Secure Access Microsoft 365 호환성을 위한 우회 동작 기능 확인

목차

문제

Microsoft 365 호환성 기능이 활성화된 상태에서 Cisco Secure Access를 구성할 때 SWG(Secure Web Gateway) 처리 및 TLS 암호 해독에서 특정 Microsoft 관련 FQDN(Fully Qualified Domain Name)이 자동으로 우회되는지 여부가 불확실합니다. 특히, 이러한 도메인에 대한 우회 동작에 대한 설명이 필요합니다.

- do.dsp.mp.microsoft.com을 참조하십시오.
- dl.delivery.mp.microsoft.com을 참조하십시오.
- manage.microsoft.com

주요 관심사는 이러한 도메인에 Do Not Decrypt List를 수동으로 추가해야 하는지 또는 Microsoft 365 호환성이 활성화될 때 자동으로 제외되는지 여부를 중점적으로 살펴봅니다. 또한 SWG 레벨 우회 및 IPS 레벨 해독 설정 간의 상호 작용에 대한 혼란이 있습니다. 특히 설명서(Do Not Decrypt List configuration(목록 해독 안 함 컨피그레이션)에 나와 있는 manage.microsoft.com의 경우)는 여전히 필요할 수 있습니다.

환경

- Cisco 보안 액세스
- Microsoft 365 호환성 기능 사용
- SWG(Secure Web Gateway) 검사 및 TLS 암호 해독 구성
- 사용 중인 IPS 암호 해독 정책
- 연결이 필요한 Microsoft 관리 및 업데이트 서비스

해결

Microsoft 365 호환성 기능 동작은 다음과 같은 결과를 통해 실험실 테스트를 통해 확인되었습니다.

Microsoft 365 호환성 기능 범위

Microsoft 365 호환성 기능은 Microsoft의 엔드포인트 범주에서 "최적화" 및 "허용"으로 표시된 Microsoft 365 관련 도메인을 SWG 검사 및 정책 시행에서 제외합니다. 이렇게 하면 해당 도메인에 대한 트래픽이 SWG 레이어에서 변경되지 않은 상태로 통과할 수 있습니다.

실험실 테스트 결과

테스트는 Microsoft 365 호환성이 활성화된 통제된 랩 환경에서 수행되었습니다. 이 동작은 지정된 FQDN에 대해 관찰되었습니다.

1단계: Microsoft 365 호환성 기능 사용

Microsoft 365 호환성 기능이 보안 액세스 구성에서 활성화되었습니다.

2단계: 대상 FQDN에 대한 트래픽 테스트

표준 인터넷 브라우저를 사용하여 3개의 FQDN 각각에 대한 웹 트래픽이 생성되었습니다.

- do.dsp.mp.microsoft.com을 참조하십시오.
- dl.delivery.mp.microsoft.com을 참조하십시오.
- manage.microsoft.com

3단계: 대시보드에서 우회 동작 확인

Secure Access 대시보드를 분석한 결과, Microsoft 365 호환성 기능이 활성화된 경우 이러한 특정 대상에 대한 트래픽에 대해 웹 트래픽 검사 및 암호 해독이 수행되지 않는 것으로 확인되었습니다.

4단계: DNS 스티어링 동작 확인

이러한 대상에 대한 DNS 트래픽은 특정 DNS 제외가 구성되지 않는 한 문서화된 동작에 부합하는 Secure Access를 통해 계속 조정되었습니다.

주요 행동 분석 결과

테스트 결과 및 문서 분석을 기반으로 합니다.

- SWG 바이패스: Microsoft 365 호환성이 활성화된 경우 지정된 3개의 FQDN이 웹 트래픽 검사에서 우회됩니다.
- TLS 암호 해독: 이러한 도메인에 대한 해독은 SWG 레이어에서 우회됩니다.
- DNS 스티어링: DNS 쿼리는 명시적으로 면제되지 않는 한 Secure Access를 통해 계속 처리됩니다.
- 도메인 커버리지: 전체 도메인으로서 "*.microsoft.com"은 사양에서 완전히 우회되지 않지만 실제로 테스트된 특정 URL은 우회됩니다.

IPS 레이어 고려 사항

Microsoft 365 호환성 기능은 SWG 레이어에서 작동합니다. IPS 레벨 암호 해독 우회의 경우에도 수동 컨피그레이션이 필요할 수 있습니다.

- 이러한 도메인에 대해 IPS 해독 우회도 원하는 경우 Do Not Decrypt List를 수동으로 추가해야 할 수 있습니다.
- Do Not Decrypt List(Do Not Decrypt 목록)는 주로 SWG 처리가 아닌 IPS측 해독에 영향을 줍니다.
- 다음은 Microsoft 365 호환성이 활성화되어 있는 경우에도 설명서에서 Do Not Decrypt List에 manage.microsoft.com을 추가하는 것을 참조할 수 있는 이유를 설명합니다.

원인

Microsoft 365 호환성이 SWG 레벨 프로세싱에 영향을 미치는 Cisco Secure Access의 계층화된 아키텍처에서 혼란이 발생하며, IPS 암호 해독은 자체 구성 요구 사항이 있는 별도의 레이어로 작동합니다. Microsoft 365 호환성 기능에서는 Microsoft 도메인을 확인하기 위해 SWG 우회를 자동으로 처리하지만, IPS 암호 해독 정책에서는 Do Not Decrypt List(암호 해독 안 함 목록)를 통해 별도의 구성을 필요로 할 수 있습니다.

관련 콘텐츠

- Cisco Secure Access Microsoft 365 호환성 문서
- Cisco Secure Access에 대한 유효한 Do Not Decrypt 목록 생성
- 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.