Secure Web Appliance에서 트래픽 차단

목차

소개

이 문서에서는 SWA(Secure Web Appliance)에서 트래픽을 차단하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SWA 관리.

Cisco에서는 다음과 같은 작업을 수행할 것을 권장합니다.

- 물리적 또는 가상 SWA가 설치되었습니다.
- SWA GUI(Graphical User Interface)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.

트래픽 차단

SWA에서 트래픽을 차단하는 것은 네트워크 보안을 보장하고, 내부 정책을 준수하며, 악의적인 활

동으로부터 보호하기 위한 중요한 단계입니다. 다음은 트래픽을 차단하는 몇 가지 일반적인 이유입니다.

소스별 차단 이유

- 단일 또는 다중 사용자에 의한 폴러딩: 한 명 이상의 사용자가 과도한 트래픽을 생성하면 네트워크가 마비되어 성능이 저하되고 서비스 중단이 발생할 수 있습니다.
- 응용 프로그램의 신뢰할 수 없는 리소스 액세스(User-Agents): 특정 응용 프로그램에서 신뢰할 수 없거나 잠재적으로 유해한 리소스에 액세스를 시도할 수 있습니다. 이러한 사용자 에이전트를 차단하면 보안 침해 및 데이터 유출을 방지할 수 있습니다.
- 특정 IP 범위에 대한 인터넷 액세스 제한: 일부 IP 주소 또는 범위는 보안 정책으로 인해 인터넷 액세스를 제한하거나 무단 사용을 방지하기 위해 필요할 수 있습니다.
- 의심스러운 트래픽 동작: 네트워크를 보호하려면 비정상적인 패턴 또는 동작을 보이는 트래픽이 악의적인 활동이나 보안 위협을 나타낼 수 있도록 차단해야 합니다.

목적지별 차단 이유

- 사내 정책 준수: 조직은 생산성과 법적 또는 규제 요구 사항의 준수를 보장하기 위해 특정 웹 사이트 또는 온라인 리소스에 대한 액세스를 제한하는 정책을 가지고 있는 경우가 많습니다.
- 신뢰할 수 없는 사이트: 신뢰할 수 없거나 잠재적으로 유해한 것으로 판단되는 웹 사이트에 대한 액세스를 차단하면 피싱, 악성코드 및 기타 온라인 위협으로부터 사용자를 보호할 수 있습니다.
- 악의적인 행동: 악의적인 콘텐츠를 호스팅하거나 유해한 활동을 하는 것으로 알려진 사이트는 보안 사고 및 데이터 침해를 방지하기 위해 차단되어야 합니다.

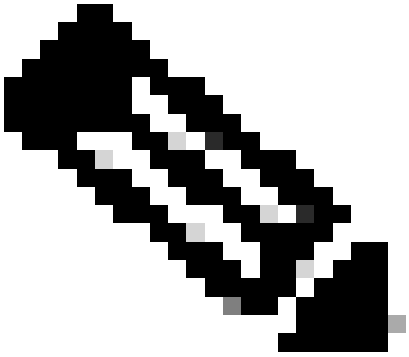
.

트래픽 차단 단계

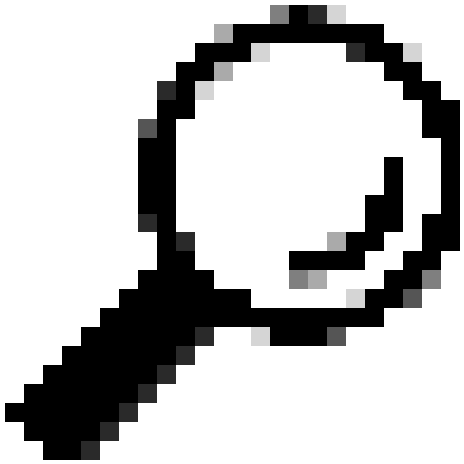
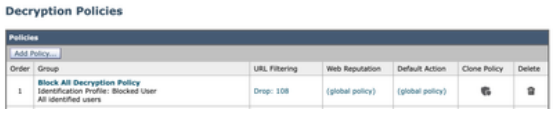
일반적으로 SWA에서는 트래픽을 차단하는 3가지 기본 단계가 있습니다.

- 사용자에 대한 식별 프로필을 생성합니다.
- 암호 해독 정책에서 HTTPS 트래픽을 차단합니다.
- 액세스 정책에서 HTTP 트래픽을 차단합니다.

단계	특정 사용자의 웹 사이트 액세스 차단	특정 사용자가 특정 웹 사이트에 액세스하지 못하도록 차단
사용자 지정 URL 범주	해당 없음.	액세스를 차단하려는 사이트에 대한 사용자 지정 URL 카테고리를 생성합니다. 자세한 내용은 다음을 참조하십시오.

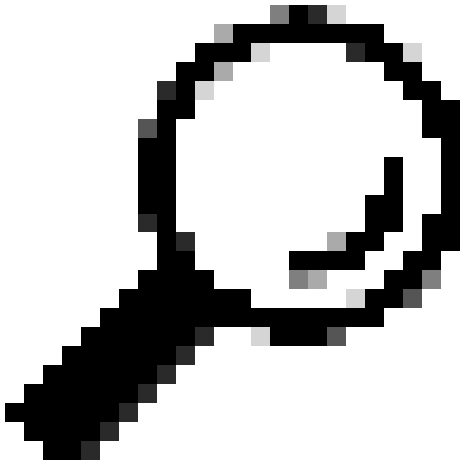
		Secure Web Appliance에서 맞춤형 URL 범주 구성 - Cisco
식별 프로필	1단계. GUI에서 Web Security Manager(웹 보안 관리자)를 선택한 다음 Identification Profiles(식별 프로필)를 클릭합니다. 2단계. 프로필을 추가하려면 Add Profile을 클릭합니다. 3단계. 이 프로파일을 활성화하거나 삭제하지 않고 신속하게 비활성화하려면 Enable Identification Profile 확인란을 사용합니다. 4단계. 고유한 프로파일 이름을 할당합니다. 5단계. (선택 사항) 설명을 추가합니다. 6단계. Insert Above 드롭다운 목록에서 이 프로파일을 테이블에 표시할 위치를 선택합니다. 7단계. User Identification Method(사용자 식별 방법) 섹션에서 Exempt from authentication/identification(인증/식별에서 제외)을 선택합니다. 8단계. 서브넷별 구성원 정의에 이 식별 프로필이 적용해야 하는 IP 주소 또는 서브넷을 입력합니다. IP 주소, CIDR(Classless Inter-Domain Routing) 블록 및 서브넷을 사용할 수 있습니다.	 참고: 모든 사용자의 특정 웹 사이트에 대한 액세스를 차단하기 위해 별도의 ID 프로필을 생성할 필요가 없습니다. 전역 암호 해독/액세스 정책을 통해 이를 효율적으로 관리할 수 있습니다. 1단계. GUI에서 Web Security Manager(웹 보안 관리자)를 선택한 다음 Identification Profiles(식별 프로필)를 클릭합니다. 2단계. 프로필을 추가하려면 Add Profile을 클릭합니다. 3단계. 이 프로파일을 활성화하거나 삭제하지 않고 신속하게 비활성화하려면 Enable Identification Profile 확인란을 사용합니다. 4단계. 고유한 프로파일 이름을 할당합니다. 5단계. (선택 사항) 설명을 추가합니다. 6단계. Insert Above 드롭다운 목록에서 이 프로파일을 테이블에 표시할 위치를 선택합니다. 7단계. User Identification Method(사용자 식별 방법) 섹션에서 Exempt from authentication/identification(인증/식별에서 제외)을 선택합니다. 8단계. 서브넷별 구성원 정의에 이 식별

		프로필이 적용해야 하는 IP 주소 또는 서브넷을 입력합니다. IP 주소, CIDR(Classless Inter-Domain Routing) 블록 및 서브넷을 사용할 수 있습니다. 9단계. Advanced(고급)를 클릭하고 액세스를 차단하려는 URL 카테고리를 추가합니다.
암호 해독 정책	1단계. GUI에서 Web Security Manager(웹 보안 관리자)를 선택한 다음 Decryption Policy(암호 해독 정책)를 클릭합니다. 2단계. 암호 해독 정책을 추가하려면 Add Policy를 클릭합니다. 3단계. Enable Policy(정책 활성화) 확인란을 사용하여 이 정책을 활성화합니다. 4단계. 고유한 정책 이름을 할당합니다. 5단계. (선택 사항) 설명을 추가합니다. 6단계. Insert Above Policy 드롭다운 목록에서 첫 번째 Policy를 선택합니다. 7단계. Identification Profiles and Users(식별 프로필 및 사용자)에서 이전 단계에서 생성한 식별 프로필을 선택합니다. 8단계. 제출합니다. 9단계. Decryption Policies(암호 해독 정책) 페이지의 URL Filtering(URL 필터링)에서 이 새 암호 해독 정책과 연결된 링크를 클릭합니다.	1단계. GUI에서 Web Security Manager(웹 보안 관리자)를 선택한 다음 Decryption Policy(암호 해독 정책)를 클릭합니다. 2단계. 암호 해독 정책을 추가하려면 Add Policy를 클릭합니다. 3단계. Enable Policy(정책 활성화) 확인란을 사용하여 이 정책을 활성화합니다. 4단계. 고유한 정책 이름을 할당합니다. 5단계. (선택 사항) 설명을 추가합니다. 6단계. Insert Above Policy 드롭다운 목록에서 첫 번째 Policy를 선택합니다. 7단계. Identification Profiles and Users(식별 프로필 및 사용자)에서 이전 단계에서 생성한 식별 프로필을 선택합니다. 8단계. 제출합니다. 9단계. Decryption Policies(암호 해독 정책) 페이지의 URL Filtering(URL 필터링)에서 이 새 암호 해독 정책과 연결된 링크를 클릭합니다. 10단계. 차단된 웹 사이트에 대해 생성된 Custom URL(맞춤형 URL) 카테고리에 대한 작업으로 Drop(삭제)을 선택합니다. 11단계. Submit(제출)을 클릭합니다. 

	 팁: 모든 URL 카테고리를 차단한다고 가정할 때 맞춤형 URL 카테고리를 제거하고 사전 정의된 URL 카테고리만 사용하여 정책을 최적화할 수 있습니다. 이렇게 하면 URL을 사용자 지정 URL 범주와 일치시키는 추가 단계를 방지하여 SWA의 처리 로드가 줄어듭니다. 10단계. 모든 URL 카테고리에 대한 작업으로 삭제를 선택합니다. 11단계. 같은 페이지에서 아래로 스크롤하여 Uncategorized URLs(분류되지 않은 URL)로 이동하고 Drop from 드롭다운 목록을 선택합니다. 12단계. 제출합니다.  이미지 - 특정 사용자에 대한 모든 웹 사이트를 차단하는 암호 해독 정책	이미지 - 암호 해독 정책에서 일부 URL 차단
액세스 정책	1단계. GUI에서 Web Security Manager(웹 보안 관리자)를 선택한 다음 Access Policy(액세스 정책)를 클릭합니다. 2단계. Add Policy(정책 추가)를 클릭하여 액세스 정책을 추가합니다.	1단계. GUI에서 Web Security Manager(웹 보안 관리자)를 선택한 다음 Access Policy(액세스 정책)를 클릭합니다. 2단계. Add Policy(정책 추가)를 클릭하여 액세스 정책을 추가합니다.

	3단계. Enable Policy(정책 활성화) 확인란을 사용하여 이 정책을 활성화합니다. 4단계. 고유한 정책 이름을 할당합니다. 5단계. (선택 사항) 설명을 추가합니다. 6단계. Insert Above Policy 드롭다운 목록에서 첫 번째 Policy를 선택합니다. 7단계. Identification Profiles and Users(식별 프로필 및 사용자)에서 이전 단계에서 생성한 식별 프로필을 선택합니다. 8단계. 제출합니다. 9단계. Access Policies(액세스 정책) 페이지의 Protocols and User Agents(프로토콜 및 사용자 에이전트)에서 이 새 액세스 정책과 연결된 링크를 클릭합니다. 10단계. Edit Protocols and User Agents Settings(프로토콜 및 사용자 에이전트 설정 수정) 드롭다운 목록에서 Define Custom Settings(사용자 지정 설정 정의)를 선택합니다. 11단계. 수신 Block Protocols에서 둘 모두에 대한 확인란 FTP over HTTP 및 HTTP. 12단계. 수신 HTTP CONNECT 포트, 모든 포트를 차단하려면 모든 포트 번호를 제거하십시오.  이미지 - 액세스 정책에서 프로토콜 및 연결 포트 차단 13단계. 제출합니다. 14단계(선택 사항) Access Policies(액	3단계. Enable Policy(정책 활성화) 확인란을 사용하여 이 정책을 활성화합니다. 4단계. 고유한 정책 이름을 할당합니다. 5단계. (선택 사항) 설명을 추가합니다. 6단계. Insert Above Policy 드롭다운 목록에서 첫 번째 Policy를 선택합니다. 7단계. Identification Profiles and Users(식별 프로필 및 사용자)에서 이전 단계에서 생성한 식별 프로필을 선택합니다. 8단계. 제출합니다. 9단계. Access Policies(액세스 정책) 페이지의 URL Filtering(URL 필터링)에서 이 새 액세스 정책과 연결된 링크를 클릭합니다 10단계. 차단된 웹 사이트에 대해 생성된 Custom URL 카테고리에 대한 작업으로 Block을 선택합니다. 11단계. 제출합니다. 12단계. 변경 사항을 커밋합니다.  Image(이미지) - 액세스 정책에서 일부 URL 차단

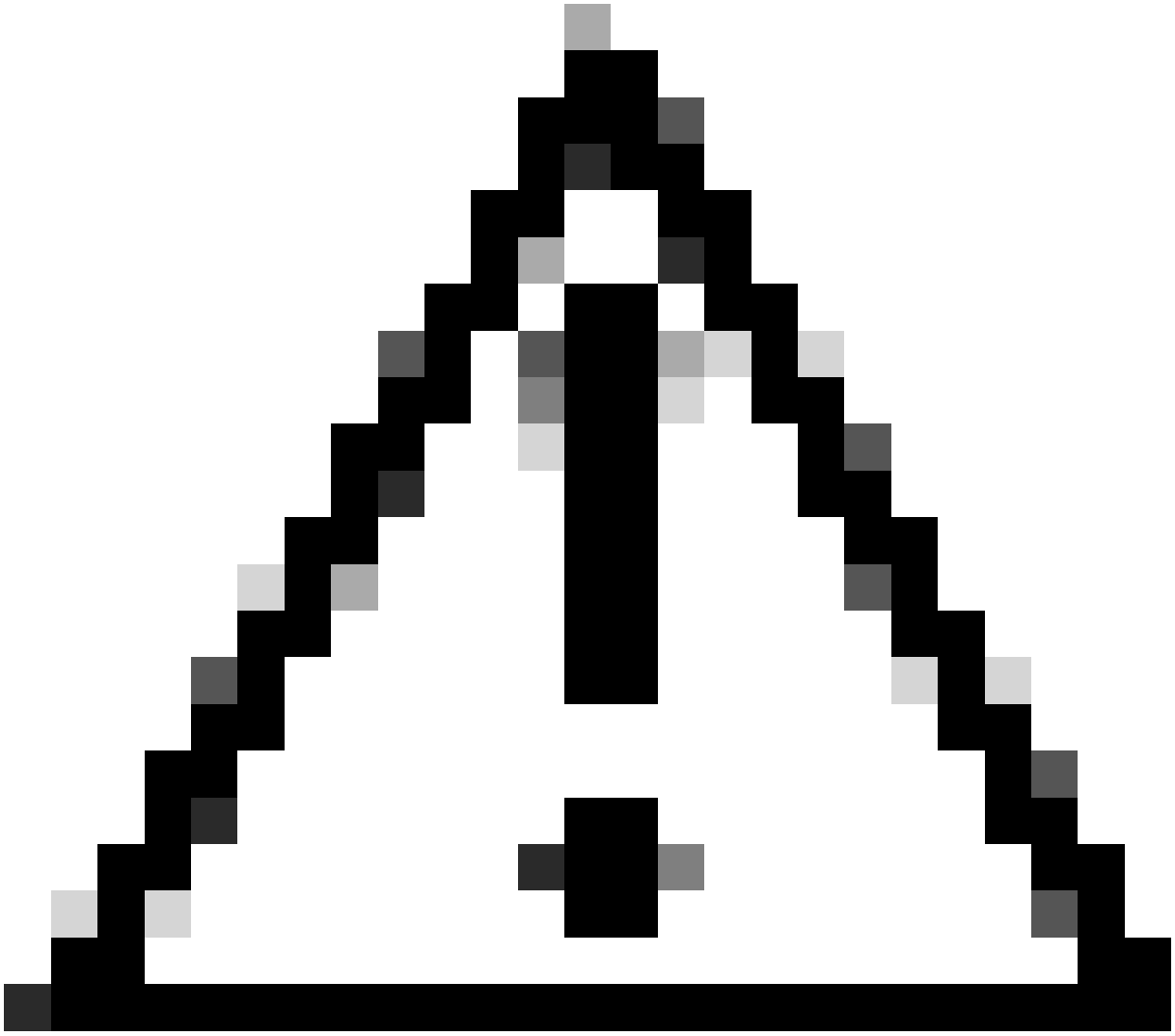
세스 정책) 페이지의 URL Filtering(URL 필터링)에서 이 새 액세스 정책과 연결된 링크를 클릭합니다. 모든 URL 카테고리에 대한 작업으로 Block(차단)을 선택하고 분류되지 않은 URL과 Submit.



팁: 모든 URL 카테고리를 차단한다고 가정할 때 맞춤형 URL 카테고리를 제거하고 사전 정의된 URL 카테고리만 사용하여 정책을 최적화할 수 있습니다. 이렇게 하면 URL을 사용자 지정 URL 범주와 일치시키는 추가 단계를 방지하여 SWA의 처리 로드가 줄어듭니다.

16단계. 변경 사항을 커밋합니다.

이미지 - 모든 사이트를 차단하는 액세스 정책



주의: 투명 프록시 구축에서 SWA는 트래픽이 해독되지 않는 한 HTTPS 트래픽에 대한 사용자 에이전트 또는 전체 URL을 읽을 수 없습니다. 따라서 User Agents(사용자 에이전트)를 사용하여 식별 프로필을 구성하거나 정규식과 함께 Custom URL Category(맞춤형 URL 카테고리)를 구성하는 경우 이 트래픽은 식별 프로필과 매칭하지 못합니다.

투명 프록시 구축에서 정규식을 사용하여 사이트 차단

투명 프록시 배포에서 정규식 조건이 있는 사용자 지정 URL 범주를 차단하려는 경우(예: 일부 YouTube 채널에 대한 액세스를 차단하는 경우) 다음 단계를 사용할 수 있습니다.

1단계. 기본 사이트에 대한 맞춤형 URL 카테고리를 생성합니다. (이 예에서는 YouTube.com).

2단계. 암호 해독 정책을 생성하고, 이 사용자 지정 URL 카테고리를 할당하고, Action(작업)을 Decrypt(암호 해독)로 설정합니다.

3단계. 액세스 정책을 생성하고 정규식을 포함하는 맞춤형 URL 카테고리(이 예에서는 YouTube 채널에 대한 맞춤형 URL 카테고리)를 할당한 다음 Action(작업)을 Block(차단)으로 설정합니다.

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

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.