SWA에서 Microsoft 업데이트 트래픽에 대한 범위 요청 구성

목차

[소개](#)

[사전 요구 사항](#)

- [요구 사항](#)
- [사용되는 구성 요소](#)

[범위 요청](#)

[프록시 환경의 범위 요청](#)

[Microsoft 업데이트에 대한 범위 요청 활성화](#)

[Microsoft 업데이트에 대해서만 범위 요청을 사용하도록 설정하는 단계](#)

- [1단계. 범위 요청을 활성화합니다.](#)
- [2단계. Microsoft 업데이트 URL에 대한 사용자 지정 URL 범주 만들기](#)
- [3단계. (선택 사항) Microsoft Updates 트래픽을 인증에서 제외하기 위한 식별 프로필을 생성합니다](#)
- [4단계. (선택 사항) Microsoft 업데이트 트래픽을 통과하기 위한 암호 해독 정책을 생성합니다](#)
- [5단계. Microsoft 업데이트 트래픽에 대한 범위 요청을 허용하는 액세스 정책 만들기](#)

[액세스 로그 수정](#)

[확인](#)

[관련 정보](#)

소개

이 문서에서는 Microsoft 업데이트 트래픽에서 SWA(Secure Web Appliance)의 범위 요청을 사용하도록 허용하는 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.

범위 요청

범위 요청은 클라이언트가 한 번에 전체 파일을 다운로드하는 대신 서버에서 파일의 특정 부분만 요청할 수 있도록 하는 HTTP 프로토콜의 기능입니다(예: 웹 브라우저 또는 다운로드 관리자). 이 기능은 중단된 다운로드, 스트리밍 미디어 또는 대용량 파일에 대한 액세스를 효율적으로 재개하는 데 특히 유용합니다. 클라이언트는 HTTP 요청의 Range 헤더에서 원하는 바이트 범위를 지정하며, 서버가 범위 요청을 지원하는 경우 206 Partial Content 상태 코드로 응답하여 파일의 요청된 세그먼트만 전달합니다.

이 메커니즘은 몇 가지 시나리오에서 성능과 사용자 경험을 향상시킵니다. 예를 들어, 비디오 스트리밍에서 범위 요청을 통해 플레이어는 재생에 필요한 세그먼트만 가져올 수 있으므로 대역폭 사용량이 줄고 응답성이 향상됩니다. 마찬가지로, 다운로드 관리자는 범위 요청을 사용하여 파일을 청크로 분할하고 병렬로 다운로드하므로 프로세스의 속도가 빨라집니다. 범위 요청은 또한 캐싱 및 프록시 시스템에서 중요한 역할을 하여 부분 업데이트를 활성화하고 중복 데이터 전송을 줄입니다.

프록시 환경의 범위 요청

프록시 환경에서는 범위 요청이 대역폭 사용을 최적화하고 콘텐츠 전송 효율성을 개선하는 데 중요한 역할을 합니다. 범위 요청이 활성화되면 프록시 서버는 원천 서버에서 필요한 바이트 세그먼트만 가져오고 로컬로 캐시할 수 있습니다. 이를 통해 클라이언트는 비디오 또는 대용량 파일의 특정 세그먼트와 같은 부분 콘텐츠를 요청하고 가능한 경우 프록시 캐시에서 빠르게 수신할 수 있습니다. 또한 병렬 다운로드 및 재시작 기능도 지원하므로, 대역폭이 제한되거나 레이턴시가 긴 환경에서 특히 유용합니다.

그러나 범위 요청이 비활성화되면 클라이언트에 작은 부분만 필요한 경우에도 프록시가 원본 서버의 전체 파일을 가져와야 합니다. 이로 인해 불필요한 데이터 전송, 프록시 및 원천 서버 모두의 부하 증가, 클라이언트의 응답 시간 단축 등이 초래됩니다. 또한 프록시에서 부분 콘텐츠를 저장하거나 제공할 수 없으므로 효율적인 캐싱 전략을 방지합니다. 스트리밍 시나리오에서 버퍼링 지연이 발생하거나 사용자 환경이 저하될 수 있습니다. 범위 요청을 비활성화하는 것은 보안 또는 정책상의 이유로 수행할 수 있지만, 성능과 유연성의 대가로 이루어지는 경우가 많습니다.

예를 들어, 사용자 10명이 프록시 서버를 통해 100MB 파일에서 각각 1MB를 다운로드하려고 하는 시나리오를 가정해보겠습니다.

범위 요청 사용 안 함:

범위 요청이 비활성화된 경우 프록시는 각 사용자에게 필요한 1MB 세그먼트만 가져올 수 없습니다. 대신 각 요청에 대해 원본 서버에서 전체 100MB 파일을 다운로드해야 합니다. 그 결과 다음과 같은 효과가 있습니다.

출발지에서 프록시까지의 총 트래픽: 10 × 100MB = 1000MB(1GB)

이 데이터 중 10MB만 클라이언트에서 실제로 사용됩니다.

나머지 990MB는 낭비되어 대역폭 사용이 비효율적이고 프록시 및 오리진 서버의 로드가 증가합니다.

범위 요청 사용:

범위 요청을 활성화하면 프록시는 요청한 사용자당 1MB만 가져옵니다.

출발지에서 프록시까지의 총 트래픽: 10 × 1MB = 10MB

프록시는 이러한 세그먼트를 캐시하고 필요한 경우 다른 사용자에게 제공할 수 있습니다.

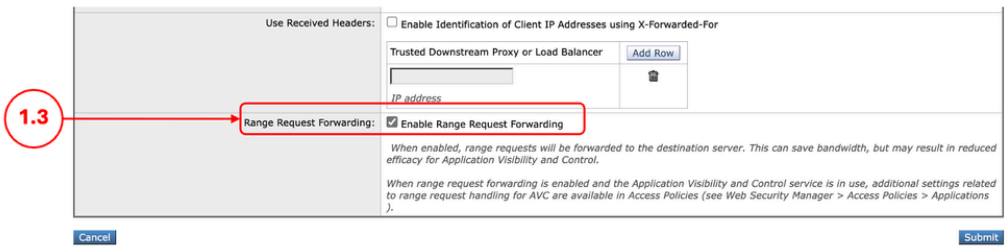
따라서 트래픽이 90배 감소하고, 응답 시간이 단축되며, 리소스 사용률이 크게 향상됩니다.

Microsoft 업데이트에 대한 범위 요청 활성화

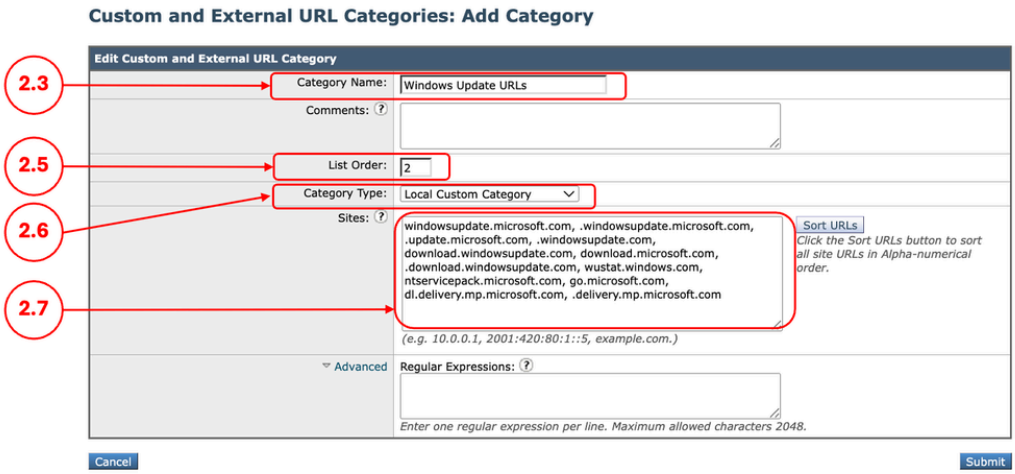
범위 요청은 성능을 향상시키지만 SWA 환경 내에서의 보안 검사 및 정책 시행을 방해합니다. 이러한 시스템은 부분 콘텐츠를 완전히 검사할 수 없기 때문입니다. 이 문서는 범위 요청 사용을 Microsoft 업데이트 트래픽으로만 제한합니다.

⚠ 주의: 범위 요청 전달을 활성화하면 정책 기반 AVC(Application Visibility and Control) 효율성에 지장을 주고 보안을 손상시킬 수 있습니다.

Microsoft 업데이트에 대해서만 범위 요청을 사용하도록 설정하는 단계

1단계. 범위 요청을 활성화합니다.	1.1단계. GUI에서 Security Services(보안 서비스)를 클릭하고 Web Proxy(웹 프록시)를 선택합니다. 1.2단계. 설정 편집을 클릭합니다. 1.3단계. Enable Range Request Forwarding(범위 요청 전달 활성화) 확인란을 선택합니다. 1.4단계. Submit(제출)을 클릭합니다.  이미지 - 범위 요청 전달 사용

2단계. Microsoft 업데이트 URL에 대한 사용자 지정 URL 범주 만들기	2.1단계.GUI에서 Web Security Manager를 선택한 다음 Custom and External URL Categories(사용자 지정 및 외부 URL 범주)를 클릭합니다.
	2.2단계.Add Categories(범주 추가)를 클릭하여 사용자 지정 URL 범주를 추가합니다.
	2.3단계.고유한 CategoryName을 할당합니다.
	2.4단계. (선택 사항) 설명을 추가합니다.
	
	2.5단계. List Order(주문 나열)에서 맨 위에 배치할 첫 번째 범주를 선택합니다.
	
	2.6단계. Category Type(카테고리 유형) 드롭다운 목록에서 Local Custom Category(로컬 맞춤형 카테고리)를 선택합니다.
	
	2.7단계. 사이트 섹션에 Microsoft 업데이트 URL을 추가합니다.
	
	팁: 다음 링크에서 Microsoft 업데이트 목록을 확인할 수 있습니다. 2단계 - WSUS 구성 | Microsoft Learn
	
	주의: Microsoft 문서에 있는 것처럼 URL을 복사/붙여넣지 마십시오. SWA 형식으로 올바르게 포맷합니다. 자세한 내용은 Configure Custom URL Categories in Secure Web Appliance - Cisco를 참조하십시오.
	
	예를 들면 다음과 같습니다.
	
	`http://windowsupdate.microsoft.com ===> windowsupdate.microsoft.com`
	`http://*.windowsupdate.microsoft.com ===> .windowsupdate.microsoft.com`
	
	2.8단계. Submit(제출)을 클릭합니다.

<table>
<tr>
<td></td>
<td> 

이미지 - 사용자 지정 URL 범주 만들기</td>
</tr>
<tr>
<td>3단계. (선택 사항) Microsoft Updates 트래픽을 인증에서 제외하기 위한 식별 프로필을 생성합니다

참고: 이 작업은 Microsoft Updates에 대한 트래픽에 대한 SWA의 인증 로드를 줄이기 위한 것입니다.</td>
<td>3.1단계.GUI에서 Web Security Manager를 선택한 다음 Identification Profiles(식별 프로필)를 클릭합니다.
3.2단계.프로파일 추가(Add Profile)를 클릭하여 프로파일을 추가합니다.
3.3단계.Enable Identification Profile(식별 프로필 활성화) 확인란이 선택되어 있는지 확인합니다.
3.4단계.고유한 profileName을 할당합니다.
3.5단계. (선택 사항) 설명을 추가합니다.
3.6단계.Insert Above(위에 삽입) 드롭다운 목록에서 이 프로파일을 테이블에 표시할 위치를 선택합니다.

3.7단계. User Identification Method(사용자 식별 방법) 섹션에서 Exempt from authentication/identification(인증/식별에서 제외)을 선택합니다.

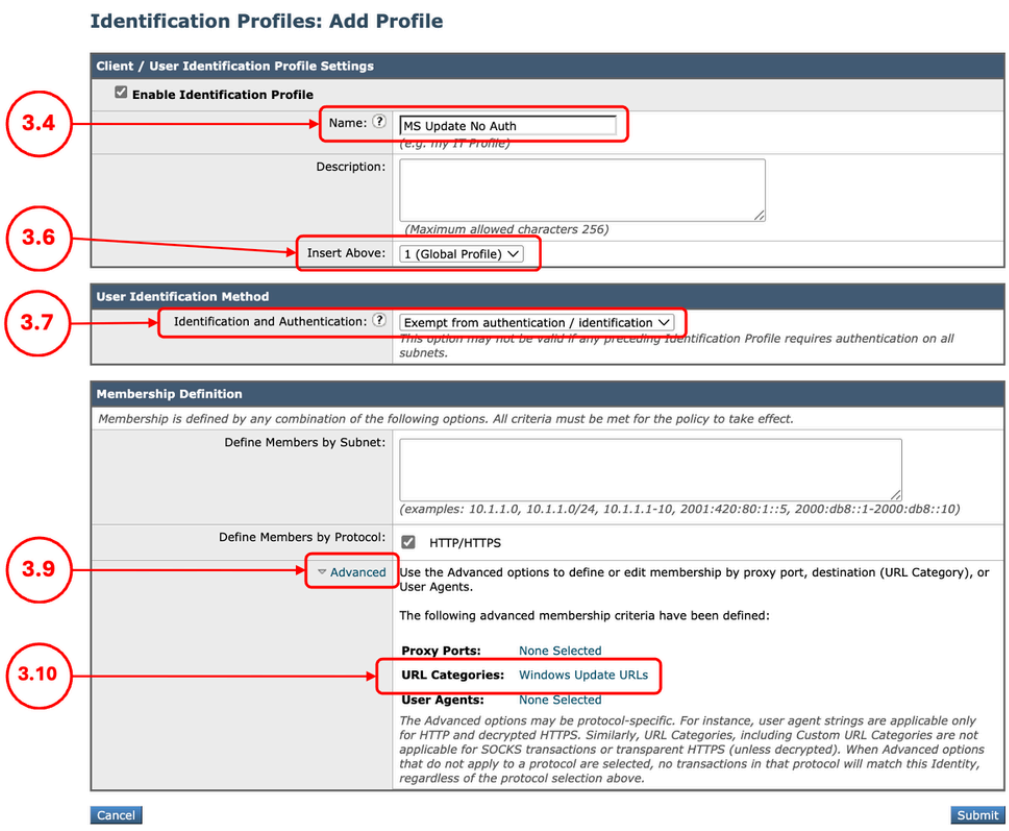
3.8단계에서 서브넷별 구성원 정의에서 특정 사용자에 대해 Microsoft 트래픽을 통과시키려면 적용할 IP 주소 또는 서브넷을 입력하거나 모든 IP 주소를 포함하려면 이 필드를 비워 둡니다.

3.9단계. Advanced(고급) 섹션에서 Custom URL Categories(사용자 지정 URL 범주)를 선택합니다.

3.10단계. Microsoft 업데이트를 위해 만든 사용자 지정 URL 범주를 추가합니다.

3.11단계. Done(완료)을 클릭합니다.

3.12단계. Submit(제출)을 클릭합니다.</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td> 

이미지 - 식별 프로필 생성</td>
</tr>
<tr>
<td>4단계. (선택 사항) Microsoft 업데이트 트래픽을 통과하기 위한 암호 해독 정책을 생성합니다

참고: Microsoft Updates는 HTTP를 사용하며 HTTPS 트래픽은 업데이트 링크를 푸시합니다. 이 작업은 SWA의 해독 로드를 줄이기 위한 것입니다.</td>
<td>4.1단계.GUI에서 Web Security Manager를 선택한 다음 Decryption Policy를 클릭합니다.

4.2단계. 정책 추가를 클릭하여 암호 해독 정책을 추가합니다.

4.3단계.고유한 PolicyName을 할당합니다.
4.4단계. (선택 사항) 설명을 추가합니다.
4.5단계Insert Above Policy 드롭다운 목록에서 첫 번째 Policy를 선택합니다.

4.6단계 식별 프로파일 및 사용자에서 하나 이상의 식별 프로파일 선택을 선택합니다.

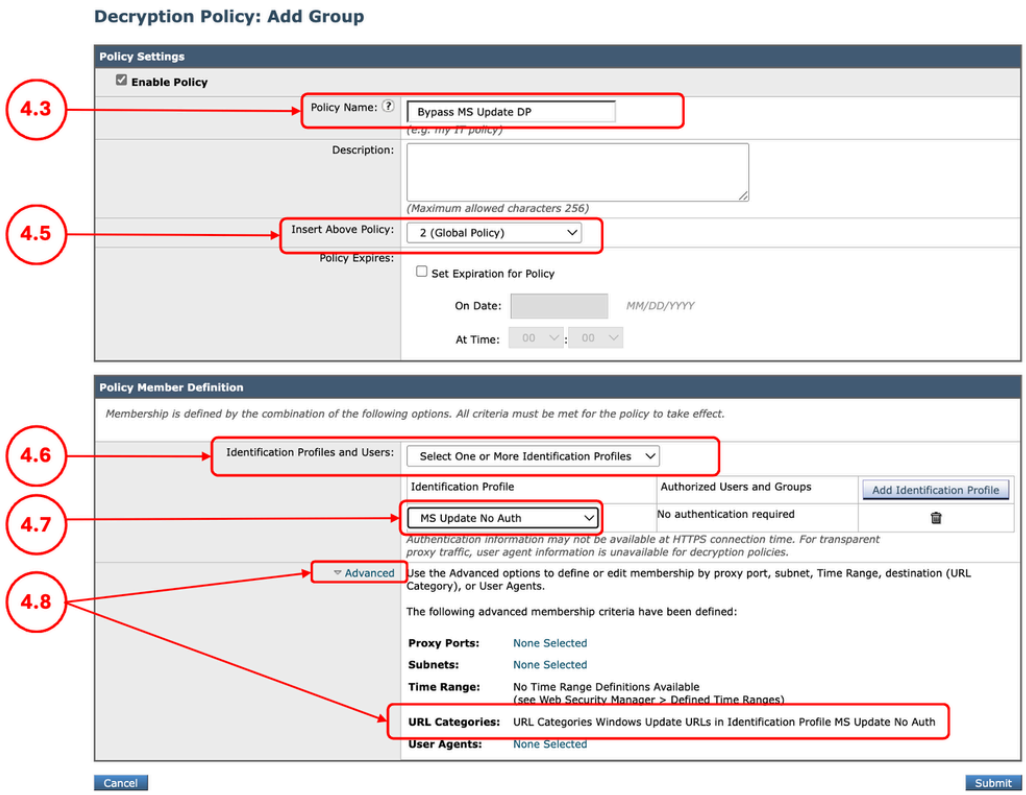
4.7단계. 3단계에서 생성한 식별 프로필을 선택하고 4.11단계로 건너뜁니다.

4.8단계 Windows 업데이트에 대한 ID 프로필을 만들지 않은 경우 Advanced(고급) 섹션에서 Custom URL Categories(사용자 지정 URL 범주)를 선택합니다.

4.9단계. 2단계에서 Microsoft 업데이트를 위해 생성한 사용자 지정 URL 카테고리를 추가합니다.

4.10단계. 완료를 누릅니다.</td>
</tr>
</table>

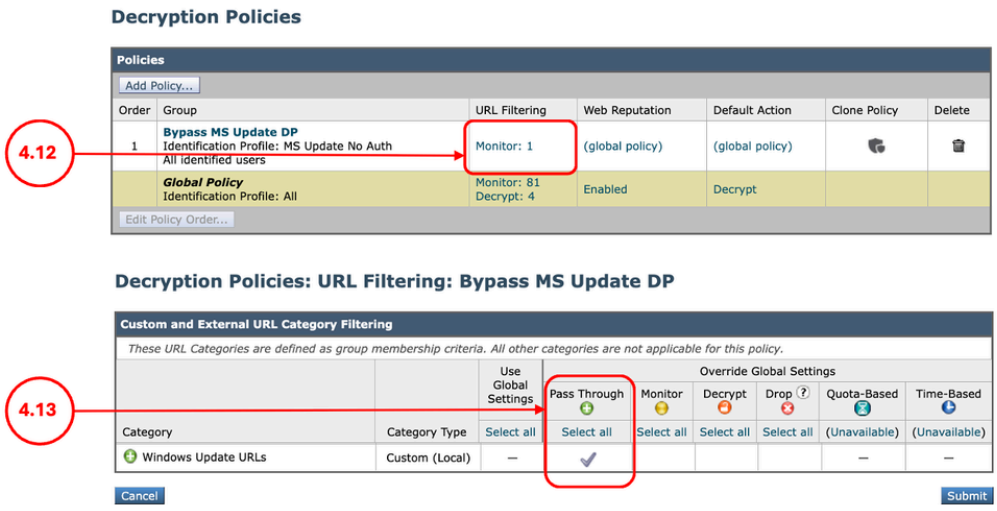
4.11단계. Submit(제출)을 클릭합니다.



이미지 - 암호 해독 정책 생성

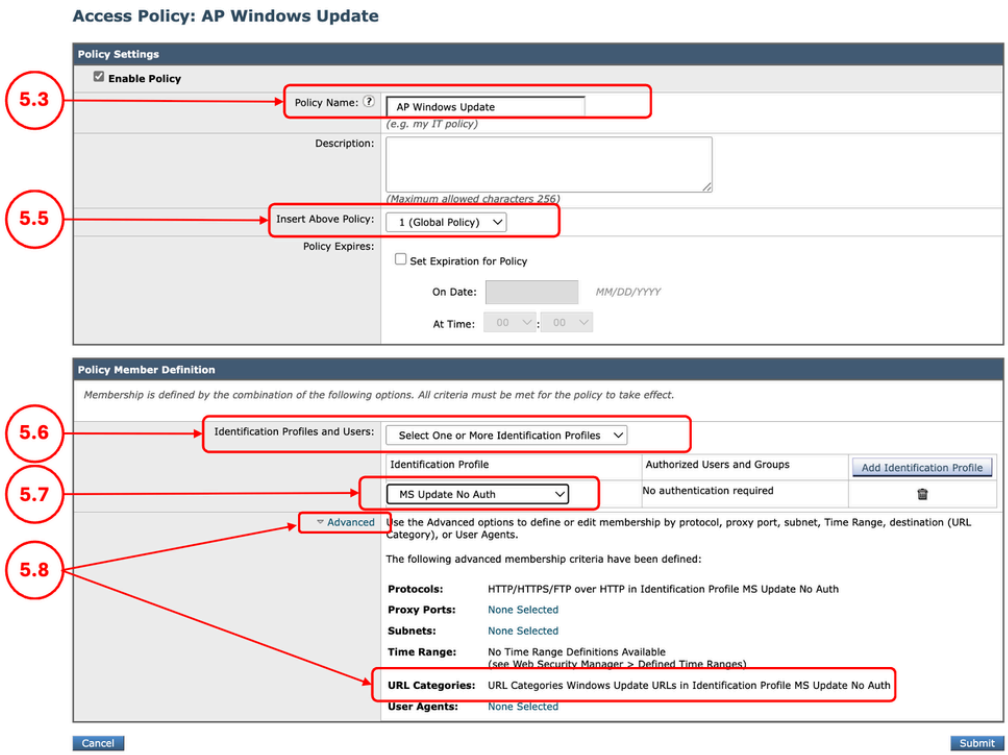
4.12단계.Decryption Policies(암호 해독 정책) 페이지의 URL Filtering(URL 필터링)에서 이 새 암호 해독 정책과 연결된 링크를 클릭합니다.

4.13단계Microsoft Updates URL 범주에 대한 작업으로 Pass Through를 선택합니다.



이미지 - URL 카테고리에 대한 작업 통과 설정

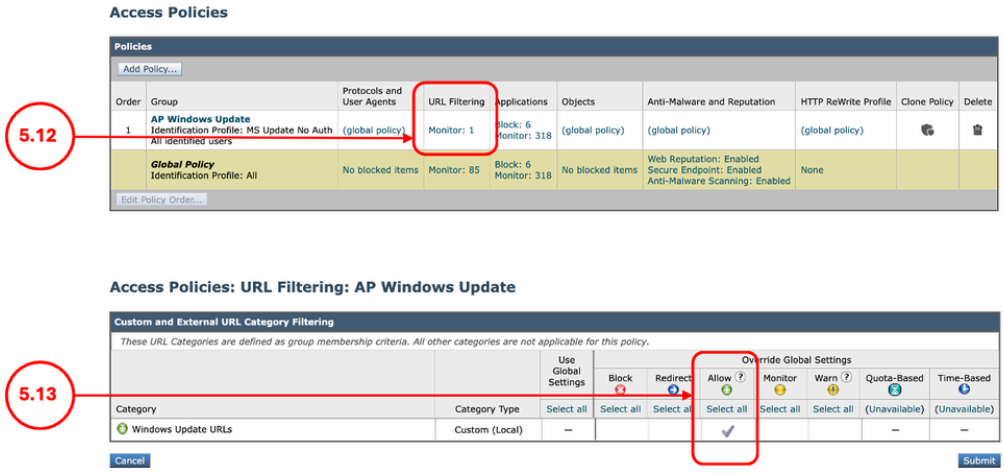
4.12단계. Submit(제출)을 클릭합니다.

5단계. Microsoft 업데이트 트래픽에 대한 범위 요청을 허용하는 액세스 정책 만들기	5.1단계.GUI에서 Web Security Manager(웹 보안 관리자)를 클릭하고 Access Policy(액세스 정책)를 선택합니다. 5.2단계. Add Policy를 클릭하여 액세스 정책을 추가합니다. 5.3단계.고유한 PolicyName을 할당합니다. 5.4단계. (선택 사항) 설명을 추가합니다. 5.5단계Insert Above Policy 드롭다운 목록에서 첫 번째 Policy를 선택합니다. 5.6단계 식별 프로파일 및 사용자에서 Select One or More Identification Profiles(하나 이상의 식별 프로파일 선택)를 선택합니다. 5.7단계. 3단계에서 생성한 식별 프로필을 선택하고 5.11단계로 건너뜁니다. 5.8단계 Windows 업데이트에 대한 ID 프로필을 만들지 않은 경우 Advanced(고급) 섹션에서 Custom URL Categories(사용자 지정 URL 범주)를 선택합니다. 5.9단계. 2단계에서 Microsoft 업데이트를 위해 생성한 사용자 지정 URL 카테고리를 추가합니다. 5.10단계. 완료를 클릭합니다. 5.11단계. 제출.  이미지 - 액세스 정책 생성 5.12단계. Access Policies(액세스 정책) 페이지의 URL Filtering(URL 필터

링)에서 이 새 액세스 정책과 연결된 링크를 클릭합니다

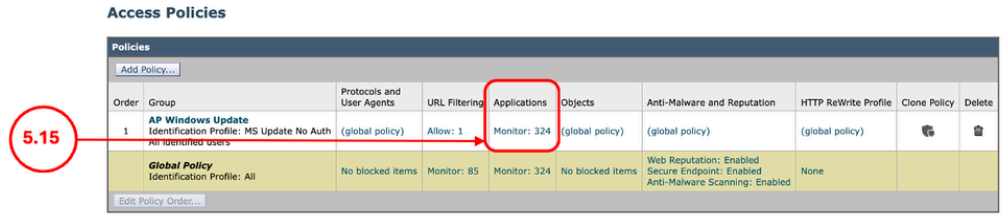
5.13단계Microsoft 업데이트를 위해 만든 사용자 지정 URL 카테고리에 대한 작업으로 Allow(허용)를 선택합니다.

5.14단계. Submit(제출)을 클릭합니다.



이미지 - URL 범주에 대한 작업 허용 설정

5.15단계. Access Policies(액세스 정책) 페이지의 Applications(애플리케이션)에서 이 새 액세스 정책과 연결된 링크를 클릭합니다

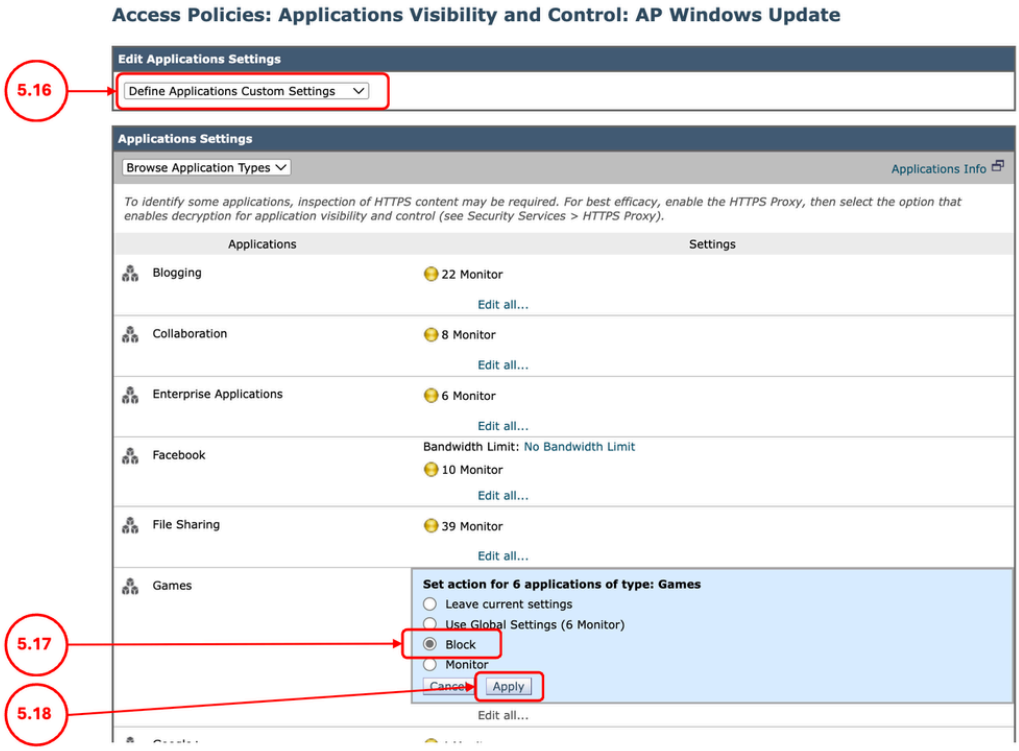


이미지 - Application Visibility and Control 수정

5.16단계. Edit Applications Settings(애플리케이션 설정 편집) 섹션에서 Define Applications Custom Settings(애플리케이션 사용자 정의 설정 정의)를 선택합니다.

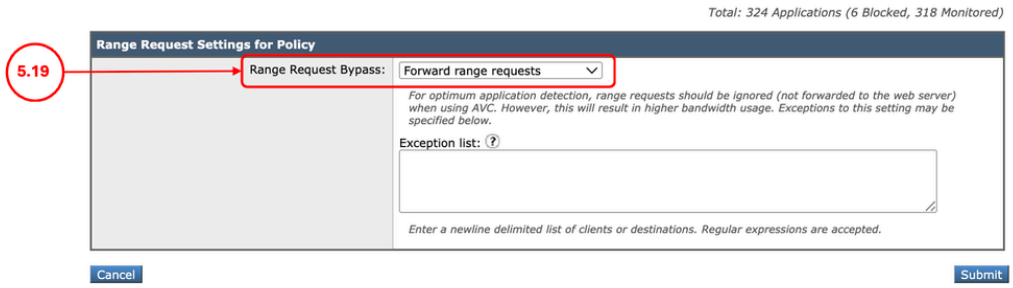
5.17단계. Applications Settings(애플리케이션 설정) 섹션에서 Edit all for Games application(게임 애플리케이션에 대해 모두 편집)을 클릭하고 Action(작업)을 Block(차단)으로 설정합니다.

5.18단계. 적용을 클릭합니다.



이미지 - 애플리케이션 작업 하나를 차단으로 설정

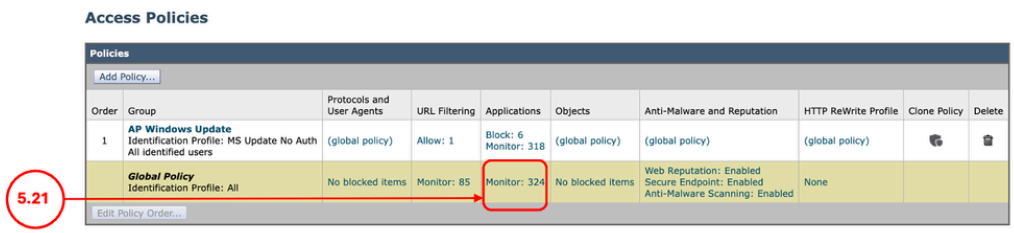
5.19단계. 아래로 스크롤하여 Range Request Settings for Policy(정책에 대한 범위 요청 설정) 섹션으로 이동한 후 Forward range requests(범위 요청 전달)가 선택되었는지 확인합니다.



이미지 - 정책에 대한 범위 요청 설정

5.20단계. 제출.

5.21단계. Access Policies(액세스 정책) 페이지의 Applications(애플리케이션) 아래에서 Global Policy(전역 정책)와 연결된 링크를 클릭합니다.



이미지 - 기본 액세스 정책 애플리케이션 설정

	5.22단계. 아래로 스크롤하여 Range Request Settings for Policy(정책에 대한 범위 요청 설정) 섹션을 찾습니다. Do Not Forward range requests(범위 요청을 전달하지 않음)가 선택되어 있는지 확인합니다. 5.23단계. 변경 사항을 커밋합니다.

액세스 로그 수정

액세스 로그의 범위 요청에 대한 더 많은 가시성을 확보하려면 다음 사용자 지정 필드를 추가할 수 있습니다.

[클라이언트 범위 = %<범위:]	클라이언트에서 요청한 범위(바이트)를 표시합니다.
[content= %>Content-Length:]	다운로드한 콘텐츠 크기(바이트)를 표시합니다.

SWA 액세스 로그에 사용자 지정 필드를 추가하는 방법에 대한 자세한 내용은 액세스 로그에서 성능 매개변수 구성 링크를 방문하십시오.

확인

이 CURL 명령을 사용하여 SWA에 범위 요청을 보냅니다.

```
curl -vvvk -H "Pragma: no-cache" -x 10.48.48.181:3128 -H 'Range: bytes=0-100' 'http://catalog.sf.dl.del
```

CURL 출력에서 HTTP 응답이 HTTP/1.1 206임을 확인할 수 있습니다.

```
> GET http://catalog.sf.dl.delivery.mp.microsoft.com/filestreamingservice/files/f263aa64-f367-42f0-9cad
> Host: catalog.sf.dl.delivery.mp.microsoft.com
> User-Agent: curl/8.7.1
> Accept: */*
> Proxy-Connection: Keep-Alive
> Pragma: no-cache
> Range: bytes=0-100
>
* Request completely sent off
< HTTP/1.1 206 Partial Content
```

액세스 로그에서 TCP_CLIENT_REFRESH_MISS/206이라는 작업을 볼 수 있습니다.

```
1773942471.096 14 10.190.0.206 TCP_CLIENT_REFRESH_MISS/206 860 GET http://catalog.sf.dl.delivery.mp.mic
```

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
- 액세스 로그의 성능 매개변수 구성
- 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.