머신 액세스 제한의 장단점 이해

목차

소개

이 문서에서는 MAR(Machine Access Restriction)에 발생한 문제에 대해 설명하고 그 해결책을 제공합니다.

사전 요구 사항

개인 소유 장치가 증가함에 따라 시스템 관리자는 회사 소유 자산에 대해서만 네트워크의 특정 부분에 대한 액세스를 제한할 수 있는 방법을 제공하는 것이 더욱 중요합니다. 이 문서에 설명된 문제는 이러한 문제 영역을 안전하게 식별하고 사용자 연결에 지장을 주지 않고 인증하는 방법에 관한 것입니다.

요구 사항

Cisco에서는 이 문서를 완전히 이해하기 위해 802.1X에 대한 지식을 갖춘 것이 좋습니다. 이 문서에서는 사용자 802.1X 인증에 익숙하다고 가정하고 MAR 사용, 더 일반적으로 머신 인증과 관련된 문제와 이점을 강조합니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제

MAR은 기본적으로 대부분의 현재 및 널리 사용되는 EAP(Extensible Authentication Protocol) 방법에 내재하는 공통 문제를 해결하려고 합니다. 즉, 머신 인증과 사용자 인증은 별도의 관련 없는 프로세스입니다.

사용자 인증은 대부분의 시스템 관리자에게 친숙한 802.1x 인증 방법입니다. 아이디어는 자격 증명(사용자 이름/비밀번호)이 각 사용자에게 주어지고, 해당 자격 증명 집합은 실제 사람을 나타냅니다(여러 사람 간에도 공유 가능). 따라서 사용자는 네트워크의 어느 곳에서든 이러한 자격 증명을 사용하여 로그인할 수 있습니다.

머신 인증은 기술적으로 동일하지만, 일반적으로 사용자에게 자격 증명(또는 인증서)을 입력하라는 메시지가 표시되지 않습니다. 컴퓨터나 머신이 자체적으로 이를 수행합니다. 이 경우 시스템에 자격 증명이 이미 저장되어 있어야 합니다. 전송된 사용자 이름은 host/<MyPCHostname>입니다. 단, 시스템에 <MyPCHostname>이(가) 호스트 이름으로 설정되어 있습니다. 즉, 호스트 /호스트 이름을 차례로 전송합니다.

Microsoft Windows 및 Cisco Active Directory와 직접 관련되지는 않지만 컴퓨터 호스트 이름이 도메인 데이터베이스에 추가되고 자격 증명이 협상되고(기본적으로 30일마다 갱신됨) 시스템에 저장되므로 컴퓨터가 Active Directory에 조인된 경우 이 프로세스가 더 쉽게 렌더링됩니다. 즉, 모든 유형의 디바이스에서 머신 인증이 가능하지만, 머신이 Active Directory에 가입되어 있고 자격 증명이 사용자에게 숨겨져 있는 경우 훨씬 더 쉽고 투명하게 렌더링됩니다.

솔루션으로서의 MAR

Cisco ACS(Access Control System) 또는 Cisco ISE(Identity Services Engine)가 MAR을 완료하기 위한 솔루션이라고 쉽게 말할 수 있지만, 이를 구현하기 전에 고려해야 할 장점과 단점이 있습니다. 이를 구현하는 방법은 ACS 또는 ISE 사용 설명서에 가장 잘 설명되어 있으므로, 이 문서에서는 고려 여부와 몇 가지 가능한 장애물에 대해 간단히 설명합니다.

장점

MAR은 사용자와 머신 인증이 완전히 분리되어 있기 때문에 발명되었습니다. 따라서 RADIUS 서버는 사용자가 회사 소유 디바이스에서 로그인해야 하는 확인을 시행할 수 없습니다. MAR을 사용하는 경우 RADIUS 서버(Cisco 측 ACS 또는 ISE)는 지정된 사용자 인증을 위해 동일한 엔드포인트에 대한 사용자 인증 앞에 X시간(일반적으로 8시간) 내에 유효한 머신 인증이 있어야 하지만 이는 구성 가능합니다)하도록 적용합니다.

따라서 머신 자격 증명이 RADIUS 서버에 의해 알려지면 머신 인증이 성공합니다. 일반적으로 머신이 도메인에 가입되어 있고 RADIUS 서버가 도메인에 대한 연결을 통해 이를 확인합니다. 성공적인 머신 인증이 네트워크에 대한 전체 액세스를 제공하는지 아니면 제한된 액세스만 제공하는지를 결정하는 것은 전적으로 네트워크 관리자의 책임입니다. 일반적으로 적어도 클라이언트와 Active Directory 간의 연결을 열어 클라이언트가 사용자 암호 갱신 또는 GPO(그룹 정책 개체) 다운로드와 같은 작업을 수행할 수 있도록 합니다.

사용자 인증이 이전 몇 시간 동안 머신 인증이 발생하지 않은 디바이스에서 온 경우, 사용자가 정상적으로 유효한 경우에도 사용자는 거부됩니다.

전체 액세스 권한은 지난 몇 시간 동안 머신 인증이 발생한 엔드포인트에서 인증이 유효하고 완료된 경우에만 사용자에게 부여됩니다.

더 컨스

이 섹션에서는 MAR 사용의 단점에 대해 설명합니다.

MAR 및 Microsoft Windows 서플리컨트

MAR의 아이디어는 사용자 인증이 성공하려면 해당 사용자에게 유효한 자격 증명이 있어야 할 뿐만 아니라 해당 클라이언트에서 머신 인증에 성공해야 한다는 것입니다. 여기에 문제가 있으면 사용자는 인증할 수 없습니다. 이 기능은 때때로 합법적인 클라이언트를 실수로 잠글 수 있으며, 이로 인해 네트워크에 대한 액세스 권한을 다시 얻기 위해 클라이언트를 재부팅해야 합니다.

Microsoft Windows는 부팅 시(로그인 화면이 나타나는 경우)에만 머신 인증을 수행합니다. 사용자가 사용자 자격 증명을 입력하는 즉시 사용자 인증이 수행됩니다. 또한 사용자가 로그오프하면(로그인 화면으로 돌아가기) 새 머신 인증이 수행됩니다.

다음은 MAR이 때때로 문제를 일으키는 이유를 보여 주는 예시 시나리오입니다.

사용자 X는 무선 연결을 통해 연결된 노트북 컴퓨터에서 하루 종일 작업했습니다. 하루 일과가 끝나면 그는 간단히 노트북을 닫고 퇴근한다. 그러면 랩톱이 최대 절전 모드로 전환됩니다. 다음 날, 그는 사무실로 돌아와 그의 노트북을 엽니다. 이제 무선 연결을 설정할 수 없습니다.

Microsoft Windows에서 절전 모드를 해제하면 로그인한 사용자의 컨텍스트가 포함된 현재 상태의 시스템 스냅샷을 가져옵니다. 하룻밤 사이에 사용자 랩톱에 대한 MAR 캐시 항목이 만료되고 삭제됩니다. 그러나 노트북 컴퓨터의 전원이 켜져 있으면 머신 인증이 수행되지 않습니다. 대신 사용자 인증으로 바로 이동합니다. 최대 절전 모드가 기록된 내용이기 때문입니다. 이 문제를 해결하는 유일한 방법은 사용자를 로그오프하거나 컴퓨터를 재부팅하는 것입니다.

MAR은 좋은 기능이지만 네트워크 중단을 초래할 수 있습니다. 이러한 중단은 MAR의 작동 방식을 이해할 때까지 해결하기 어렵습니다. MAR을 구현할 때 컴퓨터를 올바르게 종료하고 매일 모든 시스템에서 로그오프하는 방법에 대해 최종 사용자에게 교육하는 것이 중요합니다.

MAR 및 다양한 RADIUS 서버

로드 밸런싱 및 이중화를 위해 네트워크에 여러 RADIUS 서버를 두는 것이 일반적입니다. 그러나 모든 RADIUS 서버가 공유 MAR 세션 캐시를 지원하지는 않습니다. ACS 버전 5.4 이상 및 ISE 버전 2.3 이상에서만 노드 간 MAR 캐시 동기화를 지원합니다. 이 버전 이전에는 서로 일치하지 않으므로 한 ACS/ISE 서버에 대해 머신 인증을 수행하고 다른 서버에 대해 사용자 인증을 수행할 수 없습니다.

MAR 및 유무선 스위칭

많은 RADIUS 서버의 MAR 캐시는 MAC 주소를 사용합니다. 이것은 단순히 랩톱의 MAC 주소 및 마지막으로 성공한 머신 인증의 타임스탬프가 포함된 테이블입니다. 이렇게 하면 서버는 클라이언트가 지난 X시간 동안 머신 인증되었는지 여부를 알 수 있습니다.

그러나 유선 연결로 랩톱을 부팅한 다음(유선 MAC에서 머신 인증을 수행) 낮에 무선으로 전환하면 어떻게 됩니까? RADIUS 서버에는 무선 MAC 주소를 유선 MAC 주소와 상호 연결하고 지난 X시간 동안 머신 인증을 받았음을 확인할 수 있는 수단이 없습니다. 유일한 방법은 로그오프하고 Microsoft Windows에서 무선을 통해 다른 시스템 인증을 수행하도록 하는 것입니다.

솔루션

Cisco AnyConnect는 여러 가지 기능 중에서 머신 및 사용자 인증을 트리거하는 사전 구성된 프로파일의 이점을 제공합니다. 그러나 Microsoft Windows 신청자에 표시된 것과 동일한 제한 사항이 있으며, 시스템 인증은 로그오프하거나 재부팅할 때만 발생합니다.

또한 AnyConnect 버전 3.1 이상에서는 EAP 체인으로 EAP-FAST를 수행할 수 있습니다. 이는 기본적으로 단일 인증이며, 머신 사용자 이름/비밀번호와 사용자 사용자 이름/비밀번호 두 쌍의 자격 증명을 동시에 전송합니다. 그러면 ISE는 두 가지가 모두 성공적인지 더 쉽게 확인할 수 있습니다. 캐시가 사용되지 않고 이전 세션을 검색할 필요가 없으므로 안정성이 향상됩니다.

PC가 부팅되면 사용자 정보를 사용할 수 없으므로 AnyConnect에서 머신 인증만 전송합니다. 그러나 사용자 로그인 시 AnyConnect는 머신 및 사용자 자격 증명을 동시에 전송합니다. 또한 연결이 끊어지거나 케이블의 플러그를 뽑거나 다시 뽑으면 머신 및 사용자 자격 증명 모두 단일 EAP-FAST 인증으로 다시 전송됩니다. 이는 EAP 체인이 없는 이전 버전의 AnyConnect와 다릅니다.

EAP-TEAP는 특히 이러한 유형의 인증을 지원하기 위해 만들어진 장기적으로 가장 좋은 솔루션이지만, EAP-TEAP는 현재 많은 OS의 네이티브 서 플리 컨 트에서 지원 되지 않습니다

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.