VMware NSX Data Center를 통한 상황 인식 마이크로 세분화

위협의 수평적 확산으로부터 네트워크 보호

복잡하고 분산형이며 동적인 최신 애플리케이션

모든 기업 및 기관은 애플리케이션과 데이터가 핵심 요소인 모든 것이 연결된 세상에서 비즈니스를 운영하는 방법을 모색하고 있습니다. 최신 애플리케이션은 여러 데이터 센터와 클라우드 전반에 분산되어 있고 환경 가장자리까지 확장됩니다.

DevOps의 등장과 더불어 가상화, 컨테이너화 및 마이크로서비스를 통해 여느 때보다도 빠르게 애플리케이션을 구축하고 변경할 수 있습니다. 최신 애플리케이션이 분산되어 있고 빠르게 변경된다는 특성으로 인해 보안의 유지는 매우 어려운 과제로 떠올랐습니다.

더 이상 효과가 없는 기존 보안 전략

애플리케이션이 계속해서 급증함에 따라 기존의 경계 중심 보안 접근 방식은 애플리케이션과 데이터를 보호하기에 충분하지 않은 것으로 입증되었습니다. 공격자는 경계 보안 조치를 반복해서 침투하거나 우회할 수 있음을 입증했습니다. 공격자는 침투한 후 서버 간에 자유롭게 이동하여 탈취하거나 금품을 대가로 요구하기 위한 정보를 찾습니다.

최신 분산형 애플리케이션 환경에서 IT 보안 팀과 네트워킹 팀은 환경마다 서로 다른 보안 정책을 유지해야 하므로 전반전인 보안 태세에 허점이 발생하는 문제로 인해 종종 어려움을 겪고 있습니다.

데이터 센터에서 클라우드, 에지까지 일관된 보안 제공

VMware NSX® Data Center를 사용하면 애플리케이션 유형이나 배포 위치에 관계없이 전체 환경에서 일관되게 보안 정책을 정의할 수 있습니다. 정책이 개별 워크로드 수준에서 적용되므로 외부의 물리적 또는 가상 방화벽을 통해 트래픽을 헤어피닝(hairpin)하지 않고도 동일한 물리적 호스트에 상주하는 워크로드를 세분화할 수 있습니다. 이렇게 세분화된 보안 수준을 마이크로 세분화라고 합니다.

"IoT 디바이스의 수가 증가하는 상황에서, 네트워크가 더 세분화될수록 더 안전해질 것입니다. 따라서 위협이 데이터 센터 내에서 자유롭게 이동할 수 없습니다."

CHRISTOPHER FRENZ
INTERFAITH MEDICAL CENTER의
인프라 담당 이사

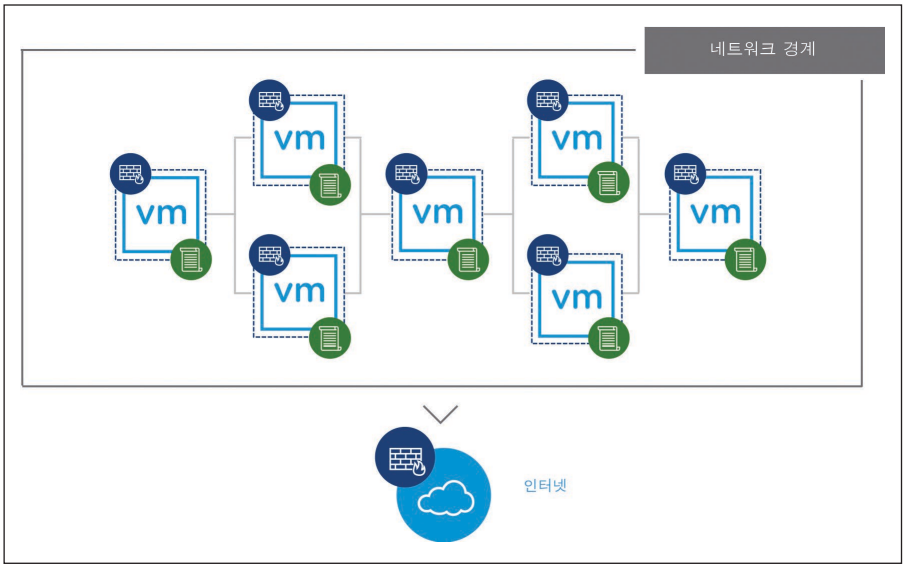

그림 1. 마이크로 세분화는 개별 워크로드 수준에서 네트워크 보안 정책을 적용하는 것을 말합니다.

핵심 요점

- 분산되고 동적인 최신 애플리케이션의 특성으로 인해 기존의 경계 중심 보안으로는 충분하지 않습니다.
- VMware NSX Data Center는 마이크로 세분화를 통해 위협의 수평적 확산으로부터 애플리케이션을 보호합니다.
- 보안 정책이 애플리케이션 컨텍스트를 기반으로 정의되고 개별 워크로드에 적용됩니다.
- 보안이 데이터 센터에서 클라우드, 에지까지 일관되게 제공됩니다.

NSX Data Center를 통해 구축된 마이크로 세분화는 소프트웨어에서 정의되고 관리되므로 대응력이 뛰어나고 자동화가 가능합니다. 새로운 워크로드가 배포될 때 프로비저닝된 위치나 이동할 위치에 관계없이 수명주기 전체에 걸쳐 워크로드와 함께 유지되는 보안 정책을 자동으로 상속합니다.

상황 인식 마이크로 세분화, 애플리케이션 및 데이터에 맞게 보안 적용

우선 순위에 따라 보안 정책을 정의하는 기능은 정책을 일관되게 제공하는 것만큼 중요합니다. NSX Data Center는 IP 주소, 포트, 프로토콜과 같은 정적 네트워크 특성에서 보안 정책을 분리하고 애플리케이션 및 인프라에 대한 상황별 이해도를 바탕으로 정책을 정의할 수 있도록 허용합니다. 이러한 상황에는 사용자 및 ID 특성, 워크로드 특성(예: 운영 체제), 규정 준수 범위 등이 포함됩니다.

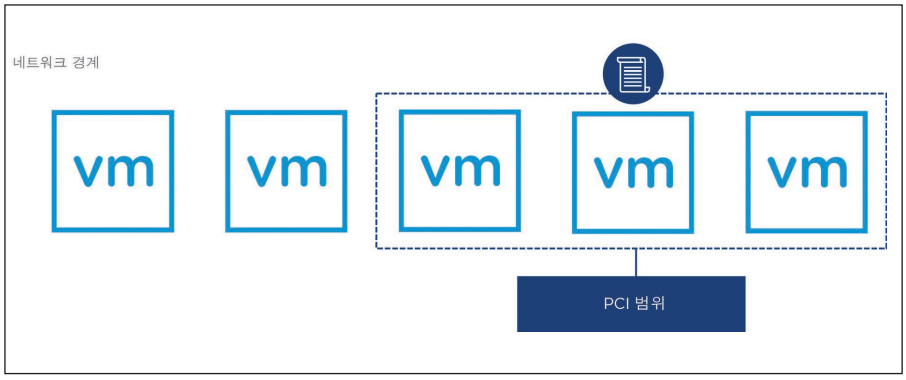

그림 2. NSX Data Center에서 마이크로 세분화는 규정 준수 범위를 비롯한 다양한 상황을 기반으로 정의할 수 있습니다.

NSX Data Center를 통한 상황 인식 마이크로 세분화를 통해 네트워크 보안 팀은 가장 중요한 요인을 기반으로 애플리케이션과 데이터를 보호하는 데 필요한 유연성을 높일 수 있습니다. 예를 들어, NSX Data Center를 사용하면 사용자 컨텍스트를 바탕으로 개별 RDSH 세션 수준까지 네트워크 정책을 적용하여 가상 데스크톱 인프라(VDI) 구축을 보호할 수 있습니다. 또는 환경 내에서 물리적으로 존재하는 위치에 관계없이 PCI(결제 카드 산업) 표준에 해당하는 모든 워크로드에 보안 정책을 적용할 수도 있습니다.

필요할 때 필요한 곳에 고급 보안 서비스 제공

NSX Data Center를 사용하면 우수한 타사 보안 서비스를 마이크로 세분화에 추가할 수 있습니다. 차세대 방화벽(NGFW), 침입 탐지 시스템(IDS)/침입 방지 시스템(IPS)과 같은 물리적 디바이스 또는 가상 어플라이언스를 통해 모든 네트워크 트래픽을 라우팅하지 않고도 NSX Data Center는 가상 네트워크 레이어에서 특정 트래픽을 해당 서비스로 동적으로 조정할 수 있습니다. 이를 통해 고급 보안 서비스를 적시에 필요한 장소에 삽입할 수 있으므로 네트워크 트래픽의 효율성을 극대화하면서 보안 서비스 자체의 효과를 높일 수 있습니다.

전체 환경에 걸쳐 네트워크 트래픽에 대한 가시성 확보

마이크로 세분화의 첫 단계는 네트워크 트래픽이 어떤 방식으로 흐르는지 이해하는 것입니다. VMware Network Insight™를 사용하면 물리적 네트워크 트래픽과 가상 네트워크 트래픽을 포함하여 데이터 센터 내 모든 네트워크 트래픽을 종합적으로 살펴볼 수 있습니다. VMware Network Insight는 네트워크 트래픽을 분석한 후 NSX Data Center에서 구현에 사용할 수 있는 마이크로 세분화 정책을 자동으로 추천합니다.

현재의 네트워크 트래픽을 분석하고 마이크로 세분화 프로젝트를 계획하려면 지금 바로 무료 가상 네트워크 평가를 시작하십시오. 자세한 내용은 https://www.vmware.com/kr/products/nsx/security를 참조하십시오.

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: 147939wf-vmw-q2fy19-sddc-launch-so-nsbu-context-aware-micro-seg-a4 5/18