보안 액세스 애플리케이션 프로토콜 차단으로 인터넷 연결 방지

목차

- 문제
- 환경
- 해결
  - 1단계: 차단 규칙 식별
  - 2단계: 응용 프로그램 설정 수정
  - 3단계: 변경 사항 적용 및 확인
- 원인
- 관련 콘텐츠

문제

Cisco Secure Access로 마이그레이션한 후 웹 서비스에 액세스하려고 할 때 인터넷 연결이 차단되었습니다. 특정 증상은 HTTP 트래픽이 보안 정책에 의해 차단되어 합법적인 웹 사이트 및 애플리케이션에 액세스하지 못하게 되는 것과 관련이 있습니다.

차단 이벤트 세부 정보에는 다음과 같은 특성이 있습니다.

- 작업: 차단됨
- 이벤트 차단 사유: AC_RULE_MATCH_BLOCK
- 대상: http://www.bing.com/api/shopping/v1/user/shoppingsettings
- 대상 포트: 443

- 범주: 분류되지 않음
- 애플리케이션 범주: 검색
- 애플리케이션 프로토콜: 하이퍼텍스트 전송 프로토콜
- 프로토콜: TCP

환경

- Cisco Secure Access 구축
- 애플리케이션 프로토콜 제한이 있는 활성 보안 정책

해결

이 해결 방법에서는 HTTP 애플리케이션 프로토콜 트래픽을 허용하면서 신뢰할 수 없는 애플리케이션에 대한 보안 상태를 유지하도록 보안 규칙 컨피그레이션을 수정하는 것이 포함됩니다.

1단계: 차단 규칙 식별

Secure Access 관리 인터페이스에서 차단을 유발하는 특정 규칙을 찾습니다.

- 규칙 이름: 테스트
- 현재 구성: Application Settings Block을 대상으로 사용

2단계: 응용 프로그램 설정 수정

규칙 구성에 액세스하고 Destination(대상)에서 Application Settings(애플리케이션 설정)의 이름을 확인합니다.

- Resources(리소스) > Internet and SaaS resources(인터넷 및 SaaS 리소스) > Application Lists(애플리케이션 목록)로 이동합니다. 그런 다음 애플리케이션을 클릭합니다.
- 애플리케이션 프로토콜 설정을 찾습니다.
- 차단된 애플리케이션 프로토콜 목록에서 HTTP의 선택을 취소하거나 제거합니다.
- 신뢰할 수 없는 실제 응용 프로그램에 대해 다른 보안 제어를 유지해야 합니다.

3단계: 변경 사항 적용 및 확인

규칙 수정 사항을 저장하고 연결을 테스트합니다.

1.- 활성 정책에 컨피그레이션 변경 사항을 적용합니다.

2.- 이전에 차단된 대상에 대한 인터넷 연결을 테스트합니다.

3. - 이제 합법적인 HTTP 트래픽이 허용되는지 확인하기 위해 보안 로그를 모니터링합니다.

4.- 다른 보안 보호가 계속 유효한지 확인합니다.

원인

근본 원인은 Cisco Secure Access의 보안 규칙 컨피그레이션이 지나치게 제한적이었기 때문입니다. 규칙은 모든 HTTP 애플리케이션 프로토콜 트래픽을 차단하도록 구성되었으며, 이로 인해 합법적인 웹 브라우징 및 애플리케이션 액세스가 차단되었습니다. HTTP 프로토콜 차단의 광범위한 애플리케이션은 합법적인 웹 서비스에 액세스하는 사용자 및 HTTP/HTTPS 프로토콜을 사용하는 애플리케이션에 영향을 미쳐 정상적인 인터넷 연결에 영향을 미쳤습니다.

관련 콘텐츠

- 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.