Cisco 멀티 클라우드 방어 FAQ

초판: 2023년 5월 17일

Cisco 멀티 클라우드 방어 FAQ

엣지, 허브, 인그레스, 이그레스는 무엇을 의미합니까?

인그레스: 애플리케이션이 VPC에서 실행 중입니다. 트래픽은 외부(인터넷)에서 VPC로 들어갑니다. 외부 사용자로부터 애플리케이션을 보호하기 위해 인그레스 게이트웨이가 구축됩니다.

이그레스: 외부 환경(인터넷)과 통신해야 하는 클라이언트/EC2 인스턴스/애플리케이션입니다. 이러한 클라이언트가 인터넷으로 이그레스되는 트래픽을 보호/제어하려면 특정 웹사이트(예: 결제 게이트웨이 또는 승인된 소스 코드 저장소)와의 통신만 제한해야 합니다. 발신 트래픽을 제어하기 위해 이그레스 게이트웨이가 구축됩니다.

엣지: 게이트웨이(이그레스 및 인그레스)를 엣지 또는 허브 모드로 구축할 수 있습니다. 엣지 모드에서 게이트웨이는 애플리케이션과 동일한 VPC에 구축됩니다. 5개의 VPC가 애플리케이션을 실행하는 경우 5개의 게이트웨이가 구축됩니다. 이는 소수의 VPC에 가장 적합합니다.

허브: 멀티 클라우드 방어에서는 새 VPC(서비스 VPC라고 함)를 생성하고 이 서비스 VPC 내부에 게이트웨이를 구축합니다. 애플리케이션을 실행하는 모든 VPC와 게이트웨이를 포함하는 서비스 VPC는 AWS Transit Gateway를 통해 연결됩니다. 멀티 클라우드 방어은 Transit 게이트웨이, VPC 첨부 파일 및 라우팅의 오케스트레이션을 자동으로 관리합니다. 고객은 VPC 라우트 테이블을 수정하여 Transit 게이트웨이를 기본 경로 대상으로 설정해야 합니다. Transit 게이트웨이는 신규이거나 기존 게이트웨이일 수 있습니다.

멀티 클라우드 방어에서는 인그레스 및 이그레스 활용 사례 각기 다른 게이트웨이를 구축해야 합니다. 단일 게이트웨이를 사용하여 인그레스 및 이그레스 트래픽을 보호할 수는 없습니다.

정방향 프록시 및 역방향 프록시란 무엇입니까?

정방향 프록시 규칙 및 서비스는 이그레스 게이트웨이에서 사용됩니다. 게이트웨이는 인그레스 및 이그레스 모드 모두에서 프록시 서버 역할을 합니다. 인그레스 케이스에서 사용자는 멀티 클라우드 방어 게이트웨이에서 제공하는 프록시 엔드포인트에 액세스합니다. 이그레스 시나리오에서 프록시는 투명합니다. VPC 내부의 클라이언트는 멀티 클라우드 방어 게이트웨이을 거쳐 라우팅을 통해 외부 사이트(인터넷)에 액세스합니다. 게이트웨이는 클라이언트에 응답합니다. 게이트웨이가 외부 사이트 인증서 서명에 사용하는 루트 인증서를 제공하라는 메시지가 표시됩니다. 클라이언트에는 이 루트 인증서가 신뢰할 수 있는 소스로 설치되어 있어야 합니다.

역방향 프록시 규칙 및 서비스는 인그레스 게이트웨이에서 사용됩니다. 서비스 정의는 프록시가 수신하는 포트 번호 및 트래픽을 전달할 대상 애플리케이션/호스트를 정의합니다.

URL 필터링이란 무엇입니까?

URL 필터링은 이그레스 게이트웨이에서만 사용됩니다. URL 프로파일은 URL과 각 URL에 대한 작업의 목록입니다. URL 프로파일을 생성하고 나면 정책 규칙과 연결됩니다. 트래픽이 URL 프로파일이 있는 규칙과 일치하면 URL 필터링 처리가 시작됩니다. 목록이 순서대로 통과되고 트래픽의 URL과 일치하는 목록에서 첫 번째 항목의 작업이 수행됩니다. 허용되는 URL과 일치하는 URL이 없는 경우 기본 정책이 사용됩니다. 프로파일에 암시(기본값 ALLOW)가 있습니다. URL은 문자열 또는 정규식으로 제공될 수 있습니다. 목록에 DENY에 대한 regex 매치가 없는 경우 일반적으로 ALLOW 규칙이 필요하지 않습니다. 예를 들어 https://website.com/news를 허용하고 동일한 웹사이트에서 나머지는 모두 DENY하도록 하려는 경우 프로파일에 2개의 항목을 정의할 수 있습니다.

https://www.website.com/news ALLOW

https://www.website.com/.* DENY

URL이 삭제되면 멀티 클라우드 방어 컨트롤러의 **Investigate(**조사**)** > **URL Filtering(URL** 필터링**)** 메뉴의 URL 필터링 이벤트에 이벤트가 기록됩니다.

URL 필터링에서 정규식을 사용할 수 있습니까?

예.

URL 필터링의 기본 작업이 허용인 경우 ALLOW 작업이 필요한 이유는 무엇입니까? 일치하는 항목이 없는 경우 URL 필터링의 기본 작업은 ALLOW(허용)입니다. 목록 아래에 매우 일반적인 DENY(거부)가 있는 경우 ALLOW(허용)에 대한 특정 작업이 유용합니다. 기본 작업을 DENY(거부)로 설정하려면 다음 규칙을 추가합니다.

.* DENY 502

이렇게 하면 모든 URL이 삭제됩니다. 이제 특정 URL을 허용하도록 열려면 이 위에 허용을 갖는 규칙을 추가합니다. 예를 들어 google.com에 대한 모든 트래픽을 허용하고 나머지는 모두 거부하려면 다음을 수행합니다.

https://www.google.com ALLOW .* DENY 502

이는 웹사이트의 더 광범위한 페이지를 제한하는 동시에 특정 페이지만 허용하는 데 사용할 수도 있습니다.

https://www.website.com/news ALLOW

https://www.website.com/.* DENY

URL 프로파일에서 URL은 어떤 모양이어야 합니까?

URL 목록의 URL은 http 또는 https가 포함된 완전한 문자열이어야 합니다. *.*(별표)*와 같은 정규식을 사용하여 google.com과 같은 일반 체계를 정의할 수 있습니다. 이는 http 또는 https와, google.com 앞의 모든 접두사 및 google.com 이후의 모든 접미사와 일치합니다.

L7 DOS란 무엇입니까?

L7 DOS는 인그레스 게이트웨이에서만 사용됩니다. 게이트웨이가 백엔드 애플리케이션을 대상으로 하는 인그레스 프록시 역할을 할 때 URL에 속도 제한을 적용할 수 있습니다. 제한은 각 HTTP 작업(GET, POST 등)에 대한 URL 레벨에서 설정할 수 있습니다. 속도 제한은 전체 게이트웨이 클러스터 레벨이 아닌 방화벽 인스턴스 레벨입니다. 따라서 속도 제한이 1,000 reqs/초로 설정되고 게이트웨이에 3개의 방화벽 인스턴스가 있는 경우 애플리케이션은 3,000 reqs/초를 수신합니다.

허브 모드 게이트웨이를 생성하고 VPC를 보호하려면 어떻게 해야 합니까?

허브 모드 게이트웨이를 사용하면 클라우드 환경의 중앙 집중식 보안 관리가 가능합니다. 애플리케이션을 실행하는 여러 스포크 VPC가 있는 경우, 허브 모드가 모든 VPC를 보호하는 데 선호되는 방법입니다. 보안 관리는 서비스 VPC에서 수행됩니다. 게이트웨이를 호스팅하는 서비스 VPC는 멀티 클라우드 방어 컨트롤러에서 관리됩니다. 모든 VPC는 Transit 게이트웨이에 연결되기 전에 중첩되지 않는 CIDR이 있어야 합니다. 게이트웨이를 생성하는 동안 인그레스 또는 이그레스(프로세스 동일)를 선택하고 허브 모드 옵션을 선택합니다. 이미 보유한 Transit 게이트웨이를 사용할 경우의 옵션을 선택하거나 새 Transit 게이트웨이를 생성하도록 선택합니다. 서비스 VPC를 이미 생성한 경우 이를 선택하거나 새 VPC를 생성하도록 선택합니다. 새 서비스 VPC를 생성하는 동안 보호하려는 스포크 VPC와 중복되지 않는 CIDR을 제공합니다. 게이트웨이 생성 프로세스를 계속합니다. 다른 서브넷 또는 보안 그룹 정보는 제공할 필요가 없습니다. 멀티 클라우드 방어에 의해 관리됩니다. 계정 온보딩의 일부로 생성된 방화벽 역할과 키 쌍을 제공합니다.

게이트웨이가 생성되면 보호하려는 스포크 VPC를 추가하도록 게이트웨이를 수정합니다. Edit Gateway(게이트웨이 편집) 옵션에서 'Protect VPCs(VPC 보호)'가 나올 때까지 화면을 내린 다음 보호할 모든 VPC를 선택합니다. 멀티 클라우드 방어은 선택한 모든 VPC에 대한 Transit 게이트웨이 첨부 파일을 생성합니다. VPC에서 서브넷을 무작위로 선택하여 연결을 수행합니다. VPC가 연결되면 애플리케이션 서브넷에 연결된 VPC 라우트 테이블을 변경하고 Transit 게이트웨이에 대한 기본 경로를 추가/설정합니다. 인그레스 허브 모드 게이트웨이의 경우 특정 경로를 기본 경로 대신 서비스 VPC CIDR로 설정할 수 있습니다. 이그레스 게이트웨이의 경우 기본 경로가 선호되는 옵션이지만, SSH/관리 작업의 경우에는 인터넷 게이트웨이를 사용하도록 구체적인 경로를 설정할 수 있습니다.

AWS 계정을 Valtix Controller에 추가하려면 어떻게 해야 합니까?

멀티 클라우드 방어 컨트롤러가 게이트웨이, 인벤토리 액세스 및 계정의 다른 작업을 생성하려면 AWS 계정에 액세스해야 합니다. 멀티 클라우드 방어에서 멀티 클라우드 방어 컨트롤러에 사용할 교차 계정 IAM 역할을 생성하는 CFT(CloudFormation 템플릿)를 제공합니다. 온보딩 프로세스의 일부로 멀티 클라우드 방어 계정 번호가 제공됩니다. IAM 역할은 이 계정에 권한을 부여합니다. 이 역할에 할당된 권한은 IAM 역할 설명서를 참조하십시오.

게이트웨이 및 방화벽이란 무엇입니까?

게이트웨이 및 방화벽이라는 용어는 솔루션 및 문서 전체에서 때때로 같은 의미로 사용됩니다. 게이트웨이는 단일 엔터티로 관리되는 방화벽 인스턴스의 클러스터입니다. NLB(Network Load Balancer)는 모든 방화벽 VM 인스턴스를 이 로드 밸런서의 대상으로 포함하는 게이트웨이 구축의 일부로 생성됩니다. 사용자는 인스턴스와 게이트웨이를 독립적으로 관리하지 않습니다. 이 모두 컨트롤러에서 관리합니다. NLB는 세션 트래픽이 동일한 방화벽 인스턴스에 도달하도록 합니다. 방화벽 인스턴스는 보안 시행자입니다.

Baltix 게이트웨이가 HA, 자동 확장을 지원합니까?

멀티 클라우드 방어 보안 플랫폼은 클라우드에서 시작됩니다. HA 및 자동 확장은 첫날부터 시스템에 내장됩니다. 게이트웨이를 생성하는 동안 여러 영역(AZ)에서 애플리케이션을 실행하는 것과 비슷하게 여러 영역에서 인스턴스를 생성할 수 있는 옵션이 제공됩니다. 2개 이상의 영역에서 게이트웨이 인스턴스를 실행하는 것이 좋습니다. 또한 실행할 게이트웨이 인스턴스 수를 선택할 수 있습니다. 최소 및 최대 인스턴스를 선택할 수 있습니다. 자동 확장에 대한 자세한 내용은 다음 질문을 검토하십시오.

자동 확장 또는Valtix는 트래픽에 따라 어떻게 확장됩니까?

게이트웨이를 생성하는 동안 실행할 방화벽 인스턴스 수를 선택하는 옵션이 제공됩니다. 최소값은 항상 1입니다. 최대값은 최대 10이 될 수 있습니다. 이는 가용성 영역(AZ)에 따른 것입니다. 최소 2개에서 시작하고 AZ가 2개 있으면 계정에서 총 4개의 인스턴스가 실행됩니다. 컨트롤러는 인스턴스의 사용량을 계속 추적하며 방화벽이 더 바빠지면 최대 수에 도달할 때까지 새 인스턴스를 자동으로 생성합니다. 트래픽 속도가 느려지면 인스턴스가 자동으로 삭제됩니다. 온디맨드 방식으로 리소스를 생성하며 사용되는/필요한 경우에만 리소스를 지불합니다. 인스턴스에 대한 사용량이 없는 경우 삭제되지만 요금이 부과되지 않습니다.

Valtix를 시작하기 위해 AWS 환경을 준비하려면 어떻게 해야 합니까?

멀티 클라우드 방어 보안 서비스는 허브 모드 또는 엣지 모드에서 작동합니다. 허브 모드는 보호하려는 여러 VPC가 있을 때 사용됩니다. AWS Transit 게이트웨이를 사용하여 모든 VPC를 연결합니다. 이 모드의 경우 멀티 클라우드 방어이 새 서비스 VPC를 생성하여 게이트웨이를 구축할 수 있도록 중첩되지 않은 CIDR을 제공해야 합니다. 서비스 VPC는 멀티 클라우드 방어 컨트롤러에서 완전히 관리됩니다.

엣지 모드 구축에서 게이트웨이는 애플리케이션과 동일한 VPC에 설치됩니다. 이 구축에는 멀티 클라우드 방어에 2개의 퍼블릭 서브넷(관리 및 데이터 경로)과 2개의 보안 그룹(관리 및 데이터 경로)이 필요합니다. 두 보안 그룹 모두 아웃바운드 트래픽을 허용하는 규칙이 필요합니다. datapath security-group은 모든 트래픽을 허용하거나 멀티 클라우드 방어 컨트롤러에서 서비스에서 구성하는 특정 포트를 활성화할 수 있습니다.

두 가지 배포 모드 모두 멀티 클라우드 방어에는 여러 IAM 역할이 필요합니다. 컨트롤러가 AWS 계정에 액세스하는 교차 계정 IAM 역할, KMS에 액세스하는 게이트웨이 인스턴스에 할당된 IAM 역할, Secrets Manager 및 S3가 PCAP 파일을 작성하는 역할입니다.

멀티 클라우드 방어는 IAM 역할 생성을 지원하고 권한에 대한 세부 정보를 포함하는 CloudFormation 템플릿을 제공합니다. 이 내용은 사용자 가이드 IAM 역할 문서에 자세히 설명되어 있습니다.

Valtix를 시작하기 위해 Azure 환경을 준비하려면 어떻게 해야 합니까?

멀티 클라우드 방어 솔루션은 허브 모드 또는 엣지 모드에서 작동합니다. 허브 모드는 보호하려는 VNet이 여러 개인 경우 사용됩니다. Azure UDR은 이러한 용도로 사용됩니다.

엣지 모드 구축에서 게이트웨이는 애플리케이션과 동일한 VNet에 설치됩니다. 이 구축에는 멀티 클라우드 방어에 2개의 퍼블릭 서브넷(관리 및 데이터 경로)과 2개의 네트워크 보안 그룹(관리 및 데이터 경로)이 필요합니다. 두 보안 그룹 모두 아웃바운드 트래픽을 허용하는 규칙이 필요합니다. Datapath security-group은 모든 트래픽을 허용하거나, 멀티 클라우드 방어 컨트롤러에서 서비스에서 구성하는 특정 포트를 활성화할 수 있습니다.

두 구축 모드 모두에 대해 멀티 클라우드 방어에는 Azure Active Directory ID(테넌트 ID), 구독 ID, 클라이언트 키 및 암호가 있는 AD(Active Directory)의 애플리케이션, 리소스 생성, 볼트 액세스 등의 권한이 있는 애플리케이션에 할당된 사용자 지정 역할이 필요합니다.

자세한 내용은 사용 설명서를 참조하십시오.

플로우 로그의 Sessionid는 무엇입니까?

멀티 클라우드 방어 게이트웨이는 인그레스 및 이그레스에 대한 프록시 역할을 합니다. 인그레스 시나리오에서는 인터넷의 외부 사용자가 게이트웨이 엔드포인트에 액세스하며 게이트웨이는 엔드포인트(대상)에 대한 새 세션을 시작합니다. 이는 두 가지 서로 다른 트래픽 플로우입니다. Sessionid는 이러한 두 플로우의 상관관계를 파악하고 플로우 로그에 표시하기 위해 함께 연결합니다.

프록시된 애플리케이션에 대한 인증서를 어떻게 제공합니까?

자체 서명 인증서를 생성하거나 이미 생성된 인증서의 콘텐츠를 가져오는 옵션이 있는 경우 TLS 암호 해독 프로파일을 정의해야 합니다.

TLS 암호 해독 프로파일을 백엔드에서 프록시된 애플리케이션의 역방향 프록시용 리스너 암호 해독 프로파일로 구성할 수 있습니다.

TLS 암호 해독 프로파일은 전달 프록시를 통해 인터넷으로 이그레스하는 클라이언트에 루트 CA 인증서 및 개인 키가 설치된 전달 프록시에 대한 루트 CA 암호 해독 프로파일로 구성할 수 있습니다.

Valtix Controller에 제공하지 않고 개인 키를 보호하려면 어떻게 해야 합니까?

TLS 암호 해독 프로파일의 정의에는 개인 키를 가져오는 여러 가지 방법이 있습니다.

- 콘텐츠를 투명하게 가져옵니다.
- AWS KMS 암호화된 개인 키입니다.
- AWS Secrets Manager 암호 이름입니다.
- 지정된 자격 증명 저장소의 Credstash 키 이름입니다.
- 지정된 키 저장소의 Azure 키 이름입니다.

멀티 클라우드 방어 컨트롤러에 개인키를 남기고 싶지 않다면 (b), (c), (d), (e)를 선택하는 것이 좋습니다.

역방향 프록시 서비스에 표시되는 모든 프로토콜 옵션은 무엇입니까?

Table 1: 역방향 프록시 서비스에 표시되는 모든 프로토콜 옵션은 무엇입니까*?*

프록시 유형	암호 해독 프로파일	프런트 엔드 프로토콜	백엔드 프로토콜
TCP-TCP	아니요	TCP	TCP
TLS-TLS	예	TCP	TCP
HTTP-HTTP	아니요	TCP	HTTP
HTTPS-HTTPS	예	TCP	HTTPS
HTTPS-HTTP	예	TCP	HTTP
WEBSOCKET-WEBSOCKET	아니요	TCP	WEBSOCKET
WEBSOCKETS-WEBSOCKETS	예	TCP	WEBSOCKET_S

SSH 애플리케이션에 대한 역방향 프록시를 어떻게 구성해야 합니까?

프록시 유형 TCP-TCP를 사용합니다.

역방향 프록시 대상에서 **HTTPS**와 **TLS**의 차이점은 무엇입니까?

TLS 프록시에서 클라이언트 또는 서버에서 수신한 TCP 페이로드는 재암호화되는 동안 그대로 유지됩니다. 이러한 TCP 페이로드 바이트 보존이 필수인 NTLM을 사용하는 RDP와 같은 애플리케이션도 있습니다.

HTTPS 프록시에서 프록시는 HTTP 연결을 종료하고, HTTP PDU에 연결된 추가 프록시 헤더를 통해 HTTP 페이로드를 프록시의 한 레그에서 다른 레그로 옮깁니다. HTTPS 프록시를 사용하면 심층 패킷 보안 관련 작업에 대해 HTTP 레벨에서 응답을 전송할 수 있습니다. 또한 URL 레벨에서 속도 제한기를 지정할 수 있습니다.

여러 게이트웨이에 동일한 정책 규칙을 적용하려면 어떻게 해야 합니까?

정책 규칙은 항상 정책 규칙 집합의 컨텍스트에서 정의됩니다. 정책 규칙 집합은 규칙 집합을 정의합니다. 이 정책 규칙 집합은 여러 게이트웨이와 연결할 수 있습니다. 게이트웨이에는 하나의 정책 규칙 집합만 있을 수 있습니다.

내 대상 애플리케이션 **IP**가 각 지역에서 다르며 변경할 수 있습니다. 서비스에서 내 백엔드 대상을 설정하려면 어떻게 해야 합니까?

애플리케이션이 실행 중인 인스턴스와 연결된 user-defined-tag를 정의합니다. 이 태그를 사용하여 백엔드 주소 개체를 정의합니다. 이 백엔드 주소 개체를 서비스의 대상으로 연결합니다. 컨트롤러는 해당 태그가 있는 인스턴스의 IP 집합 멤버십을 자동으로 유지합니다. 또한 해당 user-defined-tag가 있는 인스턴스가 가동 및 중단되거나 해당 user-defined-tag가 있는 인스턴스의 IP 주소가 변경되는 경우 멤버십 변경사항은 컨트롤러에 의해 자동으로 처리됩니다.

서비스 개체의 **SNI**란 무엇입니까?

SNI는 서버 이름 표시의 약자입니다. 서버의 FQDN을 포함하는 server_name이라는 TLS 클라이언트 hello 확장이 있습니다. 그런 다음 서비스 개체의 정의에서 이를 사용하여 트래픽을 적절한 백엔드로 라우팅할 수 있습니다. 서비스 개체에 정의된 SNI 집합을 사용하여 클라이언트에서 해당 서비스에 대한 액세스만 허용할 수 있습니다.

서비스 개체 정의에 있는 SNI의 예: service1.Enterprise.com

이는 백엔드 서비스 및 관련 FQDN이 잘 정의되어 있는 역방향 프록시에만 의미가 있습니다.

내 백엔드/대상은 여러 웹 사이트를 호스팅합니다. Valtix 게이트웨이를 통해 동일한 포트에 프록시 설정하고자 합니다. 이 목표를 달성하려면 어떻게 해야 합니까?

웹사이트별로 서비스 개체를 정의합니다. 각 서비스 개체는 동일한 리스너 포트 및 웹사이트를 사용합니다.

게이트웨이로 프록시해야 하는 여러 웹 백엔드/대상이 있습니다. 어떻게 구성합니까?

동일한 리스너 포트를 사용하여 웹 백엔드별 서비스 개체 정의 및

- SNI = 웹 백엔드 FQDN 및
- target = 백엔드 FDQN 또는 ALB FQDN 웹 백엔드의 프런트엔드 처리

암호 해독 프로필과 인증서는 어떤 관계입니까?

암호 해독 프로필은 인증서와 일대일입니다. 이 암호 해독 프로파일은 정책 규칙의 일부로 사용되는 서비스 개체와 연결할 수 있습니다. 이 간접 참조 레벨은 이 인증서에 의존하는 모든 정책 규칙/서비스를 업데이트할 필요 없이, 암호 해독 프로파일만 업데이트하여 만료된 인증서를 갱신하거나 주기적으로 인증서를 교체하도록 인증서를 더욱 쉽게 관리하는 데 도움이 됩니다.

각 백엔드에 대해 서로 다른 IPS 보호 규칙이 필요합니다. 어떻게 해야 합니까?

모든 게이트웨이에는 IPS 프로파일이 1개만 있을 수 있습니다. 이는 규칙 레벨에서 구성되더라도 게이트웨이별로 설정됩니다. 따라서 동일한 게이트웨이를 사용하여 여러 IPS 프로파일을 보유할 수 없습니다. 여러 게이트웨이를 생성해야 합니다.

IPS 규칙은 어디에 있으며, 얼마나 자주 업데이트합니까? 업데이트가 게이트웨이에 자동으로 푸시됩니까?

Cisco TALOS 규칙은 격주 간격으로 주기적으로 폴링되며, 중요한 규칙 업데이트 알림을 기반으로 더욱 짧은 기간으로 폴링됩니다. 이러한 업데이트는 컨트롤러에서 자동으로 고객에게 제공되며, 고객은 게이트웨이에 푸시할 올바른 규칙 집합 버전을 선택할 수 있습니다.

IPS 프로파일에는 많은 설정 옵션이 있습니다. 더 자세히 설명해 주실 수 있습니까?

IPS 프로파일을 사용하면 사용자는 SNORT 정책, 카테고리 또는 클래스 유형에 따라 규칙 집합에서 규칙 집합을 선택할 수 있습니다.

위협 기반 PCAP 파일 생성을 활성화하는 옵션도 있습니다.

규칙 억제는 신뢰할 수 있는 소스 CIDR을 기반으로 오탐에 대해 제공됩니다.

규칙 레벨 이벤트 필터는 복잡한 규칙에 대해 활성화하거나 모든 규칙에서 전역 프로파일 레벨 이벤트 필터를 활성화할 수 있습니다.

모든 공격의 PCAP(패킷 캡처) 파일을 가져오고 싶습니다. 가능합니까?

예. 네트워크 침입 프로파일 또는 웹 보호 프로파일에서 Enable Threat Based PCAP(위협 기반 PCAP 활성화) 확인란을 선택합니다.

저에게는 로그 분석 인프라가 있습니다. 로그를 전달할 수 있습니까?

예. 시스템 로그, Splunk 및 DataDog가 지원됩니다. 자세한 내용은 사용자 가이드를 참조하십시오.

백엔드 애플리케이션에 대한 역방향 프록시를 구성했습니다. 그 밖에 무엇을 해야 합니까?

1. 멀티 클라우드 방어 게이트웨이의 FDQN을 가리키도록 DNS 레코드를 변경합니다.
2. 공용의 직접 액세스를 방지하기 위해 기존 애플리케이션 로드 밸런서를 전용으로 변경합니다.

DNS 프로파일 및 레코드는 무엇이며 사용하는 이유는 무엇입니까?

AWS의 웹 기반 애플리케이션은 일반적으로 로드 밸런서를 생성할 때 동적으로 생성된 내부 FQDN에서 참조합니다. 멀티 클라우드 방어가 검사를 위해 해당 애플리케이션의 인그레스 경로에 있도록 하려면 고객이 멀티 클라우드 방어 게이트웨이를 참조하도록 해당 애플리케이션의 DNS 레코드를 업데이트하도록 권장합니다.

예를 들어 app.xyz.com의 DNS 레코드는 내부 애플리케이션 로드 밸런서의 CNAME을 가리킵니다. 멀티 클라우드 방어 게이트웨이가 이 애플리케이션의 인그레스 경로에 있는 경우 멀티 클라우드 방어 게이트웨이 엔드포인트의 CNAME을 가리키도록 DNS 레코드를 업데이트합니다. 멀티 클라우드 방어 DNS 프로파일을 사용하면 애플리케이션과 관련된 Route53 도메인 이름을 지정할 수 있으며, 여

기서 이 애플리케이션의 기록을 구성하고 게이트웨이 목록에서 적절한 멀티 클라우드 방어 인그레스 게이트웨이를 선택할 수 있습니다.