Umbrella 프록시가 Ninja 애플리케이션 연결을 차단합니다.

목차

문제

사용자는 Cisco Umbrella를 통해 연결된 경우 다운로드한 설정 파일을 사용하여 원격 시스템을 실행할 수 없습니다. 응용 프로그램이 Umbrella 보호에서 작동하지 않으며 특히 원격 시스템에 대한 액세스에 영향을 미칩니다. Cisco Umbrella 프록시가 비활성화되면 동일한 원격 시스템이 문제 없이 완벽하게 작동합니다.

트러블슈팅 시도에는 시스템 보안 및 대상이 ANY로 설정되었지만 문제가 지속되는 별도의 정책을 사용한 테스트가 포함되었습니다. 또한 ZTA(Zero Trust Access)를 통한 트래픽 라우팅도 시도했지만 문제는 변경되지 않았습니다. TCP/443의 보안 액세스를 통해 트래픽이 허용되었지만 엔드포인트에서 연결이 여전히 차단되었습니다.

환경

- 프록시 기능이 활성화된 Cisco Umbrella
- ZTA(Zero Trust Access) 컨피그레이션
- TCP/443 트래픽에 대해 구성된 보안 액세스 정책

해결

원격 액세스 애플리케이션에 대한 직접 연결을 허용하기 위해 Umbrella 프록시에서 특정 NinjaOne 관련 도메인을 제외하는 것이 해결책입니다.

1단계: 영향을 받는 도메인 식별

패킷 캡처 및 HAR 파일을 분석한 결과 NinjaOne 관련 도메인이 Umbrella 프록시의 영향을 받고 있음을 알 수 있습니다.

- ninjarmm.net을 참조하십시오.
- ninjarmm.com
- app.ninjarmm.com
- ninjaone.com
- agent-app.ninjaone.com

2단계: 도메인 예외 구성

식별된 도메인을 SWG(Secure Web Gateway) 인터넷 보안 정책 및 ZTA 인터넷 트래픽 조정에서 모두 제외합니다. 이 컨피그레이션 변경을 통해 이러한 도메인은 Umbrella 프록시를 우회하고 직접 연결을 설정할 수 있습니다.


참고: DND(Do Not Decrypt) 목록 컨피그레이션은 이 문제를 해결하는 데 효과가 없는 것으로 관찰되었습니다. 트래픽 조정 및 면제는 권장되는 방법입니다.

3단계: 구성 변경 사항 적용

프록시 처리에서 NinjaOne 관련 트래픽을 제외하려면 Umbrella 컨피그레이션에 도메인 예외를 구현합니다. 이렇게 하면 원격 액세스 애플리케이션이 필요한 서비스에 직접 연결할 수 있습니다.

4단계: 확인 검증

다른 트래픽에 대해 Umbrella 보호를 유지하면서 연결이 제대로 복원되도록 예외를 적용한 후 원격 액세스 애플리케이션 기능을 테스트합니다.

원인

이 문제는 트래픽이 Cisco Umbrella 프록시를 통해 라우팅될 때 NinjaOne 원격 액세스 애플리케이션이 프록시된 연결을 거부하기 때문에 발생합니다. 응용 프로그램이 제대로 작동하려면 특정 NinjaOne 도메인에 직접 연결해야 합니다. 이러한 연결이 Umbrella를 통해 프록시되는 경우 원격 액세스 서비스가 필요한 통신 채널을 설정할 수 없으므로 보안 정책이 트래픽을 허용하도록 구성된 경우에도 애플리케이션이 실패합니다.

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.