Secure Web Appliance에서 Microsoft 업데이트 트래픽 우회

목차

소개

이 문서에서는 SWA(Secure Web Appliance)에서 Microsoft 업데이트 트래픽을 우회하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SWA 관리.

Cisco에서는 다음과 같은 툴을 설치하는 것이 좋습니다.

- 물리적 또는 가상 SWA
- SWA 그래픽 사용자 인터페이스(GUI)에 대한 관리 액세스

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 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

Microsoft 업데이트

Microsoft Updates는 운영 체제 및 소프트웨어 애플리케이션을 위해 Microsoft에서 릴리스하는 필수 패치, 보안 업데이트 및 기능 개선입니다. 이러한 업데이트는 컴퓨터와 네트워크 장치의 보안, 안정성 및 성능을 유지하는 데 매우 중요합니다. 또한 시스템이 취약점으로부터 보호되고, 버그가 수정되며, 새로운 기능이나 개선 사항이 소프트웨어에 통합됩니다.

Microsoft 업데이트가 Cisco SWA와 같은 프록시 서버에 미치는 영향은 매우 클 수 있습니다. 이러한 업데이트에는 대용량 파일 또는 다수의 소규모 파일 다운로드가 수반되는 경우가 많으며, 이로 인해 상당한 대역폭이 소모되고 프록시에서 리소스를 처리할 수 있습니다. 이로 인해 혼잡이 발생하고, 네트워크 성능이 저하되고, 프록시 인프라의 로드가 증가하여 전체 사용자 환경 및 기타 중요한 네트워크 운영에 영향을 미칠 수 있습니다.

프록시에서 Microsoft Update 트래픽을 우회하는 것은 이러한 문제를 관리하는 안전하고 효과적인 방법이 될 수 있습니다. Microsoft 업데이트는 신뢰할 수 있는 Microsoft 서버에서 제공되므로 이 트래픽이 프록시를 우회하도록 허용하면 네트워크 보안을 손상시키지 않고 프록시 서버의 로드를 줄일 수 있습니다. 이를 통해 필수 업데이트가 효율적으로 제공되면서 다른 보안 및 콘텐츠 필터링 작업을 위한 프록시 리소스가 보존됩니다. 그러나 이러한 우회 구성을 신중하게 구현하여 전반적인 네트워크 보안을 유지하고 조직 정책을 준수하는 것이 중요합니다.

Microsoft 업데이트 건너뛰기

Microsoft Updates 트래픽 프록시를 피하려는 경우 두 가지 주요 방법이 있습니다

1. Bypass: 트래픽을 리디렉션하여 SWA에 도달하지 않도록 네트워크를 구성하는 것이 포함됩니다.
2. 통과: 여기에는 Microsoft Updates 트래픽을 해독하거나 검사하지 않도록 SWA를 구성하여 검사 없이 프록시를 통과시키는 것이 포함됩니다.

SWA에서 트래픽 우회

SWA가 설치된 네트워크에서 Microsoft 업데이트 트래픽을 우회하려면 프록시 구축 설정에 따라 접근 방식이 달라집니다.

구축 유형	트래픽 우회
투명한 구축	트래픽을 프록시 서버로 전달하는 라우터나 레이어 4 스위치에서 Microsoft 업데이트 트래픽을 리디렉션할 수 있습니다.
	SWA GUI(그래픽 사용자 인터페이스) 내에서 직접 우회 설정을 구성할 수 있습니다.
명시적 구축	Microsoft Updates 트래픽이 SWA에 도달하지 못하도록 하려면 소스에서 바이패스를 구성해야 합니다. 이는 트래픽이

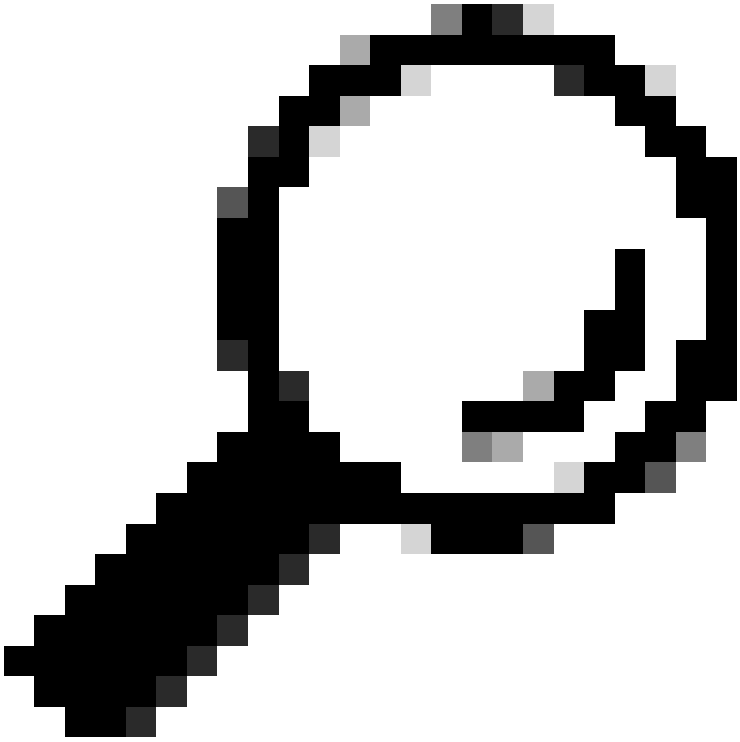
	SWA로 리디렉션되지 않도록 클라이언트 머신의 관련 URL을 제외하는 것을 의미합니다.

특정 트래픽을 우회하려면 광범위한 네트워크 재설계가 필요하며 이를 실행할 수 없는 경우, SWA가 특정 유형의 트래픽을 통과하도록 구성하는 방법이 대안입니다. 이는 SWA가 지정된 트래픽을 해독하거나 검사하지 않도록 설정하여 검사 없이 프록시를 통과하도록 허용함으로써 달성할 수 있습니다. 이 방법을 사용하면 네트워크 성능 및 프록시 리소스에 미치는 영향을 최소화하면서 필수 트래픽을 효율적으로 전달할 수 있습니다.

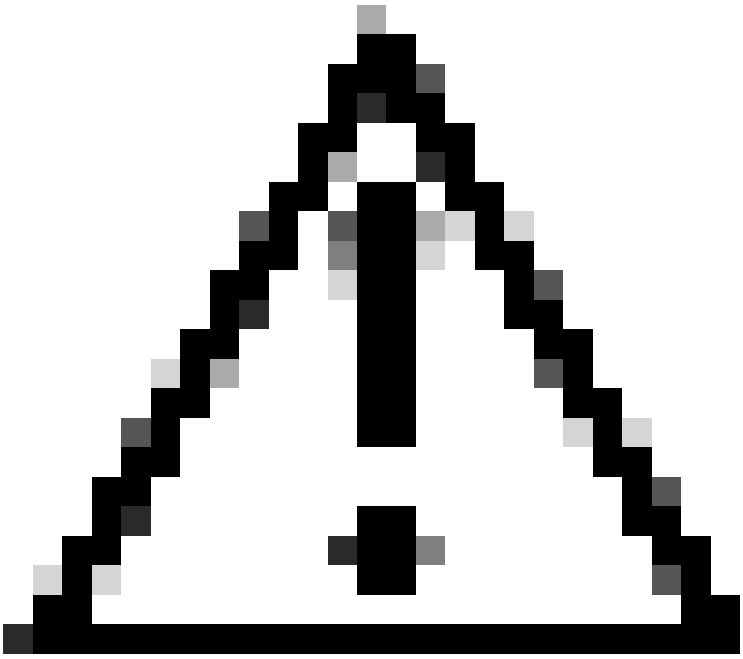
Microsoft 업데이트 통과 단계

Microsoft Updates 트래픽을 전달하는 네 가지 주요 단계가 있습니다.

단계	단계
1. Microsoft 업데이트 URL에 대한 사용자 지정 URL 범주를 만듭니다.	1단계.GUI에서 Web Security Manager를 선택한 다음 Custom and External URL Categories(사용자 지정 및 외부 URL 범주)를 클릭합니다. 2단계.Add Category(범주 추가)를 클릭하여 맞춤형 URL 범주를 추가합니다. 4단계.고유한 CategoryName을 할당합니다. 5단계. (선택 사항) 설명을 추가합니다. 6단계. List Order(목록 순서)에서 맨 위에 배치할 첫 번째 범주를 선택합니다. 7단계. Category Type(범주 유형) 드롭다운 목록에서 Local Custom Category(로컬 맞춤형 범주)를 선택합니다. 8단계. 사이트 섹션에 Microsoft 업데이트 URL을 추가합니다.



팁: 이 링크에서 Microsoft 업데이트 목록을 확인할 수 있습니다. 2단계 - WSUS 구성 | Microsoft Learn



주의: Microsoft Documents에서와 같이 URL을 복사/붙여넣지 말고 SWA 형식으로 올바르게 포맷하십시오. 자세한 내용은 Configure Custom URL Categories in Secure Web Appliance - Cisco를 참조하십시오.

	9단계. 제출합니다.
2. Microsoft 업데이트 트래픽을 인증에서 제외하기 위한 식별 프로필을 만듭니다	10단계.GUI에서 Web Security Manager를 선택한 다음 Identification Profiles(식별 프로필)를 클릭합니다. 11단계 프로파일 추가를 눌러 프로파일을 추가합니다. 12단계.Enable Identification Profile(식별 프로필 활성화) 확인란을 사용하여 이 프로필을 활성화하거나 삭제하지 않고 신속하게 비활성화합니다. 13단계.고유한 profileName을 할당합니다. 14단계. (선택 사항) 설명을 추가합니다. 15단계.Insert Above 드롭다운 목록에서 이 프로파일을 테이블에 표시할 위치를 선택합니다. 16단계. User Identification Method(사용자 식별 방법) 섹션에서 Exempt from authentication/identification(인증/식별에서 제외)을 선택합니다. 17단계.서브넷별 구성원 정의에서 특정 사용자에 대한 Microsoft 트래픽을 통과시키려면 적용할 IP 주소 또는 서브넷을 입력하거나, 모든 IP 주소를 포함하도록 이 필드를 비워 둡니다. 18단계. Advanced(고급) 섹션에서 Custom URL Categories(사용자 지정 URL 범주)를 선택합니다. 19단계. Microsoft 업데이트를 위해 만든 사용자 지정 URL 범주를 추가합니다. 20단계. 완료를 클릭합니다. 21단계. 제출합니다.
3. Microsoft 업데이트 트래픽을 통과하기 위한 암호 해독 정책을 만듭니다.	22단계.GUI에서 Web Security Manager(웹 보안 관리자)를 선택한 다음 Decryption Policy(암호 해독 정책)를 클릭합니다. 23단계. 암호 해독 정책을 추가하려면 Add Policy를 클릭합니다. 24단계.Enable Policy(정책 활성화) 확인란을 사용하여 이 정책을 활성화합니다. 25단계.고유한 PolicyName을 할당합니다. 26단계. (선택 사항) 설명을 추가합니다. 27단계.Insert Above Policy(정책 위에 삽입) 드롭다운 목록에서 첫 번째 정책을 선택합니다. 28단계.Identification Profiles and Users(식별 프로필 및 사용

	자)에서 이전 단계에서 생성한 식별 프로필을 선택합니다. 29단계. 제출합니다. 30단계.Decryption Policies(암호 해독 정책) 페이지의 URL Filtering(URL 필터링)에서 이 새 암호 해독 정책과 연결된 링크를 클릭합니다. 32단계Microsoft Updates URL 카테고리에 대한 작업으로 Passthrough를 선택합니다. 32단계. 제출합니다.
4. Microsoft 업데이트 트래픽을 허용하는 액세스 정책 만들기	33단계.GUI에서 Web Security Manager를 선택한 다음 Access Policy(액세스 정책)를 클릭합니다. 34단계. Add Policy(정책 추가)를 클릭하여 액세스 정책을 추가합니다. 35단계.Enable Policy(정책 활성화) 확인란을 사용하여 이 정책을 활성화합니다. 36단계.고유한 PolicyName을 할당합니다. 37단계. (선택 사항) 설명을 추가합니다. 38단계.Insert Above Policy(정책 위에 삽입) 드롭다운 목록에서 첫 번째 정책을 선택합니다. 39단계.Identification Profiles and Users(식별 프로필 및 사용자)에서 이전 단계에서 생성한 식별 프로필을 선택합니다. 40단계. 제출합니다. 9단계. Access Policies(액세스 정책) 페이지의 URL Filtering(URL 필터링)에서 이 새 액세스 정책과 연결된 링크를 클릭합니다 10단계.Microsoft 업데이트에 대해 만든 사용자 지정 URL 카테고리에 대한 작업 허용을 선택합니다. 11단계. 제출합니다. 12단계. 변경 사항을 커밋합니다.

관련 정보

- AsyncOS 15.0 for Cisco Secure Web Appliance 사용 설명서 - GD(일반 배포) - 정책 애플리케이션 최종 사용자 분류 [Cisco Secure Web Appliance] - Cisco
- Secure Web Appliance에서 맞춤형 URL 범주 구성 - Cisco

- Cisco WSA(Web Security Appliance)에서 Office 365 트래픽을 인증 및 암호 해독에서 제외하는 방법 - Cisco
- Use Secure Web Appliance 모범 사례 - Cisco
- Secure Web Appliance에서 인증 우회 - Cisco

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.