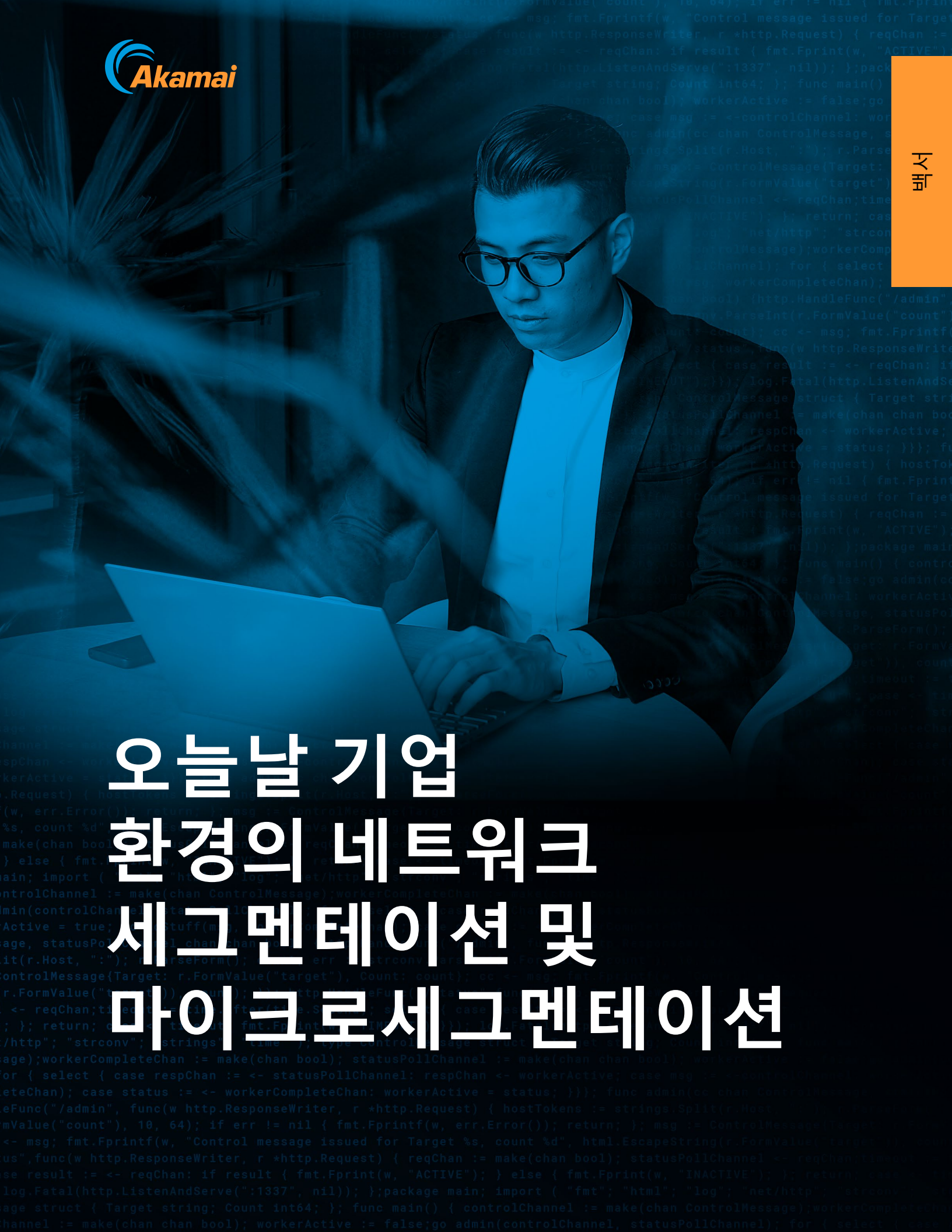
Akamai

백서



오늘날 기업 환경의 네트워크 세그멘테이션 및 마이크로세그멘테이션

개요

보안을 위한 세그멘테이션의 개념은 새로운 것이 아닙니다. VLAN 및 ACL과 함께 경계 방화벽은 대부분의 기업이 전통적으로 IT 인프라를 세그멘테이션하고 보호하는 데 사용한 것입니다. 그러나 시대는 변하고 있습니다. 컨테이너화의 증가, 소프트웨어 정의 네트워킹, 퍼블릭 및 멀티클라우드 인프라 사용, 인터넷 연결 디바이스의 확장으로 인해 해결해야 할 새로운 보안 문제가 발생했으며, 이러한 문제에는 다양한 보안 요구사항이 있는 이기종 IT 환경용으로 구축된 솔루션이 필요합니다. 또한 랜섬웨어와 국가 차원의 공격자들은 이제 모든 비즈니스에 리스크가 되었고, 공격자들은 IT 환경에 대한 가시성을 확보하기가 점점 더 어려워지는 동시에 더욱 정교해지고 있습니다. 기존의 경계 보안 조치와 심층 패킷 검사 또는 시그니처 기반 탐지를 기반으로 하는 차세대 방화벽은 오늘날 기업의 데이터 센터에서 발생하는 트래픽의 양을 따라잡는 데 어려움을 겪고 있습니다. 올바른 마이크로세그멘테이션 기법이 다른 대체 네트워크 세그멘테이션 접근 방식의 단점을 해결하기에 가장 적합한 이유를 살펴보겠습니다.

> 하이브리드 클라우드 환경이 보편화됨에 따라 기존의 경계 보안을 넘어서는 특정 요구사항의 이행이 필요

동서 트래픽에 적합하지 않은 레거시 방화벽

IT 환경 세그멘테이션을 모색할 때 기업은 먼저 레거시 경계 보안 디바이스를 살펴볼 수 있습니다. 하지만 이러한 디바이스는 북에서 남으로, 클라이언트에서 서버로 이동하는 트래픽을 모니터링하도록 설계되었습니다. 여기에는 외부 소스에서 데이터 센터로 유입되는 모든 트래픽이 포함됩니다. 최근에는 서버 사이에서 이동하는 데이터 센터 내의 트래픽 양(일반적으로 동서 트래픽이라고 함)이 기하급수적으로 증가했습니다. 그 원인으로는 하이퍼바이저, VPC, 컨테이너 기반 컴퓨팅 등 가상화 및 융합형 인프라의 성장이 큰 부분을 차지합니다.

기존의 방화벽과 같은 경계 보안 조치는 감염된 디바이스로부터 비즈니스를 보호하거나 동서 트래픽을 이용해 거점을 확장하는 공격자를 방지하는 데 아무런 도움이 되지 않습니다. TLS 암호화의 등장과 열려 있는 정상적인 애플리케이션 포트에서 편승하는 악성 트래픽을 손쉽게 은폐함으로써 많은 공격이 방화벽조차도 통과할 수 있습니다. 이 경우 기존 유출 지점을 찾아내서 이를 해결하거나 방향을 전환시킬 수 없습니다. 또한 공격자의 네트워크 체류 시간을 쉽게 제한할 수 없게 됩니다. 체류 시간이 길어질수록 유출 피해는 더 심각해집니다. Sophos의 The Active Adversary Playbook 2022에 따르면 평균 체류 시간은 15일이지만 소규모 비즈니스와 특정 업계의 경우 평균 체류 시간이 최대 34일로 훨씬 더 길게 나타났습니다.[1] 공격자가 네트워크에서 탐지되지 않을 수 있는 시간이 길수록 더 많은 피해를 입을 수 있습니다.

가상화된 방화벽을 충분히 사용하는 방식으로는 수천 개의 애플리케이션이나 워크로드를 보호할 수 없습니다. 가상화된 솔루션을 만들 수 있다 하더라도, 현재 우리가 일하고 있는 끊임없이 변화하는 동적 환경을 고려할 때 이러한 솔루션을 관리하거나 제어하기란 불가능합니다. 예를 들어 하이브리드 클라우드의 경우 기존의 방화벽은 다양한 환경에서 작동하고 여러 클라우드 사이에서 워크로드를 추적하며 단일 지점에서 제어해야 하기 때문에 사용하기가 훨씬 더 어렵습니다. 이러한 문제를 해결하기 위해 몇 가지 네트워크 세그멘테이션 접근 방식이 등장했습니다.

고려할 세 가지 세그멘테이션 접근 방식

방화벽이 가상화되었어도 하이브리드 클라우드 데이터 센터를 보호하는 데 부적합하다는 사실을 깨달은 기업들은 세 가지 기본적인 방법으로 동서 인프라 내에서 세그멘테이션을 적용할 방법을 찾고 있습니다. 앞서 논의한 바와 같이 강력한 세그멘테이션 정책과 보안 조치가 없으면 모든 포트나 서버가 서로 접속해 통신할 수 있습니다. 즉, 서버 방화벽에 유출이 발생하면 공격자가 네트워크의 다른 여러 곳으로 쉽게 이동할 수 있습니다. 서버 간 연결을 제한하는 가장 효과적인 방법은 네트워크를 세그멘테이션하는 것입니다. 네트워크 세그멘테이션에는 기본적으로 세 가지 종류가 있으며, 마이크로세그멘테이션은 기업이 점점 더 세분화된 정책과 제어를 적용하는 데 사용할 수 있는 기술입니다. 사용자는 다음과 같은 세 가지 종류의 세그멘테이션 정책을 결합해 중요하거나 위험한 애플리케이션을 위해 보다 세분화된 정책을 구축할 수 있습니다.

환경 세그멘테이션

이 접근 방식은 다양한 환경을 서로 구분합니다. 예컨대, 이 방식을 통해 기업은 프로덕션 환경으로부터 회사의 개발 부문을 세그멘테이션할 수 있습니다. 이는 모든 세그멘테이션 전략에서 매우 중요한 첫 단계이며, 이후에 보다 세분화된 정책 생성이 뒤따를 수 있습니다.

애플리케이션 세그멘테이션

세그멘테이션에서 한 발짝 더 나아가 가치가 높은 애플리케이션을 '링펜싱'하여 각각의 특정 중요 애플리케이션을 네트워크에 있는 나머지 애플리케이션과 분리하게 됩니다. 최고의 마이크로세그멘테이션 솔루션은 프로세스 수준에서 이를 제어할 수도 있습니다.

티어 세그멘테이션

가장 엄격한 형태의 세그멘테이션은 애플리케이션 자체에 있습니다. 예를 들어 동일한 애플리케이션 클러스터 내 티어 사이에서 통신을 관리하는 방법에 관한 정책을 생성함으로써 웹 서버, 애플리케이션 서버, 데이터베이스 서버 간 트래픽을 제어할 수 있습니다. 원하는 경우 프로세스 수준의 적용으로 제어할 수도 있습니다.

네트워크 세그멘테이션 방법 - VLAN을 통한 네트워크 세그멘테이션

대부분의 회사는 VLAN을 도입하는 것부터 시작합니다. 기업은 VLAN으로 라우터 자체의 접속 제어 목록(ACL) 또는 방화벽을 통한 자체 통신 경로로 각 세그먼트를 할당할 수 있습니다. 네트워크 세그멘테이션을 위해 일반적으로 VLAN을 선택하지만, 그 이면에는 많은 문제가 있습니다. VLAN이 오늘날의 보안 요구사항을 충족하는 데 적합하지 않은 선택인 이유를 자세히 살펴보겠습니다.

많은 기업이 세그멘테이션 방법으로 VLAN을 선택하는 이유는 간단합니다. 기존 아키텍처에서도 수행할 수 있기 때문에 비용이 저렴하고 배포가 간편하다고 생각되기 때문입니다. 하지만 매우 엄격하고 복잡한 세그멘테이션 접근 방식인 만큼 유지 관리 비용이 많이 들 수 있으며, 이를 구축하려면 가동 중단이 필요합니다.

VLAN의 사용을 시작하려면 각 세그멘테이션에서 서버와 의존성을 숙지한 후, 세그멘테이션하는 하나 이상의 네트워크 스위치에 대해 원하는 설정을 생성해야 합니다. 이 작업은 네트워크 엔지니어가 수행하며 종종 여러 위치에서 진행되기 때문에 오랜 기간이 걸리고 시간과 비용이 지나치게 많이 소요될 수 있습니다. 설정하는 동안 트래픽이 중단되거나 느려질 수도 있습니다.

민첩성이 주요 경쟁 우위이자 아마도 필수 요소인 시대에 비용이 많이 드는 느린 변경 작업은 수익에 재앙을 초래합니다. Forbes에 따르면 적응력은 생존에 반드시 필요합니다. '장애가 새로운 것은 아니지만, 장애의 속도, 복잡성, 글로벌 특성은 전례 없는 규모입니다. ... 가장 규모가 크거나 재정적으로 더 안정적이라고 생존할 수 있는 것이 아닙니다. 이제 생존 여부는 기하급수적으로 증가하는 변화의 속도에 성공적으로 적응하는 데 달렸습니다.'[2]

VLAN은 세그멘테이션을 염두에 두고 만들어지지 않았다는 점을 인식하는 것이 중요합니다. 처음부터 혼잡을 줄이기 위해 구축된 기술을 통신 제어에 사용하는 것은 현명한 활용 방법이 아닙니다. 여러 면에서 잘못된 사용법입니다. 이를 고려할 때 VLAN을 사용한 세그멘테이션에 제한이 따른다는 것은 놀라운 일이 아닙니다.

- **클라우드 기술** - VLAN 및 기타 기존 네트워크 세그멘테이션 정책은 클라우드로 확장할 수 없습니다. 내부 세그먼트 방화벽(ISFW) 또는 ACL을 사용해 어떤 사용자가 네트워크 세그먼트에 접속할 수 있는지를 제어하는 경우 클라우드용 소프트웨어 정의 네트워킹(SDN)에 의존해야 할 가능성이 큽니다. 보통은 가상화된 방화벽이나 서브넷을 사용하는 써드파티 소프트웨어 공급업체가 이러한 보안 조치를 수행합니다.
- **컨테이너** - IT 환경에서 컨테이너가 널리 도입되고 있기 때문에 보안은 여전히 큰 걱정거리입니다. 각 컨테이너가 동일한 커널에서 실행되므로 악용으로 인해 모든 컨테이너가 리스크에 노출될 수 있습니다. 격리는 지속적인 문젯거리였으며, 일반적인 네트워크 세그멘테이션 방법으로는 해결할 수 없습니다.
- **프로토콜 제한** - VLAN에 대한 제한은 4,096개 세그멘테이션으로, 대규모 데이터 센터에서 적절한 세그멘테이션을 제공하는 기능을 제한합니다. 보다 세분화된 세그멘테이션 접근 방식에는 이러한 제한이 없습니다.

네트워크 세그멘테이션에서 애플리케이션 세그멘테이션으로 - 레이어 4 제어 도입

온프레미스 가상화 환경을 위한 하이퍼바이저 기반 방화벽과 클라우드 환경 내 보안 그룹을 사용해 애플리케이션 세그멘테이션을 수용함으로써 이러한 문제가 대부분 개선되었습니다. 기존의 애플리케이션 세그멘테이션은 레이어 4 제어를 구축함으로써 애플리케이션이 안전한 경계를 갖도록 서비스 티어를 서로 격리할 수 있게 해줍니다. 각 티어는 전체 기능을 제공하는 데 필요한 접속 수준으로 제한되지만 그 이상은 아닙니다. 개별 애플리케이션의 티어를 서로 명확하게 구분하므로, 잠재적 감염 위협은 최소한으로 억제됩니다.

부하 분산 및 데이터베이스에서 자체 DMZ 내부 및 외부의 애플리케이션 서버에 이르기까지 표준 비즈니스에서 볼 수 있는 티어를 생각해 보시기 바랍니다. 이러한 티어를 분리하면 각 티어에 고유한 보안 룰과 기능을 적용할 수 있습니다. 애플리케이션 세그멘테이션은 각 티어에 대한 올바른 제어를 허용하고 민감한 정보 및 통신을 제한하는 동시에 필요한 경우 광범위한 사용자 접속을 허용함으로써 기업을 지원할 수 있습니다. 예를 들어 기업은 특정 데이터베이스가 인터넷과 완전히 통신하지 못하도록 하거나 공격자가 간단한 부하 분산을 유출하는 경우 데이터베이스 티어에서 더 민감한 정보에 접속하지 못하게 할 수 있습니다.

솔루션이 더욱 세분화됨에 따라 애플리케이션 세그멘테이션을 통해 기업은 비즈니스의 다른 영역에서 전체 애플리케이션 클러스터를 세그멘테이션할 수 있습니다. 이렇게 하면 공격표면 영역과 공격자가 한 티어에서 다른 티어로 측면 이동할 수 있는 능력이 줄어듭니다.

레이어 4 제어의 한계

기존의 애플리케이션 세그멘테이션은 깊이가 부족해서 가시성에 직접적인 영향을 줄 수 있습니다. 라우팅이 수행되는 네트워크 레이어에서는 시스템 간에 데이터를 이동하고 데이터 세그멘테이션이 목적지에 도달하는 경로를 자세히 기술하는 IP 주소와 프로토콜을 할당합니다. 애플리케이션 세그멘테이션은 데이터 자체의 전송 방식에 초점을 맞춰 레이어 4 네트워크 제어를 사용하는 경우가 많습니다. 더 큰 데이터 세그멘테이션은 더 작은 세그멘테이션이나 블록으로 분할되어 목적지에서 다시 합칠 준비가 됩니다. 흐름 제어를 통해 정보를 전송하거나 수신하는 디바이스가 필요로 하는 경우 이 프로세스의 속도를 동적으로 높이거나 낮출 수 있습니다.

오늘날 위협 환경에서는 이러한 레이어에 대한 제어가 필수적이지만, 경우에 따라 더 세분화된 수준에서 정책을 설정할 수 있는 기능이 필요할 수도 있습니다. 공격자들은 IP 주소를 스푸핑하고 허용된 포트에서 은폐 기법을 이용해 네트워크를 유출할 수 있는 능력을 보였습니다. 또한 레이어 4 보호는 애플리케이션 또는 티어 내에서 측면 이동을 제한하지 않으므로 여전히 공격표면이 기대치보다 더 클 수 있습니다.

레이어 4보다 더 세분화된 제어가 필요한 가장 적합한 사례 중 하나는 컴플라이언스 이니셔티브입니다. 기존의 애플리케이션 세그멘테이션 기법을 통해 기업은 PCI-DSS에 대해 CDE를 분리하거나 HIPAA에 대해 PHI를 보호하는 등 일부 특정 컴플라이언스 규정을 어느 정도 충족할 수 있었습니다. 그러나 레이어 4 기법은 과거에 컴플라이언스를 입증하는 효과적인 수단으로 받아들여졌지만 실제로는 충분하지 않을 수 있습니다. Verizon 2022 Payment Security Report에 따르면, 43%의 기업만이 '컴플라이언스를 완벽하게 이행'하고 있습니다.[3] 하지만 컴플라이언스를 100% 이행한다고 해서 100% 안전한 것은 아닙니다. 레이어 4 제어는 컴플라이언스 측면에서는 충분할 수 있어도, 보안에서 유의미한 차이를 낼 수 있을 만큼 공격표면을 줄이지는 못합니다. 이는 거스를 수 없는 진리입니다. 공격자는 별도의 프로세스(레이어 7)를 사용해 두 티어 사이에 열린 레이어 4 포트를 타고 원하는 모든 정보를 가져갈 수 있습니다.

잘 알려지지 않은 세그멘테이션의 단점 - 네트워크 및 애플리케이션 세그멘테이션에 대한 가시성 부족

기업은 애플리케이션 세그멘테이션이 올바른 방향으로 나아가는 단계라고 확신하지만, 조악한 세분화 접근 방식에 내재된 모든 문제를 해결하기에는 역부족임을 깨닫고 있습니다. 가시성 역시 해결해야 할 또 다른 과제입니다. 네트워크에 대한 정확한 실시간 개요를 볼 수 있는 기능은 세그멘테이션 프로세스의 각 단계에서 필수적이며, 많은 세그멘테이션 접근 방식의 한계이기도 합니다.

시작하기 전에 정확한 정책 룰을 작성할 수 있도록 애플리케이션 의존성을 시각화해야 할 것입니다. 세그멘테이션이 구축되면 보안 체계가 강력한지 확인하기 위해서뿐만 아니라, 필요한 경우 규제 컴플라이언스의 이행 증거를 제공하기 위해서도 세그멘테이션이 의도대로 작동하고 있다는 증거가 필요합니다.

실시간 및 과거에 대한 가시성이 없으면 자신이나 써드파티 이해관계자와 규제 기관에 대한 증거를 확보할 수 없습니다. 이 증거를 수동으로 수집하려면 상당한 시간과 비용이 소요되며 설정 오류와 실수가 발생할 가능성이 항상 존재합니다. 이러한 가시성을 제공할 수 없는 세그멘테이션 솔루션은 제 역할을 충분히 해낼 수 없습니다.

레이어 7까지의 마이크로세그멘테이션 - 애플리케이션 레이어

반면, 애플리케이션 레이어(레이어 7)에서 세그멘테이션하면 애플리케이션 클러스터 내에서도 측면 이동을 제한하는 데 매우 효과적입니다. 레이어 7은 네트워크 서비스가 운영 체제와 통합되는 곳입니다. HTTP, FTP, TFTP, SMTP와 같은 프로토콜은 모두 레이어 7 프로토콜입니다. 마이크로세그멘테이션 기술에서의 최근 발전을 통해 이 레이어에서 다른 솔루션보다 훨씬 더 심층적으로 세그멘테이션할 수 있으므로 비즈니스는 기존 레이어 4뿐만 아니라 레이어 7에서도 활동을 시각화하고 제어할 수 있습니다. 즉, 기업이 정책을 설정할 때 IP 주소와 포트에 의존하는 대신 특정 프로세스와 흐름을 사용할 수 있는 것입니다. 이 방법은 특정 티어나 애플리케이션 클러스터보다도 더 강력한 세그멘테이션 이점을 제공합니다. 또한 공격자가 승인된 프로세스나 경로를 미러링하는 경우에도 잘못된 해시와 같이 사소한 잠재적 위협을 발견할 수 있습니다.

정책 생성과 관련해 레이어 7로 세그멘테이션하면 매우 특정한 허용 목록 룰이나 예외만 허용됩니다. 이 경우 정확한 프로세스 또는 흐름만 허용되고 다른 모든 통신은 기본적으로 차단됩니다. 이렇게 하면 시스템 사이에서 데이터를 격리하되, 필수 또는 비즈니스 크리티컬 데이터 흐름을 위한 통신은 계속 허용할 수 있습니다.

비즈니스가 민첩성을 확보하는 데 필요한 가시성을 제공하는 최고의 마이크로세그멘테이션 솔루션

종합적인 마이크로세그멘테이션 솔루션은 하이퍼바이저 또는 VPC 기반, 컨테이너, 베어 메탈 서버, 심지어 IoT/OT 시스템 등 모든 워크로드의 에이전트를 통해 비즈니스에 전체 IT 인프라에 대한 완벽한 비주얼 맵을 제공할 수 있습니다. 진정한 지능형 솔루션에는 데이터 센터, 클라우드, 멀티클라우드, 하이브리드 클라우드 환경과 원격 디바이스가 포함됩니다. 기존의 애플리케이션 세그멘테이션 솔루션은 주로 네트워크 중심 기술 조합을 사용하기 때문에 이러한 올인원 보기를 얻는 데 어려움을 겪습니다.

환경에 대한 포괄적인 비주얼 맵은 어떤 보안 정책이 시행되고 있으며 실시간으로 적용되고 있는지도 보여주어야 합니다. 엔지니어와 보안 전문가는 정책 적용 범위에서 수정할 잠재적 격차나 처음부터 새로 만들거나 구축해야 하는 추가 정책을 한눈에 파악할 수 있어야 합니다.

또한 비즈니스는 이러한 가시성을 통해 업데이트된 애플리케이션이나 새 애플리케이션을 배포하기에 앞서 세그멘테이션 룰을 만들고, 새로운 소프트웨어나 기존 시스템에 대한 업데이트를 사전에 준비할 수 있습니다. 업데이트가 실행되면 보안 팀은 정상 범위를 벗어난 애플리케이션 활동을 탐지하고 해결하는 데 필요한 실시간 정보를 확보함으로써 보안 리스크가 은폐되거나 악용되지 않도록 합니다. 기업은 사후에 맥락별 툴로 인시던트를 과거 데이터와 비교하고 이상 현상이 발생하도록 허용한 정확한 환경을 파악할 수 있습니다. 정책을 강화하고 세그멘테이션을 조정하며 컴플라이언스 규정 또는 추가 연구를 위해 인시던트를 세부적으로 기술할 수 있습니다.

제로 트러스트 모델 도입

마이크로세그멘테이션의 또 다른 추가 이점은 제로 트러스트 보안 모델을 수용할 수 있다는 것입니다. 제로 트러스트라는 아이디어는 2010년 Forrester에서 처음 선보였지만 마이크로세그멘테이션과 같은 기술이 이 개념을 현실화하는 데 도움을 주고 있으며, 보안 전문가들은 계속해서 그 이점을 널리 전파하고 있습니다.[4]

아이디어는 간단합니다. 외부 소스에서든 내부 소스에서든 연결 시도가 있을 때마다 트래픽이나 사용자나 입증되고 승인될 때까지는 신뢰하지 않는 것입니다. Forrester의 제로 트러스트에 대한 세 가지 기본 원칙[5]은 모두 강력하고 세분화된 마이크로세그멘테이션 정책으로 뒷받침됩니다.

- 기본적으로 아무것도 신뢰하지 않음
- 포괄적인 보안 모니터링 구축
- 최소한의 접속 권한 적용

제로 트러스트는 경계만을 보안하는 방식과는 정반대입니다. 경계 보안 방식은 깊은 경계를 만들어 성으로 들어가는 입구를 보호하며, 내부는 외부 출입으로부터 안전하다고 가정합니다. 대부분의 기업에는 더 이상 격리된 네트워크나 데이터 센터가 없으므로 '성'이라는 개념은 시대에 뒤떨어진 것이며, 제로 트러스트와 같은 접속 최소 권한 전략은 특정 시간에 누가 내부에 있는지 파악하고 제어할 수 있는 유일한 방법입니다.

비즈니스의 미래를 보장하는 마이크로세그멘테이션

네트워크 세그멘테이션은 확실히 경계 보안을 능가할 수 있으며, 환경 세그멘테이션과 레이어 4까지의 애플리케이션 세그멘테이션은 세그멘테이션 전략을 수립하는 중요한 단계입니다. 그러나 IT 환경이 점점 복잡해짐에 따라 애플리케이션 및 티어 단계에서 티어 세그멘테이션과 레이어 7에 대한 프로세스 수준 적용을 통해 훨씬 더 세분성을 제공하는 세그멘테이션 솔루션이 필요하다고 느낄 수 있습니다.

오늘날 비즈니스는 독립형 인프라를 넘어섰습니다. 클라우드, 컨테이너, 베어 메탈 하이퍼바이저의 SDN과 같은 기술에 의존하는 경우가 많습니다. 다양한 지역과 물리적 데이터 센터에서 업무를 수행합니다.

외부 및 내부 위협으로부터 스스로 보호하는 유일한 방법은 동서 트래픽과 남북 트래픽을 비롯한 모든 트래픽을 검사하고 제어하는 솔루션을 사용하는 것입니다. 중요하거나 위험한 애플리케이션의 경우 레이어 4에서만 얻을 수 있는 것보다 더 큰 가시성을 제공해야 합니다. 애플리케이션 또는 티어 수준에서 레이어 7까지의 마이크로세그멘테이션은 전체 IT 환경을 정확하게 파악할 수 있는 기능을 제공하며 제로 트러스트 모델을 따르는 세분화된 보안 정책을 쉽게 생성하고 적용할 수 있도록 합니다. 뛰어난 마이크로세그멘테이션 솔루션은 보안과 민첩성 중에서 무엇 하나 희생할 필요가 없습니다. 따라서 기업 전체에 가장 강력한 전체 보안 체계를 제공하는 솔루션을 선택하시기 바랍니다.

자세한 내용을 확인하려면 akamai.com/guardicore를 방문하시기 바랍니다.

1 Shier, John. 2022년. "The Active Adversary Playbook 2022." Sophos. 6월 7일.

2 Gonda, Rob. 2018년. "Adaptability Is Key To Survival In The Age Of Digital Darwinism." Forbes. 5월 24일.

3 https://www.verizon.com/business/reports/payment-security-report/

4 Holmes, David. 2022년 6월. "Best Practices For Zero Trust Microsegmentation." Forrester. 4월.

5 Holmes, David and Jess Burn. 2022년 1월. "The Definition Of Modern Zero Trust." Forrester. 4월.

Akamai는 어디에서 구축하고 제공하든지 생성하는 모든 것에 보안 기능을 내장하도록 지원함으로써 고객 경험, 인력, 시스템, 데이터를 보호합니다. Akamai 플랫폼은 글로벌 위협에 대한 가시성을 바탕으로 제로 트러스트 지원, 랜섬웨어 차단, 앱 및 API 보안 또는 DDoS 공격 차단을 목표로 보안 체계를 조정하고 발전시켜 지속적으로 안심하고 혁신하며 확장하고 가능성을 현실로 구현할 수 있습니다. Akamai의 보안, 컴퓨팅, 전송 솔루션에 관해 자세히 알아보려면 akamai.com와 akamai.com/blog를 방문하거나 Twitter와 LinkedIn에서 Akamai Technologies를 팔로우하시기 바랍니다. 2023년 05월 발행.