# Cisco ASA 1000V 클라우드 방화벽

## 제품 개요

Cisco® ASA 1000V 클라우드 방화벽은 이미 입증된 Adaptive Security Appliance 보안 플랫폼의 확장으로 멀티 테넌트 사설 및 공용 클라우드 배포 테넌트 에지에 일관성 있는 보호를 제공합니다. Cisco VSG(가상 보안 게이트웨이)의 구역 기반 보안 기능을 보완하는 Cisco ASA 1000V 클라우드 방화벽은 멀티 테넌트 에지 보안과 기본 게이트웨이 기능, 네트워크 기반 공격 보호 기능을 포괄적인 클라우드 보안 솔루션을 통해 제공합니다. Cisco ASA 1000V 클라우드 방화벽은 Cisco Nexus® 1000V Series Switch 와의 통합을 통해 멀티 하이퍼바이저 지원 가능 솔루션 및 단일 ASA 1000V 인스턴스 활성화를 통한 멀티 ESX 호스트 보호를 제공합니다. 이에 따른 결과는 탁월한 배포 유연성 및 간소화된 관리로 나타납니다. Cisco VNMC(Virtual Network Management Center)는 다이내믹하면서도 정책 기반의 멀티 테넌트 관리를 운영을 가능하게 합니다.

## 기능 및 이점

Cisco ASA 1000V 클라우드 방화벽은 가상 환경에 맞게 최적화된 주류 ASA 보안 기술을 사용합니다. Cisco Nexus 1000V, VSG 및 VNMC 구성 요소와 투명하게 통합되며 물리적 ASA 어플라이언스와 함께 하이브리드(물리, 가상, 클라우드) 인프라를 위한 엔드 투 엔드 보안을 제공합니다. 기능 및 이점은 표 1 에 자세히 설명되어 있습니다.

**표 1.** Cisco ASA 1000V 클라우드 방화벽 기능 및 이점

| 기능 | 이점 |
|---|---|
| **사설 및 공용 클라우드 보호를 위한 입증된 방화벽** | • 입증된 ASA 기능의 확장을 통해 에지에서 멀티 테넌트 가상 및 클라우드 인프라를 보호<br>• 클라우드 주변 네트워크 기반 공격으로부터 보호<br>• 물리, 가상, 클라우드의 하이브리드 인프라 전체에서 일관된 기능 지원<br>• 널리 배포된 보안 연결 솔루션을 사용해 IT 인프라의 안정적인 클라우드로의 확장 및 미션 크리티컬 워크로드의 배치된 위치 간 손상 없이 전송 |
| **솔루션 유연성 및 운영 효율성 향상** | • 단일 ASA 1000V 인스턴스를 다중 ESX 호스트로 확장하기 위한 고유 기능과 함께 배포 유연성 및 더욱 단순한 관리 기능 제공<br>• 일관성 및 유연성을 위한 멀티 하이퍼바이저 가능 솔루션 활성화<br>• VXLAN 게이트웨이 기능을 통한 향상된 확장성<br>• 템플릿화된 에지 프로필에 구성된 보안 정책으로 높아진 효율성 및 간소화된 관리<br>• 다음과 같은 옵션을 통해 운영 효율성을 상승: 기존의 물리적 클라우드와 확장 클라우드 인프라 간의 일관된 주소 공간 지원 또는 클라우드 인프라 내의 여러 테넌트 사이 일관된 주소 공간 지원<br>• 가상 시스템에 빠른 속도로 IP 주소 자동 프로비저닝을 통해 완벽하게 작동하는 가상 시스템 배포에 걸리는 전체 시간 단축<br>• 타사 관리 및 조정 툴과의 통합을 지원하는 XML API 를 통해 관리 유연성 상승 |
| **새로운 가상화 워크플로에 대한 포괄적인 접근 방식** | • 클라우드 환경의 엔드 투 엔드 보안을 위해 고급 클라우드, 클라우드 레디 관리자, 투명하면서도 확장 가능한, 멀티 테넌트가 가능한 정책 기반 솔루션 제공<br>• 네트워크, 서버 및 보안 관리자를 위한 역할별 관리 인터페이스를 통해 협업 거버넌스를 보장 |

## 동적 가상화 인식 운영

가상화는 자주 반복되는 가상 시스템의 추가, 삭제 및 변경 작업으로 인해 매우 다이내믹해 질 수 있습니다. 수동 또는 프로그래밍된 VMware vMotion 이벤트를 통해 가상 시스템의 라이브 마이그레이션이 발생합니다. Cisco ASA 1000V 클라우드 방화벽은 Cisco Nexus 1000V Series(및 vPath)와 함께 작동하여 다이내믹 가상화를 지원하며 Cisco VNMC 와 함께 작동을 통해 각 LOB 또는 테넌트 에지 프로필을 생성합니다. 보안 프로필은 Cisco Nexus 1000V Series VSM(Virtual Supervisor Module)에서 작성되고 VMware vCenter 에 발행되며 Cisco Nexus 1000V Series 포트 프로필에 바인딩됩니다. 새로운 가상 시스템이 인스턴스화되면 서버 관리자는 가상 시스템의 가상

이더넷 포트에 적절한 포트 프로필을 할당합니다. 포트와 에지 프로필은 인스턴스화된 가상 시스템에 즉시 적용됩니다. 가상 시스템의 용도 변경은 다른 포트 및 에지 프로필 할당을 통해 가능합니다.

VMware vMotion 이벤트는 물리적 서버 전체에서 가상 시스템의 이동을 트리거합니다. Cisco Nexus 1000V Series 는 포트 및 에지 프로필 모두 가상 시스템을 따르도록 보장합니다. 보안 시행 및 모니터링은 VMware vMotion 이벤트와 상관없이 그대로 유지됩니다.

## 솔루션 구성 요소

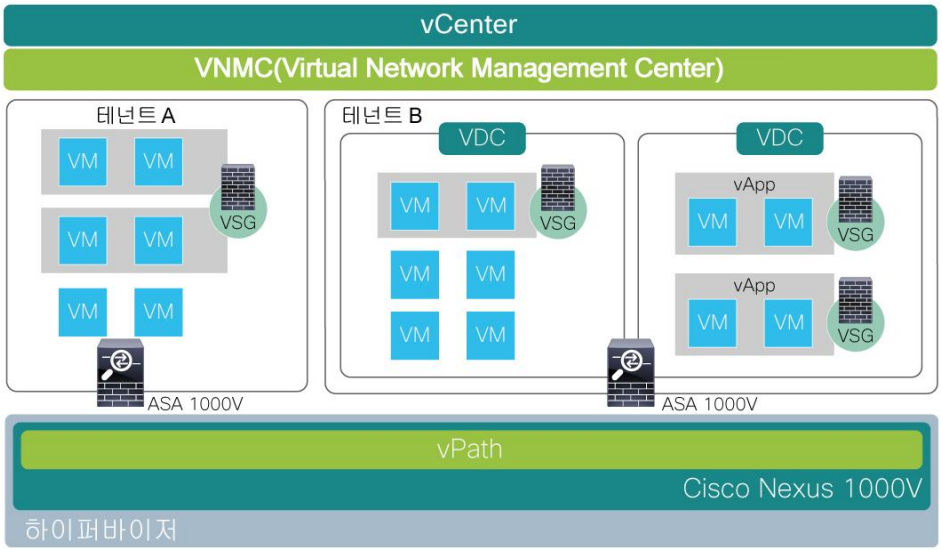
- **Nexus 1000V Series Switch 와 통합:** Cisco ASA 1000V 클라우드 방화벽은 효율적인 배포과 운영 간소화를 제공하기 위해 고급 네트워킹 개념을 적용하여 가상화된 환경을 보호합니다. VMware vSphere 하이퍼바이저의 Cisco Nexus 1000V Series 배포 가상 스위치와 함께 작동하는 Cisco ASA 1000V 클라우드 방화벽은 Nexus 1000V Series Switch 에 포함된 가상 네트워크 서비스 데이터 경로(vPath) 기술을 사용합니다.
  - **효율적인 배포:** 각 Cisco ASA 1000V 는 여러 물리적 서버에 보호 제공이 가능합니다. 물리적 서버당 하나의 가상 어플라이언스를 배포할 필요가 없습니다.
  - **독립적인 용량 계획:** Cisco ASA 1000V 는 보안 운영팀이 운영하는 전용 서버에 배치 될 수 있습니다. 이를 통해 컴퓨팅 용량이 애플리케이션 워크로드에 맞춰 적절히 할당될 수 있습니다. 또한 서버팀과 보안팀 간의 독립적인 용량 계획이 가능해지며, 보안, 네트워크 및 서버 팀에서 운영 분할을 유지할 수 있습니다.
  - **확장 가능한 클라우드 네트워킹:** Cisco ASA 1000V 는 VXLAN 과 기존 VLAN 간에 트래픽을 주고받기 위해 VXLAN 게이트웨이 역할을 합니다.
  - **서비스 체인:** vPath 는 다중 가상 네트워크 서비스를 단일 트래픽 흐름의 일부로 사용이 가능하도록 서비스 체인을 지원합니다. 예를 들어 vPath 는 네트워크 정책을 지정하는 것만으로 먼저 트래픽을 ASA 1000V 클라우드 방화벽으로 리디렉션한 뒤 테넌트 에지 보안을 제공합니다. 그리고 가상 보안 게이트웨이로 다시 리디렉션을 통해 구역 방화벽 기능을 제공할 수 있습니다.
- **Cisco VNMC 와 통합:** Cisco ASA 1000V 클라우드 방화벽은 중단 없는 관리 모델을 제공하기 위해 Cisco VNMC 를 사용해 관리됩니다.
  - 보안 관리자는 보안 프로필을 작성 및 관리하며 Cisco ASA 1000V 인스턴스를 관리할 수 있습니다. 보안 프로필은 Cisco Nexus 1000V Series 포트 프로필에서 참조됩니다.
  - 네트워크 관리자는 포트 프로필의 작성 및 관리와 Cisco Nexus 1000V Series 배포 가상 스위치를 관리할 수 있습니다. 포트 프로필은 Cisco Nexus 1000V Series VSM 의 프로그래밍된 인터페이스를 통해 VMware vCenter 에서 참조됩니다.
  - 서버 관리자는 가상 시스템을 인스턴스화할 때 VMware vCenter 에서 적절한 포트 프로필을 선택할 수 있습니다.

  또한 Cisco VSG 의 관리 및 프로비저닝 자동화를 위해 XML API 를 통해 타사 관리 및 조정 툴과 Cisco VNMC 가 프로그래밍 방식으로 상호작용할 수 있습니다.

  Cisco ASA 1000V 클라우드 방화벽은 Cisco ASDM(Adaptive Security Device Manager)에 의해 관리됩니다.
- **Cisco VSG 보완:** Cisco VSG 는 Cisco Nexus 1000V Series Switches 와 통합되어, 테넌트 내에서 세분화된 VM 간 구역 기반 보안을 제공합니다. Cisco ASA 1000V 클라우드 방화벽은 멀티 테넌트 에지 보안 및 기본 게이트웨이 기능을 제공하고 네트워크 기반 공격을 방지하기 위해 Cisco VSG 를 보완합니다.

그림 1 은 솔루션 구성 요소의 통합을 보여줍니다.

**그림 1.** Cisco ASA 1000V 클라우드 방화벽 솔루션 구성 요소




## 소프트웨어 패키지 및 설치

표 2 에서는 Cisco ASA 1000V 클라우드 방화벽을 구하는 방법에 대해 설명합니다.

**표 2.** 소프트웨어 패키지 및 설치

| 패키지 | 설명 |
|---|---|
| **OVF(개방형 가상화 형식)** | • 확장명이 .ova 인 단일 파일 형태의 다운로드 가능한 OVF 가상 어플라이언스<br>• OVF 템플릿/패키지와 함께 배포됨<br>• Cisco ASA 소프트웨어 릴리스 8.7 |

## 솔루션 구축 요구 사항

Cisco ASA 1000V 클라우드 방화벽을 사용하여 가상화된 클라우드 환경을 보호하려면 표 3 에 나열된 제품을 배포해야 합니다.

**표 3.** Cisco ASA 1000V 클라우드 방화벽 배포 요구 사항

| 제품 | 요구 사항 |
|---|---|
| **Cisco ASA 1000V 클라우드 방화벽** | **가상 어플라이언스로서의 Cisco ASA 1000V 클라우드 방화벽**<br>• 가상 CPU 1 개<br>• vRAM: 1.5GB<br>• vHard 디스크: 2.5GB<br>• 네트워크 데이터 인터페이스: 2 개<br>• 관리 인터페이스: 1 개<br>• 고가용성 인터페이스: 1 개 |
| **하이퍼바이저 및 하이퍼바이저 관리** | • VMware vSphere 4.1 이상 릴리스(VMware ESX 또는 ESXi 포함)<br>• VMware vCenter 4.1 이상 릴리스 |
| **분산된 가상 스위치** | Cisco Nexus 1000V Series Software Release 4.2(1)SV1(4) 이상, 가상 이더넷 모듈 포함(VMware vSphere ESX 또는 ESXi 하이퍼바이저에 포함됨) |
| **관리** | Cisco Virtual Network Management Center 릴리스 2.0 이상(가상 어플라이언스로서 배포) |

## 제품 성능 지침

표 4 에서는 Cisco ASA 1000V 클라우드 방화벽의 단일 인스턴스에 대한 성능 안내를 제공합니다. 테스트는 2.67GHz 와 이중 쿼드 코어의 Intel Xeon 프로세서 X5550(Nehalem)에서 실행되는 VMware ESX 4.1 호스트에서 수행했습니다. ASA 1000V 인스턴스에 vCPU 1 개, 1.5GB vRAM 및 2.5GB vHD 가 할당되었습니다.

**표 4.** Cisco ASA 1000V 클라우드 방화벽 성능 기능

| 기능 | Cisco ASA 1000V 클라우드 방화벽 |
|---|---|
| **최대 동시 세션 수** | 200,000 |
| **초당 최대 연결 수** | 10,000 |
| **VPN 처리량** | 200Mbps |
| **최대 VPN 터널 수** | 750 |

**참고：** ASA 1000V 의 성능 기능은 배포 시나리오, ASA 1000V 장치 구성, ASA 1000V 인스턴스에서 사용 가능한 리소스 및 트래픽 패턴에 따라 다릅니다. 계획 시 이러한 요소를 고려해야 합니다.

## 보증 정보

보증 정보는 Cisco.com 의 제품 보증 페이지에서 확인하십시오.

## 서비스 및 지원

Cisco 서비스는 고객의 네트워크 투자를 보호하고 네트워크 운영을 최적화하며 새로운 애플리케이션에 맞는 네트워크의 준비를 통해 네트워크 인텔리전스와 고객의 비즈니스 능력 강화에 기여합니다. Cisco 서비스는 네트워크의 계획, 배포 및 운영의 모든 부분을 지원하므로, 구현 시간을 단축하고 운영 비용을 줄이고 새로운 비즈니스 기회를 찾고 위험을 완화하고 성장을 가속화하는 데 도움이 됩니다. Cisco 보안 서비스는 공격 및 중단으로부터 조직을 보호하고, 개인정보를 보호하고, 규정 준수 제어를 지원하는 안전한 네트워크를 계획, 배포 및 운영하도록 지원할 수 있습니다. Cisco Security IntelliShield Alert Manager Service, Cisco SMARTnet® 및 Cisco Service Provider Base 는 서비스 라이프사이클의 "실행" 단계에 포함됩니다. 이러한 서비스는 기업 고객, 상용 고객 및 서비스 공급 고객에게 적합합니다.

Cisco Security IntelliShield Alert Manager Service 는 조직이 환경에 있는 잠재적 취약성에 대해 정확하고 믿을 수 있는 정보를 적시에 쉽게 액세스할 수 있도록 해주는 사용자 지정 가능한 웹 기반의 위협 및 취약성 경고 서비스를 제공합니다.

## 추가 정보

자세한 내용은 현지 고객 담당자에게 문의하거나 다음 웹 사이트를 참조하십시오.

- Cisco ASA 1000V 클라우드 방화벽: http://www.cisco.com/go/asa1000v
- Cisco Nexus 1000V Series Switch: http://www.cisco.com/go/nexus1000v
- Cisco 가상 보안 게이트웨이: http://www.cisco.com/go/vsg
- Cisco Virtual Network Management Center: http://www.cisco.com/go/vnmc
- Cisco ASA 5500 Series Adaptive Security Appliance: http://www.cisco.com/go/asa
- Cisco 보안 서비스: http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html

**미주 지역 본부**
Cisco Systems, Inc.
San Jose CA

**아시아 태평양 지역 본부**
Cisco Systems (USA) Pte. Ltd.
싱가포르

**유럽 지역 본부**
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.



인쇄지: 미국

C78-650053-05 08/12