보안 프로파일

암호 해독 프로파일

암호 해독 프로파일은 역방향 프록시 또는 정방향 프록시 시나리오에서 멀티 클라우드 방어 게이트웨이에 의해 사용됩니다. 연결이 프록시되면 프런트엔드 세션은 게이트웨이에서 종료되고, 서버에 새 백엔드 세션이 설정됩니다. 이러한 종료의 목적은 트래픽을 암호 해독하고 검사하여 악의적인 활동으로부터 보호하기 위한 것입니다. 암호화된 트래픽을 해독하려면 Decryption Profile(암호 해독 프로파일)이 필요합니다.

암호 해독 프로파일 생성

다음 절차에 따라 암호 해독 프로파일을 생성합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Decryption(**암호 해독**)**으로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Profile Name(**프로파일 이름**)** 및 **Description(**설명**)**을 지정합니다.

단계 **4** **Certificate Method(**인증서 방법**)**으로 **Select Existing(**기존 선택**)**을 선택합니다.

단계 **5** **Certificate(**인증서**)**로 원하는 인증서를 선택합니다.

단계 **6** **Min TLS Version(**최소 **TLS** 버전**)**에서 암호 해독 프로파일이 허용하는 가장 낮은 TLS 버전을 선택합니다. 기본값은 TLS 1.0입니다.

단계 **7** 기본값 이외의(비 PFS) 암호 그룹을 사용하는 경우 Diffie-Hellman 또는 PKCS (RSA) 메뉴에서 원하는 암호 그룹 집합을 선택합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

What to do next

- 프로파일 세부 정보 보기
- 프로파일에 게이트웨이 연결 추가

암호 해독 프로파일의 **TLS** 버전

멀티 클라우드 방어 게이트웨이은(는) 모든 TLS 버전(TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0)을 지원합니다. 사용자는 사용할 최소 TLS 버전을 지정할 수 있으며, 멀티 클라우드 방어 게이트웨이은(는) 지정된 최소 TLS 버전 이상인 TLS 버전을 협상합니다. 멀티 클라우드 방어 게이트웨이은(는) TLS 협상 중에 항상 가능한 가장 높은 TLS 버전을 사용합니다. 멀티 클라우드 방어 게이트웨이이(가) 지정된 최소 TLS 버전을 충족하는 버전을 협상할 수 없는 경우 멀티 클라우드 방어 게이트웨이에서는 세션을 삭제하고 `TLS_ERROR` 이벤트를 로깅합니다.

Note 게이트웨이에는 단일 최소 TLS 버전만 적용할 수 있습니다. 정책 규칙 집합 또는 정책 규칙 집합 그룹 내에서 사용되는 모든 서비스 개체에서 참조하는 모든 암호 해독 프로파일에 일관된 최소 TLS 버전을 사용해야 합니다. 다른 최소 TLS 버전이 지정된 경우, 적용할 최소 TLS 버전을 미리 결정할 수 없습니다.

암호 그룹

멀티 클라우드 방어 게이트웨이는 사용자가 선택 가능한 기본 암호 그룹 집합을 지원합니다. 기본 집합은 항상 선택되는 PFS 암호 그룹입니다. 사용자 선택 가능한 집합은 Diffie-Hellman 및 PKCS(RSA) 암호 그룹(사용자가 선택할 수 있음)입니다. 결합된 암호 그룹 집합(기본 및 사용자 선택)은 게이트웨이에서 안전한 프런트 엔드 암호화 세션을 설정하는 데 사용됩니다. 클라이언트는 선호하는 암호 그룹의 순서가 지정된 목록을 전송합니다. 게이트웨이는 클라이언트가 제출한 순서가 지정된 집합과 게이트웨이에서 사용 가능한 집합에서 선택한 암호 그룹으로 응답합니다. 클라이언트가 서버가 순서를 정의하도록 허용하는 경우, 게이트웨이에서 사용 가능한 순서가 지정된 집합과 클라이언트가 제출한 집합에서 암호 그룹을 선택합니다.

다음은 게이트웨이에서 지원하고 암호 해독 프로파일에서 사용 가능한 암호 그룹의 순서가 지정된 목록입니다.

카테고리	암호 그룹	키 교환	암호화	해시	기본
PFS	ECDHE-RSA-AES256-GCM-SHA384	ECDHE-RSA	AES256-GCM	SHA384	☐
PFS	ECDHE-RSA-AES256-CBC-SHA384	ECDHE-RSA	AES256-CBC	SHA384	☐
Diffie-Hellman	DH-RSA-AES256-GCM-SHA384	DH-RSA	AES256-GCM	SHA384	
PFS	DHE-RSA-AES256-GCM-SHA384	DHE-RSA	AES256-GCM	SHA384	☐
PFS	DHE-RSA-AES256-CBC-SHA256	DHE-RSA	AES256-CBC	SHA384	☐
PFS	DHE-RSA-AES256-CBC-SHA	DHE-RSA	AES256-CBC	SHA	☐
Diffie-Hellman	DH-RSA-AES256-SHA256	DH-RSA	AES256-CBC	SHA256	
Diffie-Hellman	DH-RSA-AES256-SHA	DH-RSA	AES256-CBC	SHA160	
PKCS(RSA)	AES256-GCM-SHA384	PKCS-RSA	AES256-GCM	SHA384	
PKCS(RSA)	AES256-SHA256	PKCS-RSA	AES256-CBC	SHA256	
PKCS(RSA)	AES256-SHA	PKCS-RSA	AES256-CBC	SHA160	
PFS	ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA	AES128-GCM	SHA256	☐
PFS	ECDHE-RSA-AES128-CBC-SHA256	ECDHE-RSA	AES128-CBC	SHA256	☐
Diffie-Hellman	DH-RSA-AES128-GCM-SHA256	DH-RSA	AES128-GCM	SHA256	
PFS	DHE-RSA-AES128-GCM-SHA256	DHE-RSA	AES128-GCM	SHA256	☐
PFS	DHE-RSA-AES128-CBC-SHA256	DHE-RSA	AES128-CBC	SHA256	☐
Diffie-Hellman	DH-RSA-AES128-SHA256	DH-RSA	AES128-CBC	SHA256	
Diffie-Hellman	DH-RSA-AES128-SHA	DH-RSA	AES128-CBC	SHA160	
PKCS(RSA)	AES128-GCM-SHA256	PKCS-RSA	AES128-GCM	SHA256	
PKCS(RSA)	AES128-SHA256	PKCS-RSA	AES128-CBC	SHA256	
PKCS(RSA)	AES128-SHA	PKCS-RSA	AES128-CBC	SHA160	
PFS	ECDHE-RSA-DES-CBC3-SHA	ECDHE-RSA	DES-CBC3	SHA	☐
PFS	ECDHE-RSA-RC4-SHA	ECDHE-RSA	RC4	SHA	☐
PKCS(RSA)	RC4-SHA	PKCS-RSA	RC4	SHA160	
PKCS(RSA)	RC4-MD5	PKCS-RSA	RC4	SHA160	

네트워크 침입**(IDS/IPS)** 프로파일

네트워크 침입 프로파일은 트래픽이 악의적이지 않은지 확인하는 트랜잭션을 평가하는 데 사용할 수 있는 침입 탐지 및 보호(IDS/IPS) 규칙의 모음입니다.

멀티 클라우드 방어에서는 다음 IDS/IPS 규칙 집합을 지원합니다.

Table 1: 멀티 클라우드 방어에서는 다음 ***IDS/IPS*** 규칙 집합을 지원합니다.

규칙 집합	설명
Talos 규칙	Rules규칙은 애플리케이션 및 프레임워크에 고급 수준의 보호를 제공하는 실제 조사, 침입 테스트 및 연구를 통해 수집된 인텔리전스를 기반으로 하는 Cisco의 고급 규칙 집합입니다.
맞춤형 규칙	맞춤형 규칙은 맞춤형 애플리케이션에 특수 수준의 보호를 제공하며 고객이 작성한 특정 규칙 집합입니다.

IDS/IPS 프로파일 생성

다음 절차에 따라 IPS/IDS 프로파일을 생성하고 규칙 집합에 추가합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **IPS/IDS**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **General Settings(**일반 설정**)** 탭을 클릭합니다.

단계 **4** 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.

단계 **5** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **6** IDS/IPS 프로파일이 악성 활동을 탐지하는 경우 위협 PCAP 옵션 파일을 토글합니다. 이 옵션을 켜는 경우 게이트웨이에 PCAP 프로파일이 연결되어 있어야 합니다.

단계 **7** 일반 설정의 **Rule Set(**규칙 집합**)** 섹션에서 규칙 라이브러리(Talos, 맞춤형)의 규칙 세트가 IDS/IPS 프로파일에 하나 이상 지정되어 있어야 합니다. Talos 규칙 및 맞춤형 규칙 집합을 사용하는 경우, 둘 중 하나 이상을 활성화해야 합니다. 전체 IDS/IPS 프로파일을 비활성화하려는 경우 정책 규칙 집합에서 IDS/IPS 프로파일을 제거하면 IDS/IPS 프로파일이 평가되지 않습니다. 드롭다운 메뉴를 사용하여 이 프로파일 내의 모든 규칙에 적용되는 다음 설정 중 하나를 선택합니다.

- **Disabled(**비활성화됨**)** - Talos 규칙 사용을 비활성화할지 여부를 지정합니다.
- **Manual(**수동**)** - Talos 규칙 버전을 지정합니다.
- **Automatic(**자동**)** - 게시 날짜로부터 최신 Talos Rules 버전으로의 자동 업데이트를 연기할 기간(일)을 지정합니다.

다른 드롭다운 메뉴를 사용하여 이 프로파일의 규칙을 업데이트할 시기를 선택합니다. Talos가 업데이트를 전송한 직후 또는 업데이트 며칠 후에 규칙 집합을 업데이트하도록 선택할 수 있습니다.

단계 **8** **Talos Rules: Policy(Talos** 규칙**:** 정책**)**를 클릭하고 표에서 기본으로 사용할 정책 프로파일을 선택합니다. 프로파일은 하나만 선택할 수 있습니다.

창 보기가 최대화되지 않은 경우, 창의 오른쪽으로 스크롤하여 선택한 프로파일에 대해 작업을 할당합니다.

- **Rule Default(**규칙 기본값**)** - 트리거된 각 규칙에 지정된 작업에 따라 요청을 허용하거나 거부하고 이벤트를 로깅합니다.
- **Allow Log(**허용 로그**)** - 요청을 허용하고 이벤트를 로깅합니다.
- **Allow No Log(**허용 로그 없음**)** - 요청을 허용하고 이벤트를 로깅하지 않습니다.
- **Deny Log(**거부 로그**)** - 요청을 거부하고 이벤트를 로깅합니다.
- **Deny No Log(**거부 로그 없음**)** - 요청을 거부하고 이벤트를 로깅하지 않습니다.

단계 **9** **Talos Rules: Category(Talos** 규칙**:** 범주**)** 탭을 클릭하고 표에서 프로파일에 있는 범주를 하나 이상 선택합니다.

단계 **10** **Talos rules: Class(Talos** 규칙**:** 클래스**)** 탭을 클릭하고 표에서 프로파일에 대한 클래스를 하나 이상 선택합니다.

단계 **11** 화면 상단에서 **Advanced Settings(**고급 설정**)** 탭을 클릭합니다.

단계 **12** **Rule Supression(**규칙 억제**)**에서 **Add(**추가**)**를 클릭하고 IP 주소의 유효한 **Source IP/CIDR List(**소스 **IP/CIDR** 목록**)** 및 해당 **Rule ID List(**규칙 **ID** 목록**)**를 입력합니다. 일련의 목록을 제거하려면 행 오른쪽의 빼기 아이콘을 클릭합니다.

단계 **13** **Event Filtering: Profile Event Filtering(**이벤트 필터링**:** 프로파일 이벤트 필터링**)**에서 다음 정보를 입력합니다.

- **Type(**유형**)** - 속도 또는 샘플을 선택할 수 있습니다. 생성된 이벤트는시간 평가 간격(초) 동안 지정된 트리거 **Number of Events(**이벤트 수**)**에 따라 속도 또는 샘플 제한이 적용됩니다.
- **Number of Events(**이벤트 수**)** - 허용되는 이벤트 수의 값을 수동으로 입력합니다.
- (속도 유형에서 사용 가능) **Time (Seconds)(**시간**(**초**))** - 숫자 값을 초 단위로 입력합니다.

단계 **14** **Event Filtering: Rule Event Filtering(**이벤트 필터링**:** 규칙 이벤트 필터링**)**에서 **Add(**추가**)**를 클릭합니다. 다음 정보를 입력합니다.

- **Rule ID List(**규칙 **ID** 목록**)** - 쉼표로 구분된 규칙 ID 목록을 지정합니다.
- **Number of Events(**이벤트 수**)** - 허용되는 이벤트 수의 값을 수동으로 입력합니다.
- (속도 유형에서 사용 가능) **Time (Sec)(**시간**(**초**))** - 숫자 값을 초 단위로 입력합니다.
- **Type(**유형**)** - 속도 또는 샘플을 선택합니다. 생성된 이벤트는 시간 평가 간격(초) 동안 지정된 트리거 이벤트 수에 따라 속도 또는 샘플 제한이 적용됩니다.

단계 **15** 고급 설정의 **Rule Setting List** (규칙 설정 목록) 섹션에서 **Add** (추가)를 클릭하고 다음을 입력합니다.

- **Source IP/CIDR List(**소스 **IP/CIDR** 목록**)** - 쉼표로 구분된 IP 또는 CIDR 목록을 제공합니다.

- **Rule ID List(**규칙 **ID** 목록**)** - 쉼표로 구분된 규칙 ID 목록을 제공합니다. 많은 수의 규칙에는 규칙 ID만 필요합니다. 수가 적은 규칙의 경우, 규칙 ID에 GID 및 ID를 GID:ID로 지정해야 합니다. 예를 들면 119:3와 같습니다.
- **Action(**작업**)** - 소스 IP/CIDR 목록 또는 규칙 ID 목록이 트리거되는 경우의 작업을 선택합니다. 규칙이 억제되면 어떤 작업도 수행되지 않으며 로그가 전송 또는 캡처되지 않습니다.
  - **Allow Log(**허용 로그**)** - 요청을 허용하고 이벤트를 로깅합니다.
  - **Allow No Log(**허용 로그 없음**)** - 요청을 허용하고 이벤트를 로깅하지 않습니다.
  - **Deny Log(**거부 로그**)** - 요청을 거부하고 이벤트를 로깅합니다.
  - **Deny No Log(**거부 로그 없음**)** - 요청을 거부하고 이벤트를 로깅하지 않습니다.

What to do next

- 프로파일 세부 정보 보기
- 프로파일에 게이트웨이 연결 추가

데이터 손실 방지(DLP) 프로파일

DLP(Data Loss Prevention) 프로파일은 멀티 클라우드 방어 솔루션이 정방향 프록시(이그레스) 모드로 구축될 때 데이터에서 유출 패턴을 찾는 것을 탐지하고 조치를 취하는 정책 규칙을 지정할 수 있는 기능을 멀티 클라우드 방어 고객에게 제공합니다.

멀티 클라우드 방어은(는) 고객이 이를 통해 맞춤형 PCRE 기반 정규식 패턴 외에도 사회 보장 번호(SSN), AWS 비밀번호, 신용카드 번호와 같은 사전 패키징된 일반적인 데이터 패턴을 지정할 수 있도록 합니다. 따라서 쉽게 PCI, PII 및 PHI 데이터에 대한 보호를 시행하여 규정 준수 요건을 충족할 수 있습니다. 이 기능은 별도의 DLP 서비스가 필요하지 않은 기존 멀티 클라우드 방어 기능 집합과 통합됩니다.

데이터 손실 방지 프로파일 생성

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Network Threats(**네트워크 위협**)**로 이동합니다.
단계 **2** **Create Intrusion Profile(**침입 프로파일 생성**)**을 클릭합니다.
단계 **3** **Data Loss Prevention(**데이터 손실 방지**)**을 선택합니다.
단계 **4** 프로파일의 고유한 이름을 제공하고 설명을 입력합니다.
단계 **5** 테이블에 **DLP** 필터 목록을 입력합니다.
단계 **6** 필요에 따라 행을 더 삽입하려면 **Add(**추가**)**를 클릭합니다.
단계 **7** 필터에 대한 설명을 제공합니다.

단계 **8** 드롭다운 목록에서 사전 정의된 정적 패턴(예: CVE 번호)을 선택하거나 사용자 정의 정규식을 제공합니다.

단계 **9** 카운트를 입력하여 트래픽에서 패턴이 표시되어야 하는 횟수를 정의합니다.

단계 **10** 패턴이 개수와 일치하는 경우 수행할 작업을 선택합니다.

참고 패턴이 더 제한적이므로 AWS 액세스 키 및 AWS 암호 키에 대해 사전 정의된 패턴이 DLP 검사에서 일치하지 않는 경우가 있습니다. DLP 프로파일에서 다음과 같은 완화된 사용자 지정 패턴을 사용하여 AWS 액세스 키와 AWS 암호 키를 탐지합니다. 이렇게 하면 오탐 로그 이벤트가 생성될 수 있습니다.

```
AWS 액세스 키: (?<![A-Z0-9])[A-Z0-9]{20}(?![A-Z0-9])

AWS 암호 키: (?<![AZa-z0-9/+=])[A-Za-z0-9/+=]{40}(?![A-Za-z0-9/+=])
```

다음에 수행할 작업

- 프로파일 세부 정보 보기
- 프로파일에 게이트웨이 연결 추가

Anti-Malware Profile

안티 멀웨어 프로파일은 Talos ClamAV 바이러스 탐지 엔진을 사용하여 안티 멀웨어 보호를 활성화합니다. ClamAV®는 트로이 목마, 바이러스, 악성코드 및 기타 악성 위협을 탐지하기 위한 안티바이러스 엔진입니다.

다음 단계에서는 안티 멀웨어 프로파일을 생성하고 정책 규칙에 연결하는 방법을 설명합니다.

안티맬웨어 프로파일 생성

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Network Threats(**네트워크 위협**)**로 이동합니다.

단계 **2** **Anti-malware(**악성코드 차단**)**를 선택합니다.

단계 **3** 고유한 이름을 입력하고 설명을 입력합니다.

단계 **4** Talos 규칙 집합에 대해 다음 모드 중 하나를 선택합니다.

- **Manual Mode(**수동 모드**)** - 드롭다운에서 Talos Ruleset Version(Talos 규칙 집합 버전)을 선택합니다. 선택한 규칙 집합 버전은 이 프로파일을 사용하는 모든 게이트웨이의 멀티 클라우드 방어 데이터 경로 엔진에 의해 사용되며 최신 규칙 집합 버전으로 자동 업데이트되지 않습니다.
- Automatic(자동) 모드 - 멀티 클라우드 방어에서 규칙 집합 버전을 게시한 후 구축을 며칠 단위로 지연할지 선택합니다. 멀티 클라우드 방어에서는 새 규칙 집합을 매일 게시하며 이 프로파일을 사용하는 게이트웨이는 **N** 일 이상의 최신 규칙 집합 버전으로 자동 업데이트됩니다. 여기서 **N**은 드롭다운에서 선택한 "delay by days(지연 일수)" 인수입니다. 예를 들어 2024년 1월 10일의 구축을 5일 연기하도록 선택하는 경우 멀티 클라우드 방어 컨트롤러은(는) 1월 5일 또는 그 이전에 게시된 규칙 집합 버전을 선택합니다. 해당 규칙 집합 버전을 사용한 내부 테스트가 어떤 이유로 실패할 경우 멀티 클라우드 방어이(가) 게시되지 않을 수도 있습니다.

단계 **5** 바이러스 서명과 일치하는 항목이 발견된 경우 수행할 작업을 선택합니다.

다음에 수행할 작업

- 프로파일 세부 정보 보기
- 프로파일에 게이트웨이 연결 추가

웹 애플리케이션 방화벽(WAF) 프로파일

웹 보호 프로파일은 트래픽이 악의적이지 않은지 확인하기 위해 웹 기반 트랜잭션을 평가하는 데 사용할 수 있는 WAF(Web Application Firewall) 규칙 모음입니다.

멀티 클라우드 방어에서는 다음 WAF 규칙 집합을 지원합니다.

Table 2: 멀티 클라우드 방어에서는 다음 ***WAF*** 규칙 집합을 지원합니다.

규칙 집합	설명
핵심 규칙	핵심 규칙은 모든 웹 애플리케이션에 기본 보호 레벨을 제공하는 ModSecurity CRS(핵심 규칙 집합)의 표준 규칙 집합입니다.
TrustWave 규칙	TrustWave 규칙은 특정 웹 애플리케이션 및 프레임워크에 고급 수준의 보호를 제공하는 실제 조사, 침입 테스트 및 연구를 통해 수집된 인텔리전스를 기반으로 하는 ModSecurity의 고급 규칙 집합입니다.
맞춤형 규칙	맞춤형 규칙은 맞춤형 웹 애플리케이션에 특수 수준의 보호를 제공하며 고객이 작성한 특정 규칙 집합입니다.

WAF 프로파일 생성

다음 절차에 따라 WAF 프로파일을 생성합니다.

Note 핵심 규칙 집합이 지정된 경우, 핵심 규칙을 비활성화할 수 없습니다. 핵심 규칙을 비활성화하려면 WAF 프로파일에서 모든 핵심 규칙 집합을 제거하여 평가되지 않도록 합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **WAF**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 다음 일반 설정을 지정합니다.

a) 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.
b) (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 프로파일을 구분하는 데 도움이 될 수 있습니다.
c) 다음 작업을 지정합니다.
    - **Rule Default(**규칙 기본값**)** - 트리거된 각 규칙에 지정된 작업에 따라 요청을 허용하거나 거부하고 이벤트를 로깅합니다.
    - **Allow Log(**허용 로그**)** - 요청을 허용하고 이벤트를 로깅합니다.
    - **Deny Log(**거부 로그**)** - 요청을 거부하고 이벤트를 로깅합니다.
d) WAF 프로파일이 악의적인 활동을 탐지하는 경우, 위협 HAR 파일을 생성할지 여부를 지정합니다. 이 기능을 사용하려면 게이트웨이에 Pcap 프로파일이 첨부되어 있어야 합니다.
e) WAF 프로파일이 악의적인 활동을 탐지하는 경우 HTTP 요청 HAR 파일을 생성할지 여부를 지정합니다.
f) **RULE SETS(**규칙 설정**)** 섹션의 왼쪽에 있는 세로 탭에서 **Core Rules(**핵심 규칙**)**을 클릭합니다. 규칙 라이브러리(Core, TrustWave, Custom)에서 하나 이상의 규칙 집합을 지정해야 합니다.
    - 다음 항목을 지정합니다.
        - **Manual(**수동**)** - 사용할 핵심 규칙 버전을 지정합니다.
        - **Automatic(**자동**)** - 게시 날짜로부터 최신 핵심 규칙 버전으로의 자동 업데이트를 지연하는 기간(일)을 지정합니다.
    - 프로파일에 추가할 규칙을 확인하고 **Add to Profile(**프로파일에 추가**)**을 클릭합니다. 선택 사항이 오른쪽 테이블에 표시됩니다.
g) 왼쪽에 있는 세로 방향 탭에서 **TrustWave Rules(TrustWave** 규칙**)**를 클릭합니다.
    - 다음 항목을 지정합니다.
        - **Disabled(**비활성화됨**)** - Trustwave 규칙 사용을 비활성화할지 여부를 지정합니다.
        - **Manual(**수동**)** - 사용할 TrustWave 규칙 버전을 지정합니다.
        - **Automatic(**자동**)** - 게시 날짜로부터 최신 TrustWave Rules 버전으로의 자동 업데이트를 연기할 기간(일)을 지정합니다.
    - 프로파일에 추가할 규칙을 확인하고 **Add to Profile(**프로파일에 추가**)**을 클릭합니다. 선택 사항이 오른쪽에 있는 **Profile Selections(**프로파일 선택**)** 표에 표시됩니다.
h) 왼쪽에 있는 세로 방향 탭에서 **Custom Rules(**맞춤형 규칙**)**를 클릭합니다.
    - 다음 옵션 중 하나를 지정합니다.
        - **Disabled(**비활성화됨**)** - 맞춤형 규칙 사용을 비활성화할지 여부를 지정합니다.
        - **Manual(**수동**)** - 사용할 맞춤형 규칙 버전을 지정합니다.
        - **Automatic(**자동**)** - 게시 날짜로부터 최신 맞춤형 규칙 버전으로의 자동 업데이트를 지연하는 기간(일)을 지정합니다.

- 프로파일에 추가할 규칙을 확인하고 **Add to Profile(**프로파일에 추가**)**을 클릭합니다. 선택 사항이 오른쪽에 있는 **Profile Selections(**프로파일 선택**)** 표에 표시됩니다.

단계 **4** 창 상단으로 스크롤하고 **Advanced Settings(**고급 설정**)** 탭을 클릭합니다.

a) "Rule Suppression(규칙 억제)"에서 **Add(**추가**)**를 클릭하여 규칙에 대한 행을 하나 이상 추가합니다. 특정 IP 또는 CIDR 목록에 대한 규칙을 억제할 수 있습니다.

- **Source IP/CIDR List(**소스 **IP/CIDR** 목록**)**에서 쉼표로 구분된 IP 또는 CIDR 목록을 제공합니다.
- **Rule ID List(**규칙 **ID** 목록**)**에 쉼표로 구분된 규칙 ID 목록을 제공합니다.

b) "Event Filtering(이벤트 필터링)"에서 다음 정보를 제공합니다.

- **Type(**유형**) - Rate(**속도**)** 또는 **Sample(**샘플**)**
- 이벤트 수
- 시간**(**초**)**

c) "Rule Event Filtering(규칙 이벤트 필터링)"에서 **Add(**추가**)**를 클릭하여 규칙에 대한 행을 하나 이상 추가합니다. 생성하는 모든 행에 대해 유효한 **Rule ID List(**규칙 **ID** 목록**)**, **Number of Events(**이벤트 수**)**, **Time (Sec)(**시간**(**초**))** 을 입력하고 유형 또는 샘플 중 하나를 **Type(**유형**)**으로 선택합니다.

d) "Core Rule Set(핵심 규칙 집합)"에서 **Request Anomaly(**요청 이상 징후**)** 및 **Response Anomaly(**응답 이상 징후**)** 모두에 대한 값을 선택합니다. "Request Anomaly(요청 이상 징후)"에 대해 3보다 작은 값을 사용하면 방대한 양의 알림이 생성됩니다.

e) **Paranoia Level(**편집증 수준**)**을 선택합니다. 옵션 범위는 1~4입니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

What to do next

- 프로파일 세부 정보 보기
- 프로파일에 게이트웨이 연결 추가

이벤트 필터링

WAF 프로파일이 트리거될 때 생성되는 보안 이벤트 수를 줄이기 위해, **Advanced Settings(**고급 설정**)**에서 이벤트 속도를 제한하거나 샘플링하도록 이벤트 필터링을 구성할 수 있습니다. 설정은 탐지 또는 보호 동작을 변경하지 않습니다.

Type(유형)을 **Rate(**속도**)**로 지정하면 생성되는 이벤트는 *Time(*시간*)* 평가 간격(초) 동안 트리거된 지정된 *Number of Events(*이벤트 수*)*에 따라 속도가 제한됩니다. 예를 들어 *Number of Events(*이벤트 수*)*가 50으로 지정되고 *Time(*시간*)*이 5초로 지정된 경우 초당 10개 이벤트만 생성됩니다.

Type(유형)을 **Sample(**샘플**)**로 지정하면 생성된 Events(이벤트)는 지정된 *Number of Events(*이벤트 수*)*를 기준으로 샘플링됩니다. 예를 들어 *Number of Events(*이벤트 수*)*가 10으로 지정된 경우, 트리거된 10개 이벤트마다 1개의 이벤트만 생성됩니다.

프로파일 이벤트 필터링

프로파일 이벤트 필터링은 WAF 프로파일에 설정된 모든 규칙에 적용됩니다.

- Type(유형)을 **Rate(**속도**)** 또는 **Sample(**샘플**)**로 지정합니다.
  - **Rate(**속도**)** - *Number of Events(*이벤트 수*)* 및 *Time(*시간*)* 평가 간격(초)을 지정합니다.
  - **Sample(**샘플**)** - *Number of Events(*이벤트 수*)*를 지정합니다.

규칙 이벤트 필터링

WAF 프로파일이 트리거될 때 생성되는 보안 이벤트 수를 줄이기 위해 이벤트 속도를 제한하거나 샘플링하도록 이벤트 필터링을 구성할 수 있습니다. 설정은 탐지 또는 보호 동작을 변경하지 않습니다.

규칙 이벤트 필터링은 WAF 프로파일에 구성된 특정 규칙에 적용됩니다.

단계 **1** Rule Event Filtering(규칙 이벤트 필터링) 아래에서 **Add(**추가**)**를 클릭합니다.

단계 **2** **Rule ID List(**규칙 **ID** 목록**)**에서 쉼표로 구분된 **Rule ID(**규칙 **ID)** 목록을 지정합니다.

단계 **3** Type(유형)을 **Rate(**속도**)** 또는 **Sample(**샘플**)**로 지정합니다.

- **Rate(**속도**) - Number of Events(**이벤트 수**)** 및 **Time(**시간**)** 평가 간격(초)을 지정합니다.
- **Sample(**샘플**) - Number of Events(**이벤트 수**)**를 지정합니다.

다음에 수행할 작업

WAF 프로파일을 정책 규칙과 연결

L7 DoS 프로파일 생성

멀티 클라우드 방어 게이트웨이는 백엔드 웹 서버에 대한 클라이언트 요청을 지속적으로 모니터링하여 애플리케이션 계층 공격을 모니터링, 탐지 및 치료할 수 있는 기능을 제공합니다. 레이어 7 DoS 공격은 웹 서버 리소스를 고갈시키기 위한 것으로, 많은 HTTP 요청을 전송하여 서비스 가용성에 영향을 미칩니다. 이 기능은 웹 기반 애플리케이션의 가용성을 유지하기 위해 게이트웨이가 백엔드 웹 서비스에 대한 인바운드 연결을 프록시하도록 활성화된 경우 활성화됩니다. 이 기능을 활성화하면 프론트엔드 로드 밸런서가 지원하지 않거나 애플리케이션 DoS 공격을 탐지하고 교정하도록 최적화되지 않은 경우에도 게이트웨이가 추가적인 보안을 제공할 수 있습니다.

이 기능은 API 서비스를 호스팅하는 백엔드 웹 서버에 대한 DoS 보호를 제공하는 데에도 사용할 수 있습니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)**로 이동합니다.

단계 **2** **Layer 7 DOS**를 선택합니다.

단계 **3** 고유한 프로파일 이름을 제공합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름을 가질 수 있는 다른 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** 요청 속도 제한을 추가합니다.

리소스에 대한 과도한 요청은 다음 매개변수를 기반으로 제한합니다. 이 매개변수의 값은 레이어 7 DoS 옵션으로 보호하려는 웹 서비스의 트래픽 패턴 측정 및 이해를 기반으로 해야 합니다.

Table 3: 매개변수

매개변수	설명
URI	리소스에 대한 요청을 제한하는 경로를 나타내는 데 사용되는 상대적 URI입니다. 예를 들어 https://www.example.com/login.html에서 서비스 리소스를 모니터링하고 보호하려는 경우 **Request Rate Limits(**요청 속도 제한**)** 테이블에 URI 매개변수로 /login.html을 입력합니다.
HTTP 메서드	리소스 URI당 HTTP 메서드를 지정하여 클라이언트 요청에서 속도가 제한되는 HTTP 메서드와 속도가 제한되지 않는 HTTP 메서드를 제어할 수 있습니다. 테이블의 각 행에 대해 드롭다운에서 여러 메서드를 선택할 수 있습니다. 빈 HTTP 메서드 목록은 메서드가 무시되고 속도가 리소스에 대한 모든 호출에 적용됨을 의미합니다. **Note** 속도는 각 리소스별로 적용됩니다. 따라서 여러 메서드가 해당 행의 요청 속도에 지정된 속도 제한을 공유합니다. 예를 들어 속도가 매초 3개 요청이고 GET, POST 및 PUT이 HTTP 메서드에 지정되어 있으며 동일한 시간(초)에 단일 클라이언트 IP에서 해당 URI에 2개의 GET과 1개의 POST가 발생하는 경우, 같은 초에 PUT은 허용되지 않습니다.
요청 속도	1초당 요청 수 단일 클라이언트가 규칙의 URI 부분에 언급된 URI 리소스에 요청을 전송할 수 있는 속도를 결정합니다.
Burst Size(버스트 크기)	클라이언트가 규칙의 URI 부분에 언급된 URI 리소스에 전송할 수 있는 최대 동시 요청 수를 지정합니다. 이 임계값을 초과하며 동시에 프록시에 도착하는 요청은 백엔드 서버로 전송되지 않습니다.

단계 **6** 완료되면 **Save(**저장**)**를 클릭합니다. 규칙은 위에서 아래로 확인되고 첫 번째 일치에 적용되므로 URI를 기준으로 하면 규칙의 순서가 중요합니다. 목록의 상위에 추가된 URI가 그 아래에 있는 규칙의 리소스를 포함하는 리소스 경로를 포함하는 경우, 일치하는 첫 번째 규칙이 적용됩니다.

What to do next

- 프로파일 세부 정보 보기
- 서비스 개체에 L7 DoS 프로파일을 추가합니다. 그런 다음 프로파일에 게이트웨이 연결 추가. 규칙 집합을 업데이트하는 경우, 변경 사항이 즉시 구축되지 않을 수 있습니다.

URL(Uniform Resource Locator) 필터 프로파일

URL 필터링 프로파일은 HTTP 요청의 URL을 평가하고 트래픽을 허용 또는 거부하는 작업을 적용합니다. URL을 평가하려면 정방향 프록시 규칙으로 트래픽을 처리해야 합니다. 프로파일의 URL 집합은 전체 경로를 나타내는 문자열 또는 PCRE(Perl Compatible Regular Expression)를 나타내는 문자열로 지정할 수 있습니다. 도메인 필터링만 필요한 경우 FQDN 필터링 프로파일을 사용하는 것이 가장 좋습니다. FQDN 필터링 프로파일은 URL 필터링과 함께 사용할 수도 있습니다. 여기서 도메인은 FQDN 필터링 프로파일을 사용하여 평가되고 URL은 URL 필터링 프로파일을 사용하여 평가됩니다.

URL 필터링 프로파일은 사전 정의된 범주 집합을 사용할 수 있습니다. 범주에 대한 자세한 내용은 FQDN / URL 필터링 범주의 내용을 참조하십시오.

Note URL 필터링은 2개의 기본 행(**Uncategorized(**미분류**)** 및 **ANY(**모두**)**와 함께 사용자가 지정한 행(URL 및 Categories(범주))을 포함하는 테이블로 구성됩니다. 원하는 경우 각 행 내에서 범주와 URL을 결합할 수 있습니다.

각 URL 필터링 프로파일의 제한은 다음과 같습니다.

- 사용자 지정 최대 행: 254(독립형 또는 독립형 그룹)
- 행당 최대 범주 및 URL: 60
- 최대 URL 문자 길이: 2048

다단계 도메인(예: 'www.example.com')을 지정할 때 '.' 문자를 이스케이프해야 합니다(예: 'www\.example\.com'). 그렇지 않으면 단일 문자에 대한 와일드카드로 처리됩니다.

미분류

- **Uncategorized(**미분류**)**로 표시되는 URL 필터링 프로파일의 마지막에서 두 번째 행.
- 사용자가 지정한 URL과 일치하지 않거나 범주가 없는 URL에 대해 수행할 정책 작업을 지정합니다.
- 그룹 프로파일에서 독립형 프로파일이 사용되고 그룹 프로파일이 정책 규칙 집합 규칙에 적용된 경우 **Uncategorized(**미분류**)** 행은 그룹 프로파일에서 가져옵니다. 독립형 프로파일의 **Uncategorized(**미분류**)** 행은 독립형 프로파일이 정책 규칙 집합 규칙에 직접 적용된 경우에만 적용 가능합니다.

기본값**(ANY)**

- **ANY(**모든**)**로 표시되는 URL 필터링 프로파일의 마지막 행.
- 사용자가 지정한 URL 또는 범주와 일치하지 않거나 미분류가 아닌 URL에 대해 수행할 정책 작업을 지정합니다.

- 그룹 프로파일에서 독립형 프로파일이 사용되고 그룹 프로파일이 정책 규칙 집합 규칙에 적용된 경우 **ANY(**모든**)** 행은 그룹 프로파일에서 가져옵니다. 독립형 프로파일의 **ANY(**모든**)** 행은 독립형 프로파일이 정책 규칙 집합에 직접 적용된 경우에만 적용 가능합니다.

URL 필터링 프로파일 생성

다음 절차를 사용하여 독립형 URL 필터링 프로파일을 생성합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **URL Filtering(URL** 필터링**)**으로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 이름을 제공합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** **Add(**추가**)**를 클릭하여 새 행을 생성합니다.

단계 **6** 개별 URL을 지정합니다(예: https://www.google.com).

- 각 URL은 PCRE(Perl Compatible Regular Expression)로 지정됩니다.
- 각 URL은 전체 경로로 지정해야 합니다.
- 소수점 "." 문자를 이스케이프하지 않으면 단일 문자 와일드카드로 처리됩니다.

단계 **7** **Category(**범주**)**를 지정합니다(예: 게임, 스포츠, 소셜 네트워킹).

단계 **8** 정책이 적용되는 HTTP 메서드를 지정합니다.

단계 **9** 메서드의 하위 집합으로 다음 중 하나를 선택합니다.

- Delete
- Get
- Head
- Options
- Patch
- Post
- Put

단계 **10** 모든 메서드에 대해 **All(**모두**)**을 지정합니다.

단계 **11** 사용자 지정 URL/Categories(URL/범주), Uncategorized(미분류) 및 ANY(모든) 행에 대한 Policy(정책) 작업을 지정합니다.

- **Allow Log(**허용 로그**)** - 요청을 허용하고 이벤트를 로깅합니다.
- **Allow No Log(**허용 로그 없음**)** - 요청을 허용하고 이벤트를 로깅하지 않습니다.

- **Deny Log(**거부 로그**)** - 요청을 거부하고 이벤트를 로깅합니다.
- **Deny No Log(**거부 로그 없음**)** - 요청을 거부하고 이벤트를 로깅하지 않습니다.

단계 **12** 반환 상태 코드를 지정합니다.

단계 **13** **100** 이상 **600** 미만의 정수 값을 지정합니다. 값은 요청을 수행하는 클라이언트에 반환될 HTTP 상태를 나타냅니다. 일반적인 반환 코드는 **503**입니다.

단계 **14** **Save(**저장**)**를 클릭합니다.

What to do next

- 프로파일 세부 정보 보기
- 프로파일에 게이트웨이 연결 추가

FQDN(Fully Qualified Domain Name) 필터 프로파일

FQDN(Fully Qualified Domain Name) 필터 프로파일은 트래픽과 연결된 FQDN을 평가하고 트래픽을 허용 또는 거부하는 작업을 적용합니다. FQDN을 평가하려면 트래픽이 TLS로 암호화되어 있어야 하며 TLS hello 헤더의 SNI 필드에 FQDN이 포함되어 있어야 합니다. FQDN에서는 전달 또는 전달 프록시 규칙에 의해 처리된 트래픽을 평가할 수 있습니다. 프로파일의 FQDN 집합은 전체 도메인을 나타내는 문자열 또는 PCRE(Perl Compatible Regular Expression)로 표시되는 문자열로 지정할 수 있습니다. 도메인 허용 목록만 필요한 경우에는 FQDN 필터링 프로파일을 사용하는 것이 가장 좋습니다. FQDN 필터링 프로파일을 URL 필터링 프로파일과 함께 사용할 수도 있습니다. 여기서 도메인은 FQDN 필터링 프로파일 사용하여 평가되고 URL은 URL 필터링 프로파일을 사용하여 평가됩니다.

FQDN 필터링을 사용하여 규칙 일치 후 기준에 따라 허용하거나 거부할 범주를 필터링합니다. 세분화된 수준에서 필터를 설정할 수 있습니다. FQDN 필터 행에는 거부 또는 허용과 같은 로그 관련 작업이 포함되어 있습니다.

FQDN 필터링 프로파일은 사전 정의된 범주 집합을 사용할 수도 있습니다. 범주에 대한 자세한 내용을 FQDN / URL 필터링 범주를 참조하십시오.

Note FQDN 필터링 프로파일은 사용자가 지정한 행(FQDN 및 Categories(범주))을 포함하는 테이블 형식으로 구성되며, 두 개의 기본 행(Uncategorized(미분류) 및 ANY(모든))이 있습니다. 필요한 경우 각 행 내에서 범주 및 FQDN을 결합할 수 있습니다.

각 FQDN 필터 프로파일의 제한은 다음과 같습니다.

- 사용자 지정 최대 행: 254(독립형 또는 독립형 그룹)
- 행당 최대 범주 및 FQDN: 60
- 최대 FQDN 문자 길이: 255

다단계 도메인(예: 'www.example.com')을 지정할 때 `.' 문자를 이스케이프해야 합니다(예: `www.example\.com'). 그렇지 않으면 단일 문자에 대한 와일드카드로 처리됩니다.

독립형 및 그룹

FQDN 필터 프로파일은 독립형 또는 그룹으로 지정할 수 있습니다.

독립형 FQDN 필터 프로파일에는 FQDN 및 범주가 포함됩니다. 프로파일은 하나 이상의 정책 규칙 집합에 직접 적용되거나 FQDN 그룹 프로파일과 연결됩니다.

FQDN 필터 그룹 프로파일에는 다양한 용도로 정의하고 그룹 프로파일로 함께 결합할 수 있는 독립형 프로파일의 순서가 지정된 목록이 포함되어 있습니다. 그룹 프로파일을 하나 이상의 정책 규칙 집합에 직접 적용할 수 있습니다. 각 팀은 특정 독립형 프로파일을 생성하고 관리할 수 있습니다. 이러한 독립형 프로파일은 그룹 프로파일로 결합하여 활용 사례에 따라 계층 구조 또는 다양한 조합을 생성할 수 있습니다. 모든 항목에 적용되는 전역 FQDN 목록, 서로 다른 CSP에 적용되는 CSP 관련 목록, 그리고 애플리케이션에 적용되는 애플리케이션 관련 목록 등의 조합을 예로 들 수 있습니다.

미분류

- **Uncategorized(**미분류**)**로 표시되는 FQDN 필터 프로파일의 두 번째에서 마지막 행.
- 사용자가 지정한 FQDN과 일치하지 않거나 범주가 없는 FQDN에 대해 수행할 정책 작업을 지정합니다.
- 그룹 프로파일에서 독립형 프로파일이 사용되고 그룹 프로파일이 정책 규칙 집합 규칙에 적용된 경우 **Uncategorized(**미분류**)** 행은 그룹 프로파일에서 가져옵니다. 독립형 프로파일의 **Uncategorized(**미분류**)** 행은 독립형 프로파일이 정책 규칙 집합 규칙에 직접 적용된 경우에만 적용 가능합니다.

기본값**(ANY)**

- **ANY(**모든**)**로 표시되는 FQDN 필터 프로파일의 마지막 행.
- 사용자가 지정한 FQDN 또는 범주와 일치하지 않거나 미분류가 아닌 FQDN에 대해 수행할 정책 작업을 지정합니다.

- 그룹 프로파일에서 독립형 프로파일이 사용되고 그룹 프로파일이 정책 규칙 집합 규칙에 적용된 경우 **ANY(**모든**)** 행은 그룹 프로파일에서 가져옵니다. 독립형 프로파일의 **ANY(**모든**)** 행은 독립형 프로파일이 정책 규칙 집합에 직접 적용된 경우에만 적용 가능합니다.

독립형 FQDN 필터 프로파일 생성

다음 절차에 따라 독립형 FQDN 필터 프로파일을 생성합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **FQDN Filtering(FQDN** 필터링**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 이름을 제공합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** Type(유형)을 **Standalone(**독립형**)**으로 지정합니다.

단계 **6** **Add(**추가**)**를 클릭하여 새 행을 생성합니다.

단계 **7** 개별 FQDN 지정합니다(예: google.com).

a) 각 FQDN은 PCRE(Perl Compatible Regular Expression)로 지정됩니다.

b) "**.**" 문자를 이스케이프하지 않으면 단일 문자 와일드카드로 처리됩니다.

단계 **8** **Category(**범주**)**를 지정합니다(예: 게임, 스포츠, 소셜 네트워킹).

단계 **9** 사용자 지정 FQDN/Categories(FQDN/범주), Uncategorized(미분류) 및 ANY(모든) 행에 대한 정책 작업을 지정합니다.

- **Allow Log(**허용 로그**)** - 요청을 허용하고 이벤트를 로깅합니다.
- **Allow No Log(**허용 로그 없음**)** - 요청을 허용하고 이벤트를 로깅하지 않습니다.
- **Deny Log(**거부 로그**)** - 요청을 거부하고 이벤트를 로깅합니다.
- **Deny No Log(**거부 로그 없음**)** - 요청을 거부하고 이벤트를 로깅하지 않습니다.

단계 **10** (선택 사항) 암호 해독이 바람직하지 않거나 가능한 FQDN에 대해 **Decryption Exception(**암호 해독 예외**)**을 지정합니다. 암호 해독 예외를 고려해야 하는 가능한 이유는 다음과 같습니다.

- 암호화된 트래픽(예: 금융 서비스, 방위, 의료 등)의 검사에 대한 거부 요청
- 암호 해독이 불가능한 SSO 인증 트래픽
- 프록시 설정할 수 없는 NTLM 트래픽

단계 **11** 완료되면 **Save(**저장**)**를 클릭합니다.

What to do next

- 프로파일 세부 정보 보기

- 프로파일에 게이트웨이 연결 추가

그룹 FQDN 필터 프로파일 생성

다음 절차를 사용하여 두 개 이상의 독립형 프로파일이 있는 그룹 FQDN 필터 프로파일을 생성합니다.

단계 1 **Manage(**관리**)** > **Profiles(**프로파일**)** > **FQDN Filtering(FQDN** 필터링**)**로 이동합니다.

단계 2 **Create(**생성**)**를 클릭합니다.

단계 3 고유한 이름을 제공합니다.

단계 4 (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름을 가질 수 있는 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 5 Type(유형)을 **Group(**그룹**)**으로 지정합니다.

단계 6 초기 독립형 프로파일을 선택합니다(하나 이상의 독립형 프로파일이 필요함).

단계 7 **Add FQDN Profile(FQDN** 프로파일 추가**)**을 클릭하여 추가 프로파일에 대해 새 행을 생성합니다.

단계 8 독립형 프로파일을 선택합니다.

단계 9 Uncategorized(미분류) FQDN에 대한 Policy(정책) 작업을 지정합니다.

단계 10 **ANY(**모두**)** FQDN에 대한 Policy(정책) 작업을 지정합니다(기본값).

단계 11 선택 사항: 암호 해독이 필요하지 않거나 가능한 경우 Uncategorized(미분류) 또는 ANY(모두)로 암호 해독 예외를 지정합니다. 암호 해독 예외를 고려해야 하는 가능한 이유는 다음과 같습니다.

- 암호화된 트래픽(금융 서비스, 방위, 의료 등)의 검사에 대한 거부 요청
- 암호 해독이 불가능한 SSO 인증 트래픽
- 프록시 설정할 수 없는 NTLM 트래픽

단계 12 **Save(**저장**)**를 클릭합니다.

What to do next

- 프로파일 세부 정보 보기
- 프로파일에 게이트웨이 연결 추가

악의적인 IP 프로파일

추가 보안 보호 기능을 활성화하여 알려진 악성 IP와의 통신을 차단할 수 있습니다. 이러한 악성 IP는 TrustWave에서 정의하며 보안 프로파일 규칙 집합으로 멀티 클라우드 방어에 통합됩니다. 규칙 집합은 TrustWave에서 업데이트를 제공하므로 자주 업데이트됩니다. 업데이트는 자동 업데이트 구성 또

는 수동 업데이트 구성을 사용하여 정책 규칙 집합에 동적으로 또는 수동으로 적용할 수 있습니다. 자세한 내용은 악의적인 IP 프로파일 생성, on page 19를 참고하십시오.

Note TrustWave는 학습된 다양한 동작을 기반으로 악성 IP를 식별합니다.

- 웹 허니팟에서 악의적인 공격자 식별
- 봇넷 C&C 호스트
- TOR 출구 노드
- 기타 학습된 행동

악의적인 IP 프로파일 생성

다음 절차에 따라 악의적인 IP 프로파일을 생성합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Malicious IP(**악성 **IP)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 프로파일 이름을 제공합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** **IP Reputation(IP** 평판**)**을 활성화하려면 확인란을 선택합니다.

단계 **6** **TrustWave Ruleset Version(TrustWave** 규칙 집합 버전**)** 드롭다운 메뉴의 두 가지 옵션 중 하나를 선택합니다.

- **Manual(**수동**)** - 선택한 규칙 집합 버전은 이 프로파일을 사용하는 모든 게이트웨이의 멀티 클라우드 방어 데이터 경로 엔진에 사용됩니다. 프로파일은 최신 규칙 집합 버전으로 자동 업데이트되지 않습니다.
- **Automatic(**자동**)** - 멀티 클라우드 방어에서 규칙 집합 버전을 게시한 후 업데이트를 지연할 일수를 선택합니다. 새 규칙 집합은 멀티 클라우드 방어에 의해 자주 게시됩니다. 이 프로파일을 사용하는 게이트웨이는 **N**일 이상의 최신 규칙 집합 버전으로 자동 업데이트됩니다. 여기서 **N**은 드롭다운에서 선택한 "delay by days(지연 일수)" 인수입니다. 예를 들어 2021년 1월 10일의 구축을 5일 연기하도록 선택하는 경우 멀티 클라우드 방어 컨트롤러는 1월 5일 또는 그 이전에 게시된 규칙 집합 버전을 선택합니다. 해당 규칙 집합 버전을 사용한 내부 테스트가 어떤 이유로 실패할 경우 멀티 클라우드 방어이(가) 게시되지 않을 수도 있습니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

What to do next

- 프로파일 세부 정보 보기
- 프로파일에 게이트웨이 연결 추가

IP 평판

IP Reputation(IP 평판) 확인란은 프로파일을 활성화 또는 비활성화하는 수단으로 사용됩니다. 프로파일을 선택하고 프로파일이 정책 규칙 집합에 첨부되면, 악성 IP 보호가 시행됩니다. 선택하지 않고 프로파일이 정책 규칙 집합에 첨부되면, 악성 IP 보호가 시행되지 않습니다. 항상 IP 평판 확인란을 선택하는 것이 좋습니다. 악성 IP 프로파일을 비활성화하려면 확인란의 선택을 취소하는 대신 정책 규칙 집합에서 해당 연결을 제거합니다.

패킷 캡처 프로파일

패킷 캡처 프로파일은 멀티 클라우드 방어 게이트웨이에 구성되고 연결됩니다. 그리고 정책 규칙, 네트워크 위협 프로파일, 웹 보호 프로파일에서 활성화됩니다. 패킷 캡처는 트래픽 흐름(PCAP 파일)과 애플리케이션 및 네트워크 위협(HAR 파일)을 캡처할 수 있습니다.

패킷 캡처 형식

다음 형식 규칙을 고려하십시오.

Policy Rule Capture - <bucketname>/<cspaccountname>/<gatewayname>/flow-packet-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<policyname>.pcap.gz

IPS Threat Capture - <bucketname>/<cspaccountname>/<gatewayname>/network-threats-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<sessionid>.pcap.gz

WAF Threat Capture - <bucketname>/<cspaccountname>/<gatewayname>/web-protection-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<sessionid>.har.gz

API Logging - <bucketname>/<cspaccountname>/<gatewayname>/api-logging-captures/<year>/<month>/<day>/<instanceid>_<timestamp>_<sessionid>.har.gz

패킷 캡처 프로파일 생성

다음 절차에 따라 팩 캡처 프로파일을 생성합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Packet Capture(**패킷 캡처**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 이름을 지정합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** **CSP** 계정을 지정합니다.

단계 **6** 클라우드 서비스 제공자의 유형에 따라 스토리지 버킷의 매개변수를 결정할 수 있습니다. 클라우드 서비스 제공자별 다음 요구 사항에 유의하십시오.

- **AWS** - S3 버킷.
- **Azure** - 스토리지 계정 이름, 블로그 컨테이너 및 스토리지 액세스 키.
- **GCP** - 스토리지 버킷.

단계 **7** **Save(**저장**)**를 클릭합니다.

What to do next

- 프로파일 세부 정보 보기
- 프로파일에 게이트웨이 연결 추가

로그 전달 프로파일

로그 전달 프로파일을 사용하면 게이트웨이, VPC 및 VNet 로그 모음을 서드파티에 전송할 수 있습니다. 멀티 클라우드 방어과 선택한 서드파티 간의 통신에는 전달해야 하는 로그 유형 및 로그가 전송될 대상 서버 프로파일이 포함됩니다. 단일 프로파일을 사용하거나 여러 엔드포인트에 로그를 동시에 전송하는 프로파일 그룹을 사용할 수도 있습니다.

이 프로파일은 메트릭을 포함하지 않습니다. 로그 메트릭 전달에 대한 자세한 내용은 게이트웨이 메트릭 전달 프로파일, 22 페이지를 참조하십시오.

독립형 로그 전달 프로파일 생성

다음 절차에 따라 독립형 로그 전달 프로파일을 생성합니다.

단계 **1** **Manager(**관리자**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일과 구분할 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 메뉴를 확장하고 **Standalone(**독립형**)**을 선택합니다.

단계 **6** **Destination(**대상**)** 드롭다운 메뉴를 확장하고 로그를 전송할 서드파티 애플리케이션을 선택합니다.

단계 **7** 6단계에서 선택한 대상 유형에 따라 로그가 전달되는 최종 엔드포인트를 보호하라는 메시지가 표시되면 적절한 정보를 입력합니다. 대상 유형에 따라 모든 옵션을 사용할 수 있는 것은 아닙니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 프로파일 세부 정보 보기
- 프로파일에 게이트웨이 연결 추가

로그 전달 그룹 생성

다음 절차에 따라 그룹화된 메트릭 전달 프로파일을 생성합니다.

시작하기 전에

- 이 프로파일을 생성하기 전에 메트릭을 전달할 서드파티 애플리케이션이 하나 이상 있어야 합니다.
- 둘 이상의 독립형 메트릭 전달 프로파일이 이미 생성되어 있어야 합니다. 자세한 내용은 독립형 로그 전달 프로파일 생성, 21 페이지를 참조하십시오.

단계 **1** **Manager(**관리자**)** > **Profiles(**프로파일**)** > **Log Forwarding(**로그 전달**)**으로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일과 구분할 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 메뉴를 확장하고 **Group(**그룹**)**을 선택합니다.

단계 **6** **Group Details(**그룹 세부 정보**)**에서 프로파일에 추가해야 하는 모든 새 행에 대해 **Add(**추가**)**를 클릭합니다.

단계 **7** 각 행에 대한 드롭다운 메뉴를 확장하여 그룹에 추가할 프로파일을 선택합니다. 저장하기 전에 언제든지 프로파일을 제거하려면, 해당 프로파일의 확인란을 선택하고 **Remove(**제거**)**를 선택합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 프로파일 세부 정보 보기
- 프로파일에 게이트웨이 연결 추가

게이트웨이 메트릭 전달 프로파일

이 프로파일은 데이터 모니터링 및 분석을 위해 멀티 클라우드 방어 게이트웨이에 의해 생성된 게이트웨이 메트릭을 전달하는 데 사용됩니다. 메트릭은 게이트웨이에 의해 생성되지만 메트릭을 서드파티 분석 애플리케이션에 전달하는 멀티 클라우드 방어 컨트롤러입니다. 이 전달 프로파일을 사용하면 멀티 클라우드 방어에 로그인하지 않고도 게이트웨이 메트릭을 모니터링, 분석 및 구성할 수 있습니다. 이 정보를 사용하여 게이트웨이 환경의 성능 및 동작을 측정합니다. 또한 환경 문제 해결을 위해 이 정보를 활용합니다.

참고 멀티 클라우드 방어 컨트롤러 버전 23.09부터는 DataDog만 서드파티 분석 애플리케이션으로 지원됩니다.

DataDog와 같이 사용 가능한 대부분의 분석 애플리케이션의 경우, 반드시 권한이 부여된 사용자여야 툴의 API 및 렌더링된 데이터에 액세스할 수 있습니다.

독립형 메트릭 전달 프로파일 생성

다음 절차에 따라 독립형 프로파일을 생성하고 서드파티에서 처리할 메트릭을 전달합니다.

시작하기 전에

이 프로파일을 생성하기 전에 메트릭을 전달할 서드파티 애플리케이션이 하나 이상 있어야 합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **Metrics Forwarding(**메트릭 전달**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 프로파일 이름을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일과 구분할 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 메뉴를 확장하고 **Standalone(**독립형**)**을 선택합니다.

단계 **6** **Destination(**대상**)** 드롭다운 메뉴를 확장하고 메트릭을 처리하고 분석할 서드파티 애플리케이션을 선택합니다.

단계 **7** 메트릭의 엔드포인트 위치로 사용할 **Endpoint(**엔드포인트**)**를 입력합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

분석 애플리케이션으로 DataDog를 선택하는 경우, 엔드포인트는 기본적으로 HTTP Webhook로 채워집니다. 이 항목이 기본값인 경우 프로파일을 저장하기 전에 수정할 수 있습니다.

다음에 수행할 작업

- 프로파일 세부 정보 보기
- 프로파일에 게이트웨이 연결 추가

그룹 메트릭 전달 프로파일 생성

이 프로세스에서는 프로파일을 생성한 다음 특정 게이트웨이에 할당합니다. 그룹 프로파일은 최대 5개의 독립형 메트릭 전달 프로파일을 결합한 다음 단일 게이트웨이에 할당할 수 있습니다. 다음 절차를 사용하여 그룹화된 메트릭 전달 프로파일을 생성합니다.

시작하기 전에

- 이 프로파일을 생성하기 전에 메트릭을 전달할 서드파티 애플리케이션이 하나 이상 있어야 합니다.
- 둘 이상의 독립형 메트릭 전달 프로파일이 이미 생성되어 있어야 합니다. 자세한 내용은 독립형 메트릭 전달 프로파일 생성, 23 페이지를 참조하십시오.

단계 **1** 멀티 클라우드 방어 컨트롤러 인터페이스에서 **Manager(**관리자**)** > **Profiles(**프로파일 **)** > **Metrics Forwarding(**메트릭 전달**)**으로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** **Type(**유형**)** 드롭다운 메뉴를 확장하고 **Group(**그룹**)**을 선택합니다.

단계 **6** **Group Details(**그룹 세부 정보**)**에서 프로파일에 추가해야 하는 모든 새 행에 대해 **Add(**추가**)**를 클릭합니다.

단계 **7** 각 행에 대한 드롭다운 메뉴를 확장하여 그룹에 추가할 프로파일을 선택합니다. 저장하기 전에 언제든지 프로파일을 제거하려면, 해당 프로파일의 확인란을 선택하고 **Remove(**제거**)**를 선택합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 프로파일 세부 정보 보기
- 프로파일에 게이트웨이 연결 추가

NTP

멀티 클라우드 방어 게이트웨이은(는) NTP를 사용하여 동기화된 시간을 보장합니다. NTP는 관리 인터페이스를 통해 작동하며 관리 목적으로 사용되는 Linux 쉘의 일부로 설정됩니다. NTP 기본 구성은 다음과 같이 각 CSP마다 약간 다릅니다.

- **AWS:** `2.centos.pool.ntp.org`, `169.254.169.123`
- **Azure:** `0.centos.pool.ntp.org`, `1.centos.pool.ntp.org`, `2.centos.pool.ntp.org`, `3.centos.pool.ntp.org`
- **GCP:** `metadata.google.internal`
- **OCI:** `0.centos.pool.ntp.org`, `1.centos.pool.ntp.org`, `2.centos.pool.ntp.org`, `3.centos.pool.ntp.org`, `169.254.169.254`

기본 설정을 재정의하기 위해 NTP 프로파일을 생성하여 각 게이트웨이에 적용할 수 있습니다. NTP 프로파일이 게이트웨이에 적용되면 새 설정이 사용됩니다. 이 작업은 즉시 적용됩니다.

프로파일 생성

다음 절차에 따라 NTP 프로파일을 생성합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **NTP**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유한 이름을 지정합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일을 구분하는 데 도움이 될 수 있습니다.

단계 **5** NTP 서버 목록을 지정합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

What to do next

- 프로파일 세부 정보 보기
- 프로파일에 게이트웨이 연결 추가

BGP 프로파일

BGP(Border Gateway Protocol)는 IETF(Internet Engineering Task Force) 표준이며 모든 라우팅 프로토콜 중에서 가장 확장성이 뛰어납니다. BGP는 글로벌 인터넷 및 통신 사업자 프라이빗 네트워크의 라우팅 프로토콜입니다. BGP를 사용하면 VPN 게이트웨이와 BGP 인접한 라우터가 커넥터의 양쪽에 있는 게이트웨이에 관련 게이트웨이 또는 라우터의 가용성을 알리는 경로를 교환할 수 있습니다.

BGP 프로파일 생성

다음 절차에 따라 멀티 클라우드 방어 컨트롤러 대시보드에서 BGP 프로파일을 생성합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **BGP**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일과 구분할 수 있습니다.

단계 **5** **LocalAS** 값을 입력합니다. 이 값은 BGP4 디바이스가 상주하는 로컬 자율 시스템(AS)을 나타냅니다.

단계 **6** **Add Neighbor(**네이버 추가**)**를 클릭하여 프로파일에 하나 이상의 피어를 추가합니다.

단계 **7** **Neighbor(**인접한 라우터**)**에 다음 정보를 추가합니다.

a) **IP Address(IP** 주소**)** - IP 주소 및 BGP 피어 그룹의 단일 주소 또는 범위를 입력합니다. 여러 주소를 추가하는 경우에는 공백으로 각 주소를 구분합니다.

b) **Autonomous System(**자동 시스템**)** - 인접한 라우터가 상주하는 위치에 대한 **LocalAS**를 입력합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

BGP 프로파일을 멀티 클라우드 방어 게이트웨이에 추가합니다. 새 게이트웨이를 생성 하거나 새 프로파일을 포함하도록 기존 게이트웨이를 편집할 수 있습니다.

IPSec 프로파일

가상 터널 인터페이스에 IPSec(Internet Protocol Security) 프로파일을 사용하면 원격 액세스를 위한 보호를 제공해야 하는 경우 구성 프로세스를 간소화할 수 있습니다. IPSec 프로파일에는 두 사이트 간 VPN 피어 간의 안전한 논리적 통신 경로를 보장하는 데 필요한 필수 보안 프로토콜 및 알고리즘이 포함되어 있습니다. VPN은 네트워크-네트워크, 호스트-네트워크, 호스트-호스트 통신에 IPsec 터널에 의존하므로 터널을 생성할 때 필수 구성 요소입니다.

IPsec 프로파일을 사용하면 추가 보안 및 암호화 보호를 위해 IKE 및 IPSEC 매개 변수를 한 곳에서 구성할 수 있습니다.

IPSec 프로파일 생성

다음 절차에 따라 멀티 클라우드 방어 컨트롤러 대시보드에서 IPSec 프로파일을 생성합니다.

단계 **1** **Manage(**관리**)** > **Profiles(**프로파일**)** > **IPSec**으로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** 고유 **Profile Name(**프로파일 이름**)**을 입력합니다.

단계 **4** (선택 사항) **Description(**설명**)**을 입력합니다. 이렇게 하면 유사한 이름의 다른 프로파일과 구분할 수 있습니다.

단계 **5** 프롬프트가 표시되면 적절한 IKE 정보를 입력합니다.

a) **DH Group(DH** 그룹**)** - DH(Diffie-Hellman) 그룹은 키 교환 프로세스에 사용되는 키의 강도를 결정합니다. 드롭다운 메뉴를 확장하여 프로파일에 적절한 그룹을 선택합니다.

b) **Authentication(**인증**)** - 이 터널에 대해 원하는 인증 유형을 선택하려면 드롭다운 메뉴를 확장합니다.

c) **Encryption(**암호화**)** - 가로채기된 스택에는 암호화 및 암호 해독이 필요합니다. 드롭다운 메뉴를 확장하여 암호화 방법을 선택합니다.

d) **Hash(**해시**)** - SHA1은 160비트 다이제스트를 생성하는 단방향 해싱 알고리즘입니다. 드롭다운 메뉴를 사용하여 적절한 옵션을 선택합니다.

e) **Key Lifetime(**키 수명**)** - 키가 지속되는 시간 값을 초 단위로 입력합니다. 사용 가능한 값은 60초 ~ 86400초입니다.

f) **IKE Version(IKE** 버전**)** - IKE(Internet Key Exchange)는 IP 패킷의 강력한 인증 및 암호화를 제공하는 IPSec 프로토콜 제품군의 보안 연결을 설정하는 데 사용되는 프로토콜입니다. 드롭다운 메뉴를 사용하여 IKE 버전 1 또는 버전 2를 선택합니다. 버전 간에는 상당한 차이점이 있으므로 환경에 가장 적합한 버전을 선택해야 합니다.

단계 **6** 프롬프트가 표시되면 적절한 IPsec 정보를 입력합니다.

a) **Authentication(**인증**)** - 드롭다운 메뉴를 확장하여 인증 방법으로 None(없음), SHA256, SHA 또는 Null을 선택합니다.

b) **Encryption(**암호화**)** - 드롭다운을 확장하고 키 유형(AES GCM 256, AES GCM 192 또는 AES GCM)을 선택합니다. 이렇게 하면 연결된 디바이스 간 고유 키 교환이 생성되므로 각 디바이스에서 다른 디바이스의 메시지를 암호 해독할 수 있습니다.
c) **Mode(**모드**)** - 드롭다운 메뉴를 확장하여 IPSec 정책 인증 프로토콜을 선택합니다. 둘 이상 선택할 수 있습니다.

다음에 수행할 작업

사이트 간 VPN 터널에 IPSec 프로파일을 연결합니다. 사이트 간 터널 연결 생성를 수행하거나 새 IPSec 프로파일을 포함하도록 기존 터널을 편집할 수 있습니다.