# VMware NSX Cloud

## 퍼블릭 클라우드에서 기본적으로 실행되는 애플리케이션에 대한 일관된 네트워킹 및 보안

### 요약 정보

VMware NSX® Cloud는 퍼블릭 클라우드에서 기본적으로 실행되는 애플리케이션에 일관된 네트워킹과 보안을 제공합니다. NSX Cloud는 NSX Data Center와 동일한 관리 플레인 및 컨트롤 플레인을 사용하므로 프라이빗 데이터 센터에서 퍼블릭 클라우드까지 단일 네트워크 및 보안 솔루션을 사용할 수 있습니다.

### 주요 이점

AWS 및 Azure와 같은 퍼블릭 클라우드 전반에서 일관된 네트워킹 및 보안을 제공하여 낮은 운영 비용으로 확장성, 제어 및 가시성을 크게 향상시킵니다.

- 가상 네트워크, 가용성 영역, 지역 및 퍼블릭 클라우드 전반에서 간단하게 확장 가능합니다.
- 보안 및 네트워킹 서비스를 정밀하게 제어하여 애플리케이션을 보호하고 표준화합니다.
- 네트워킹 및 보안에 대한 완벽한 가시성을 통해 퍼블릭 클라우드에서 애플리케이션의 상태 및 규정 준수를 보장합니다.

### 가격 책정

- 1년 및 3년 라이센스로 제공되는 서브스크립션 기반 가격 책정
- 가상 네트워크(예: AWS VPC, Azure VNet)의 수에 관계없이 퍼블릭 클라우드 내에서 가동 중인 워크로드에서 사용하는 vCPU 기반
- 클라우드 전용 사용 사례에는 NSX Data Center 라이센스가 필요하지 않음

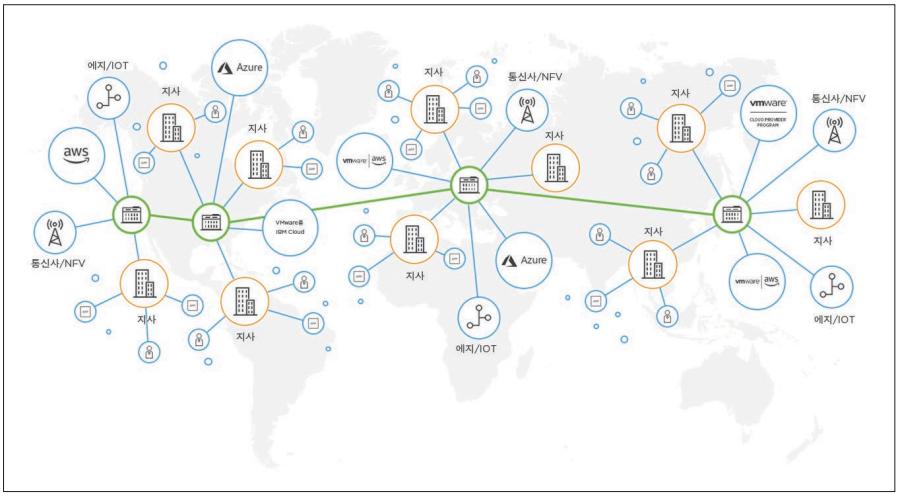


그림 1: 가상 클라우드 네트워크

## 클라우드 원칙에 맞게 구축된 네트워크

VMware NSX Cloud는 퍼블릭 클라우드에서 기본적으로 실행되는 애플리케이션에 일관된 네트워킹과 보안을 제공합니다. VMware NSX Cloud를 VMware NSX 제품군과 함께 사용하면 데이터 센터, 클라우드, Endpoint, IoT(사물 인터넷) 전반으로 확장 가능한 네트워킹에 대한 소프트웨어 정의 접근 방식인 가상 클라우드 네트워크를 구현할 수 있습니다.

## 사용 사례

### 클라우드 간 일관된 보안

NSX Cloud는 여러 퍼블릭 클라우드 전반에서 실행되는 워크로드에 대한 정책을 지원합니다. NSX Cloud는 NSX Data Center와 동일한 컨트롤 플레인 및 데이터 플레인을 활용하므로 데이터 센터와 클라우드 전반에서 포괄적인 정책 관리가 가능합니다. 정책은 한 번 정의하면 클라우드 가상 네트워크, 지역, 가용성 영역 및 멀티 클라우드 공급업체 전반에서 어디에든 워크로드를 적용할 수 있습니다. 보안 정책은 애플리케이션 특성 및 사용자 정의 태그에 따라 각 워크로드에 동적으로 적용됩니다. 악성 워크로드나 손상된 워크로드에 적절한 마이크로 세분화 보안 정책이 적용되지 않은 경우 자동으로 차단할 수도 있습니다.

### 정밀한 클라우드 네트워킹 제어

VMware NSX Cloud는 Amazon(AWS) 및 Microsoft Azure와 같은 기본 퍼블릭 클라우드에 맞게 설계되었습니다. NSX Cloud는 이러한 퍼블릭 클라우드 공급업체가 지원하는 기본 서비스를 보완합니다. NSX Cloud를 통해 계속해서 워크로드에 대한 퍼블릭 클라우드 공급업체의 인프라와 애플리케이션 서비스를 제한 없이 사용할 수 있습니다(예: AWS ELB/Azure Load Balancer, AWS Route53/Azure DNS, AWS Direct Connect/Azure ExpressRoute, Amazon RDS/Azure Database). 기존 자동화 툴을 사용하여 REST API 요청을 통해 프로비저닝 및 구성 관리를 자동화할 수 있습니다.

**VMWARE 제품에 대한 자세한 내용 또는 구입 방법**

**문의**

vmware_kr@vmware.com

**웹 사이트 방문**

www.vmware.com/kr/products/nsx-cloud.html 또는 http://www.vmware.com/kr/products를 방문하여 온라인으로 공인 파트너사를 검색하십시오.

## 종합적인 운영 제어 및 가시성

VMware NSX Cloud는 클라우드 네트워크에서 네트워크 및 보안 데이터에 액세스할 수 있도록 표준 인터페이스 및 프로토콜을 제공합니다. 흐름, 패킷 및 이벤트 정보는 IPFIX, Traceflow, 포트 미러링 및 Syslog를 통해 제공됩니다. 이 데이터는 기존 사내 운영 툴에서 사용할 수 있으며 모니터링, 문제 해결 및 감사를 위한 심도 있고 완벽한 가시성을 제공하는 데 사용할 수 있습니다. 풍부한 운영 데이터로 애플리케이션의 사내 배포와 퍼블릭 클라우드 배포를 비롯한 전체 하이브리드 클라우드 배포 전반에서 네트워크 연결, 성능 및 보안 문제를 파악하고 해결하는 시간을 크게 단축할 수 있습니다.

## 주요 기능

**멀티 클라우드, 다중 사이트 네트워킹 및 보안:** NSX Cloud는 멀티 클라우드 전반의 Endpoint에 네트워킹 및 보안 기능을 제공할 뿐만 아니라 NSX Data Center와 통합하여 클라우드 및 데이터 센터 사이트 전반에서 네트워킹 및 보안 관리를 지원합니다.

**마이크로 세분화:** 퍼블릭 클라우드에서 기본적으로 실행되는 애플리케이션 워크로드 간 횡방향 트래픽을 제어합니다.

**보안 그룹:** 인스턴스 이름, OS 유형, AMI ID 및 사용자 정의 태그와 같은 풍부한 정책 구조를 기반으로 보안 그룹 및 규칙을 정의할 수 있습니다.

**동적 정책:** 보안 정책이 인스턴스 특성 및 사용자 정의 태그를 기반으로 자동으로 적용됩니다. 인스턴스를 클라우드 내 또는 클라우드 간에 이동할 때 정책이 이를 자동으로 따릅니다.

**인스턴스 차단:** 마이크로 세분화 보안 없이 퍼블릭 클라우드 내에서 실행되는 악성 및 손상된 워크로드를 차단합니다. 차단된 인스턴스는 클라우드 네트워크와 통신할 수 없습니다.

**분산 아키텍처:** NSX Cloud의 분산형 방화벽 아키텍처를 사용하면 외부 방화벽을 거치지 않고 각 인스턴스의 가상 네트워크 인터페이스에 정책이 적용되기 때문에 추가 네트워크 홉 및 트래픽이 필요 없습니다.

**Edge 방화벽:** NSX Cloud는 가상 네트워크 및 퍼블릭 인터넷의 인스턴스 간 종방향 트래픽 흐름을 필터링하는 상태 저장 방화벽을 제공합니다.

**RESTful API:** RESTful API 및 자동화 툴은 프로그래밍 방식으로 네트워킹 및 보안 인프라를 온디맨드로 프로비저닝 및 구성합니다.

**템플릿화:** 기존 자동화 및 조정 툴을 사용하여 표준화된 애플리케이션 템플릿을 생성하고 퍼블릭 클라우드 전반의 네트워킹 및 보안 서비스 프로비저닝 및 관리를 간소화합니다.

**횡방향 트래픽 가시성:** VPC 내 및 전반의 횡방향 트래픽에 대한 가시성을 확보하기 위해 기존 2일 차 운영 툴을 사용합니다.

**보안 로깅:** 허가/거부 및 차단 인시던트와 같은 보안 이벤트에 대한 실시간 가시성을 제공하며 이를 감사합니다. Syslog 또는 SIEM 서버에 보안 이벤트 정보를 전송합니다.

**VMware, Inc.** 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
서울시 강남구 영동대로 517 아셈타워 13층 (우) 06164 e-메일: vmware_kr@vmware.com

Item No: 149451wf-vmw-q2fy19-sddc-launch-ds-nsx-cld-a4 6/18