주소 개체

주소 개체

주소 개체는 정의된 방법에 따라 보안 정책 규칙 집합 규칙의 소스 또는 대상 또는 역방향 프록시 서비스 개체의 대상 백엔드 주소로 사용할 하나 이상의 IP, CIDR 또는 FQDN 집합을 나타냅니다. 주소 개체는 기존 구조를 사용하여 정적으로 구성하거나 클라우드 구조를 사용하여 동적으로 구성할 수 있습니다.

주소 개체는 보안 정책 규칙 또는 규칙 집합 내의 **Source(**소스**)**, **Destination(**대상**)** 또는 **Reverse Proxy Target(**역방향 프록시 대상**)** 필드에 있는 하나 이상의 IP, CIDR 또는 FQDN 집합을 나타냅니다. 이는 역방향 프록시 서비스 개체 내에서 대상 백엔드 주소로 정의될 수도 있습니다. 이 섹션에서는 소스 및 대상 개체에 중점을 둡니다.

Src/Dest

이러한 개체는 IP 주소 또는 CIDR에 명시적으로 매핑되는 일치 기준을 정의하는 데 사용됩니다. 개체는 정책 규칙 내에서 참조되며 정책 규칙이 처리될 때 게이트웨이 인스턴스로 들어가는 트래픽에 대해 평가됩니다.

소스 및 대상 주소 개체는 게이트웨이 인스턴스로 들어오는 애플리케이션 트래픽을 매칭하기 위해 IP 주소와 CIDR이 명시적으로 필요한 경우에 유용합니다. 이러한 개체는 정책 규칙 정의의 소스 및 대상 필드 내에서 참조됩니다. 이 각각의 필드를 채우는 데 사용되는 주소 개체 유형은 트래픽 흐름, 애플리케이션 유형, 활용 사례에 따라 달라집니다.

소스 및 대상 주소 개체

소스 또는 대상 주소 개체는 보안 정책 규칙 집합 내부의 규칙에 대한 소스 또는 대상을 지정합니다. 규칙에서 소스 또는 대상 IP 주소를 기준으로 트래픽을 매칭하는 데 사용됩니다. 다양한 유형의 주소 개체는 다음과 같이 정의됩니다.

IP/CIDR/FQDN(고정**)** 주소 개체

IP/CIDR/FQDN 주소 개체는 IP 주소, CIDR 블록 또는 FQDN의 집합으로 구성됩니다. 다음은 IP/CIDR 주소 개체의 예입니다.

- DNS 서버의 대상 IP.
- SMTP 릴레이 서버의 대상 IP.
- NTP 서버의 대상 IP.
- 애플리케이션 워크로드의 소스 IP 또는 서브넷.

FQDN 주소 개체는 DNS 확인을 기반으로 IP를 허용 또는 차단하기 위한 명시적 FQDN 집합을 정의합니다. FQDN이 FQDN 주소 개체 내에서 정의된 다음 정책 규칙 내에서 참조되는 경우 게이트웨이 인스턴스는 DNS 확인을 수행하여 수신 트래픽과 일치하는 해당 IP 주소를 검색합니다. 기본적으로 캐싱은 활성화되어 있지 않습니다. 이 경우 DNS 확인은 60초마다 이루어지며 게이트웨이 인스턴스는 60초 동안 검색된 확인을 사용합니다. FQDN 주소 개체 내에 지정된 FQDN이 대규모 IP 주소 집합(예: 각각 400개 초과)으로 확인되는 경우 캐싱을 활성화할 수 있습니다. 이 경우 캐시 크기 및 캐시 TTL과 함께 DNS 확인 간격을 지정할 수 있습니다.

FQDN 주소 개체는 UDP 기반(예: NTP)이거나 요청 패킷에 호스트 정보가 없는 TCP 트래픽(예: SMTP)인 애플리케이션 트래픽에서 일치시킬 때 유용합니다. 두 경우 모두 내부 워크로드가 연결해야 하는 모든 적절한 NTP 서버 또는 SMTP 서버에 대한 IP 주소 목록을 수동으로 정의하는 대신 이러한 종류의 애플리케이션 트래픽에서 일치시킬 FQDN 주소 개체를 사용하는 것이 좋습니다.

동적 클라우드 구문

클라우드-네이티브 주소 개체는 주기적인 재고 목록 수집(API 기반) 또는 실시간 이벤트 추적(GCP Pub/Sub 통합)을 통해 멀티 클라우드 방어 컨트롤러에서 검색한 동적 클라우드 리소스입니다. 이러한 리소스는 VPC/VNET, 인스턴스 ID, 보안 그룹, 서브넷 ID와 같은 개별 리소스 또는 사용자 정의 태그를 통해 참조되는 리소스 집합일 수 있습니다. 멀티 클라우드 방어 컨트롤러는 실시간 이벤트 추적과 대상 API 호출을 결합하여 클라우드 리소스와 연결된 IP 주소를 동적으로 채웁니다. 따라서 클라우드 네이티브 리소스에 대한 모든 후속 변경 사항은 이 리소스를 참조하는 주소 개체 내부에 자동으로 반영됩니다.

Note 클라우드 네이티브 구조를 사용하여 소스 또는 대상 주소 개체를 정의하면 단일 및 멀티 클라우드 환경 모두에서 동적 클라우드 정책을 생성할 수 있습니다. 클라우드 환경 내에서 클라우드 리소스가 추가, 삭제 또는 변경되면 주소 개체가 동적으로 업데이트되어 이러한 변경 사항을 반영하므로 환경의 모든 애플리케이션 및 기능에서 보안 태세가 자동으로 업데이트됩니다.

VNet 및 VPC 환경의 사용자 정의 태그

태그는 일련의 태그로 정의된 클라우드 리소스의 IP 주소 또는 CIDR을 주소 개체에 매핑합니다. GCP에서 레이블은 다양한 환경(예: 개발, 스테이징, 프로덕션 등) 전용 리소스를 분류하는 데 자주 사용되는 키-값 쌍입니다. 소스 또는 대상 주소 개체 내에서 사용자 정의 태그를 사용하여 인스턴스, VPC/VNET, 서브넷, 보안 그룹 등의 리소스를 참조할 수 있습니다. 대개 조직에서는 태그를 사용하여 인스턴스를 분류합니다.

태그 기반 정책 규칙은 동적 클라우드 정책의 매우 강력한 구성 요소입니다. 특정 태그가 있는 인스턴스 그룹에 대해 세분화된 정책 규칙을 정의할 수 있습니다. 이러한 정책 규칙이 있으면 새 인스턴스가 적절한 태그를 사용하여 구축될 때마다, 새 인스턴스가 속한 인스턴스 범주에 대해 정의된 원하는 보안 정책을 자동으로 상속합니다. 이는 멀티 클라우드 방어 컨트롤러이(가) 새 인스턴스가 구축된 것을 검색할 뿐만 아니라 해당 인스턴스에 할당된 태그도 검색하기 때문입니다. 그런 다음 이 인스턴스 기반 태그를 참조하는 소스 또는 대상 주소 개체를 새 인스턴스의 IP 주소와 함께 동적으로 업데이트합니다. 잘못된 태그를 사용하여 인스턴스가 구축되었거나 태그가 없는 경우 적절한 정책 규칙이 일치하지 않으므로 다른 리소스와 통신할 수 없습니다.

VNet 및 VPC에서 태그는 VPC와 연결된 CIDR을 주소 개체 CIDR에 매핑합니다. VPC 또는 VNET 내에 구축된 인스턴스와 일치하는 규칙을 생성하는 상황에 맞는 방법을 제공합니다. 특정 VPC 또는 VNET과 연결된 CIDR을 수동으로 파악하는 대신 검색된 VPC 또는 VNET의 이름을 사용하여 일치 기준을 정의할 수 있습니다. VPC 또는 VNET에 대한 변경 사항은 개입 없이 정책 규칙에서 동적으로 업데이트됩니다. VPC 또는 VNET이 제거되고 새 VPC/VNET이 생성되는 경우, CIDR을 재사용하더라도 규칙이 더 이상 적용되지 않습니다.

인스턴스 ID

인스턴스 ID는 인스턴스와 연결된 IP 주소를 주소 개체 내의 IP 주소 목록에 매핑합니다. 이를 통해 인스턴스의 구성 방식을 수동으로 파악하지 않고도 특정 인스턴스에 대한 정책 규칙을 상황에 따라 생성할 수 있습니다. 정책 규칙은 인스턴스 변경 사항 또는 제거 사항을 반영합니다. 인스턴스를 삭제하고 동일한 구성의 새 인스턴스로 교체하더라도, 정책 규칙은 다른 인스턴스에 적용할 수 없습니다.

보안 그룹

보안 그룹은 보안 그룹과 연결된 네트워크 인터페이스의 IP 주소를 주소 개체 내의 IP 주소 목록에 매핑합니다. 모든 인터페이스 관련 변경 사항(예: 보안 그룹에 추가 또는 제거된 필드)은 주소 개체 내의 IP 주소 목록에 동적으로 반영됩니다. 이를 통해 조직은 기존 보안 그룹을 게이트웨이 데이터 경로 파이프라인의 고급 보안 기능에 조정할 수 있습니다.

서브넷 ID

서브넷 ID는 서브넷과 연결된 CIDR을 주소 개체 CIDR에 매핑합니다. 이를 통해 서브넷의 구성 방식을 수동으로 파악하지 않고도 특정 서브넷 ID와 연결된 모든 리소스에 대한 정책 규칙을 상황에 따라 생성할 수 있습니다. VPC 또는 VNET은 일반적으로 여러 서브넷으로 구분되며 이러한 서브넷 내에 구축된 리소스는 다양한 용도로 사용될 수 있습니다. 예를 들어, 서브넷의 인스턴스에 특정 고급 보안 프로파일 집합이 필요하거나 트래픽 흐름 요구 사항이 다를 수 있습니다. 각 서브넷에 대해 서로 다른 보안 규칙을 생성하는 프로세스를 간소화하기 위해 멀티 클라우드 방어을(를) 사용하면 서브넷의 이름을 일치 기준으로 사용하여 정책 규칙을 정의할 수 있습니다. 따라서 각 서브넷은 고유한 보

안 프로파일을 가진 고유한 정책 규칙을 가질 수 있습니다. 서브넷 및 서브넷 내에 구축된 인스턴스에 대한 변경 사항은 정책 규칙에 동적으로 반영됩니다.

지역 IP

지역 IP 주소 개체는 지역 IP 국가 이름 집합으로 구성됩니다. 이러한 개체는 지리적 위치(국가)를 기준으로 IP 주소에서 들어오거나 IP 주소로 나가는 트래픽을 허용하거나 차단하는 데 사용됩니다. 멀티 클라우드 방어은(는) 업데이트된 GeoIP 목록을 유지하기 위해 MaxMind GeoIP2 데이터베이스와 통합됩니다.

국가 이름과 코드의 전체 목록 또는 IP 주소에서 GeoIP 국가 코드에 이르는 IP 주소를 검토하려면 GeoName 웹사이트로 이동하십시오.

그룹

그룹 주소 개체는 소스 또는 대상 주소 개체의 집합으로 구성됩니다. 그룹은 개별 주소 개체를 정의한 다음 함께 그룹화하여 유연성을 제공하며, 그룹의 멤버에 따라 트래픽을 일치시키는 데 필요한 규칙 수를 간소화합니다. 그룹은 멤버가 고정, 동적 또는 이 둘의 조합인지 여부에 상관없이 그룹 멤버로부터 IP, CIDR 또는 FQDN 집합을 상속합니다.

소스 또는 대상 주소 개체 매개변수

유형	모드: 동적 또는 정적	매개변수	필수 또는 선택	참고
IP/CIDR/FQDN	고정	값	필수	주소 개체당 총 FQDN의 수는 200으로 제한되며, 각 FQDN은 최대 400개의 IP로 확인할 수 있습니다. 멀티 클라우드 방어 게이트웨이에서는 DNS 레코드 TTL에 관계없이 60초마다 DNS 확인을 수행합니다.
VPC/VNet ID	동적	CSP 계정	필수	
		지역	필수	
		리소스 그룹	선택 사항	Azure 전용
		VPC/VNet ID	필수	

유형	모드: 동적 또는 정적	매개변수	필수 또는 선택	참고
보안 그룹	동적	CSP 계정	필수	
		지역	필수	
		VPC/VNet ID	필수	
		리소스 그룹	선택 사항	Azure 전용
		보안 그룹 ID	필수	
애플리케이션 보안 그룹	동적	CSP 계정	필수	Azure 전용
		지역	필수	
		리소스 그룹	필수	
		애플리케이션 보안 그룹	필수	
인스턴스 ID	동적	CSP 계정	필수	
		지역	필수	
		VPC/VNet ID	필수	
		리소스 그룹	선택 사항	선택 사항
		인스턴스 ID	필수	
서브넷 ID	동적	CSP 계정	필수	
		지역	필수	
		VPC/VNet ID	필수	
		리소스 그룹	선택 사항	Azure 전용
		서브넷 ID	필수	

유형	모드: 동적 또는 정적	매개변수	필수 또는 선택	참고
사용자 정의 태그	동적	CSP 계정	선택 사항	
		지역	선택 사항	
		VPC/VNet ID	선택 사항	
		리소스 그룹	선택 사항	Azure 전용
		리소스/태그/값	필수	리소스 및 태그 키-값 쌍의 목록입니다. 리소스는 인스턴스, VPC/VNet, 서브넷, 로드 밸런서, 보안 그룹, 보안 그룹(Azure)일 수 있습니다.
지역 IP		값	필수	
그룹		주소	필수	

역방향 프록시 대상 주소 개체

역방향 프록시 대상 주소 개체는 역방향 프록시 서비스 개체에 백엔드 대상 주소로 지정됩니다. 서비스 개체에서 애플리케이션에 백엔드 연결을 설정하는 데 사용됩니다. 애플리케이션은 IP 또는 FQDN 형식의 하나 이상의 애플리케이션 로드 밸런서 또는 인스턴스 주소일 수 있습니다. 다양한 유형의 역방향 프록시 대상 주소 개체는 다음과 같이 정의됩니다.

정적 **IP/FQDN** 주소 개체

IP/FQDN 주소 개체는 IP 주소 또는 FQDN의 집합으로 구성됩니다. 둘 이상의 IP 또는 FQDN이 구성된 경우 게이트웨이는 백엔드 연결을 설정할 때 구성된 필드 중 우선순위 없이 주소를 처리합니다. FQDN이 구성되면 게이트웨이에서는 DNS를 통해 FQDN을 확인하여 백엔드 연결을 설정할 때 사용할 IP 주소를 결정합니다.

동적 애플리케이션 주소 개체

애플리케이션 주소 개체는 애플리케이션 태그에 의해 결정되는 개별 애플리케이션 로드 밸런서 클라우드 리소스로 구성됩니다. 구성은 멀티 클라우드 방어 실시간 재고 목록 검색을 사용하여 클라우드 계정에서 가져온 클라우드 리소스로 표시되는 IP 또는 FQDN을 동적으로 채웁니다. 클라우드 리소스에 대한 모든 변경 사항은 주소 개체에 자동으로 반영됩니다. 구성으로 인해 IP 또는 FQDN이 두 개 이상 생성되면 게이트웨이는 백엔드 연결을 설정할 때 설정된 필드 중 우선 순위가 없는 필드를 처리합니다. 구성 결과가 FQDN인 경우 게이트웨이는 DNS를 통해 FQDN을 확인하여 백엔드 연결을 설정할 때 사용할 IP 주소를 결정합니다.

역방향 프록시 대상 주소 개체 매개변수

유형	모드: 동적 또는 정적	매개변수	필수 또는 선택	참고
IP/FQDN	고정	값	필수	
애플리케이션	동적	CSP 계정	필수	
		지역	필수	
		VPC/VNet ID	필수	
		리소스 그룹	선택 사항	Azure 전용
		태그/값	필수	단일 태그 키-값 쌍

시스템 개체

멀티 클라우드 방어은(는) 정책 생성을 간소화하기 위해 사전 정의된 주소 개체 목록을 제공합니다. 모든 시스템 개체는 편집하거나 삭제할 수 없습니다. 사용자는 수정이 필요한 경우 시스템 개체를 복제하도록 선택할 수 있습니다.

이름	설명
모두	전체 IPv4 주소 공간을 나타냅니다.
any-private-rfc-1918	RFC-1918에 정의된 모든 IPv4 전용 주소를 나타냅니다.
인터넷	전체 IPv4 공용 주소 공간에서 프라이빗 IPv4 주소(RFC1918)를 뺀 것을 나타냅니다.

주소 개체 생성

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Addresses(**주소**)**로 이동합니다.

단계 **2** **Create(**생성**)**를 클릭합니다.

단계 **3** **Src/Dest(**소스/대상**)** 또는 **Reverse Proxy Target(**역방향 프록시 대상**)**을 선택합니다.

단계 **4** 주소 개체를 식별하기 위한 고유한 이름을 입력합니다.

단계 **5** (선택 사항) 개체의 설명을 입력합니다. 이 명령은 개체를 다른 개체와 구분하는 데 도움이 되는 컨텍스트를 제공할 수 있습니다.

단계 **6** 개체 유형 선택 개체 유형과 개체 유형에 대한 자세한 내용은 주소 개체, on page 1의 내용을 참조하십시오. 다음 유형 중 하나를 선택합니다.

- IP/CIDR/FQDN
- VPC/VNet ID
- 보안 그룹
- 애플리케이션 ID(Azure만 해당)
- 인스턴스 ID
- 서브넷 ID
- 사용자 정의 태그
- 지역 IP
- 서비스 엔드포인트(클라우드 서비스 IP)

단계 **7** 6단계에서 선택한 유형에 따라 다음 매개 변수를 입력합니다.

- **Value(**값**)** - 유효한 IP, CIDR 또는 FQDN IP 주소를 입력합니다.
- **CSP Account(CSP** 계정**)** - 드롭다운 메뉴를 사용하여 컨트롤러에 이미 연결된 클라우드 서비스 제공자 계정을 선택합니다.
- **Region(**지역**)** - 클라우드 서비스 제공자가 위치한 지역을 선택합니다.
- **VPC** - 드롭다운 메뉴를 사용하여 VPC 또는 VNet을 선택합니다. 선택하는 클라우드 서비스 제공자 계정에 따라 사용 가능한 옵션이 달라질 수 있습니다.
- **Subnet(**서브넷**)** - 드롭다운 메뉴를 사용하여 VPC 또는 VNet에 적용할 서브넷을 선택합니다.
- (Azure 전용) **Resource Group(**리소스 그룹**)** - 드롭다운 메뉴를 사용하여 선택 항목과 호환되는 리소스 그룹을 선택합니다.
  - **Resource Level(**리소스 레벨**)** - 드롭다운 메뉴를 사용하여 값을 선택합니다.
  - **Resource Tag(**리소스 태그**)** - 드롭다운 메뉴를 사용하여 키워드를 리소스 태그로 선택합니다.
  - **Value(**값**)** - 리소스 그룹에 대한 유효한 값을 입력합니다. 이는 IP/CIDR/FQDN 개체에 필요한 값 항목과는 다릅니다.
- **Geo IP(**지역 **IP)** - 드롭다운 메뉴를 사용하여 선택한 지리위치와 연결된 특정 IP를 선택합니다.
- **X-Forwarded-For Match Enabled(X-Forwarded-For** 일치 활성화**)** - 게이트웨이를 XFF HTTP 헤더 필드와 일치시킬 수 있게 하려면 이 확인란을 선택합니다.

단계 **8** 완료되면 **Save(**저장**)**를 클릭하십시오.

주소 개체 편집

수정할 수 없는 매개변수를 수정할 경우 주소 개체를 주소 개체 복제한 다음 매개변수를 원하는 대로 변경해야 합니다.

주소 개체를 편집하려면 다음 단계를 수행합니다. 모든 매개변수를 편집할 수 있는 것은 아닙니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Addresses(**주소**)**로 이동합니다.
단계 **2** 편집할 주소 개체 옆의 확인란을 선택합니다.
단계 **3** **Edit(**편집**)**를 클릭합니다.
단계 **4** 필요에 따라 매개변수를 수정합니다.
단계 **5** 완료되면 **Save(**저장**)**를 클릭하십시오.

주소 개체 복제

원본 대신 복제본을 사용하려는 경우 원본의 모든 연결을 복제본과 교체해야 합니다. 연결은 하나 이상의 보안 정책 규칙 집합 규칙 또는 역방향 프록시 서비스 개체의 집합에 포함됩니다. 세부사항 보기를 확인하여 연결을 확인할 수 있습니다.

기존 주소 개체를 복제하려면 다음 단계를 수행합니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Addresses(**주소**)**로 이동합니다.
단계 **2** 복제할 주소 개체 옆의 확인란을 선택합니다.
단계 **3** **Clone(**복제**)**를 클릭합니다.
단계 **4** 매개변수를 지정하고 원하는 대로 수정합니다.
단계 **5** 완료되면 **Save(**저장**)**를 클릭하십시오.

주소 개체 삭제

주소 개체가 정책 규칙 집합 규칙 또는 역방향 프록시 서비스 개체에서 활발하게 사용되는 경우, 주소 개체가 하나 더 연결되게 되며 주소 개체를 삭제할 수 없습니다. 주소 개체를 삭제하려면 먼저 모든 연결을 제거해야 합니다. 그러면 주소 개체를 삭제할 수 있습니다. 세부사항 보기를 확인하여 연결을 확인할 수 있습니다.

단계 **1** **Manage(**관리**)** > **Security Policies(**보안 정책**)** > **Addresses(**주소**)**로 이동합니다.
단계 **2** 삭제할 주소 개체 옆의 확인란을 선택합니다.

단계 **3** **Delete(**삭제**)**를 클릭합니다.

단계 **4** **Save(**저장**)**를 클릭하여 삭제를 확인합니다.

세부사항 보기

Manage(관리**)** > **Security(**보안**)** > **Addresses(**주소**)** 페이지에서 개체의 **Name(**이름**)**을 클릭하여 주소 개체 **Details(**세부 정보**)**를 볼 수 있습니다. **Details(**세부 정보**)**에는 해당 유형 및 구성에 따라 채워진 IP, CDIR 및 FQDN이 표시됩니다. 또한 정책 규칙 집합 및 모든 개체 서비스와의 연결도 표시됩니다.