# 서비스 개체



# 역방향 프록시 서비스 개체(인그레스)

인그레스 서비스 개체는 인그레스/역방향 프록시 규칙에서 사용됩니다. 개체는 멀티 클라우드 방어 게이트웨이가 수신하고 대상/백엔드 주소에 전달하는 트래픽을 수신하는 리스너 포트를 정의합니다. TLS 인증서가 구성된 암호 해독 프로파일로 리스너 포트를 구성할 수 있습니다. 트래픽이 리스너 포트에 도달하면 멀티 클라우드 방어 게이트웨이은(는) 설정된 TLS 인증서를 반환합니다. 다음과 같은 구성 가능한 옵션을 고려하십시오.

- 이 포트에서 SNI를 설정할 수 있습니다. 이렇게 하면 단일 리스너 포트(예: 443)를 SNI를 기반으로 여러 백엔드 대상에 프록시할 수 있습니다.
- 서비스에 L7 DoS(L7 Denial of Service)를 구성하여 URI 및/또는 HTTP 메서드에 대한 속도 제한을 설정할 수 있습니다.
- 대상은 트래픽을 전달할 포트 및 백엔드 주소 개체를 정의합니다. 프록시 설정된 트래픽은 HTTP, HTTPS, TCP 또는 TLS로 전달할 수 있습니다.

역방향 프록시 서비스 개체를 생성하고 추가하려면 다음 절차를 따르십시오.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Reverse Proxy(**역방향 프록시**)**를 클릭합니다.

단계 **4** **Name(**이름**)**과 **Description(**설명**)**을 제공합니다.

단계 **5** 아래에 정의된 대로 프록시 매개변수를 구성합니다.

| 옵션 | 설명 |
|---|---|
| 암호 해독 프로파일 | 프록시 서비스에 사용할 서버 인증서도 포함하는 암호 해독 프로파일을 할당합니다. |
| 대상 포트 | 대상 포트를 할당합니다. 대부분의 웹 기반 서비스의 경우 대상 포트는 443입니다. 이 포트는 수신 트래픽을 수신하는 포트 멀티 클라우드 방어 게이트웨이입니다. |
| 프로토콜 | TCP가 기본값입니다. |
| SNI | SNI 목록을 입력합니다. |
| L7 DoS | 이 프록시 서비스에 할당할 레이어 7 DoS 프로파일을 입력합니다. |
| 대상 백엔드 포트 | 대상/백엔드 애플리케이션 포트 번호를 입력합니다. |
| 프로토콜 | 백엔드 프로토콜을 선택합니다. |
| 주소 | 백엔드 IP 주소를 선택합니다. 대부분의 경우 IP 주소는 내부 로드 밸런서의 프런트엔드 IP가 됩니다. |

**Note** 여러 포트에서 프록시 서비스를 실행해야 하는 경우 항목을 더 추가할 수 있습니다. 그러나 모든 포트는 동일한 인증서를 제공하며 동일한 백엔드 대상 주소 개체에 프록시됩니다.

# 전달 프록시 서비스 개체(이그레스/이스트-웨스트)

전달 프록시 서비스는 특히 HTTP 기반 트래픽에 사용됩니다. 개체는 멀티 클라우드 방어 게이트웨이이(가) 수신 트래픽을 수신하고 TLS SNI 확장 헤더 또는 HTTP 호스트 헤더에서 사용 가능한 주소/호스트에 전달하는 리스너 포트를 정의합니다.

**Note** 이그레스/이스트웨스트 트래픽에 이를 사용하는 것이 좋습니다.

다음 절차를 사용하여 정방향 프록시 서비스를 생성하고 추가합니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Forward Proxy(**전달 프록시**)**를 클릭합니다.

단계 **4** 이름과 설명을 제공합니다.

단계 **5** 경우에 따라 일치시킬 애플리케이션 ID를 선택합니다.

단계 **6** 아래에 정의된 대로 프록시 매개변수를 구성합니다.

| 옵션 | 설명 |
|---|---|
| 암호 해독 프로파일 | 인증서도 포함하는 암호 해독 프로파일을 할당합니다. 멀티 클라우드 방어은(는) 이 프로파일에서 제공하는 인증서로 서명하여 외부 인증서를 가장합니다. 루트 인증서는 모든 클라이언트 애플리케이션 인스턴스에 설치된 것으로 가정됩니다. |
| 대상 포트 | 대상 포트를 할당합니다. 대부분의 웹 기반 서비스의 경우 대상 포트는 443입니다. |
| 프로토콜 | HTTP 또는 HTTPS. |

**Note**
- 멀티 클라우드 방어은(는) **Dst Port(**대상 포트**)** 에서 수신 대기하고 HTTP 호스트 헤더 또는 TLS SNI 헤더 패킷을 기다립니다. 멀티 클라우드 방어이(가) 패킷을 수신한 후 프로토콜을 사용하여 호스트에 연결합니다. 프로토콜이 HTTPS인 경우, 외부 호스트에서 수신된 인증서 데이터는 암호 해독 프로파일의 인증서에 의해 서명되고 클라이언트로 전송됩니다. 인증서 오류를 방지하려면 클라이언트 앱 인스턴스에 루트 인증서를 설치해야 합니다.
- 지정된 대상 포트의 경우 모든 서비스 개체의 정책 규칙 집합에는 암호 해독 프로파일(루트 CA 인증서) 연결이 하나만 있을 수 있습니다.
- 정방향 프록시 세션 중에 멀티 클라우드 방어 게이트웨이에서는 DNS 요청 시간 초과 30초 및 캐시 만료 시간 초과 TTL 초로 대상에 대한 DNS 조회를 수행합니다.

# 서비스 개체 전달(이그레스/이스트-웨스트)

전달 서비스 개체는 전달 규칙에서 사용됩니다. 이 유형의 규칙/서비스와 일치하는 트래픽은 프록시 설정되지 않고 있는 그대로 전달됩니다. 이는 암호화된 트래픽에 대한 심층 패킷 검사와 애플리케이션 ID가 없음을 의미합니다.

**Note** East-West 트래픽에 이 옵션을 사용하는 것이 좋습니다.

전달 서비스 개체를 생성하고 추가하려면 다음 절차를 따르십시오.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Services(**서비스**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Forwarding(**전달**)**을 클릭합니다.

단계 **4** 이름과 설명을 제공합니다.

단계 **5** 멀티 클라우드 방어은(는) 서비스 레벨별 소스 NAT를 지원합니다. 소스 IP 보존이 필요한 트래픽(예: 이스트-웨스트 트래픽)의 경우 SNAT를 비활성화합니다.

이그레스 트래픽의 경우 SNAT는 항상 활성화되어야 합니다.

단계 **6** 아래에 정의된 대로 포트 매개변수를 구성합니다.

| 옵션 | 설명 |
|---|---|
| 대상 포트 | 대상 포트 또는 대상 포트 범위를 `start-end`로 할당합니다. |
| 프로토콜 | TCP, UDP, ICMP |

**Note** 전달 정책에서 심층 패킷 검사 작업은 암호화되지 않은 트래픽 에서만 발생합니다.