Secure Access 클라이언트 기반 ZTA Posture 컨피그레이션 및 동작 사양

목차

문제

인터넷 액세스에 사용할 때 Cisco Secure Access 클라이언트 기반 ZTA(Zero Trust Access) 상태 기능의 특정 동작 및 구성 기능에 대한 질문이 제기되었습니다. 구체적인 우려 사항은 다음과 같습니다.

- 운영 체제 포스처 요구 사항이 필수 OS 버전을 충족하지 않더라도 디바이스가 ZTA 모듈을 사용하여 인터넷 대상에 액세스할 수 있는 최대 365일의 구성 가능한 유예 기간을 지원하는지 여부.
- 운영 체제 이외의 상태 요구 사항(방화벽, 시스템 비밀번호 등)이 충족되지 않을 경우 목적지 액세스를 즉시 차단할지 여부.
- 보안 액세스 GUI 인터페이스를 통해 포스처 요건 실패에 대해 사용자 지정 경고 메시지 또는 차단 이외의 작업(예: 모니터링)을 구성할 수 있는지 여부.

환경

- ZTNA(Zero Trust Access) 기능이 포함된 Cisco Secure Access
- 클라이언트 기반 ZTA 상태 구현
- 인터넷 액세스 활용 사례 시나리오
- 운영 체제, 방화벽 및 시스템 비밀번호 조건을 포함한 상태 요구 사항

해결

Secure Access 클라이언트 기반 ZTA 상태 동작 및 컨피그레이션 기능에 대해서는 다음 섹션에서 설명하는 설명이 제공되었습니다.

운영 체제 상태 유예 기간

설명된 운영 체제 포스처 요구 사항 동작이 정확합니다. 운영 체제 포스처 조건이 구성되면 최대 365일의 구성 가능한 유예 기간을 지원합니다. 이 유예 기간 동안 필요한 OS 버전을 충족하지 않는 디바이스는 대상 버전으로 업그레이드하는 동안 ZTA 모듈을 사용하여 인터넷 대상에 액세스할 수 있습니다.

비 운영 체제 상태 요구 사항

운영 체제 이외의 상태 조건(예: 방화벽, 시스템 비밀번호 및 기타 보안 제어)의 경우 이러한 요구 사항이 충족되지 않으면 대상에 대한 액세스가 즉시 차단됩니다. 이러한 포스처 유형은 운영 체제 요구 사항에 사용할 수 있는 유예 기간 기능을 지원하지 않습니다.

상태 실패 작업 및 사용자 지정 메시지

포스처 요구 사항 실패에 대한 작업은 액세스 정책 컨피그레이션을 통해 제어됩니다.

액세스 정책은 다음을 비롯한 여러 작업 유형을 지원합니다.

- 허용
- 차단
- 경고
- 격리

액세스 정책 보안 프로파일 설정을 통해 상태 실패에 대한 사용자 지정 경고 메시지 및 알림 페이지를 구성할 수 있습니다. 경고 및 알림 페이지 관리는 Manage Notification Pages(알림 페이지 관리) 문서 및 컨피그레이션 인터페이스를 통해 처리됩니다.

즉 차단 이외의 작업(예: 경고 작업을 통한 모니터링)을 사용할 수 있으며 차단 작업만 가능했다는

초기 평가와 달리 구성할 수 있습니다.

원인

이러한 질문은 운영 체제 상태 요구 사항과 기타 상태 유형 간의 구체적인 행동 차이를 이해하고, 보안 액세스 GUI 인터페이스에서 즉시 확인할 수 없는 상태 오류 처리를 위해 사용 가능한 컨피그레이션 옵션을 명확히 해야 하는 필요성에서 비롯되었습니다.

관련 콘텐츠

- 보안 액세스를 위한 알림 페이지 문서 관리
- Cisco 기술 지원 및 다운로드

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.