규칙 및 규칙 집합

규칙

일반적으로 규칙은 도메인 내에서 지정된 유형 및 상태의 개체에 액세스할 수 있는 사용자, 그룹, 역할 또는 조직의 권한을 지정합니다. 멀티 클라우드 방어은(는) 다양한 클라우드 서비스 제공자를 지원하며 이러한 각 환경에는 규칙에 대한 고유한 요구 사항 또는 방법이 있습니다. 클라우드 어카운트에서 생성된 규칙은 멀티 클라우드 방어 컨트롤러에서 생성된 규칙과 다르게 처리될 수 있습니다. 일부 규칙은 기본적으로 게이트웨이 및 인스턴스에 적용되므로 최적의 성능 및 커버리지를 위해 규칙과 정책을 계속 추가하고 수정하면 환경이 기본 보호 레벨을 갖게 됩니다.

규칙 유형은 제공하려는 게이트웨이 환경의 유형을 고려할 때 중요합니다. 모든 규칙 또는 규칙 유형이 모든 게이트웨이 환경과 완전히 호환되는 것은 아닙니다. 멀티 클라우드 방어 컨트롤러에서 지원되는 게이트웨이 유형은 인그레스, 이그레스, 이스트-웨스트입니다.

규칙 및 규칙 집합에 대한 정보 또는 정책 및 그룹에 대한 규칙과 규칙 집합을 생성 또는 수정하는 방법은 이 장의 나머지 부분을 참조하십시오.

정책 관리

정책은 멀티 클라우드 방어 대시보드에서 생성되거나 멀티 클라우드 방어 Terraform 제공자를 사용하는 오케스트레이션을 통해 생성됩니다. 정책은 멀티 클라우드 방어 컨트롤러 데이터베이스의 일부로 저장 및 유지됩니다. 게이트웨이는 주기적 하트비트를 통해 정책 또는 정책 변경 사항을 검색합니다. 여기서 게이트웨이는 컨트롤러 상태 및 텔레메트리 정보를 제공하는 동시에 적용해야 하는 정책 변경이 있는지 요청합니다. 게이트웨이-컨트롤러 통신은 상호 TLS 세션을 통해 완전히 암호화되고 설정됩니다. 하트비트는 5초마다 전송되어 게이트웨이의 정책이 사용자가 생성하거나 수정한 정책과 동기화되도록 합니다.

정책 규칙 집합 게이트웨이 및 관리

정책 규칙 관리

게이트웨이에 할당된 정책 규칙 집합은 다른 정책 규칙 집합으로 동적으로 변경할 수 있습니다. 다른 정책 규칙 집합을 활성 게이트웨이로 교체해야 하는 경우, 이 작업은 영향을 미치지 않는 방식으로 시작될 수 있습니다. 새 정책 규칙 집합의 할당은 게이트웨이 업데이트/업그레이드 프로세스와 유사하게 작동합니다. 새 게이트웨이 인스턴스는 새 정책 규칙 집합으로 인스턴스화됩니다. 새 트래픽 세션이 활성 상태이고 정상 상태이면 새 게이트웨이 인스턴스에 리디렉션됩니다. 이전 트래픽 세션은 이전 게이트웨이 인스턴스에서 플러시됩니다. 이전 게이트웨이 인스턴스는 삭제됩니다. 작업은 몇 분 내에 완료됩니다. 이 변경은 게이트웨이 구성 설정의 일부로 시작됩니다. **Manage(**관리**)** > **Gateways(**게이트웨이**)** > **Gateways(**게이트웨이**)**로 이동합니다. 멀티 클라우드 방어 포털 또는 멀티 클라우드 방어 Terraform 제공자를 사용하여 변경을 시작할 수 있습니다.

정책 규칙 집합 게이트웨이 상태

정책 규칙과 정책 규칙이 연결된 게이트웨이 간 연결 상태는 다음 두 가지 옵션 중 하나일 수 있습니다.

- **Updated(**업데이트됨**)** - 정책이 게이트웨이에서 활성 상태이며 컨트롤러와 동기화되었습니다.
- **Updating(**업데이트 중**)** - 게이트웨이가 정책 변경을 처리 중입니다. 정책 변경 사항은 게이트웨이에 알려지지만 아직 활성화되지 않았습니다. 게이트웨이는 현재 정책을 사용하여 여전히 트래픽을 처리합니다.

규칙 집합 및 규칙 집합 그룹

규칙 집합

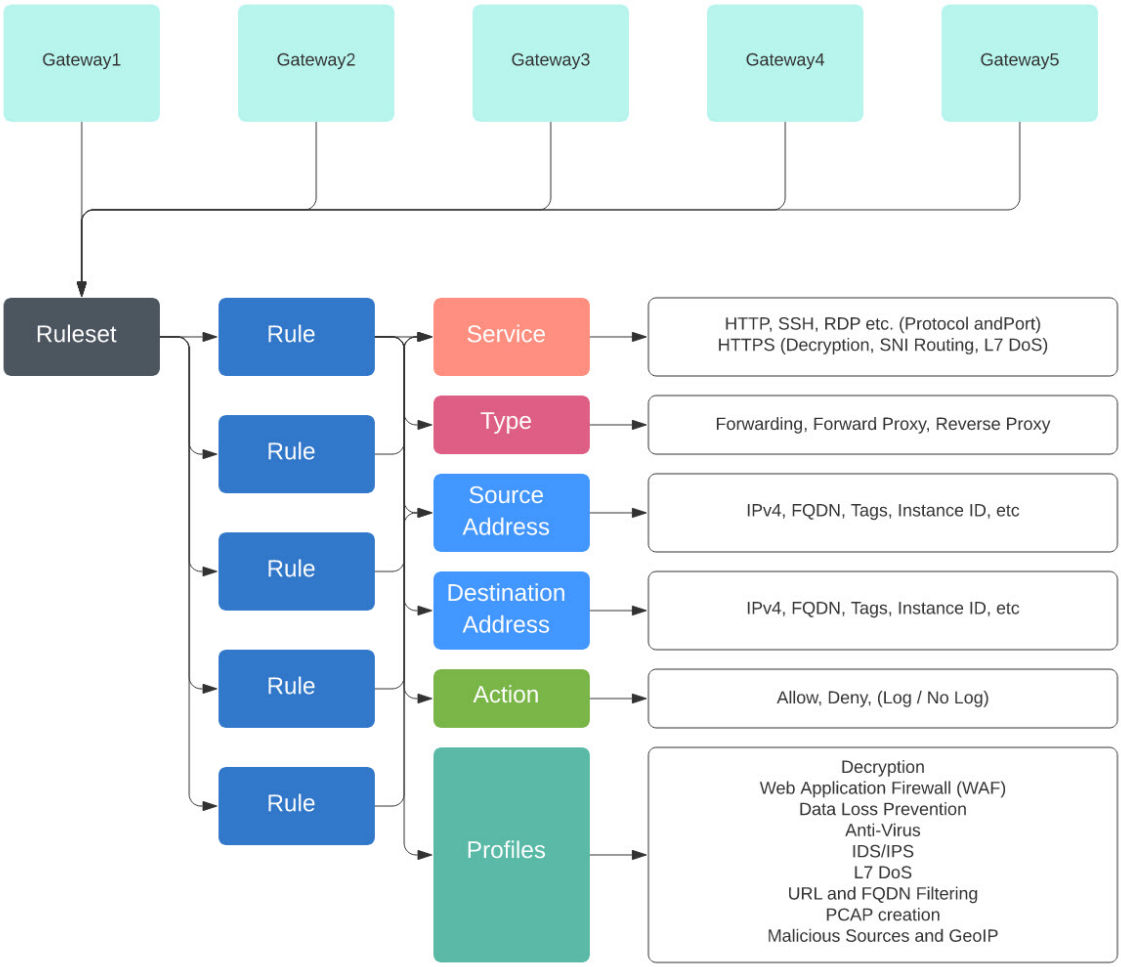
규칙 집합은 애플리케이션 및 워크로드 보호를 수용하기 위해 하나 이상의 게이트웨이 집합에 적용되는 세분화 및 고급 보안 정책을 정의하는 규칙 집합으로 구성됩니다. 규칙은 트래픽이 일치하는 규칙에 의해 처리되는 우선순위 목록으로 구성되고, 허용하거나 거부하기 위해 일반적인 작업이 수행되며, 고급 보안을 통해 추가 검사가 수용됩니다.

규칙 집합은 하나 이상의 멀티 클라우드 방어 게이트웨이와 연결되어야 합니다. 다음과 같은 제한 사항이 규칙 집합에 적용됩니다.

- 규칙 집합은 클라우드 환경에 구애 받지 않고 여러 클라우드에서 하나 이상의 게이트웨이 작업에 적용할 수 있습니다.
- 규칙 집합 그룹을 사용하여 둘 이상의 규칙 집합을 적용할 수 있지만 게이트웨이는 단일 규칙 집합에만 연결할 수 있습니다.
- 규칙 집합 내의 규칙은 검색된 클라우드 자산 정보를 사용하여 변경 사항에 대해 실시간으로 적용되는 정책인 동적 정책을 형성할 수 있습니다.

- 규칙 집합은 클라우드 환경을 통과하는 게이트웨이에 적용되지만, 특정 클라우드 어카운트 및/또는 클라우드 영역에만 적용되는 규칙을 포함할 수 있습니다. 예를 들면 다음과 같습니다.
  - 두 클라우드의 두 게이트웨이에 적용되는 규칙 집합 내의 규칙에 사용되는 동적 태그 기반 주소 개체는 한 클라우드의 게이트웨이와 연결된 IP 주소 집합으로 확인하면서 다른 클라우드의 게이트웨이와 연결된 다른 IP 주소 집합으로 확인할 수 있습니다.

- 규칙 집합은 **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Rule Sets(**규칙 집합**)** 페이지에서 또는 게이트웨이 생성 워크플로우 내에서 생성할 수 있습니다. 다음 다이어그램은 여러 게이트웨이에 적용된 단일 규칙 집합을 보여줍니다.



지원되는 또 다른 활용 사례는 여러 게이트웨이와 연결된 여러 규칙 집합입니다.

정책 규칙 집합 그룹

정책 규칙 집합 그룹은 독립형 규칙 집합의 모음입니다. 사용자는 여러 독립형 규칙 집합을 하나의 정책 규칙 집합 그룹으로 결합하고 그룹을 하나 이상의 멀티 클라우드 방어 게이트웨이에 연결할 수

있습니다. 정책 규칙 집합 그룹을 사용하면 조직에서 정책을 체계에 따라 분리하고 하나의 전반적인 정책에 결합할 수 있습니다.

Note

- 정책 규칙 집합 그룹은 규칙 집합 멤버로만 구성될 수 있습니다.
- 정책 규칙 집합 그룹과 연관된 모든 규칙 집합에 충돌하는 규칙이 없는지 확인합니다.
- 정책 규칙 집합 그룹에는 최대 100개의 규칙 집합 멤버를 포함할 수 있습니다.

정책 규칙 집합 생성

정책 규칙 집합을 생성하려면 다음을 수행합니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Rule Sets(**규칙 집합**)**로 이동합니다.
단계 **2** **Create(**생성**)**를 클릭합니다.
단계 **3** 정책 규칙 집합의 이름과 설명을 추가합니다.
단계 **4** **Save(**저장**)**를 클릭합니다.

What to do next

정책 규칙 집합이 생성되면 규칙 집합에 규칙 집합에서 정방향 프록시 규칙 추가 또는 편집합니다.

규칙 집합에서 규칙 생성

-

규칙 집합에서 전달 규칙 추가 또는 편집

다음 절차를 사용하여 기존 규칙을 정책 규칙 집합에 추가하거나 정책 규칙 집합에 이미 포함된 규칙을 편집합니다.

시작하기 전에

멀티 클라우드 방어 게이트웨이 내에서 새 규칙을 생성할 수 있습니다. 규칙 집합에 규칙을 추가하거나 편집하기 전에 다음 제한 사항에 유의하십시오.

- 단일 정책 규칙 집합에는 최대 2,047개의 규칙을 사용할 수 있습니다.
- 정책 규칙 집합 그룹에는 최대 2,047개의 규칙 집합을 포함할 수 있습니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Rule Sets(**규칙 집합**)**로 이동합니다.

단계 **2** 정책 규칙 집합을 보려면 정책 규칙 집합 이름을 클릭합니다.

단계 **3** **Add Rule(**규칙 추가**)**를 클릭하여 새 규칙을 생성하거나 기존 규칙을 추가합니다. 프롬프트가 생성됩니다.

단계 **4** 다음 속성을 입력합니다.

- **Name(**이름**)** -규칙을 참조하는 데 사용되는 친숙하고 고유한 이름입니다.
- (선택 사항) **Description(**설명**)** - 규칙에 대한 간단한 설명입니다.
- **Type(**유형**)** - **Forwarding(**정방향**)**을 선택합니다.

단계 **5** 다음 개체 정보를 입력합니다.

- **Service(**서비스**)** - 규칙을 적용할 프로토콜 및 포트를 결정하는 데 사용되는 서비스 개체입니다.
- **Source(**소스**)** - 규칙을 적용할 리소스를 결정하는 데 사용되는 주소 개체입니다.
- **Destination(**대상**)** - 규칙을 적용할 대상 리소스를 결정하는 데 사용되는 주소 개체입니다. **ReverseProxy** 규칙 유형의 경우 대상은 항상 멀티 클라우드 방어 게이트웨이입니다. **ForwardProxy** 규칙 유형의 경우 대상은 항상 any(모두)입니다.
- **FQDN** - 드롭다운 메뉴를 사용하여 SNI 일치에 사용되는 FQDN 집합을 선택합니다. **Forwarding(**전달**)** 규칙 유형에만 적용됩니다.

단계 **6** 다음 세부사항을 입력합니다.

- **Action(**작업**)** - 작업은 트래픽을 허용할지 아니면 거부할지, 그리고 트래픽을 Events(이벤트)에 기록할지 여부를 정의합니다. 트래픽은 Action(작업)이 **Log(**로그**)** 또는 **No Log(**로그 없음**)**로 설정되어 있는지 여부에 상관없이 항상 Traffic Summary(트래픽 요약)에 로깅됩니다. 규칙에서 허용하는 트래픽의 경우 고급 보안 프로파일이 평가됩니다. 각 고급 보안 프로파일에는 이 작업을 사용하거나 재정의하는 자체 작업이 있습니다.
- **Reset On Deny(**거부 시 재설정**)** - 활성화된 경우 멀티 클라우드 방어 게이트웨이에서는 이 정책과 일치하는 세션에 대해 TCP 재설정 패킷을 전송하지만 게이트웨이에 의해 삭제됩니다. **Forwarding(**전달**)** 규칙 유형에만 적용됩니다.

단계 **7** 다음 프로파일 정보를 입력합니다.

- (선택 사항) **Network Intrusion(**네트워크 침입**)** - 고급 보안에 사용할 IPS(Network Intrusion) 프로파일입니다.
- (선택 사항) **Anti-malware(**악성코드 차단**)** - 고급 보안에 사용할 악성코드 차단 프로파일입니다. 악성코드 차단 프로파일을 아직 생성하지 않은 경우 **+ Create an Anti Malware(+** 악성코드 차단 생성**)**를 클릭합니다.
- (선택 사항) **Data Loss Prevention(**데이터 손실 방지**)** - 고급 보안에 사용할 DLP(데이터 손실 방지) 프로파일입니다. **ForwardProxy** 규칙 유형에만 적용됩니다.
- (선택 사항) **FQDN Filtering(FQDN** 필터링**)** - 고급 보안에 사용할 FQDN(FQDN Filtering)(FQDN) 프로파일입니다.
- (선택 사항) **Malicious IPs(**악의적인 **IP)** - 고급 보안에 사용할 MIP(Malicious IP) 프로파일입니다.
- (선택 사항) **PCAP** - 활성화하려면 이 확인란을 선택합니다. 규칙에 대해 패킷 캡처를 활성화할지 아니면 비활성화할지 여부입니다. 트래픽이 PCAP가 활성화된 규칙과 일치할 때마다 세션 트래픽의 패킷 캡처가 발생하고

PCAP는 PCAP 프로파일에 의해 지정된 위치에 저장됩니다. PCAP 프로파일은 멀티 클라우드 방어 게이트웨이에 구성됩니다.

단계 **8** 규칙에 대한 구성을 지정한 후 **Save(**저장**)**를 클릭합니다.

단계 **9** 규칙을 계속 추가합니다. 원하는 규칙을 모두 추가했으면 **Save Changes(**변경 사항 저장**)**를 클릭합니다. 규칙 집합에 대한 모든 변경 사항의 전후 보기가 표시됩니다. 변경 사항에 만족하면 **Save(**저장**)**를 클릭합니다. 추가로 변경해야 하는 경우에는 **Cancel(**취소**)**을 클릭하여 규칙 집합 편집으로 돌아갑니다.

규칙 집합에서 정방향 프록시 규칙 추가 또는 편집

다음 절차를 사용하여 기존 규칙을 정책 규칙 집합에 추가하거나 정책 규칙 집합에 이미 포함된 규칙을 편집합니다.

시작하기 전에

멀티 클라우드 방어 게이트웨이 내에서 새 규칙을 생성할 수 있습니다. 규칙 집합에 규칙을 추가하거나 편집하기 전에 다음 제한 사항에 유의하십시오.

- 단일 정책 규칙 집합에는 최대 2,047개의 규칙을 사용할 수 있습니다.
- 정책 규칙 집합 그룹에는 최대 2,047개의 규칙 집합을 포함할 수 있습니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Rule Sets(**규칙 집합**)**로 이동합니다.

단계 **2** 정책 규칙 집합을 보려면 정책 규칙 집합 이름을 클릭합니다.

단계 **3** **Add Rule(**규칙 추가**)**를 클릭하여 새 규칙을 생성하거나 기존 규칙을 추가합니다. 프롬프트가 생성됩니다.

단계 **4** 다음 속성을 입력합니다.

- **Name(**이름**)** -규칙을 참조하는 데 사용되는 친숙하고 고유한 이름입니다.
- (선택 사항) **Description(**설명**)** - 규칙에 대한 간단한 설명입니다.
- **Type(**유형**)** - **ReverseProxy**를 선택합니다.

단계 **5** 다음 개체 정보를 입력합니다.

- **Service(**서비스**)** - 규칙을 적용할 프로토콜 및 포트를 결정하는 데 사용되는 서비스 개체입니다.
- **Source(**소스**)** - 규칙을 적용할 리소스를 결정하는 데 사용되는 주소 개체입니다.
- **Destination(**대상**)** - 규칙을 적용할 대상 리소스를 결정하는 데 사용되는 주소 개체입니다. **ReverseProxy** 규칙 유형의 경우 대상은 항상 멀티 클라우드 방어 게이트웨이입니다.
- **Target(**대상**)** - 멀티 클라우드 방어 게이트웨이에서 게이트웨이-서버 연결을 설정할 대상을 지정하는 데 사용되는 주소 개체입니다.

단계 **6** 기본 규칙 **Action(**작업**)**을 선택합니다. 트래픽을 허용할지 아니면 거부할지, 그리고 트래픽을 Events(이벤트)에 기록할지 여부를 정의합니다. 트래픽은 Action(작업)이 **Log(**로그**)** 또는 **No Log(**로그 없음**)**로 설정되어 있는지 여부에

상관없이 항상 Traffic Summary(트래픽 요약)에 로깅됩니다. 규칙에서 허용하는 트래픽의 경우 고급 보안 프로파일이 평가됩니다. 각 고급 보안 프로파일에는 이 작업을 사용하거나 재정의하는 자체 작업이 있습니다.

단계 **7** 다음 프로파일 정보를 입력합니다.

- (선택 사항) **Network Intrusion(**네트워크 침입**)** - 고급 보안에 사용할 IPS(Network Intrusion) 프로파일입니다.
- (선택 사항) **Anti-malware(**악성코드 차단**)** - 고급 보안에 사용할 악성코드 차단 프로파일입니다. 악성코드 차단 프로파일을 아직 생성하지 않은 경우 **+ Create an Anti Malware(+** 악성코드 차단 생성**)**를 클릭합니다.
- (선택 사항) **Web Protection(**웹 보호**)** - 고급 보안에 사용할 WAF(Web Protection) 프로파일입니다. 이는 **ReverseProxy** 규칙 유형에만 적용됩니다.
- (선택 사항) **URL Filtering(URL** 필터링**)** - 고급 보안에 사용할 URL(URL 필터링) 프로파일입니다. 이는 **ForwardProxy** 및 **ReverseProxy** 규칙 유형에만 적용됩니다.
- (선택 사항) **Malicious IPs(**악의적인 **IP)** - 고급 보안에 사용할 MIP(Malicious IP) 프로파일입니다.
- (선택 사항) **PCAP** - 활성화하려면 이 확인란을 선택합니다. 규칙에 대해 패킷 캡처를 활성화할지 아니면 비활성화할지 여부입니다. 트래픽이 PCAP가 활성화된 규칙과 일치할 때마다 세션 트래픽의 패킷 캡처가 발생하고 PCAP는 PCAP 프로파일에 의해 지정된 위치에 저장됩니다. PCAP 프로파일은 멀티 클라우드 방어 게이트웨이에 구성됩니다.

단계 **8** 규칙에 대한 구성을 지정한 후 **Save(**저장**)**를 클릭합니다.

단계 **9** 규칙을 계속 추가합니다. 원하는 규칙을 모두 추가했으면 **Save Changes(**변경 사항 저장**)**를 클릭합니다. 규칙 집합에 대한 모든 변경 사항의 전후 보기가 표시됩니다. 변경 사항에 만족하면 **Save(**저장**)**를 클릭합니다. 추가로 변경해야 하는 경우에는 **Cancel(**취소**)**을 클릭하여 규칙 집합 편집으로 돌아갑니다.

규칙 집합에서 정방향 프록시 규칙 추가 또는 편집

다음 절차를 사용하여 기존 규칙을 정책 규칙 집합에 추가하거나 정책 규칙 집합에 이미 포함된 규칙을 편집합니다.

Before you begin

멀티 클라우드 방어 게이트웨이 내에서 새 규칙을 생성할 수 있습니다. 규칙 집합에 규칙을 추가하거나 편집하기 전에 다음 제한 사항에 유의하십시오.

- 단일 정책 규칙 집합에는 최대 2,047개의 규칙을 사용할 수 있습니다.
- 정책 규칙 집합 그룹에는 최대 2,047개의 규칙 집합을 포함할 수 있습니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Rule Sets(**규칙 집합**)**로 이동합니다.

단계 **2** 정책 규칙 집합을 보려면 정책 규칙 집합 이름을 클릭합니다.

단계 **3** **Add Rule(**규칙 추가**)**를 클릭하여 새 규칙을 생성하거나 기존 규칙을 추가합니다. 프롬프트가 생성됩니다.

단계 **4** 다음 속성을 입력합니다.

- **Name(**이름**)** -규칙을 참조하는 데 사용되는 친숙하고 고유한 이름입니다.

- (선택 사항) **Description(**설명**)** - 규칙에 대한 간단한 설명입니다.
- **Type(**유형**)** - **ForwardProxy**를 선택합니다.

단계 **5** 다음 개체 정보를 입력합니다.

- **Service(**서비스**)** - 규칙을 적용할 프로토콜 및 포트를 결정하는 데 사용되는 서비스 개체입니다.
- **Source(**소스**)** - 규칙을 적용할 리소스를 결정하는 데 사용되는 주소 개체입니다.
- **Destination(**대상**)** - 규칙을 적용할 대상 리소스를 결정하는 데 사용되는 주소 개체입니다. **ForwardProxy** 규칙 유형의 경우 대상은 항상 any(모두)입니다.
- **FQDN** - 드롭다운 메뉴를 사용하여 SNI 일치에 사용되는 FQDN 집합을 선택합니다. **Forwarding(**전달**)** 규칙 유형에만 적용됩니다.

단계 **6** 기본 규칙 **Action(**작업**)**을 입력합니다. 트래픽을 허용할지 아니면 거부할지, 그리고 트래픽을 Events(이벤트)에 기록할지 여부를 정의합니다. 트래픽은 Action(작업)이 **Log(**로그**)** 또는 **No Log(**로그 없음**)**로 설정되어 있는지 여부에 상관없이 항상 Traffic Summary(트래픽 요약)에 로깅됩니다. 규칙에서 허용하는 트래픽의 경우 고급 보안 프로파일이 평가됩니다. 각 고급 보안 프로파일에는 이 작업을 사용하거나 재정의하는 자체 작업이 있습니다.

단계 **7** 다음 프로파일 정보를 입력합니다.

- (선택 사항) **Network Intrusion(**네트워크 침입**)** - 고급 보안에 사용할 IPS(Network Intrusion) 프로파일입니다.
- (선택 사항) **Anti-malware(**악성코드 차단**)** - 고급 보안에 사용할 악성코드 차단 프로파일입니다. 악성코드 차단 프로파일을 아직 생성하지 않은 경우 **+ Create an Anti Malware(+** 악성코드 차단 생성**)**를 클릭합니다.
- (선택 사항) **Data Loss Prevention(**데이터 손실 방지**)** - 고급 보안에 사용할 DLP(데이터 손실 방지) 프로파일입니다. **ForwardProxy** 규칙 유형에만 적용됩니다.
- (선택 사항) **URL Filtering(URL** 필터링**)** - 고급 보안에 사용할 URL(URL 필터링) 프로파일입니다. 이는 **ForwardProxy** 및 **ReverseProxy** 규칙 유형에만 적용됩니다.
- (선택 사항) **FQDN Filtering(FQDN** 필터링**)** - 고급 보안에 사용할 FQDN(FQDN Filtering)(FQDN) 프로파일입니다.
- (선택 사항) **Malicious IPs(**악의적인 **IP)** - 고급 보안에 사용할 MIP(Malicious IP) 프로파일입니다.
- (선택 사항) **PCAP** - 활성화하려면 이 확인란을 선택합니다. 규칙에 대해 패킷 캡처를 활성화할지 아니면 비활성화할지 여부입니다. 트래픽이 PCAP가 활성화된 규칙과 일치할 때마다 세션 트래픽의 패킷 캡처가 발생하고 PCAP는 PCAP 프로파일에 의해 지정된 위치에 저장됩니다. PCAP 프로파일은 멀티 클라우드 방어 게이트웨이에 구성됩니다.

단계 **8** 규칙에 대한 구성을 지정한 후 **Save(**저장**)**를 클릭합니다.

단계 **9** 규칙을 계속 추가합니다. 원하는 규칙을 모두 추가했으면 **Save Changes(**변경 사항 저장**)**를 클릭합니다. 규칙 집합에 대한 모든 변경 사항의 전후 보기가 표시됩니다. 변경 사항에 만족하면 **Save(**저장**)**를 클릭합니다. 추가로 변경해야 하는 경우에는 **Cancel(**취소**)**을 클릭하여 규칙 집합 편집으로 돌아갑니다.

규칙 집합의 규칙 비활성화, 편집, 복제 또는 삭제

다음 절차를 사용하여 규칙 집합에 대해 구성된 기존 규칙을 편집하거나 복제합니다. 현재 정책 또는 규칙 집합에 대해 활성화할 필요가 없는 경우에는 규칙을 비활성화할 수도 있습니다. 지금 또는 향후 구축에 필요하지 않은 경우 규칙을 삭제할 수 있습니다.

한 번에 하나의 규칙만 편집하거나 복제할 수 있다는 점에 유의하십시오. 여러 규칙을 동시에 삭제하거나 비활성화할 수 있습니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Rule Sets(**규칙 집합**)**로 이동합니다.

단계 **2** 비활성화, 편집, 복제 또는 삭제할 규칙이 포함된 규칙 집합을 찾은 다음 규칙 집합 이름을 클릭합니다.

단계 **3** 독립형 규칙의 확인란을 선택합니다.

단계 **4** **Actions(**작업**)** 버튼을 확장합니다.

단계 **5** 실행 가능한 항목을 선택합니다.

- **Disable(**비활성화**)** - 이 옵션은 규칙 집합의 규칙을 유지하지만 트래픽에 영향을 미치지 않는 규칙 및 구성된 규칙 작업을 비활성화합니다.
- **Edit(**편집**)** - 이 옵션은 Properties(속성) 창을 실행하며 규칙의 구성을 편집할 수 있습니다. **Save(**저장**)**를 클릭하여 변경 사항을 저장합니다.
- **Clone(**복제**)** - 이 옵션은 규칙의 복제본을 생성하며, 복제된 규칙의 이름을 지정하거나 규칙의 구성을 추가로 변경할 수 있는 Properties(속성) 창을 엽니다. **Save(**저장**)**를 클릭하여 구성을 확인합니다. 복제된 규칙을 저장하면 현재 보고 있는 규칙 집합에 자동으로 추가됩니다.
- **Delete(**삭제**)** - 이 옵션은 규칙 집합에서 규칙을 영구적으로 제거합니다. 그 결과 게이트웨이에서도 규칙이 제거되었습니다.

단계 **6** **Save Changes(**변경사항 저장**)**를 클릭하여 규칙에 대해 수행한 변경사항을 확인하고 규칙 집합을 간접적으로 수행합니다. 변경 사항을 저장하지 않으려면 **Cancel(**취소**)**을 클릭합니다. 게이트웨이에 대한 변경 사항의 손실이 정상적인지 확인합니다.

정책 규칙 집합 그룹 생성

정책 규칙 집합 그룹을 생성하려면 다음을 수행합니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Rules(**규칙**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 정책 규칙 집합의 이름과 설명을 추가합니다.

단계 **4** **Type(**유형**)**을 Group(그룹)으로 선택합니다.

단계 **5** 드롭다운 메뉴를 확장하여 **Rule Set List(**규칙 집합 목록**)** 섹션에서 규칙 집합을 추가합니다. 규칙 집합을 더 추가하려면 **Add Rule Sets(**규칙 집합 추가**)**를 클릭하여 다른 행을 추가합니다.