제로 트러스트 아키텍처 무엇이며 어떻게 도달하는가

Alcatel·Lucent Enterprise

eBook
제로 트러스트 아키텍처

목차

제로 트러스트 아키텍처란 무엇입니까?

제로 트러스트 아키텍처(ZTA)는 무엇을 의미합니까? 바로 데이터에 대한 액세스가 허용되기 전에 모든 사용자와 장치가 인증되고 승인되어야 함을 의미합니다. '아무도 믿지 않음. 모든 것을 인증'하는 전략이 그것입니다.

다음과 같은 비유가 이해에 도움이 될 것입니다.

전통적인 보안을 마을을 보호하는 요새로 생각하면 마을(=기업) 주변에 요새 벽(= 방화벽)을 쌓을 것입니다. 요새 외부에서 들어오는 모든 것은 신뢰할 수 없고 면밀한 조사를 받지만 요새 내부의 모든 것은 묵시적으로 신뢰되고 허용됩니다. 이 트러스트 경계는 귀하가 요새의 어느쪽에 있는지에 따라 물리적이거나 암시적일 수 있습니다. 왜냐하면 경계의 '오른쪽' 측에 있는 한, 더 이상의 검사가 필요하지 않기 때문입니다. 엔터프라이즈 네트워크의 관점에서 이 접근 방식을 생각하면 VLAN, SSID, 서브넷 또는 방화벽에 연결된 인터페이스의 형태로 몇 가지 기본 분할이 있을 수 있지만 이 분할은 정적이며 보안과 함께 네트워크 확장성 및 관리 용이성과 더 관련이 있습니다.

그러나 오늘날 방화벽(요새) 접근 방식은 여러 가지 이유로 그 자체로는 덜 효과적입니다. 첫 번째는 이동성입니다. 사용자는 기업 외부의 다른 네트워크에 접속하고 이 과정에서 위협 요소를 가져올 수 있습니다. 둘째, 게스트가 반드시 신뢰할 수 있는 것은 아닙니다. 직원(요새 내부에 있는 사람)도 맹목적으로 신뢰해서는 안 된다고 주장할 수 있습니다. 셋째, 점점 더 많은 IoT 장치가 네트워크에 추가되고 있습니다. IT 부서에서 승인 및 관리하지 않을 수 있고 일반적으로 보안 기능이 부족하기 때문에 보안 위험이 더 높습니다. 기존의 '요새/마을', '방화벽/엔터프라이즈' 접근 방식을 사용하면 사용자 또는 장치가 손상된 경우 위협이 다른 사용자 및 장치로 확산되는 것을 막을 방법이 거의 없습니다. 경계 안으로 들어가면 자유롭게 이동할 수 있습니다.

요새와의 비유에서 침입자로부터 마을을 보호하는 유일한 것이 성벽이라면 그들이 성벽을 오르는 방법을 배우는 날, 그리고 그렇게 될 것입니다. 대학살이 일어날 것입니다.

문제는 우리가 무엇을 할 수 있을까 입니다. 이를 '아무도 믿지 않음' 또는 '제로 트러스트' 접근 방식에서 생각해 보겠습니다.

제로 트러스트에서는 사용자나 장치를 신뢰할 수 없습니다. 온프레미스든 사내에 있든 상관없이 동일한 확인을 거쳐야 합니다. 내부 사용자라고 해서 무조건 신뢰할 수는 없습니다. 모든 액세스가 인증되고 권한이 부여 됩니다.

요새 비유에서 그것은 외부 위협으로부터 마을을 보호하는 요새 외에도 모든 집, 모든 건물에는 요새 내부에 사는 사악한 시민들로부터 오는 위험으로부터 보호하기 위해 자체 보안이 있음을 의미합니다. 엔터프라이즈 측면에서 소프트웨어 정의 마이크로 세분화로 알려진 것은 한 발자국 더 나아간 단계를 말합니다. 요새의 꼭대기와 건물 주변의 보안에는 우리가 어디를 가든지 우리를 따라다니는 개인 경비원이 있습니다. 그리고 어디를 가든지 여권을 요구할 것입니다. 이 엔터프라이즈 네트워크 신뢰 경계는 흐릿하고 분산되어 있으며 모바일입니다. 구체적인 위치, 스위치 포트 또는 VLAN과 연결되어 있지 않습니다. ID, 장치, 상황 및 시간에 따라 다릅니다. 이것이 소프트웨어 정의이고 즉시조정이 가능합니다. 이 접근 방식은 구성 요소의 관리가 필요하고 워크플로우의 위협이나 변화에 대응하기 위해 필요에 따라 대응하고 재구성할 수 있어야 한다는 것입니다.

매크로 및 마이크로 세분화 이해

제로 트러스트 아키텍처에는 두 가지 종류의 세분화, 매크로 및 마이크로 세분화가 있습니다. 비유하자면 성벽은 거시적 세분화이고 개인 경비원은 미시적 세분화입니다.

매크로 **세분화**에서는 물리적 네트워크가 서로 다른 논리적 세그먼트로 분할됩니다. 이 세그먼트는 VLAN과 VRF의 조합인 VLAN이 될 수 있으며 최단 경로 브리징(SPB), MPLS 또는 VXLAN 또는 GRE 터널과 관련 될 경우 VPN이 될 수도 있습니다. 서로 다른 세그먼트의 사용자 또는 장치 간 모든 트래픽은 방화벽에 의해 제어됩니다. 모든 기업은 세그멘테이션을 어떠한 모양이나 형태로 사용하지만 보안상의 이유로 항상 그런 것은 아닙니다. 종종 이러한 종류의 세분화는 확장성, 관리 또는 조직상의 이유로 사용됩니다. 두 장치가 서로 다른 VLAN에 매핑되지만, 방화벽을 통과하지 않고 통신할 수 있는 경우 동일한 매크로 세그먼트에 있게 됩니다. 이러한 종류의 세분화의 일반적인 예는 PC와 논리적으로 격리된 별도의 VLAN 및 VRF에서 IP 전화를 실행하는 것입니다.

문제는 이러한 세그먼트에 사용자 또는 장치를 매핑하는 방법입니다. 예를 들어 스위치 포트 또는 SSID를 통해 정적으로 수행할 수 있지만 실제로는 더 이상 사용되지 않는 방식입니다. 너무 고지식해서 모바일 사용자에게는 좋지 않습니다. 이상적으로는 사용자 또는 장치가 연결하고 인증할 때 프로필이 할당되도록 소프트웨어 정의 인증 시스템이 있어야 합니다. 프로필은 물리적 위치, 스위치 포트 또는 SSID에 관계없이 올바른 세그먼트에서 사용자 또는 장치를 프로비저닝합니다.

매크로 세분화는 보안상의 이점이 있지만 많은 경우 조직 또는 관리상의 이유로 수행됩니다. 예를 들어 카메라 및 도어락은 액세스 보안 그룹의 제어에 해당되는 반면 온도 조절 장치의 경우 건물 유지 관리 그룹의 제어에 속할 수 있습니다.

마이크로 세분화는 한 걸음 더 나아갑니다. 모든 사용자가 동일하지는 않으며 사용자 모두가 모든 리소스에 액세스할 필요가 있는 것은 아닙니다. 사용자를 세그먼트에 매핑하는 프로필에는 Finance나 HR과 같이 역할마다 다른 사용자/장치 권한 제어를 지정하는 정책 집합도 포함 됩니다. 이를 ' 역할 기반 **액세스**'라고 하며, **'최소 특권 원칙**'과 직접 관련이 있습니다. 따라서 카메라와 도어락이 모두 같은 세그먼트에 있더라도 동일한 리소스를 사용할 필요가 없습니다. 카메라는 비디오 레코더, 서버 및 도어락과 통신해야 합니다. 도어록이 다른 도어락과 통신할 필요가 없기 때문에 카메라가 도어록과 통신할 필요는 없습니다. 이러한 부드러운 권한은 프로파일의 일부이며 인증 후 디바이스에 동적으로 적용되는 정책을 통해 구현됩니다.

마이크로 세분화는 여러 가지 이유로 소프트웨어 정의가 필요합니다. 사용자나 IoT 장치는 고정되어 있지 않으며 이동하고 연결하고 연결을 끊습니다. 정책은 위치나 포트에 묶일 수 없습니다. 사실, 마이크로 세분화 구성은 사용자 또는 장치의 ID, 시간 및 위치를 포함하지만 이에 국한되지 않는 여러 요소의 조합을 기반으로 동적이어야 합니다.

요약하면, 서로 다른 세그먼트 간의 통신이 방화벽에 의해 제어받는 것이 매크로 세분화입니다. 동일한 세그먼트 내의 통신이 장치 또는 사용자 역할과 연결된 NAC(네트워크 액세스 제어) 정책에 의해 제어되는 경우, 이는 마이크로 세분화입니다.

둘 다 필요한 이유

한 가지 유형의 세분화만 사용하면 어떤 일이 일어날까요?

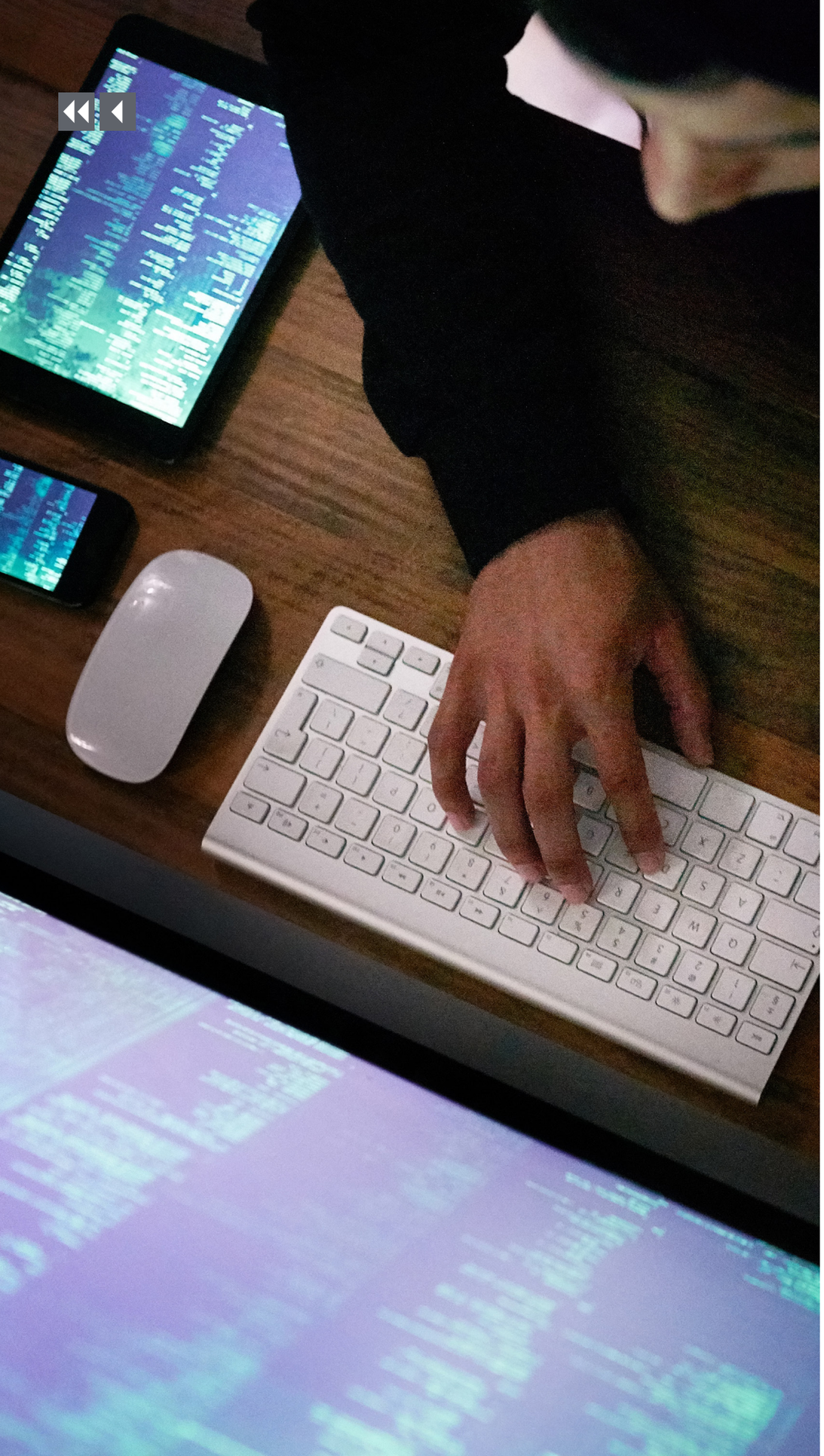
이제 매크로 분할을 살펴보겠습니다. 이 접근 방식만 사용할 때의 문제는 모든 트래픽이 인증 및 권한 부여를 위해 방화벽을 통과해야 하므로 방화벽에 병목 현상이 발생하게 됩니다. 이로 인해 성능 문제가 발생할 수 있습니다. 배포 계층에 더 많은 방화벽을 배포할 수 있지만 방화벽은 유선 속도가 아니기 때문에 비용이 많이 들고 성능이 반드시 향상되지 않을 수도 있습니다. 또한 현재 정책을 최신 상태로 유지해야 하는 여러 정책 시행 지점과 여러 위치가 있어 관리하기가 번거롭습니다.

마이크로 세분화만 사용하는 다른 옵션도 문제가 됩니다. NAC 정책을 통해 유일한 정책 적용이 수행되면 정책 목록이 길고 복잡해지고 장치 용량 제한을 소모시킬 수 있습니다.

결론은 이 두 가지 형태의 세분화 사이에 균형을 유지하는 것이 더 낫다는 것입니다. 방화벽이 서로 다른 세그먼트 간의 트래픽(수직)을 제어할 수 있으며 NAC 정책은 지정된 세그먼트(측면) 내의 트래픽을 제어합니다.

이 두 가지를 결합하여 한 보안 세그먼트에서 다른 보안 세그먼트로 유출되는 보안 위협과 동일한 세그먼트에서 옆으로 이동하는 보안 위협에 대처할 수 있습니다. 좀 더 구체적으로 말하면, 마이크로 세분화는 카메라 손상에 성공한 공격자가 보안 침해를 피봇으로 사용하여 도어록과 같은 다른 리소스를 손상시키는 것을 막는 것입니다.

목표는 모든 연결을 인증하고 각 사용자 또는 장치에 권한을 할당하는 것입니다. 이는 분할을 사용하여 측면 이동을 통한 위협 전파를 방지하고 규정을 준수하지 않는 모든 사용자 또는 장치를 지속적으로 모니터링하고 격리하는 것을 의미합니다.



도달 방법

초기 단계부터 마이크로 세분화를 사용하여 제로 트러스트 아키텍처를 구축하는 것은 미개발 환경에서 비교적 쉬울 것입니다. 그러나 브라운필드 상황에서 마이크로 세분화로 네트워크를 개조하면 인증 실패 또는 불완전한 정책으로 인해 사용자, 장치 및 애플리케이션이 네트워크에서 잠길 수 있습니다. 기업이 단일 리프레시 주기로 한 번에 마이그레이션할 수 있다는 것은 어렵거나 가능성이 낮습니다.

브라운필드 환경에서는 비제로 트러스트와 제로 트러스트 아키텍처가 공존하는 기간이 있으며 마이그레이션은 한 번에 한 계층 또는 한 위치에서 발생합니다. 중요한 것은 배포하는 인프라 요소와 배포 방식이 유연하고 다른 인프라 요소가 준비되었을 때 제로 트러스트 또는 마이크로 세분화 모드에서 작동할 수 있는지 확인하는 것입니다. 이는 인프라가 기존 및 미래 구성 요소와 상호 운용되어야 함을 의미합니다.

방법론

제로 트러스트 아키텍처에는 모니터링, 검증 및 평가, 계획, 시뮬레이션 및 시행의 5 단계가 있습니다.

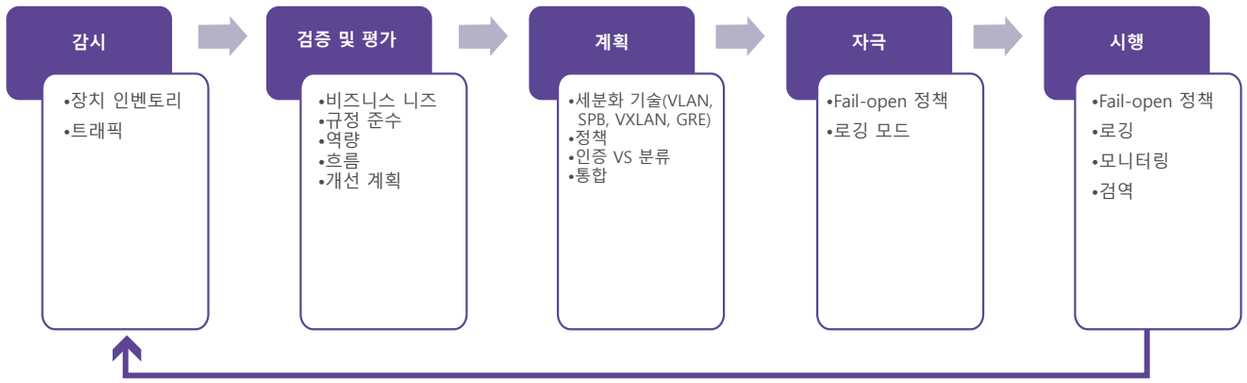


그림 1 - 방법론

1단계: 모니터링

다른 작업을 수행하기 전에 네트워크에 있는 항목의 지도와 인벤토리를 모니터링하고 구축하기 시작해야 합니다.

ZTA로 마이그레이션하려면 자산(물리적 및 가상), 주제(사용자 권한 포함), 네트워크에 연결된 비즈니스 프로세스에 대한 자세한 지식이 필요합니다. 불완전한 지식은 정보 부족으로 인해 액세스가 거부되는 실패로 이어지는 경우가 많습니다. 이는 조직 내에 알려지지 않은 "섀도우 IT" 또는 "섀도우 IoT"가 있는 경우 특히 문제입니다.

장치 및 트래픽 흐름 모니터링을 시작합니다. 장치 유형, 제조업체, 모델, 운영 체제별로 분류된 네트워크에서 볼 수 있는 모든 장치로 인벤토리 보고서를 생성합니다. 보고서에는 장치가 마지막으로 본 스위치 포트 또는 SSID도 표시되어야 합니다. 이 정보는 MAC 주소, DHCP 서명 및 HTTP 사용자 에이전트와 같은 요소에서 수집할 수 있습니다.

대부분의 타사 도구는 장비 유형이 아닌 IP 주소만 제공합니다. 각 유형의 장치에 대한 빠르고 쉬운 NAC 프로필 생성을 용이하게 하기 위해 IoT/장치 인벤토리를 생성하는 도구를 갖는 것이 이상적입니다.

정책 생성에 필요한 다른 정보는 트래픽 흐름입니다. 보유하고 있는 장비에 따라 sFlow, Netflow 또는 DPI(Deep Packet Inspection)와 같은 흐름 모니터링 도구에서 이 정보를 얻을 수 있습니다.

이 프로세스는 반복됩니다. 모니터링을 처음 활성화하면 보고서가 의미가 없을 수 있지만 다른 단계로 진행하면 보고서가 더 구체적이고 유용해집니다. 이 단계에서 수집한 정보는 다음 단계의 핵심이 됩니다.

2단계: 검증 및 평가

다음 단계는 이러한 결과를 검증하는 것입니다. 비즈니스 요구 사항을 평가합니다. 정당화될 수 없는 모든 섀도 IoT는 공격 표면을 불필요하게 증가시키므로 제거해야 합니다. 나머지는 정책에 반영해야 하므로 주체(사용자 및 장치), 트래픽 흐름 및 워크플로를 식별해야 합니다. 예를 들어 특정 자산에 액세스할 수 있는 사람과 해당 자산으로 수행할 수 있는 작업이 있습니다. 최소 권한 원칙을 적용합니다.

마이크로 세분화는 암호 정책이나 펌웨어 업데이트와 같은 다른 보안 정책을 완화하는 것을 의미하지 않습니다. 개인의 권한도 평가돼야 합니다. 이러한 장치가 인증서 기반 인증을 지원할 수 있습니까? 해당 인증서를 발급 및 적용할 수 있는 관리 도구가 있습니까? 필요한 트래픽 흐름은 무엇입니까? 제조업체로부터 이 정보를 얻어야 할 수도 있지만 자신의 트래픽 분석 보고서와 대조해야 합니다. 회사 정책을 준수하지 않는 자산을 발견한 경우 자산이 규정을 준수하도록 수정 계획이 필요합니다. 그렇지 않으면 추가 제어를 적소에 배치해야 합니다.

3단계: 계획

이 단계에서는 자산, 주제(사용자), 트래픽 및 워크플로를 이미 알고 있습니다. 이제 이 지식을 인증 및 보안 정책으로 전환하여 필요한 마이크로 세분화 아키텍처를 구현해야 합니다. 이전에 언급했듯이 최상의 결과를 얻으려면 매크로 및 마이크로 세분화의 조합을 포함해야 합니다. 대부분의 브라운필드 시나리오에서는 이미 존재하는 아키텍처에 의해 제약을 받을 것이라는 점을 기억하십시오.

매크로 세분화의 경우 VLAN, VRF, SPB VPN, VXLAN 또는 GRE 터널과 같은 여러 옵션과 사설 VLAN과 같은 특수 기능이 있습니다. 이들 각각에는 장단점이 있으며 다양한 상황에서 유용할 수 있습니다. 마이크로 세분화의 경우 각 사용자 또는 장치 유형에 대해 프로필에 포함할 정책을 알아야 합니다. 마지막으로 사용자와 장치를 해당 세그먼트 및 정책에 매핑하는 방법을 정의해야 합니다. 이것은 장치 지문을 포함할 수 있는 인증 또는 분류로 귀결됩니다.

이상적으로는 네트워크 프로필을 쉽게 업데이트할 수 있도록 유연한 인증 정책을 생성할 수 있는 기술(소프트웨어 정의 세분화)에 투자해야 합니다.

다음 순서로 인증 흐름을 설계하는 것이 좋습니다.

1. RADIUS 서버를 사용하는 802.1x 인증서를 통한 인증. 인증은 인증 레코드를 생성합니다. 방화벽과 공유할 수 있는 정보입니다.
2. 802.1x 인증서를 통해 장치를 인증할 수 없으면 다음으로 MAC 인증을 시도해야 합니다. MAC 인증은 802.1x만큼 안전하지는 않지만 전혀 인증하지 않는 것보다는 낫습니다. 802.1x로 진행할 준비가 될 때까지 사용하십시오.
3. 프로필이 반환되지 않으면 프로필 세그먼트 및 규칙에 매핑하는 데 사용할 수도 있는 지문을 시도할 수 있습니다. 이것은 인증 또는 계정 기록을 생성하지 않지만 IoT 인벤토리 데이터베이스에 등록됩니다.
4. 마지막으로 프로필이 반환되지 않거나 다른 모든 것이 실패하는 경우를 대비하여 기본 "catch all"을 설정할 수 있습니다. 초기 단계에서는 여전히 동일한 세그먼트 및 규칙으로 연결되고 인벤토리 데이터베이스에 장치를 기록하는 프로필에 장치를 매핑해야 합니다.

이 흐름은 진행하면서 조정할 수 있도록 유연한 방식으로 구성되어야 합니다. 예를 들어 처음에는 MAC 인증을 제거하고 인벤토리 보고서에서 MAC 주소 목록을 얻은 후 나중에 추가할 수 있습니다. 또한, 프로세스를 세분화하면서 기본 프로필에 연결된 세그먼트 및 규칙을 배스천 호스트에만 액세스할 수 있는 매우 제한적인 규칙으로 변경할 수 있습니다.

방화벽 규칙이 서브넷/IP 주소가 아닌 장치 역할을 기반으로 할 수 있도록 장치 역할을 방화벽과 공유할 수도 있습니다. 이 통합의 장점은 두 가지입니다. 첫째, 방화벽은 이러한 IoT 장치에 세분화된 정책을 적용할 수 있습니다. 둘째, 방화벽 정책은 이제 사용자 또는 역할 기반이므로 더 이상 서브넷이나 IP 주소에 연결되지 않으므로 향후 네트워크를 재설계하고 재분할할 수 있습니다.

이 프로세스는 반복적이며 인증 및 세분화 사용이 더 성숙해짐에 따라 조정, 조정 및 개선해야 합니다.

4단계: 시뮬레이션

아무리 많은 계획을 세운다 해도 처음에는 제대로 이루어지지 않을 것입니다. 인증 체계 설계의 모든 오류, 보안 정책 "허용 목록"의 누락으로 인해 비즈니스 프로세스가 중단됩니다. "fail-open" 모드에서 인증 및 액세스 정책을 적용해야 합니다. 이것이 의미하는 바는 인증에 실패한 장치와 사용자가 네트워크에서 계속 허용되고 예기치 않은 트래픽 흐름이 계속 허용된다는 것입니다. 그러나 이 모든 것이 기록되고 이 로그를 사용하여 인증 및 정책 체계를 구체화할 수 있습니다.

5단계: 시행

미세 조정 후에는 더 이상 인증 실패 또는 합법적 플로우 거부가 관찰되지 않습니다. 그런 다음 해당 정책을 "fail-open"에서 "fail-close"로 이동할 수 있습니다. 즉, 불량 장치가 차단되고 예기치 않은 플로우가 중단됩니다.

물론 예상치 못한 장치와 트래픽 흐름을 계속 모니터링해야 하며 필요에 따라 전체 주기를 반복해야 합니다.

하나 더

지속적인 모니터링, 로깅 및 격리의 일환으로 외부 침입 탐지 시스템(IDS)에도 투자할 것을 권장합니다. 스위치 자체에서 직접 식별할 수 있는 다양한 DDoS(Distributed Denial of Service) 공격이 있지만 외부 IDS는 바이러스 또는 기타 이상 현상과 같은 광범위한 공격도 탐지할 수 있습니다. 몇 년 전 여러 대의 비디오 감시 카메라가 Mirai 멀웨어에 감염되었거나 이러한 장치가 Twitter, Spotify 또는 Paypal과 같은 서비스에 영향을 미치는 글로벌 DNS 서버에 대한 공동 공격을 시작한 날을 기억하고 있을 겁니다. 이러한 공격은 스위치에서 감지되지 않을 수 있지만 전용 IDS는 확실히 감지할 것입니다.

공격이 감지되면 IDS는 영향을 받는 장치의 IP 주소를 네트워크 관리 시스템(NMS)에 알립니다. 이상적으로는 NMS가 데이터베이스에서 이러한 장치를 찾을 수 있고 프로필을 "격리 역할"로 변경할 수 있습니다.

'격리 역할'은 매우 제한적인 역할이며 일반적으로 배스천 호스트와의 통신만 허용하므로 특히 강력한 비밀번호를 설정하거나 펌웨어를 업데이트하는 등의 방법으로 기기를 수정할 수 있습니다.

왜 ALE인가?

Alcatel-Lucent Enterprise 디지털 에이지 네트워킹 솔루션은 제로 트러스트 아키텍처를 향한 단계적 진화를 허용하는 동적 DPI NAC 정책과 강력하고 유연한 소프트웨어 정의 세분화를 통합합니다.

디지털 에이지 네트워킹은 기업과 조직이 디지털 에이지에 진입하고 디지털 비즈니스를 성장시킬 수 있도록 지원하는 Alcatel-Lucent Enterprise의 청사진입니다. 세 가지 축을 기반으로 합니다.

- 사람, 프로세스, 애플리케이션 및 개체를 쉽고 자동으로 안전하게 연결하는 자율 네트워크. ALE 자율 네트워크는 진정한 통합 관리 플랫폼으로 완성된 간소화된 포트폴리오를 기반으로 하며 LAN 및 WLAN 전반에 걸쳐 공통 보안 정책을 제공합니다. 자율 네트워크는 실내, 실외, 산업 환경에서 배포 유연성도 제공합니다. 네트워크 관리는 고객 선호도에 따라 온프레미스, 클라우드 또는 하이브리드 배포로 제공될 수 있습니다.
- 안전하고 효율적인 IoT 장치 온보딩: 세그멘테이션을 통해 장치를 전용 세그먼트에 보관하며 장치 및 네트워크가 손상될 위험을 최소화합니다. IoT 세그멘테이션은 장치가 제대로 작동하는지 여부를 기업이 쉽게 자동으로 이해하고 네트워크를 안전하게 유지하는 데 도움이 될 수 있습니다.
- 워크플로 자동화를 한 비즈니스 혁신: 사용자, 애플리케이션 및 IoT 메트릭스를 지오로케이션 데이터와 실시간으로 협업 플랫폼에 통합하여 새롭고, 자동화된 디지털 비즈니스 프로세스 및 위반이 발생하면 보안 및 네트워크 관리자에게 알리는 것을 포함하는 서비스의 생성과 출시를 단순화합니다.

귀사에 IoT/장치 인벤토리를 생성하는 도구가 있습니까? 애플리케이션 흐름을 모니터링할 수 있는 도구가 있습니까? 귀하의 현재 스위치와 무선 액세스 포인트는 소프트웨어 정의 세분화를 위해 준비되어 있습니까? 현재 이러한 도구가 없는 경우 당사에 문의해 주시면 도움을 드릴 수 있습니다.

우리가 확실히 아는 것

몇 가지 키 포인트를 정리하며 마무리 하겠습니다.

- 진정으로 효율적인 ZTA를 사용하려면 매크로 및 마이크로 세분화를 모두 사용해야 합니다.
- ZTA에는 모니터링, 검증 및 평가, 계획, 시뮬레이션 및 시행의 5단계가 있습니다.
- 마이크로 세분화를 기반으로 하는 ZTA는 다음과 같은 세 가지 원칙에 기반합니다. 인증, 802.1x EAP-TLS를 가장 중요한 표준으로 사용; 최소 권한 원칙으로 돌아가는 사용자 또는 장치 역할과 관련된 차별화된 정책 지속적인 모니터링 및 격리
- 하이브리드 및 모바일 환경에서 마이크로 세분화는 소프트웨어 정의여야 합니다. 즉, 정적으로 정의되지 않고 동적 및 정책 기반이어야 합니다. 그렇지 않으면 비실용적입니다.

마이크로 세분화를 통해 ZTA로 마이그레이션하는 것은 프로세스이므로 규모가 큰 기업이 단일 리프레시 주기에 도달할 가능성은 거의 없습니다. 그러나 모든 리프레시, 재설계 또는 지속적인 개선 주기에서 올바른 인프라와 설계를 제자리에 배치하면 해당 목표에 더 가까워질 수 있습니다.

Alcatel-Lucent Enterprise는 조직이 디지털 전환을 통해 비즈니스 잠재력을 실현할 수 있도록 지원하는 네트워킹 기술과 솔루션을 개발하는 데 전념하고 있습니다.

Alcatel·Lucent Enterprise