threat Defense 디바이스 사이에서 번갈아 전송되는 경우 특정 트래픽에 대한 TCP 상태 우회를 구성할 수 있습니다. TCP 상태 우회는 빠른 경로에서 세션이 설정되는 방식을 변경하고 빠른 경로 확인을 비활성화합니다. 이 기능은 UDP 연결을 처리하듯 TCP 트래픽을 처리합니다. 지정된 네트워크와 일치하는 비 SYN 패킷이 Firepower Threat Defense 디바이스로 들어가고 빠른 경로 항목이 없으면, 빠른 경로에서 연결을 설정할 수 있도록 패킷이 세션 관리 경로로 들어가게 됩니다. 빠른 경로에 있게 되면 이 트래픽은 빠른 경로 확인을 우회합니다.

TCP 상태 우회 가이드라인 및 제한 사항

TCP 상태 우회지원되지 않는 기능

다음 기능은 TCP 상태 우회를 사용할 때 지원되지 않습니다.

- 애플리케이션 검사 - 검사를 수행하려면 인바운드 트래픽과 아웃바운드 트래픽이 모두 동일한 Firepower Threat Defense 디바이스를 통과해야 하므로 검사는 TCP 상태 우회 트래픽에 적용되지 않습니다.
- Snort 검사 - 검사에서는 인바운드 및 아웃바운드 트래픽이 동일한 디바이스를 통과해야 합니다. 하지만 Snort 검사는 TCP 상태 우회 트래픽에 대해 자동으로 우회하지 않습니다. 또한 TCP 상태 우회를 구성할 동일한 트래픽 클래스에 대해 사전 필터 fastpath 규칙을 구성해야 합니다.
- TCP 가로채기, 최대 원시 연결 제한, TCP 시퀀스 번호 임의 설정 - Firepower Threat Defense 디바이스는 연결 상태를 추적하지 않으므로 이러한 기능은 적용되지 않습니다.
- TCP 정규화 - TCP 노멀라이저는 사용되지 않습니다.

- 상태 기반 시스템 대체 작동

TCP 상태 우회 NAT 지침

변환 세션은 Firepower Threat Defense 디바이스에 대해 별도로 설정되기 때문에 두 디바이스 모두에서 TCP 상태 우회 트래픽에 대한 상태 NAT를 구성해야 합니다. 동적 NAT를 사용하는 경우 디바이스 1의 세션에 대해 선택되는 주소는 디바이스 2의 세션에 대해 선택되는 주소와 다릅니다.

TCP 상태 우회 구성

비동기 라우팅 환경에서 TCP 상태 검사를 우회하려면 영향을 받는 호스트 또는 네트워크에만 적용되도록 트래픽 클래스를 신중하게 정의한 다음, 서비스 정책을 사용하여 트래픽의 TCP 상태 우회를 활성화합니다. 또한 트래픽이 검사를 우회할 수 있도록 동일한 트래픽에 대해 해당 사전 필터 fastpath 정책을 구성해야 합니다.

우회는 네트워크의 보안을 약화시키므로 가능한 한 애플리케이션을 제한합니다.

프로시저

단계 **1** 트래픽 클래스를 정의하는 확장 ACL을 생성합니다.

예를 들어 10.1.1.1에서 10.2.2.2까지의 TCP 트래픽에 대한 트래픽 클래스를 정의하려면 다음을 수행합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Access List(**액세스 목록**)** > **Extended(**확장**)**를 선택합니다.
c) **Add Extended Access List(**확장된 액세스 목록 추가**)**를 클릭합니다.
d) 개체의 이름을 입력합니다(예: bypass).
e) **Add(**추가**)**를 클릭하여 규칙을 추가합니다.
f) 작업에 대해 **Allow(**허용**)**를 유지합니다.
g) **Source(**소스**)** 목록 아래에 10.1.1.1을 입력하고 **Add(**추가**)**를 클릭하고 **Destination(**대상**)** 목록 아래에 있는 10.2.2.2를 클릭하고 **Add(**추가**)**를 클릭합니다.
h) **Port(**포트**)**를 클릭하고 **Selected Source Ports(**선택한 소스 포트**)** 목록 아래에 있는 **TCP (6)**를 선택한 다음 **Add(**추가**)**를 클릭합니다. 포트 번호는 입력하지 마십시오. 모든 포트를 포함하는 TCP를 프로토콜로 추가하면 됩니다.
i) Extended Access List Entry(확장된 액세스 목록 항목) 대화 상자에서 **Add(**추가**)**를 클릭하여 규칙을 ACL에 추가합니다.
j) ACL 개체를 저장하려면 Extended Access List Object(확장된 액세스 목록 개체) 대화 상자에서 **Save(**저장**)**를 클릭합니다.

단계 **2** TCP 상태 우회 서비스 정책 규칙을 구성합니다.

예를 들어 이 트래픽 클래스에 대해 TCP 상태 우회를 전역적으로 구성하려면 다음을 수행합니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**를 선택하고 이 서비스를 필요로 하는 디바이스에 할당된 정책을 편집합니다.

b) **Advanced(**고급**)**를 클릭하고 **Threat Defense Service Policy(Threat Defense Service** 정책**)**에 대해 수정( )을 클릭합니다.
c) **Add Rule(**규칙 추가**)**을 클릭합니다.
d) **Apply Globally(**전역으로 적용**)** > **Next(**다음**)**를 선택합니다.
e) 이 규칙에 대해 생성한 확장 ACL 개체를 선택하고 **Next(**다음**)**를 클릭합니다.
f) **Enable TCP State Bypass(TCP** 상태 우회 활성화**)**를 선택합니다.
g) (선택 사항). 우회 연결에 대한 **Idle(**유휴**)** 시간 초과를 조정합니다. 기본은 2분입니다.
h) **Finish(**마침**)**를 클릭하여 규칙을 추가합니다. 필요한 경우 규칙을 서비스 정책의 원하는 위치로 드래그합니다.
i) 서비스 정책에 변경 사항을 저장하려면 **OK(**확인**)**를 클릭합니다.
j) **Advanced(**고급**)**에서 **Save(**저장**)**를 클릭하여 액세스 제어 정책의 변경 사항을 저장합니다.

단계 **3** 트래픽 클래스에 대한 사전 필터 fastpath 규칙을 구성합니다.

사전 필터 규칙에서 ACL 개체를 사용할 수 없으므로 사전 필터 규칙에서 직접 트래픽 클래스를 다시 생성하거나, 먼저 클래스를 정의하는 네트워크 개체를 생성해야 합니다.

다음 절차는 사용자가 이미 액세스 제어 정책에 사전 필터 정책을 연결했다고 가정합니다. 사전 필터 정책을 아직 생성하지 않은 경우 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Prefilter(**사전 필터**)**로 이동하여 먼저 정책을 생성합니다. 그런 다음 이 절차에 따라 액세스 제어 정책에 연결하고 규칙을 생성할 수 있습니다.

이 절차는 예제를 유지하면서 10.1.1.1에서 10.2.2.2까지의 TCP 트래픽에 대한 fastpath 규칙을 생성합니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**를 선택하고 TCP 우회 서비스 정책 규칙이 있는 정책을 편집합니다.
b) 정책 설명 바로 아래 왼쪽에 있는 **Prefilter Policy(**사전 필터 정책**)**의 링크를 클릭합니다.
c) Prefilter Policy(사전 필터 정책) 대화 상자에서 올바른 정책이 선택되지 않은 경우 디바이스에 할당할 정책을 선택합니다. 아직 OK(확인)를 클릭하지 마십시오.

   기본 사전 필터 정책에 규칙을 추가할 수 없으므로 사용자 정의 정책을 선택해야 합니다.

d) Prefilter Policy(사전 필터 정책) 대화 상자에서 수정( )을 클릭합니다. 이 작업을 수행하면 정책을 편집할 수 있는 새 브라우저 창이 열립니다.
e) **Add Prefilter Rule(**사전 필터 규칙 추가**)**을 클릭하고 다음 속성이 있는 규칙을 구성합니다.
   - **Name(**이름**)** - TCP Bypass와 같이 유의미한 이름을 사용할 수 있습니다.
   - **Action(**작업**)** - **Fastpath**를 선택합니다.
   - **Interface Objects(**인터페이스 개체**)** - 전역 규칙으로 TCP 상태 우회를 설정한 경우, 소스와 대상 모두 기본값(any)으로 유지합니다. 인터페이스 기반 규칙을 생성한 경우 **Source Interface Objects(**소스 인터페이스 개체**)** 목록에서 규칙에 사용한 인터페이스 개체와 동일한 인터페이스 개체를 선택하고 any를 대상으로 유지합니다.
   - **Networks(**네트워크**)** - **Source Networks(**소스 네트워크**)** 목록에 10.1.1.1을 추가하고 **Destination Networks(**대상 네트워크**)** 목록에 10.2.2.2를 추가합니다. 네트워크 개체를 사용하거나 수동으로 주소를 추가할 수 있습니다.

- **Ports(**포트**) - Selected Source Ports(**선택한 소스 포트**)**에서 TCP(6), **do not enter a port(**포트 입력 안 함**)**를 선택하고 **Add(**추가**)**를 클릭합니다. 이렇게 하면 TCP 포트 번호에 관계없이 모든(및 유일한) TCP 트래픽에 규칙이 적용됩니다.

f) **Add(**추가**)**를 클릭하여 사전 필터 정책에 규칙을 추가합니다.

g) 사전 필터 정책에 변경 사항을 저장하려면 **Save(**저장**)**를 클릭합니다.

이제 사전 필터 편집 창을 닫고 액세스 제어 정책 편집 창으로 돌아갈 수 있습니다.

h) 액세스 제어 정책 편집 창에서 여전히 Prefilter Policy(사전 필터 정책) 대화 상자가 열려 있어야 합니다. 사전 필터 정책에 변경 사항을 저장하려면 **OK(**확인**)**를 클릭합니다.

i) 변경한 경우, 변경된 사전 필터 정책 할당을 저장하려면 액세스 제어 정책에서 **Save(**저장**)**를 클릭합니다.

이제 영향을 받는 디바이스에 변경 사항을 구축할 수 있습니다.

TCP 시퀀스 임의 설정 비활성화

각 TCP 연결에는 각각 클라이언트와 서버에서 생성된 두 개의 ISN(초기 시퀀스 번호)이 있습니다. Firepower Threat Defense 디바이스는 인바운드와 아웃바운드 두 방향 모두로 전달되는 TCP SYN의 ISN을 임의로 설정합니다.

보호된 호스트의 ISN을 임의로 설정하면 공격자가 새 연결을 위한 다음 ISN을 예측하지 못하며 잠재적으로 새 세션의 가로채기가 방지됩니다.

필요한 경우 예를 들어 데이터 암호화로 인해 TCP 초기 시퀀스 번호 임의 설정을 사용 해제할 수 있습니다. 다음은 임의 지정을 비활성화할 수 있는 몇 가지 상황입니다.

- 다른 인라인 방화벽에서도 초기 시퀀스 번호를 임의로 설정하는 경우에는 두 방화벽 모두 이 작업을 수행할 필요가 없습니다. 이는 이 작업이 트래픽에 영향을 주지 않는 경우에도 마찬가지입니다.
- 디바이스를 통해 eBGP 멀티 홉을 사용하는 경우 eBGP 피어는 MD5를 사용합니다. 임의 설정은 MD5 체크섬을 중단합니다.
- 연결의 시퀀스 번호를 임의 설정하지 않으려면 Firepower Threat Defense 디바이스가 필요한 WAAS 디바이스를 사용합니다.
- ISA 3000에서 하드웨어 우회를 활성화하면 ISA 3000이 더 이상 데이터 경로의 일부가 아닐 때 TCP 연결이 끊어집니다.

프로시저

단계 **1** 트래픽 클래스를 정의하는 확장 ACL을 생성합니다.

예를 들어 호스트에서 10.2.2.2까지의 TCP 트래픽에 대한 트래픽 클래스를 정의하려면 다음을 수행합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Access List(**액세스 목록**)** > **Extended(**확장**)**를 선택합니다.
c) **Add Extended Access List(**확장된 액세스 목록 추가**)**를 클릭합니다.
d) 개체의 이름을 입력합니다(예: preserve-sq-no).
e) **Add(**추가**)**를 클릭하여 규칙을 추가합니다.
f) 작업에 대해 **Allow(**허용**)**를 유지합니다.
g) **Source(**소스**)** 목록을 빈 상태로 두고 **Destination(**대상**)** 목록 아래에 10.2.2.2를 입력하고 **Add(**추가**)**를 클릭합니다.
h) **Port(**포트**)**를 클릭하고 **Selected Source Ports(**선택한 소스 포트**)** 목록 아래에 있는 **TCP (6)**를 선택한 다음 **Add(**추가**)**를 클릭합니다. 포트 번호는 입력하지 마십시오. 모든 포트를 포함하는 TCP를 프로토콜로 추가하면 됩니다.
i) Extended Access List Entry(확장된 액세스 목록 항목) 대화 상자에서 **Add(**추가**)**를 클릭하여 규칙을 ACL에 추가합니다.
j) ACL 개체를 저장하려면 Extended Access List Object(확장된 액세스 목록 개체) 대화 상자에서 **Save(**저장**)**를 클릭합니다.

단계 **2** TCP 시퀀스 번호 임의 지정을 비활성화하는 서비스 정책 규칙을 구성합니다.

예를 들어 이 트래픽 클래스에 대해 임의 지정을 비활성화하려면 다음을 수행합니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**를 선택하고 이 서비스를 필요로 하는 디바이스에 할당된 정책을 편집합니다.
b) **Advanced(**고급**)**를 클릭하고 **Threat Defense Service Policy(**위협 방어 서비스 정책**)**에 대해 수정( )을 클릭합니다.
c) **Add Rule(**규칙 추가**)**을 클릭합니다.
d) **Apply Globally(**전역으로 적용**)** > **Next(**다음**)**를 선택합니다.
e) 이 규칙에 대해 생성한 확장 ACL 개체를 선택하고 **Next(**다음**)**를 클릭합니다.
f) **Randomize TCP Sequence Number(TCP** 일련 번호 임의 지정**)**를 선택 취소합니다.
g) (선택 사항). 필요에 따라 다른 연결 옵션을 조정합니다.
h) **Finish(**마침**)**를 클릭하여 규칙을 추가합니다. 필요한 경우 규칙을 서비스 정책의 원하는 위치로 드래그합니다.
i) 서비스 정책에 변경 사항을 저장하려면 **OK(**확인**)**를 클릭합니다.
j) **Advanced(**고급**)**에서 **Save(**저장**)**를 클릭하여 액세스 제어 정책의 변경 사항을 저장합니다.

이제 영향을 받는 디바이스에 변경 사항을 구축할 수 있습니다.

서비스 정책 규칙 예시

다음 항목에서는 서비스 정책 규칙의 예를 제공합니다.

SYN 플러딩 DoS 공격(TCP 가로채기)로부터 서버 보호

공격자가 호스트에 일련의 SYN 패킷을 보낼 때 SYN 플러딩 DoS(Denial of Service: 서비스 거부) 공격이 발생합니다. 일반적으로 이러한 패킷은 스푸핑된 IP 주소에서 시작합니다. SYN 패킷에 대한 지속적인 플러딩은 서버 SYN 큐를 꽉 찬 상태로 유지하여 합법적인 사용자의 연결 요청에 대응하지 못하도록 합니다.

원시 연결 수를 제한하면 SYN 플러딩 공격을 방지하는 데 도움이 될 수 있습니다. 원시 연결은 소스와 대상 간에 필요한 핸드셰이크를 완료하지 않은 연결 요청입니다.

어떤 연결의 최초 연결 임계값을 초과하면 Firepower Threat Defense 디바이스는 SYN 쿠키 메서드(SYN 쿠키에 대한 자세한 내용은 Wikipedia 참조)를 사용하여 서버의 프록시 역할을 하면서 클라이언트 SYN 요청에 대해 SYN-ACK 응답을 생성합니다. Firepower Threat Defense 디바이스는 클라이언트에서 ACK를 다시 받은 후 클라이언트가 실제 클라이언트인지 인증하고 서버에 연결하도록 허용합니다. 프록시를 수행하는 구성 요소를 TCP 가로채기라고 합니다.

연결 제한을 설정하면 SYN 플러드 공격으로부터 서버를 보호할 수 있습니다. 선택적으로 TCP 가로채기 통계를 활성화하고 정책 결과를 모니터링할 수 있습니다. 다음 절차에서는 이러한 엔드 투 엔드 프로세스에 대해 설명합니다.

시작하기 전에

- 보호하려는 서버의 TCP 백로그 큐보다 원시 연결 제한을 낮게 설정해야 합니다. 그렇지 않을 경우 SYN 공격이 이루어지는 동안 유효한 클라이언트가 서버에 더 이상 액세스할 수 없게 됩니다. 원시 제한에 합당한 값을 정하려면 서버의 용량, 네트워크, 서버 사용량을 신중하게 분석합니다.
- Firepower Threat Defense 디바이스 모델의 CPU 코어 수에 따라 각 코어에서 연결을 관리하는 방식으로 인해 최대 동시 및 원시 연결이 구성된 개수를 초과할 수도 있습니다. 최악의 경우 디바이스는 최대 n-1개(여기서 n은 코어 수)의 추가 연결 및 원시 연결을 허용합니다. 예를 들어 모델에 4개의 코어가 있는 경우 6개의 동시 연결과 4개의 원시 연결을 구성하면 유형별로 3개가 추가될 수 있습니다. 모델의 코어 수를 확인하려면 디바이스 CLI에 **show cpu core** 명령을 입력합니다.

프로시저

단계 **1** 보호하려는 서버 목록인 트래픽 클래스를 정의하는 확장 ACL을 생성합니다.

예를 들어 트래픽 클래스를 정의하여 웹 서버를 IP 주소 10.1.1.5 및 10.1.1.6로 보호하려면 다음을 수행합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Access List(**액세스 목록**)** > **Extended(**확장**)**를 선택합니다.
c) **Add Extended Access List(**확장된 액세스 목록 추가**)**를 클릭합니다.
d) 개체의 이름을 입력합니다(예: protected-servers).
e) **Add(**추가**)**를 클릭하여 규칙을 추가합니다.
f) 작업에 대해 **Allow(**허용**)**를 유지합니다.

g) **Source(**소스**)** 목록을 빈 상태로 두고 **Destination(**대상**)** 목록 아래에 10.1.1.5를 입력하고 **Add(**추가**)**를 클릭합니다.

h) 또한 **Destination(**대상**)** 목록 아래에 10.1.1.6을 입력하고 **Add(**추가**)**를 클릭합니다.

i) **Port(**포트**)**의 사용 가능한 포트 목록에서 **HTTP**를 선택하고 **Add to Destination(**대상에 추가**)**을 클릭합니다. 서버가 HTTPS 연결도 지원하는 경우 해당 포트도 추가합니다.

j) Extended Access List Entry(확장된 액세스 목록 항목) 대화 상자에서 **Add(**추가**)**를 클릭하여 규칙을 ACL에 추가합니다.

k) ACL 개체를 저장하려면 Extended Access List Object(확장된 액세스 목록 개체) 대화 상자에서 **Save(**저장**)**를 클릭합니다.

단계 **2** 원시 연결 제한을 설정하는 서비스 정책 규칙을 구성합니다.

예를 들어 총 동시 원시 제한을 1000개의 연결로 설정하고 클라이언트당 제한을 50개의 연결로 설정하려면 다음을 수행합니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**를 선택하고 이 서비스를 필요로 하는 디바이스에 할당된 정책을 편집합니다.

b) **Advanced(**고급**)**를 클릭하고 **Threat Defense Service Policy(Threat Defense Service** 정책**)**에 대해 수정( )을 클릭합니다.

c) **Add Rule(**규칙 추가**)**을 클릭합니다.

d) **Apply Globally(**전역으로 적용**)** > **Next(**다음**)**를 선택합니다.

e) 이 규칙에 대해 생성한 확장 ACL 개체를 선택하고 **Next(**다음**)**를 클릭합니다.

f) **Connections(**연결**)** > **Maximum Embryonic(**최대 원시**)**에 1000을 입력합니다.

g) **Connections Per Client(**클라이언트당 연결**)** > **Maximum Embryonic(**최대 원시**)**에 50을 입력합니다.

h) (선택 사항). 필요에 따라 다른 연결 옵션을 조정합니다.

i) **Finish(**마침**)**를 클릭하여 규칙을 추가합니다. 필요한 경우 규칙을 서비스 정책의 원하는 위치로 드래그합니다.

j) 서비스 정책에 변경 사항을 저장하려면 **OK(**확인**)**를 클릭합니다.

k) **Advanced(**고급**)**에서 **Save(**저장**)**를 클릭하여 액세스 제어 정책의 변경 사항을 저장합니다.

단계 **3** (선택 사항). TCP 가로채기 통계의 속도를 구성합니다.

TCP 가로채기는 다음 옵션을 사용하여 통계를 수집하는 속도를 결정합니다. 모든 옵션에는 기본값이 있으므로 이러한 비율이 적합한 경우 이 단계를 건너뛸 수 있습니다.

- Rate Interval(속도 간격) - 기록 모니터링 기간의 크기입니다(1~1440분). 기본값은 30분입니다. 이 간격 동안 시스템은 30회의 공격을 샘플링합니다.
- Burst Rate(버스트 속도) - 시스템 로그 메시지 생성의 임계값입니다(25~2147483647). 기본값은 400/초입니다. 버스트 속도가 초과되면 디바이스에서 시스템 로그 메시지 733104를 생성합니다.
- Average Rate(평균 속도) - 시스템 로그 메시지 생성의 평균 속도 임계값입니다(25~2147483647). 기본값은 200/초입니다. 평균 속도가 초과되면 디바이스에서 시스템 로그 메시지 733105를 생성합니다.

이 옵션을 조정하려면 다음을 수행합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) **FlexConfig** > **Text Object(**텍스트 개체**)**를 선택합니다.
c) threat_defense_statistics 시스템 정의 개체에 대해 수정( )을 클릭합니다.
d) 값을 직접 변경할 수는 있지만 **Override(**재정의**)**섹션을 열고 **Add(**추가**)**를 클릭하여 디바이스 재정의를 생성하는 것이 좋습니다.
e) 액세스 제어 정책 할당을 통해 서비스 정책을 할당할 디바이스를 선택하고 **Add(**추가**)**를 클릭하여 선택한 목록으로 이동합니다.
f) **Override(**재정의**)**를 클릭합니다.
g) 개체에는 3개의 항목이 있어야 하므로 3개가 될 때까지 필요에 따라 **Count(**개수**)**를 클릭합니다.
h) 속도 간격, 버스트 속도 및 평균 속도와 같이 1~3의 순서로 필요한 값을 입력합니다. 값을 올바른 순서로 입력했는지 확인하려면 개체 설명을 참조하십시오.
i) Object Override(개체 재정의) 대화 상자에서 **Add(**추가**)**를 클릭합니다.
j) Edit Text Object(텍스트 개체 편집) 대화 상자에서 **Save(**저장**)**를 클릭합니다.

단계 **4** TCP 가로채기 통계를 활성화합니다.

TCP 가로채기 통계를 활성화하려면 FlexConfig 정책을 구성해야 합니다.

a) **Devices(**디바이스**)** > **FlexConfig**를 선택합니다.
b) 이미 디바이스에 정책이 할당되어 있는 경우 편집합니다. 그렇지 않으면 새 정책을 생성하고 영향을 받는 디바이스에 할당합니다.
c) **Available FlexConfig(**사용 가능한 **FlexConfig)** 목록에서 **Threat_Detection_Configure** 개체를 선택하고 **>>**를 클릭합니다. 개체가 **Selected Append FlexConfigs** 목록에 추가됩니다.
d) **Save(**저장**)**를 클릭합니다.
e) (선택 사항). **Preview Config(**구성 미리보기**)**를 클릭하고 디바이스 중 하나를 선택하여 올바른 설정인지 확인할 수 있습니다.

시스템은 다음 구축 중에 디바이스에 기록될 CLI 명령을 생성합니다. 이 명령에는 위협 탐지 통계에 필요한 명령뿐만 아니라 서비스 정책에 필요한 명령도 포함됩니다. 미리보기 하단으로 스크롤하여 추가된 CLI를 확인합니다. TCP 가로채기 통계 명령은 기본값을 사용하는 경우 다음과 유사해야 합니다 (명확성을 위해 줄바꿈이 추가됨).

```
###Flex-config Appended CLI ###

threat-detection statistics tcp-intercept rate-interval 30
       burst-rate 400 average-rate 200
```

단계 **5** 이제 영향을 받는 디바이스에 변경 사항을 구축할 수 있습니다.

단계 **6** 다음 명령을 사용하여 디바이스 CLI에서 TCP 가로채기 통계를 모니터링합니다.

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**] - 공격에서 보호된 상위 10개의 서버를 확인합니다. **all** 키워드는 추적된 모든 서버의 기록 데이터를 보여줍니다. **detail** 키워드는 기록 샘플링 데이터를 보여줍니다. 이 속도 간격 중에 시스템은 공격 횟수를 30회로 샘플링하므로, 기본값인 30분 동안 60초마다 통계가 수집됩니다.

  참고 **shun** 명령을 사용하여 공격 호스트 IP 주소를 차단할 수 있습니다. 차단을 제거하려면 **no shun** 명령을 사용합니다.

- **clear threat-detection statistics tcp-intercept**- TCP 가로채기 통계를 지웁니다.

예제:

```
hostname(config)# show threat-detection statistics top tcp-intercept
Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
<Rank> <Server IP:Port> <Interface> <Ave Rate> <Cur Rate> <Total> <Source IP (Last Attack
Time)>
--------------------------------------------------------------------------------
1    10.1.1.5:80 inside 1249 9503 2249245 <various> Last: 10.0.0.3 (0 secs ago)
2    10.1.1.6:80 inside 10 10 6080 10.0.0.200 (0 secs ago)
```

Firepower Threat Defense 디바이스가 트레이스라우트(traceroute)에 표시되도록 설정

기본적으로 Firepower Threat Defense 디바이스는 트레이스라우트에 홉으로 나타나지 않습니다. 디바이스를 표시하려면 디바이스를 통과하는 패킷에서 TTL(Time to Live)을 줄이고 ICMP 연결 불가 메시지의 속도 제한을 늘려야 합니다. 이를 위해 서비스 정책 규칙을 구성하고 ICMP 플랫폼 설정 정책을 조정해야 합니다.

참고 TTL(time-to-live)을 줄이면 TTL이 1인 패킷이 삭제되지만, 연결이 더 큰 TTL이 있는 패킷을 포함할 수 있다는 가정하에 세션에 대한 연결이 열립니다. OSPF Hello 패킷과 같은 일부 패킷은 TTL 이 1로 전송되어 TTL을 줄이면 예기치 않은 결과가 발생할 수 있습니다. 트래픽 클래스를 정의할 때는 다음 사항을 고려하십시오.

프로시저

단계 **1** 트레이스라우트(traceroute) 보고를 활성화할 트래픽 클래스를 정의하는 확장 ACL을 생성합니다.

예를 들어 OSPF 트래픽을 제외한 모든 주소에 대한 트래픽 클래스를 정의하려면 다음을 수행합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택합니다.
b) 목차에서 **Access List(**액세스 목록**)** > **Extended(**확장**)**를 선택합니다.
c) **Add Extended Access List(**확장된 액세스 목록 추가**)**를 클릭합니다.
d) 개체의 이름을 입력합니다(예: traceroute-enabled).
e) OSPF를 제외하는 규칙을 추가하려면 **Add(**추가**)**를 클릭합니다.
f) 작업을 **Block(**차단**)**으로 변경하고 **Port(**포트**)**를 클릭하고 **Destination Ports(**대상 포트**)** 목록 아래의 프로토콜로 **OSPFIGP (89)**를 선택한 다음 **Add(**추가**)**를 클릭하여 선택한 목록에 프로토콜을 추가합니다.
g) Extended Access List Entry(확장된 액세스 목록 항목) 대화 상자에서 **Add(**추가**)**를 클릭하여 OSPF 규칙을 ACL에 추가합니다.

h) **Add(**추가**)**를 클릭하여 다른 모든 연결을 포함하는 규칙을 추가합니다.
i) 작업에 대해 **Allow(**허용**)**를 유지하고 소스 및 대상 목록을 비워 둡니다.
j) Extended Access List Entry(확장된 액세스 목록 항목) 대화 상자에서 **Add(**추가**)**를 클릭하여 규칙을 ACL에 추가합니다.

   OSPF 거부 규칙이 Allow Any(모두 허용) 규칙 위에 있는지 확인합니다. 필요한 경우 드래그 앤 드롭하여 규칙을 이동합니다.

k) ACL 개체를 저장하려면 Extended Access List Object(확장된 액세스 목록 개체) 대화 상자에서 **Save(**저장**)**를 클릭합니다.

단계 **2** TTL(time-to-live) 값을 감소시키는 서비스 정책 규칙을 구성합니다.

예를 들어 전역적으로 TTL(time-to-live)을 감소시키려면 다음을 수행합니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**를 선택하고 이 서비스를 필요로 하는 디바이스에 할당된 정책을 편집합니다.
b) **Advanced(**고급**)**를 클릭하고 **Threat Defense Service Policy(Threat Defense Service** 정책**)**에 대해 수정( )을 클릭합니다.
c) **Add Rule(**규칙 추가**)**을 클릭합니다.
d) **Apply Globally(**전역으로 적용**)**를 선택하고 **Next(**다음**)**를 클릭합니다.
e) 이 규칙에 대해 생성한 확장 ACL 개체를 선택하고 **Next(**다음**)**를 클릭합니다.
f) **Enable Decrement TTL(TTL** 감소 활성화**)**을 선택합니다.
g) (선택 사항). 필요에 따라 다른 연결 옵션을 조정합니다.
h) **Finish(**마침**)**를 클릭하여 규칙을 추가합니다. 필요한 경우 규칙을 서비스 정책의 원하는 위치로 드래그합니다.
i) 서비스 정책에 변경 사항을 저장하려면 **OK(**확인**)**를 클릭합니다.
j) **Advanced(**고급**)**에서 **Save(**저장**)**를 클릭하여 액세스 제어 정책의 변경 사항을 저장합니다.

   이제 영향을 받는 디바이스에 변경 사항을 구축할 수 있습니다.

단계 **3** ICMP 연결 불가 메시지의 속도 제한을 늘립니다.

a) **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택합니다.
b) 이미 디바이스에 정책이 할당되어 있는 경우 편집합니다. 그렇지 않으면 새 Firepower Threat Defense 플랫폼 설정 정책을 생성하고 영향을 받는 디바이스에 할당합니다.
c) 목차에서 **ICMP**를 선택합니다.
d) **Rate Limit(**속도 제한**)**를 늘립니다(예: 50). 사용되지 않는 경우 **Burst Size(**버스트 크기**)**를 무시할 수 있습니다.

   이 작업과 관련이 없는 경우 ICMP 규칙 테이블을 비워 둘 수 있습니다.

e) **Save(**저장**)**를 클릭합니다.

단계 **4** 이제 영향을 받는 디바이스에 변경 사항을 구축할 수 있습니다.

서비스 정책 모니터링

디바이스 CLI를 사용하여 서비스 정책 관련 정보를 모니터링할 수 있습니다. 다음은 몇 가지 유용한 명령입니다.

- **show conn** [**detail**]

  연결 정보를 표시합니다. 자세한 정보는 특수 연결 특성을 나타내는 플래그를 사용합니다. 예를 들어 "b" 플래그는 TCP 상태 우회의 트래픽 대상을 나타냅니다.

  detail 키워드를 사용하면 DCD(Dead Connection Detection) 검색 관련 정보를 확인할 수 있습니다. 이니시에이터와 응답자가 연결을 탐지하는 방법을 보여줍니다. 예를 들어 DCD가 활성화된 연결에 대한 상세정보는 다음과 같이 표시됩니다.

```
TCP dmz: 10.5.4.11/5555 inside: 10.5.4.10/40299,
    flags UO , idle 1s, uptime 32m10s, timeout 1m0s, bytes 11828,
cluster sent/rcvd bytes 0/0, owners (0,255)
  Traffic received at interface dmz
        Locally received: 0 (0 byte/s)
  Traffic received at interface inside
        Locally received: 11828 (6 byte/s)
  Initiator: 10.5.4.10, Responder: 10.5.4.11
  DCD probes sent: Initiator 5, Responder 5
```

- **show service-policy**

  DCD 통계를 포함하여 서비스 정책 통계를 표시합니다.

- **show threat-detection statistics top tcp-intercept** [**all** | **detail**]

  공격에서 보호된 상위 10개의 서버를 확인합니다. **all** 키워드는 추적된 모든 서버의 기록 데이터를 보여줍니다. **detail** 키워드는 기록 샘플링 데이터를 보여줍니다. 이 속도 간격 중에 시스템은 공격 횟수를 30회로 샘플링하므로, 기본값인 30분 동안 60초마다 통계가 수집됩니다.

Firepower Threat Defense Service 정책 기록

기능	버전	설명
Firepower Threat Defense Service 정책.	6.3	이제 액세스 제어 정책 고급 옵션의 일부로 Firepower Threat Defense Service 정책을 구성할 수 있습니다. 특정 트래픽 클래스에 서비스를 적용하기 위해 Firepower Threat Defense Service 정책을 사용할 수 있습니다. 지원되는 기능에는 TCP 상태 우회, TCP 시퀀스 번호 임의 지정, 패킷의 TTL(time-to-live) 값 감소, Dead Connection Detection, 트래픽 클래스 및 클라이언트당 최대 연결 수 및 원시 연결 수에 대한 제한 설정, 원시 연결, 절반이 닫힌 연결 및 유휴 연결에 대한 시간 초과가 포함됩니다. 새 화면: **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**, **Advanced(**고급**)** 탭, **Threat Defense Service Policy(Threat Defense Service** 정책**)**. 지원 플랫폼: Firepower Threat Defense
DCD(Dead Connection Detection)의 이니시에이터 및 응답자 정보와, 클러스터에서의 DCD 지원입니다.	6.5	DCD(Dead Connection Detection)를 활성화하면, **show conn detail** 명령을 이용해 이니시에이터 및 응답자 정보를 얻을 수 있습니다. DCD(Dead Connection Detection)를 이용하면 비활성 연결을 유지할 수 있으며, **show conn** 출력은 엔드포인트를 얼마나 자주 조사했는지 알려줍니다. 또한 이제 DCD는 클러스터에서도 지원됩니다. 신규/수정된 명령: **show conn** (출력 전용) 지원 플랫폼: Firepower Threat Defense