



Datacenter Security Product Updates

Security Specialist

김용호 부장

2013. 1. 23

데이터 센터 보안 중점 사항

세그먼테이션

- 네트워크, 컴퓨팅 및 가상화에 대한 **경계 수립**
- 기능, 디바이스 및 조직별 차별화된 **보안정책 적용**
- 네트워크, 자원 및 응용프로그램에 대한 **접근 제어**

위협방어

- 내외부 공격 차단
- **보안 감시 영역** 선정 및 에지 경계 보호
- 접근 및 사용에 대한 **정보 통제**

가시성

- 자원 사용에 대한 **투명성** 제공
- 비즈니스 상황이 반영된 네트워크 **활동 모니터링**
- 운영 **간소화** 및 규정 준수 **리포팅**

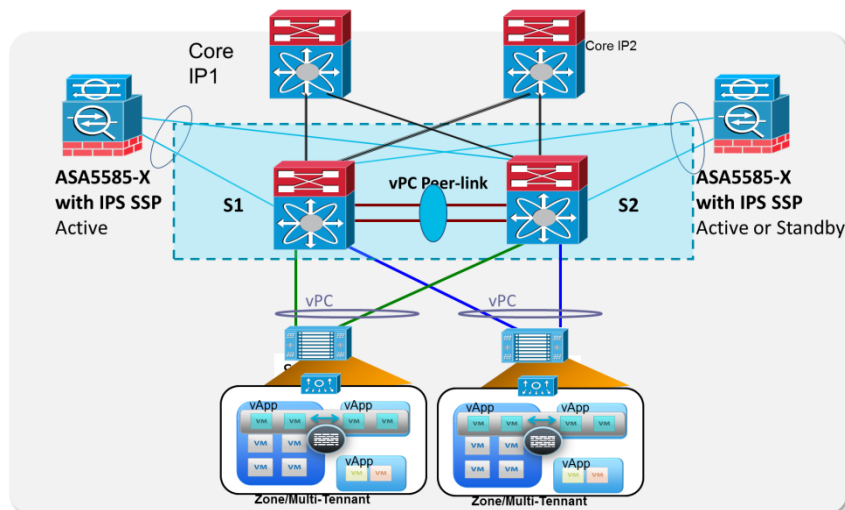
물리적 환경에서의 ASA 포지셔닝

데이터 센터 경계 방화벽/VPN 또는 IPS 기능 통합 수행

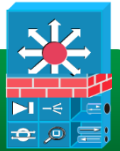
ASA5585-X



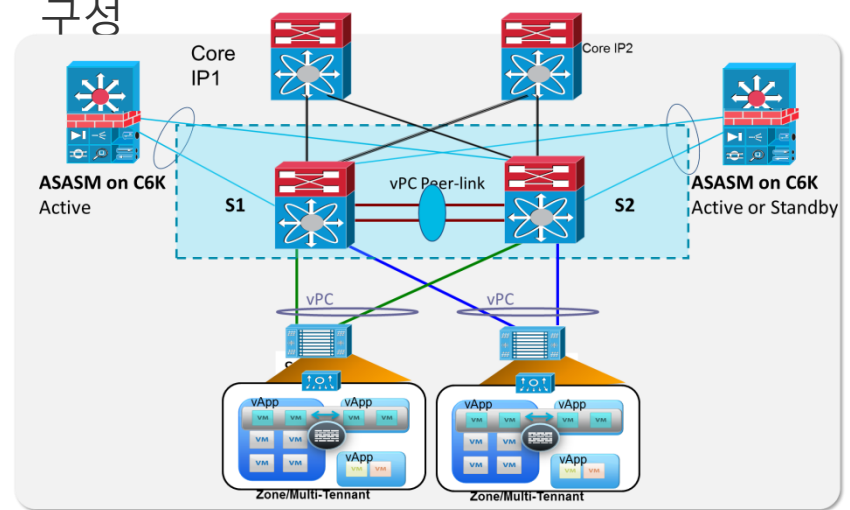
- ASA CX 또는 ASA IPS 모듈과 함께 배치
- 대용량 트래픽에 대한 클러스터링
- 데이터센터내 코어 또는 분산 영역의 보안 서비스 노드 구성



ASA Service Module



- IPS 4500 Series 또는 WSA와 함께 배치
- 주로 데이터 센터내의 분산 영역에 대한 보안 서비스 노드 구성
- 가상화 및 브랜치와 데이터센터간 VPN 망 구성



차세대 네트워크 보안을 위한 혁신

ASA S/W 9.0 및 9.1 버전 주요 업데이트

가상방화벽 기능 추가

- 다이나믹 라우팅 프로토콜 지원, OSPF, EIGRP
- IKEv2 기반 Site to Site IPSec VPN (IPSec 및 SSL 기반 Remote Access VPN 추후 지원 예정)
- L2 및 L3 혼합모드 다중 가상방화벽 지원

신규 시스코 클라우드 기반 웹 콘텐츠 보안 서비스 통합

IPv6 방화벽 및 VPN 기능 추가

- IPv4 및 IPv6 보안 정책 통합 관리 및 적용
- Network Address Translation (NAT) 66/64 및 DNS 64 지원
- Dynamic Host Configuration Protocol (DHCP) v.6 relay 지원
- Open Shortest Path First (OSPF) v.3 (dynamic routing for IPv6) 지원

신규 방화벽 클러스터링 기능

리모트 액세스 VPN 기능 추가

신규 방화벽 클러스터링 기능

최대 300Gbps 방화벽 또는 120Gbps 방화벽 + IPS 성능 제공

구성방식

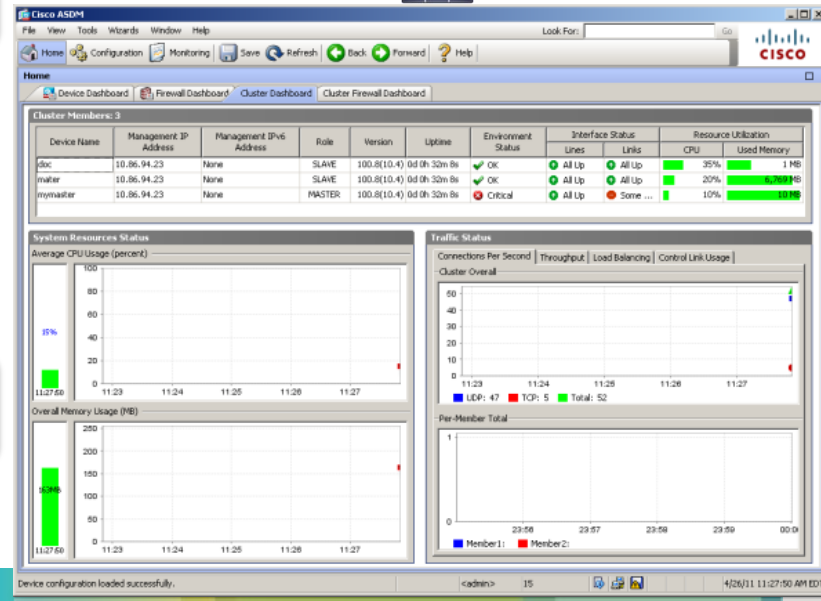
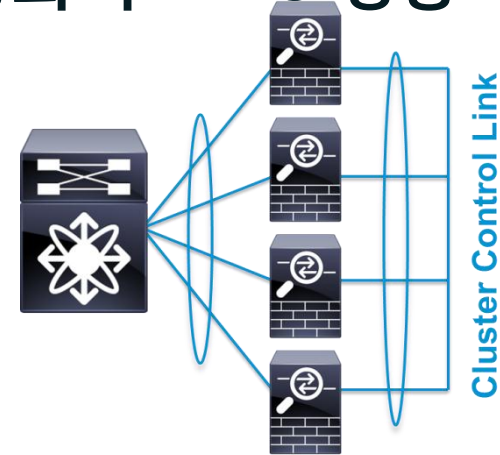
- ASA5585 8대 또는 8개의 방화벽 SSP까지 클러스터링 지원
- 일반적인 스위치 및 라우터를 이용한 로드밸런싱
- ECLB(Ether Channel Load Balancing), ECMP(Equal Cost Multi-Path) 또는 시스코 PBR(Policy Based Routing)을 이용

동작방식

- 시스코에서 개발된 ASA의 Cluster Control Protocol를 이용하여 상태 정보 및 커넥션 정보 공유
- 시스코 VSS 및 VPC 환경 지원
- 클러스터링 구성 멤버간고가용성 지원, 서비스 무중단 업그레이드 지원

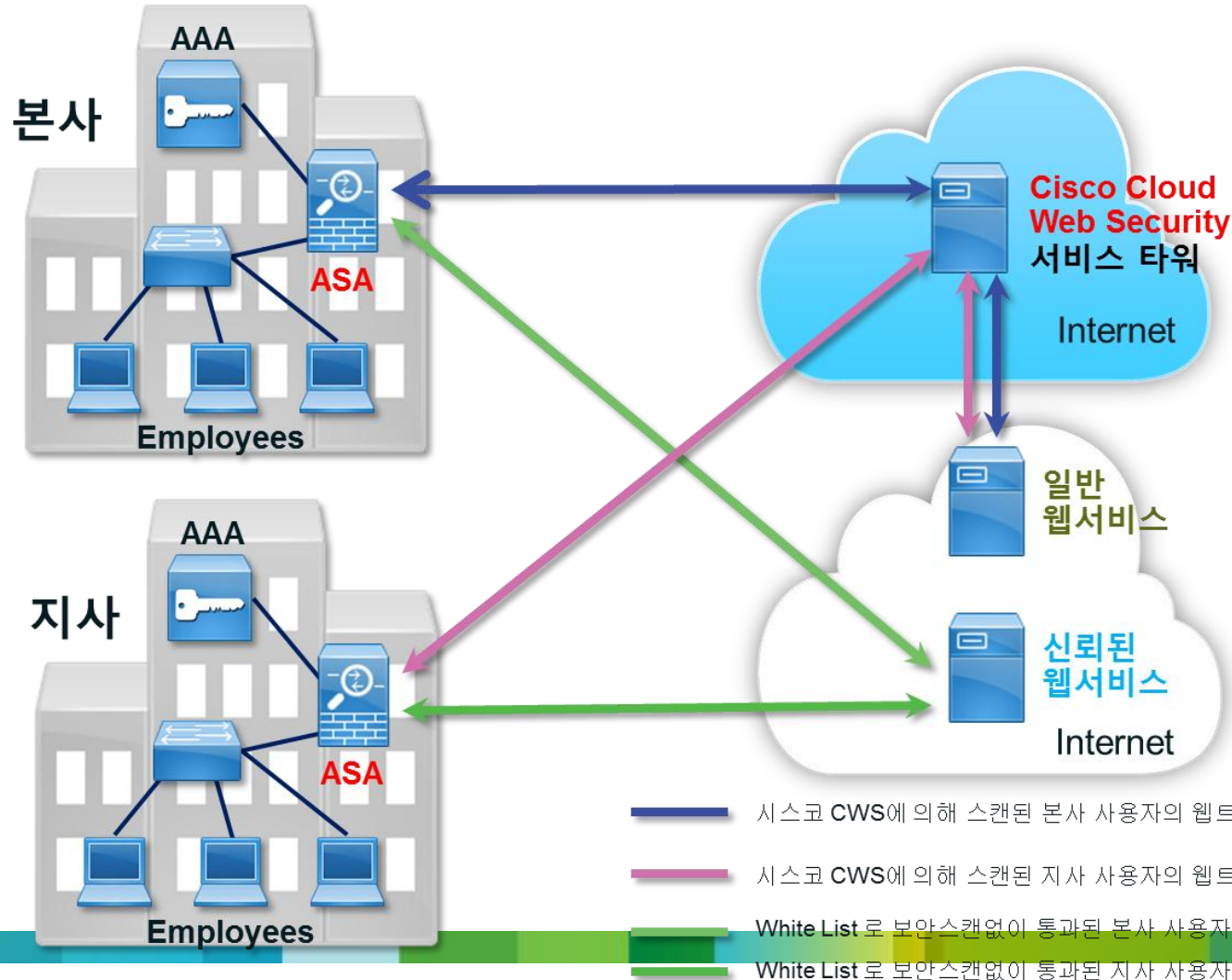
관리방식

- One Management 로 단일 방화벽처럼 정책관리 및 모니터링



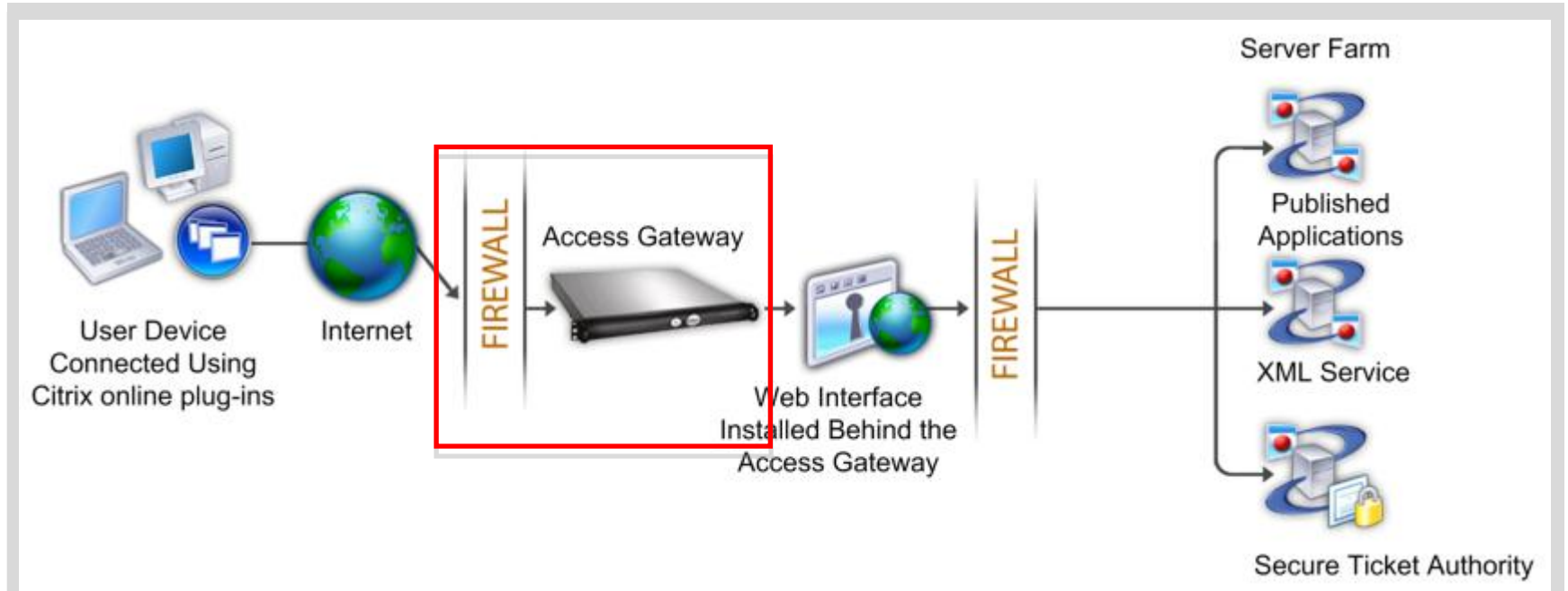
신규 시스코 클라우드 기반 웹 콘텐츠 보안 서비스 통합

사용자 설정 없이 간편한 웹 콘텐츠 보안 정책 적용



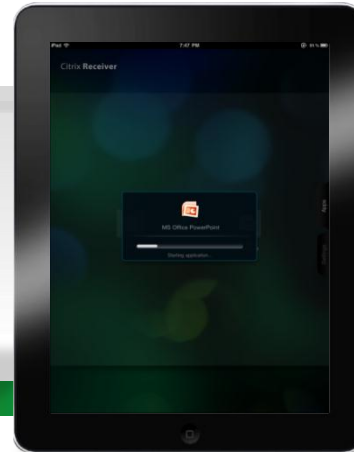
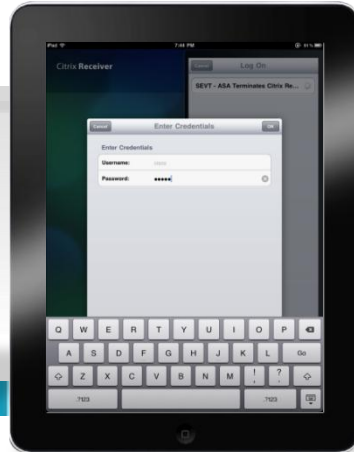
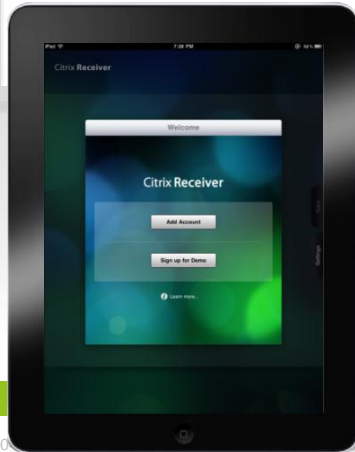
리모트 액세스 VPN 기능 추가

시트릭스 모바일 리시버 대체 ASA Clientless VPN으로 간소화된 보안 VDI 접속



리모트 액세스 VPN 기능 추가

시트릭스 모바일 리시버 대체 ASA Clientless VPN으로 간소화된 보안 VDI 접속



가상화 환경에서의 ASA 포지셔닝

가상 데이터센터 또는 VDI 환경을 위한 방화벽/VPN 기능 수행

ASA 1000v 클라우드 방화벽

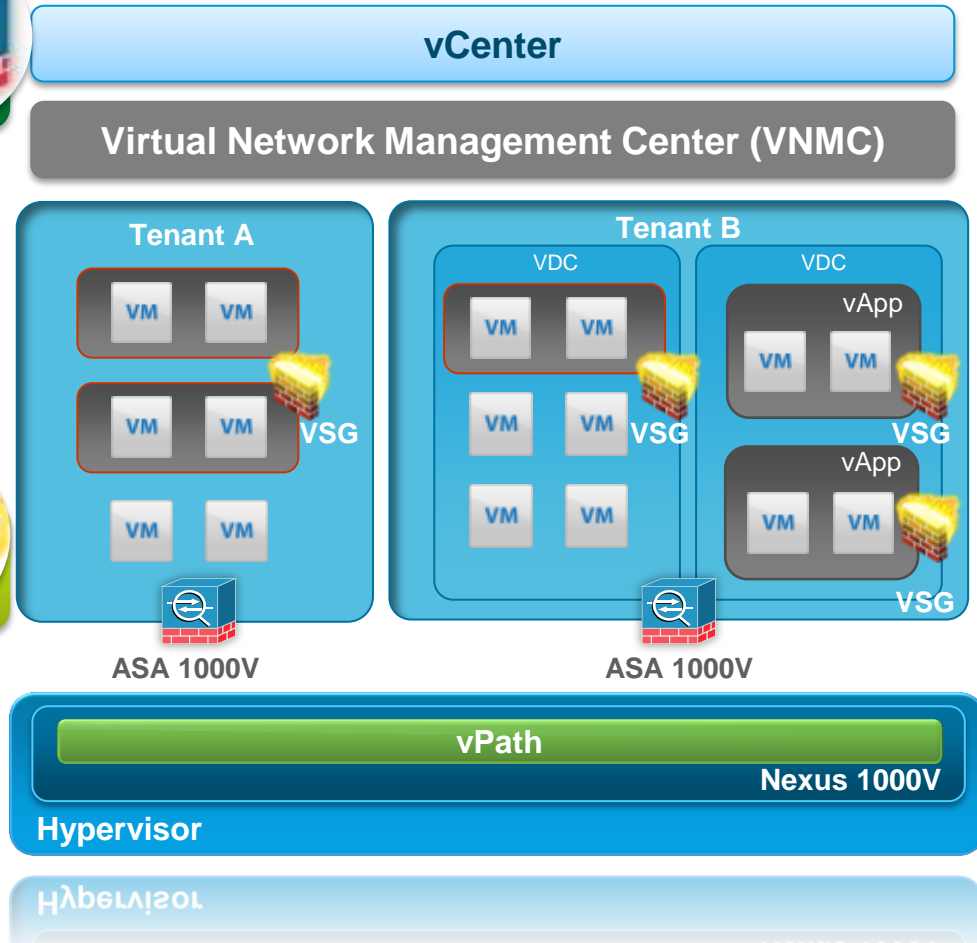


- VDC 방화벽 및 VPN 기능
- 가상데이터센터 간 트래픽에 대한 보안 정책 적용
- 브랜치와 가상데이터간 S2S IPsec VPN 망 구성

Virtual Security Gateway



- 서비스 영역별 가상 보안 게이트 웨이
- 가상 데이터센터내 서버팜별, 서비스영역별 및 Front-End Application 과 Back-End Application 간 접근 제어



시스코 ASA 1000V 기능 및 호환성

ASA 방화벽 기술 기반 빌드

서비스 체이닝을 통한 VSG 연동

가상확장 LAN 지원 (VXLAN)

VNMC를 이용한 다중 소유 관리

IPSec VPN (Site-to-Site)

NAT

DHCP

Default Gateway

Static Routing

Stateful Inspection

IP Audit

위협 방어 옵션

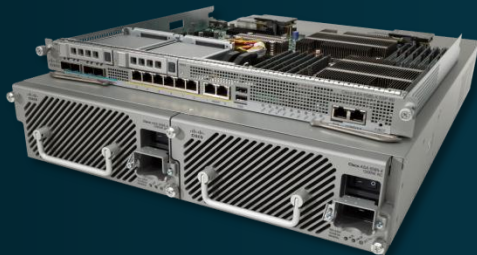
Cisco® IPS 4500



데이터 센터급 고성능 보안 위협 방어

- 빈번히 발생하는 내외부 네트워크, 서버 및 어플리케이션 **침해 사고 방어** 기능 지원
- 고밀집도의 포트 및 확장형 샤시 형태의 **하드웨어 기반의 10G 급 IPS**
- 실시간으로 업데이트되는 보안 시그니처 및 SIO 활동을 통해 수집되는 보안 위협 및 평판 정보 반영을 통한 **상황인식기반의 IPS** 기능 지원

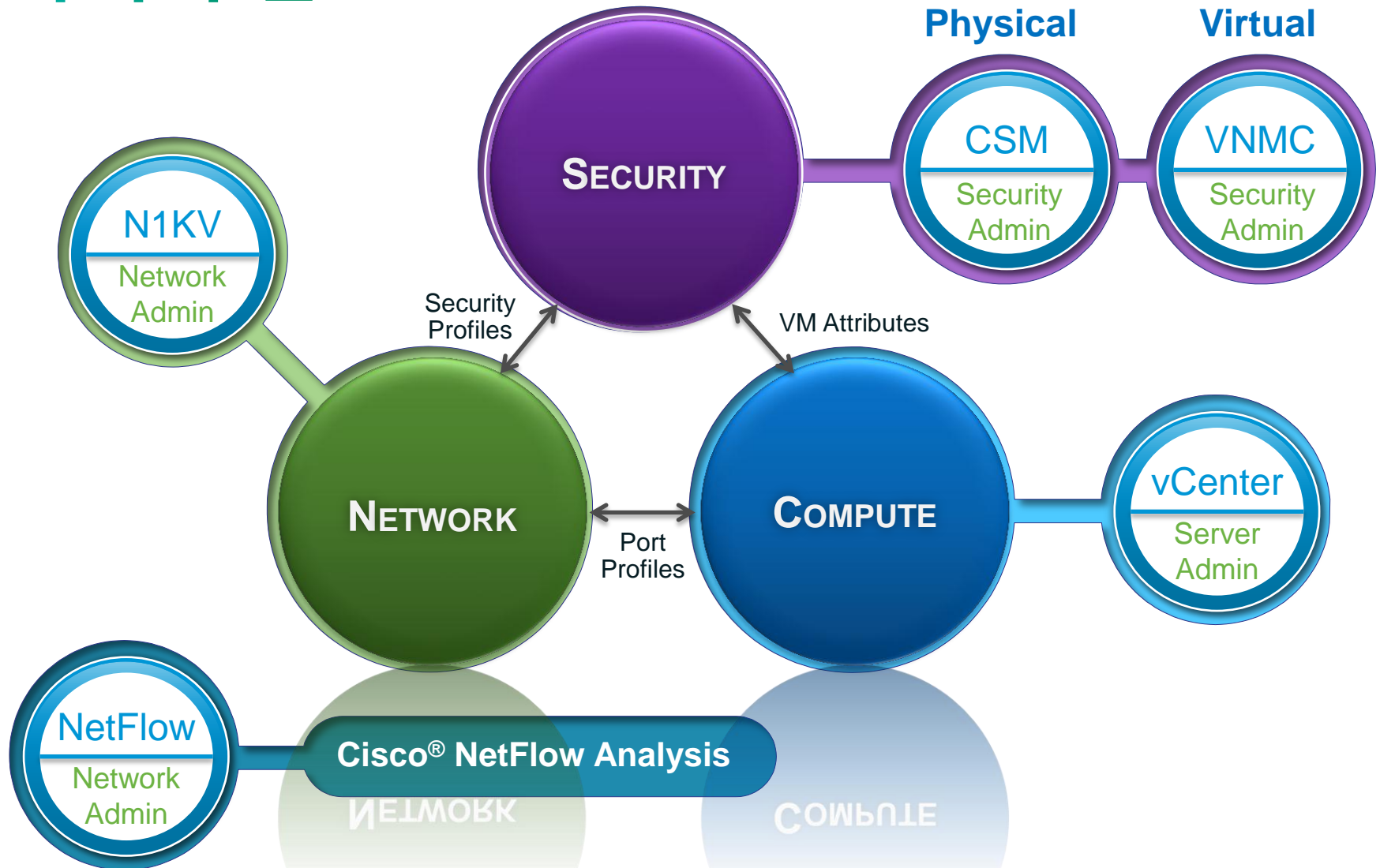
Cisco ASA CX



상황인식 기반 차세대 방화벽 모듈

- 어플리케이션 및 마이크로 어플리케이션까지 포함한 **광범위한 어플리케이션 가시화 및 통제**
- 어플리케이션 분류, 사용자 및 그룹 등 **세밀한 상황적 보안 정책**
- **하드웨어 모듈 기반**의 어플리케이션 인지 및 상황인식 기반 접근 제어
- **SSL 암호화된 트래픽**에 대한 어플리케이션 식별 및 가시화를 통한 접근 제어

가시화 옵션



데이터 센터 보안 포트폴리오



세그먼테이션



ASA 5585-X, ASASN



ASA 1000V



VSG



Nexus 1000V



TrustSec



위협방어



IPS 4500



ASA CX

SIO



가시성



CSM



NetFlow



ISE



VNMC

Thank you.

