# Secure Web Appliance에서 트래픽 우회

## 목차



## 소개

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

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SWA 관리.
- 기본 네트워킹 및 프록시 프로토콜

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.

## 서로 다른 유형의 우회

SWA에서는 트래픽을 우회하여 프록시 구축(명시적 또는 투명 구축)에 따라 SWA에 도달하지 못하거나 SWA에서 분석하고 검사하지 못하는 세 가지 개념이 있습니다. 이 세 가지 개념에 대해 간략하게 살펴보겠습니다.

- BYPASS: 트래픽이 SWA에 도달하지 못하도록 하는 설정으로, NIC(Network Interface Card) 활용률이 낮아지고 사용자와 어플라이언스 간의 세션이 필요하지 않습니다.
- 통과: 이 컨피그레이션은 SWA가 HTTPS 트래픽을 해독하지 못하도록 합니다. 그럼에도 불구하고 SWA는 두 가지 세션을 계속 지원합니다. 클라이언트와 SWA 간, 그리고 SWA와 웹 서버 간 두 번째입니다.
- 허용: HTTP 또는 암호 해독된 트래픽이 AMP, Sophos, WebRoot 및 애플리케이션 필터와 같은 내부 SWA 엔진의 검사를 건너뛰는 액세스 정책 내의 설정입니다. 이 경우에도 SWA에서 사용 중인 세션이 2개 있습니다.

| Type | Applies to | Transparent Deployment | Explicit Deployment | Configuration Path | Logging | Number of Sessions | Description |
|---|---|---|---|---|---|---|---|
| **Bypass from SWA** | HTTPS & HTTP | ✓ | ✗ | GUI > Web Security Manager > Bypass Settings | Bypasslogs | 1 | SWA routes the traffic to configured gateway (Layer 3 redirection) |
| **Bypass from WCCP Router** | HTTPS & HTTP | ✓ | ✗ | WCCP Router | No Logs on SWA | 0 | Traffic Redirects to the Gateway from Router |
| **Bypass from PAC** | HTTPS & HTTP | ✗ | ✓ | From the PAC file | No Logs on SWA | 0 | Requests are not sent to the proxy. |
| **Bypass from Browser** | HTTPS & HTTP | ✗ | ✓ | From the Browser or Group Policy | No Logs on SWA | 0 | Requests are not sent to the proxy. |
| **Pass Through** | HTTPS & HTTP | ✓ | ✓ | GUI > Web Security Manager > Decryption Policy | Accesslogs | 2 | SWA does not decrypt the traffic and sends the same ClientHello to the web server. |
| **Allow** | Decrypted Traffic & HTTP | ✓ | ✓ | GUI > Web Security Manager > Access Policy | Accesslogs | 2 | SWA does not Scan the traffic with its scanning engines, such as AMP, Sophos, WebRoot, AVC and ... |

이미지 - 비교 차트

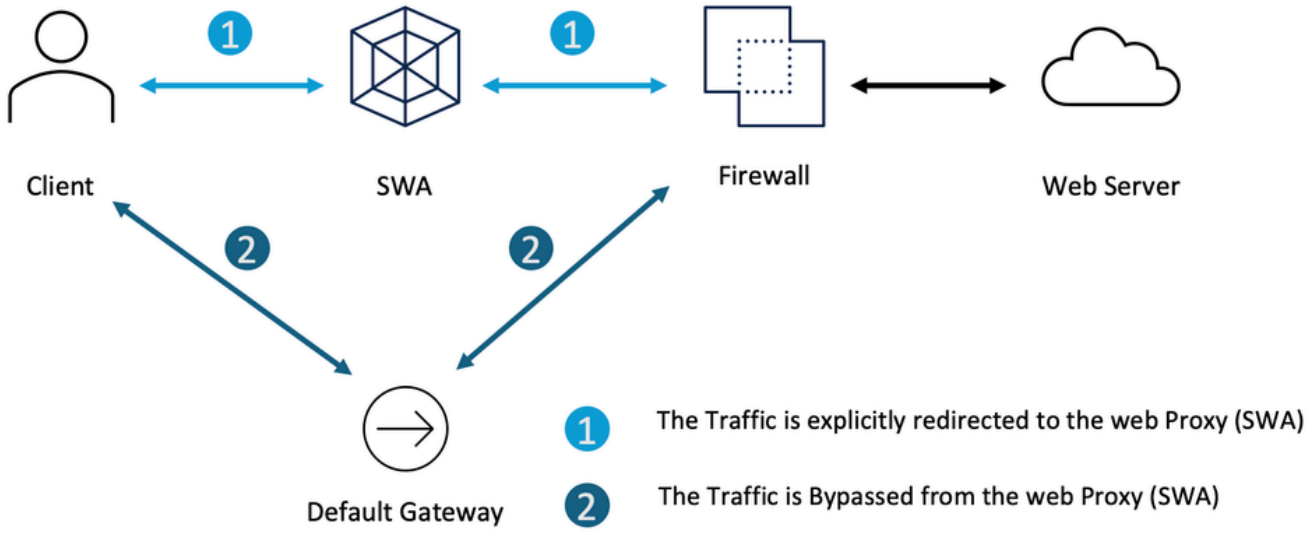
# 구축 유형별 SWA 바이패스 절차

우회 절차는 프록시 구축 모델에 따라 다릅니다. 각 유형에 대한 간략한 개요는 다음과 같습니다.

- 명시적 구축: 클라이언트는 트래픽을 프록시로 디렉션하도록 수동으로 구성됩니다.
- 투명한 구축: 네트워크 인프라는 트래픽을 프록시로 자동으로 리디렉션하므로 클라이언트 측 컨피그레이션이 필요하지 않습니다.

## 명시적 구축에서 트래픽 우회

명시적 구축에서 트래픽을 우회하려면 원하는 URL에 대한 웹 요청을 SWA로 전달하지 않도록 클라이언트를 구성해야 합니다. 이 네트워크 다이어그램에 표시된 것처럼, 일부 트래픽은 SWA(경로 번호 2)를 우회하기 위해 방화벽 또는 기본 게이트웨이로 직접 이동합니다.

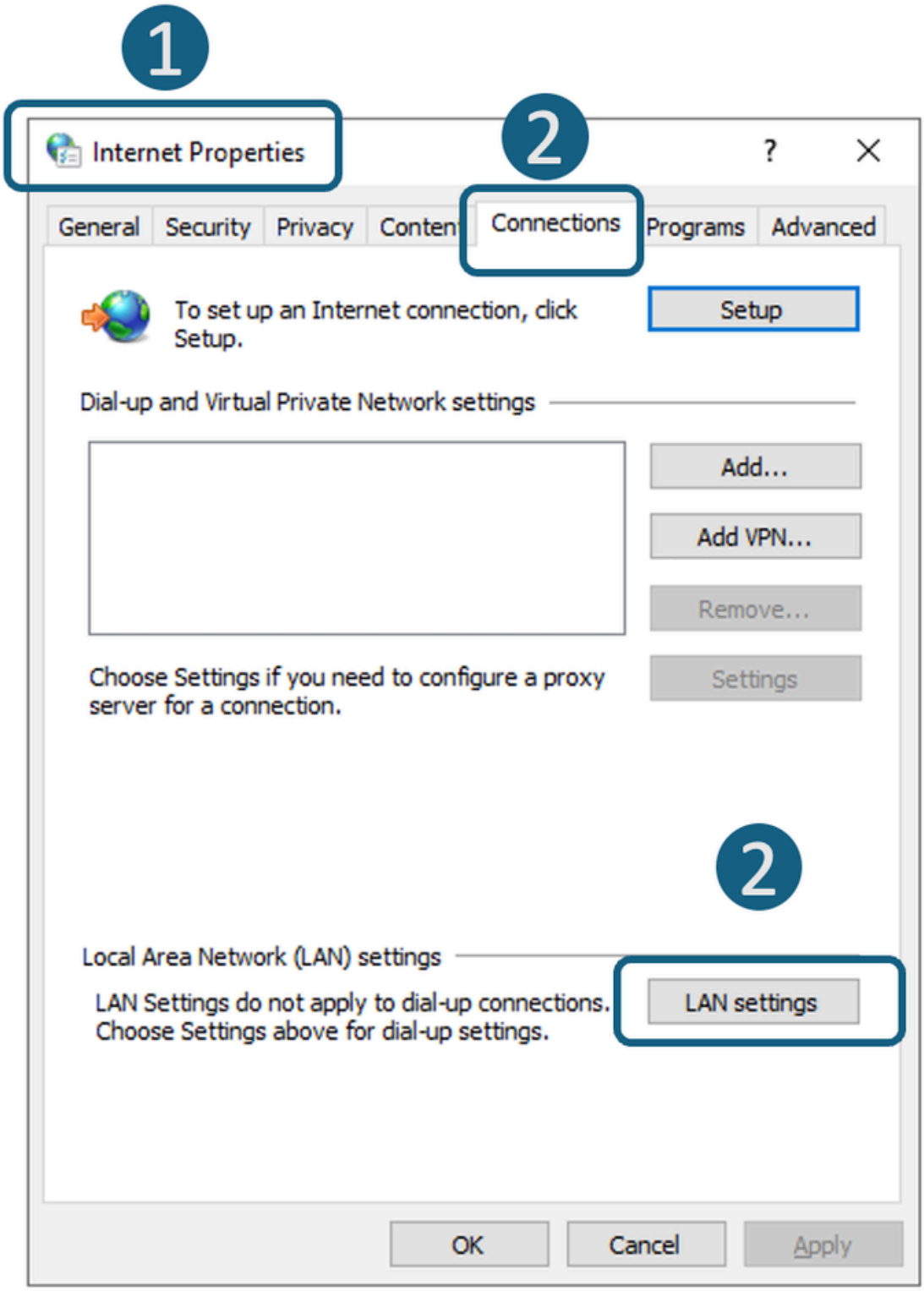



이미지 - 명시적 구축에서 트래픽 우회

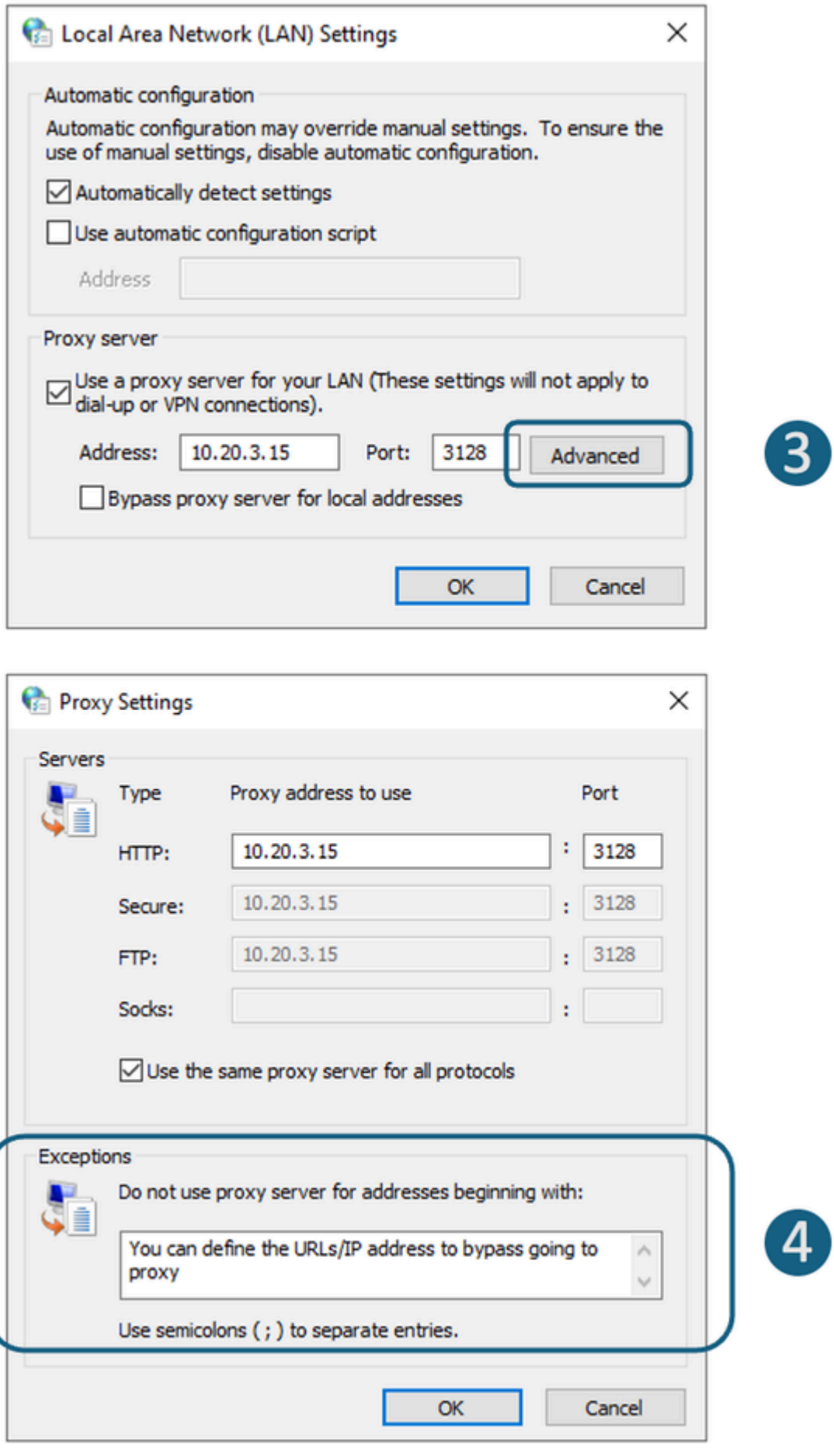
명시적 프록시 구축에 따라 SWA로 리디렉션할 일부 URL을 제외할 수 있습니다.

| | |
|---|---|
| 명시적 프록시 컨피그레이션 | URL이 SWA에 도달하지 못하도록 제외하는 단계 |
| PAC 파일 컨피그레이션 | PAC 파일을 구성한 방법에 따라 예외 목록을 정의하고 작업을 DIRECT로 설정할 수 있습니다.<br><br>다음은 SWA에 도달하지 못하도록 사설 IP 주소를 우회하는 몇 가지 샘플입니다<br><br>`var resolved_ip = dnsResolve(host);`<br>`if (isInNet(resolved_ip, "10.0.0.0", "255.0.0.0") ||`<br>`isInNet(resolved_ip, "172.16.0.0", "255.240.0.0") ||`<br>`isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") ||`<br>`isInNet(resolved_ip, "127.0.0.0", "255.255.255.0"))`<br>`return "DIRECT";`<br><br>다음은 SWA를 리디렉션하지 않고 www.cisco.com으로 트래픽을 우회하는 예입니다<br><br>`if (localHostOrDomainIs(host, "www.cisco.com")) return "DIRECT";`<br><br>이 예에서는 cisco.com의 모든 하위 도메인을 우회하여 SWA를 리디렉션하는 것입니다 |

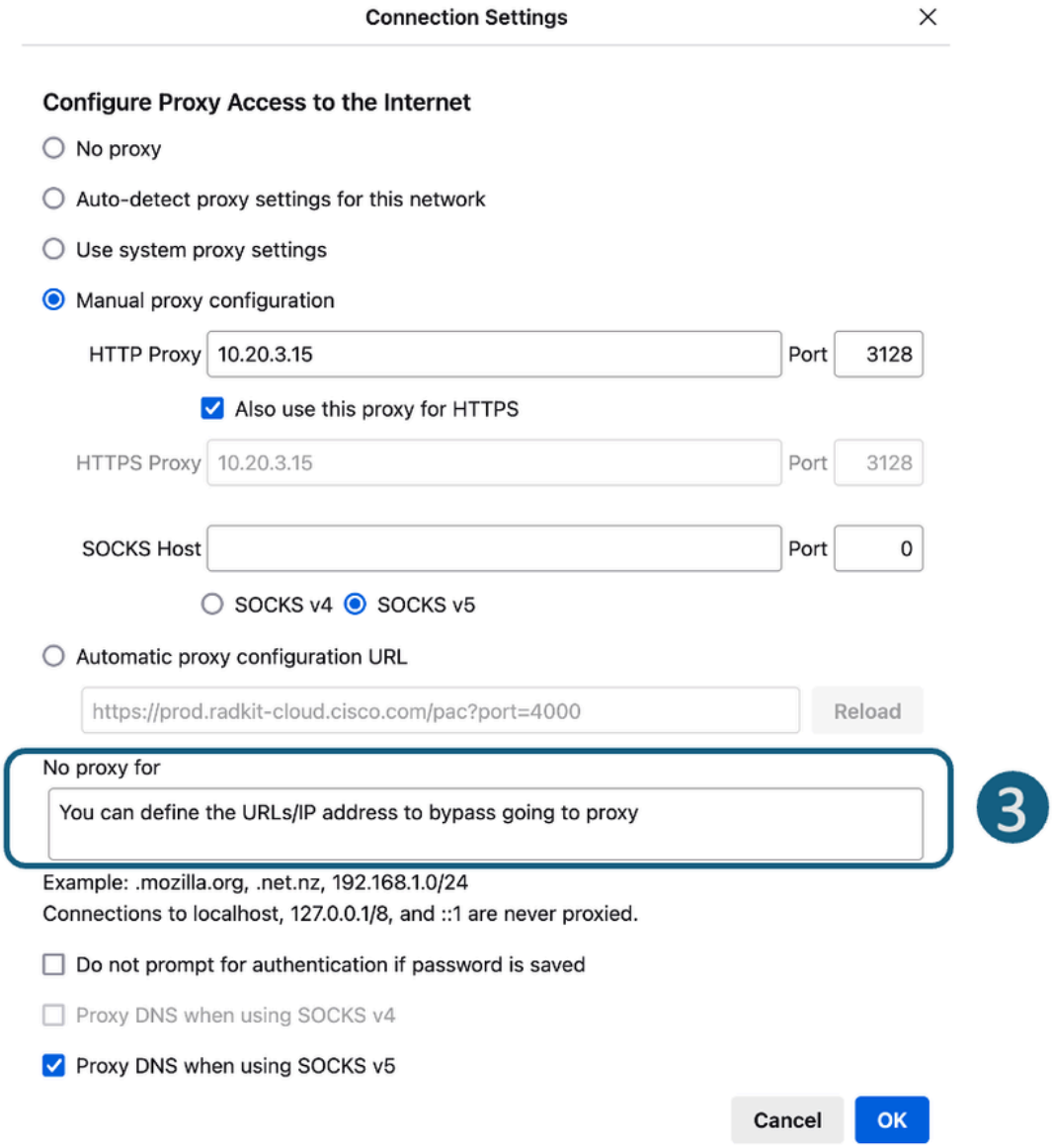
| | |
|---|---|
| | `if (dnsDomainIs(host, ".cisco.com")) return "DIRECT";`<br><br>참고: PAC 파일은 Cisco 제품이 아니므로 귀하의 편의를 위해 정보가 제공됩니다. 자세한 내용은 소프트웨어 공급업체에 문의하십시오. |
| 브라우저 구성(Microsoft Edge, Internet Explorer, Google Chrome) | 1단계. Start(시작) 메뉴에서 "Internet Options(인터넷 옵션)"를 입력하고 Enter를 누릅니다<br><br>2단계. Connections(연결) 탭으로 이동하고 LAN Settings(LAN 설정)를 클릭합니다<br><br>3단계. Advanced(고급)를 클릭합니다<br><br>4단계. 예외 섹션에서 원하는 URL을 정의합니다. |

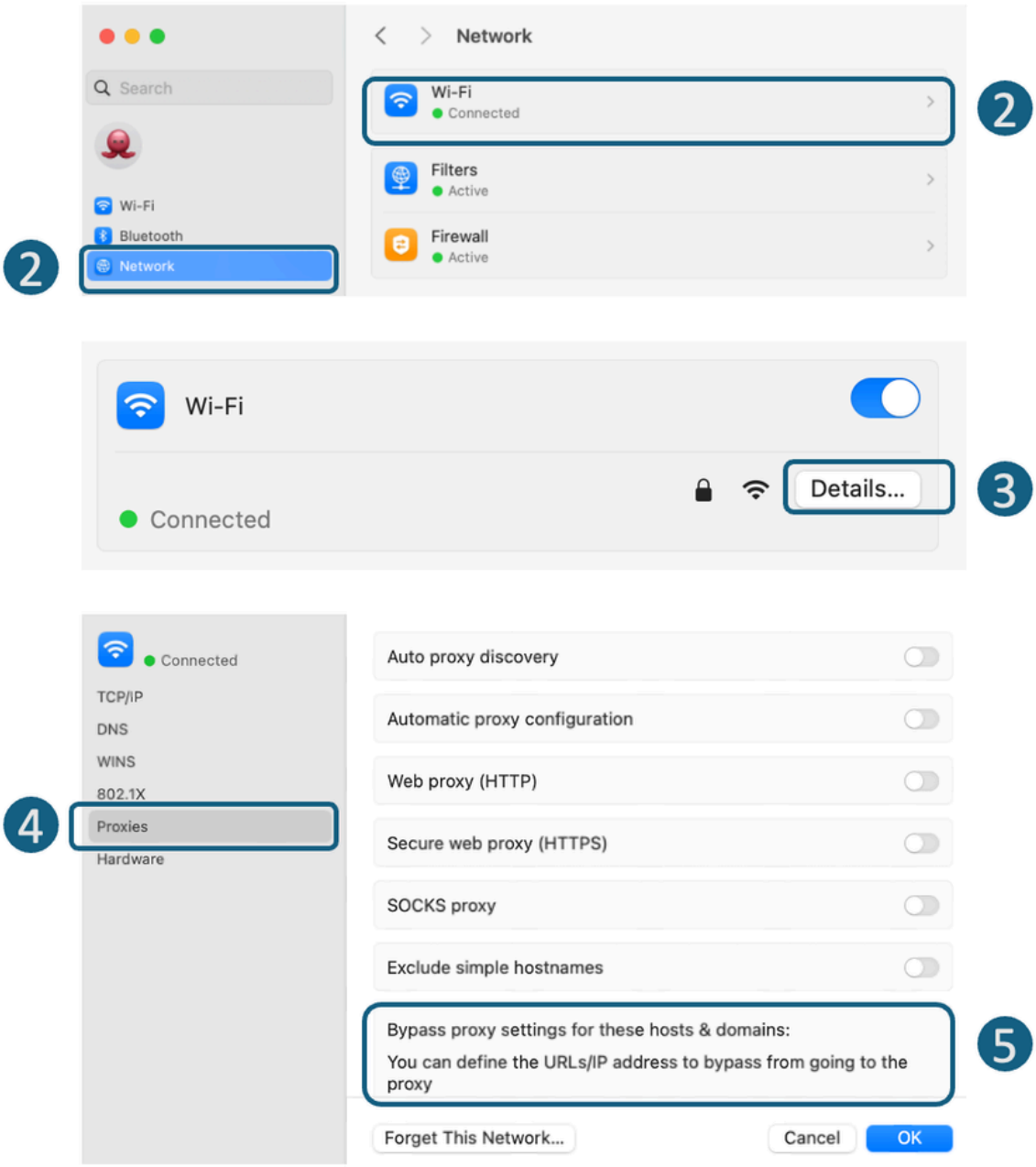



이미지 - Lan 설정으로 이동


Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address: 10.20.3.15
Port: 3128
Advanced
Bypass proxy server for local addresses
OK
Cancel
3
Proxy Settings
Servers
Type
Proxy address to use
Port
HTTP: 10.20.3.15 : 3128
Secure: 10.20.3.15 : 3128
FTP: 10.20.3.15 : 3128
Socks: :
Use the same proxy server for all protocols
Exceptions
Do not use proxy server for addresses beginning with:
You can define the URLs/IP address to bypass going to proxy
Use semicolons ( ; ) to separate entries.
OK
Cancel
4

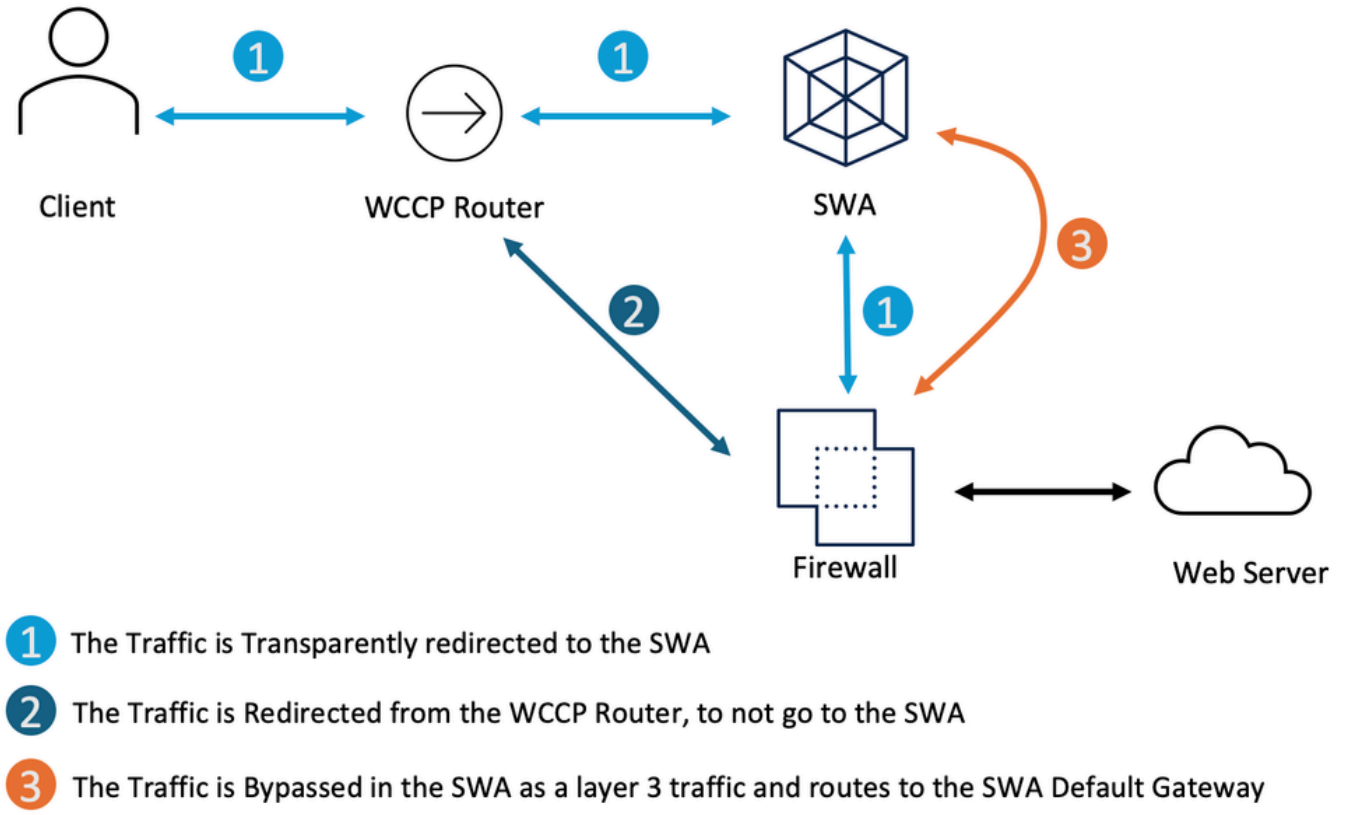
이미지 - 예외 정의

| | |
|---|---|
| 브라우저 컨피그레이션(Mozila FireFox) | 1단계. 오른쪽 상단 모서리에서 3개의 막대 메뉴를 클릭하고 Settings(설정)를 선택합니다.<br><br>2단계. 검색 표시줄에 proxy를 입력합니다.<br><br>3단계. No Proxy for(프록시 없음) 섹션에서 원하는 URL을 정의합니다.<br><br>  <br>Image(이미지) - Fire Fox에서 예외 정의 |
| 브라우저 구성(Apple Safari) | 1단계. 왼쪽 상단 모서리에서 Apple 아이콘을 클릭하고 System Settings(시스템 설정)를 선택합니다.<br><br>2단계. 왼쪽 패널에서 Network(네트워크)로 이동하여 인터넷에 액세스하는 데 사용 중인 Network Interface(네트워크 인터페이스)를 선택합니다. |

| | |
|---|---|
| | 3단계. Details(세부사항)를 클릭합니다.<br><br>4단계. 왼쪽 패널에서 Proxies(프록시)를 선택합니다.<br><br>5단계. Bypass Proxy Settings(프록시 설정 우회) 섹션에서 원하는 URL을 정의합니다.<br><br>  <br><br>Image(이미지) - Fire Fox에서 예외 정의 |
| 그룹 정책 컨피그레이션 | 프록시 설정을 푸시하도록 그룹 정책을 구성한 방법에 따라 예외 목록을 정의할 수 있습니다. |

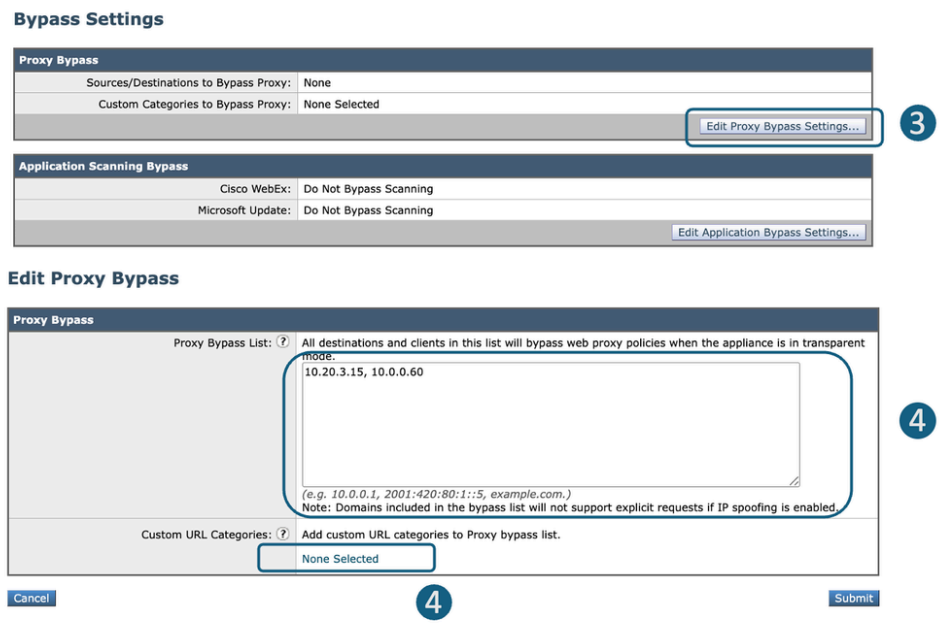
## 투명 구축에서 트래픽 우회

WCCP 라우터 또는 SWA Bypass 설정을 사용하여 투명 구축에서 트래픽을 우회할 수 있습니다. SWA Bypass는 레이어 3에서 작동하여 기본 게이트웨이로 트래픽을 라우팅하고 어플라이언스를 완전히 우회하므로 처리 및 별도의 세션 생성이 방지됩니다.




이미지 - 투명 구축에서 트래픽 우회

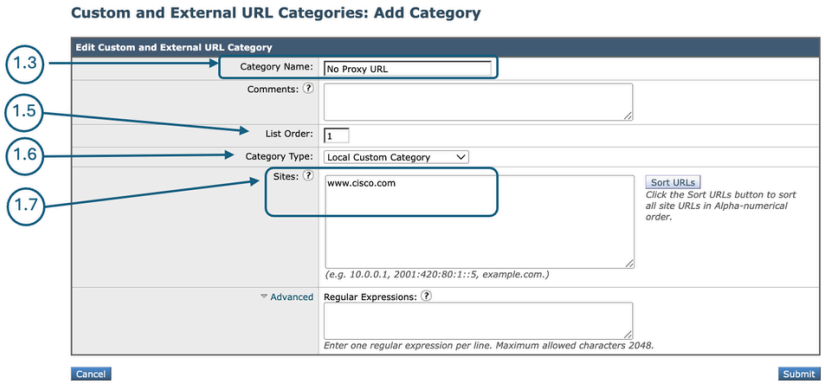
| 투명 프록시 구축 트래픽 우회 | 트래픽이 SWA에 도달하지 않도록 우회하는 단계 |
|---|---|
| SWA Bypass 설정 | 1단계. GUI에서 Web Security Manager(웹 보안 관리자)를 선택합니다.<br><br>2단계. Bypass Settings를 선택합니다.<br><br>3단계. Edit Proxy Bypass Settings(프록시 우회 설정 편집)를 클릭합니다.<br><br>4단계. URL, IP 주소를 입력하거나 목록에 사용자 지정 URL 카테고리를 추가할 수 있습니다.<br><br>5단계. 변경 사항을 제출하고 커밋합니다. |

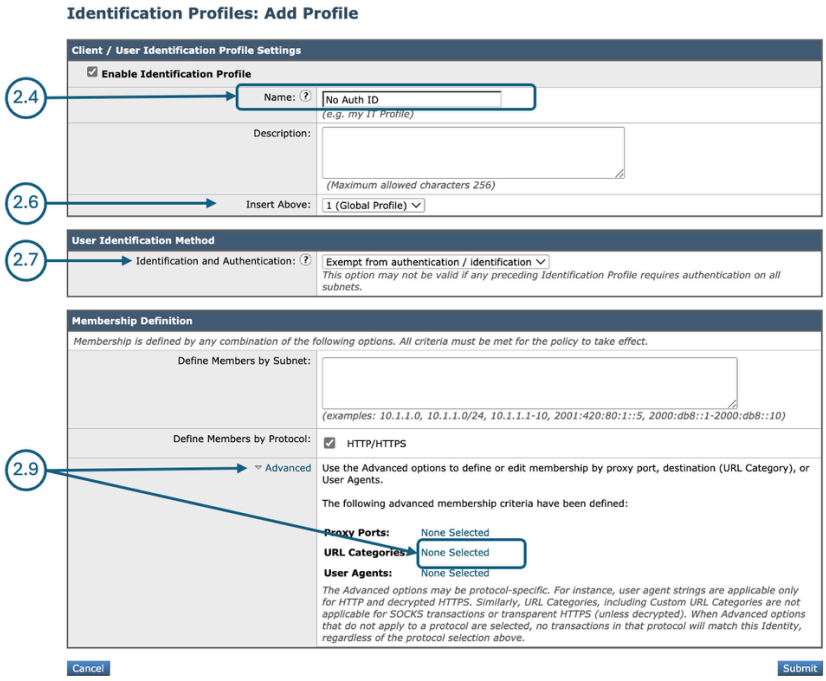
| | |
|---|---|
| |  <br>이미지 - Bypass 설정 구성<br><br>팁: 이 설정으로 우회된 트래픽은 액세스 로그에 기록되지 않으며 Bypass_Logs에서 볼 수 있습니다. |
| WCCP/PBR 라우터에서 트래픽 리디렉션 | 일부 트래픽을 SWA로 리디렉션하지 않도록 WCCP 또는 PBR(Policy Based Router)에서 소스 또는 대상 IP 주소를 구성할 수 있습니다. |

# SWA에서 통과 구성 및 트래픽 허용

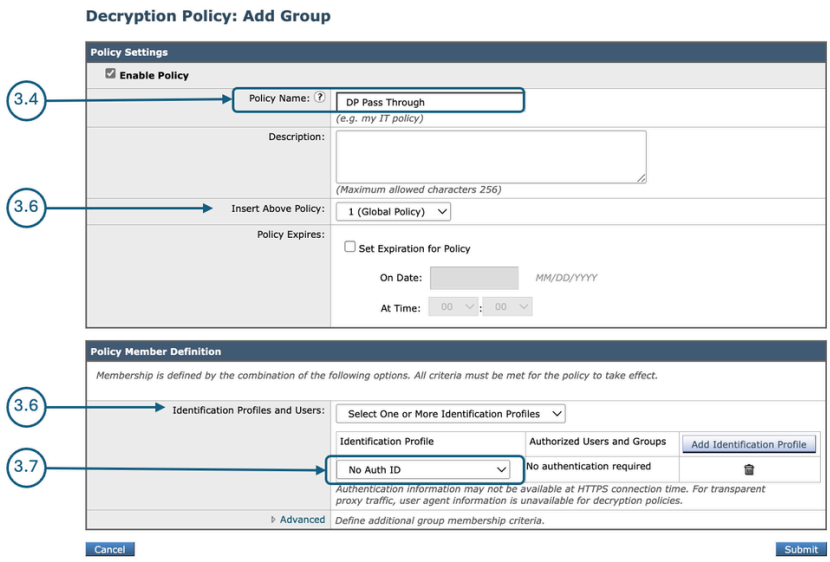
트래픽이 SWA에 도달하고 있으며 개인 정보 보호 문제로 인해 SWA의 부하를 줄이기 위해 SWA에서 일부 URL의 트래픽을 검사하지 않으려면 다음 단계를 수행합니다.

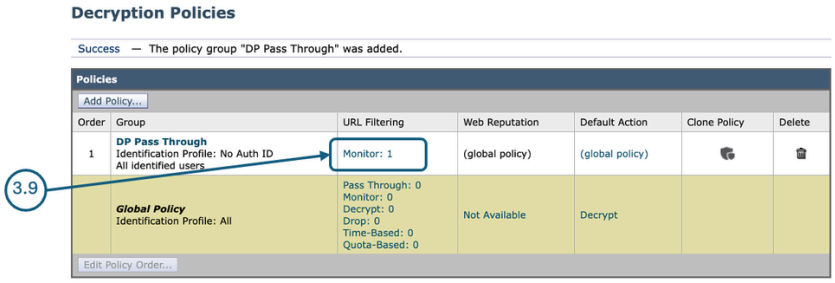
| 단계 | 단계 |
|---|---|
| 1단계. URL에 대한 맞춤형 URL 카테고리를 생성합니다. | 1.1단계.GUI에서 Web Security Manager를 선택한 다음 Custom and External URL Categories(사용자 지정 및 외부 URL 범주)를 클릭합니다.<br>1.2단계.Add Categories(범주 추가)를 클릭하여 사용자 지정 URL 범주를 추가합니다.<br>1.3단계.고유한 CategoryName을 할당합니다.<br>1.4단계. (선택 사항) 설명을 추가합니다.<br><br>1.5단계. List Order(주문 목록)에서 맨 위에 배치할 첫 번째 범 |

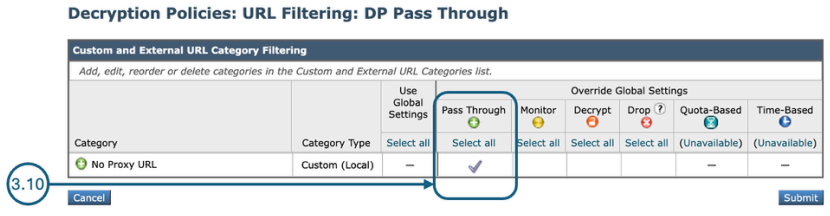
| | |
|---|---|
| | 주를 선택합니다.<br><br>1.6단계. Category Type(카테고리 유형) 드롭다운 목록에서 Local Custom Category(로컬 맞춤형 카테고리)를 선택합니다.<br><br>1.7단계. 사이트 섹션에서 원하는 URL을 추가합니다.<br><br>1.8단계. 제출.<br><br>  <br><br><br>이미지 - 사용자 지정 URL 범주 만들기 |
| 2단계. 인증에서 트래픽을 제외할 식별 프로필을 생성합니다. | 2.1단계.GUI에서 Web Security Manager를 선택한 다음 Identification Profiles(식별 프로필)를 클릭합니다.<br>2.2단계.프로파일 추가(Add Profile)를 클릭하여 프로파일을 추가합니다.<br>2.3단계.Enable Identification Profile(식별 프로필 활성화) 확인란을 사용하여 이 프로필을 활성화하거나 삭제하지 않고 신속하게 비활성화합니다.<br>2.4단계.고유한 profileName을 할당합니다.<br>2.5단계. (선택 사항) 설명을 추가합니다.<br>2.6단계.Insert Above(위에 삽입) 드롭다운 목록에서 이 프로파일을 테이블에 표시할 위치를 선택합니다.<br><br>2.7단계. User Identification Method(사용자 식별 방법) 섹션에서 Exempt from authentication/identification(인증/식별에서 제외)을 선택합니다.<br><br>2.8단계 특정 IP 주소에 대한 트래픽을 통과시키려는 경우가 아니면 서브넷별 구성원 정의(Define Members by Subnet)에서 모든 클라이언트 IP 주소를 포함하려면 이 필드를 비워 둡니다.<br><br>2.9단계. Advanced(고급) 섹션에서 Custom URL Categories(사용자 지정 URL 범주)를 선택합니다. |

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

이미지 - 식별 프로필 추가<br><br>2.10단계. 1단계에서 생성한 맞춤형 URL 카테고리를 추가합니다.<br><br>2.11단계. 완료를 누릅니다.<br><br>2.12단계. 제출.</td>
</tr>
<tr>
<td>3단계. 트래픽을 통과하기 위한 암호 해독 정책을 생성합니다.</td>
<td>3.1단계.GUI에서 Web Security Manager를 선택한 다음 Decryption Policy를 클릭합니다.<br><br>3.2단계. 정책 추가를 클릭하여 암호 해독 정책을 추가합니다.<br><br>3.3단계.Enable Policy(정책 활성화) 확인란을 사용하여 이 정책을 활성화합니다.<br>3.4단계.고유한 PolicyName을 할당합니다.<br>3.5단계. (선택 사항) 설명을 추가합니다.<br>3.6단계Insert Above Policy 드롭다운 목록에서 첫 번째 Policy를 선택합니다.<br><br>3.7단계.Identification Profiles and Users(식별 프로필 및 사용자)에서 2단계에서 생성한 식별 프로필을 선택합니다.<br><br>3.8단계. 제출.</td>
</tr>
</table>

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


이미지 - 암호 해독 정책 생성<br><br>
3.9단계.Decryption Policies(암호 해독 정책) 페이지의 URL Filtering(URL 필터링)에서 이 새 암호 해독 정책과 연결된 링크를 클릭합니다.<br><br>


이미지 - URL 필터링 선택<br><br>
3.10단계. 1단계에서 생성된 URL 카테고리에 대한 작업으로 통과를 선택합니다.<br><br>


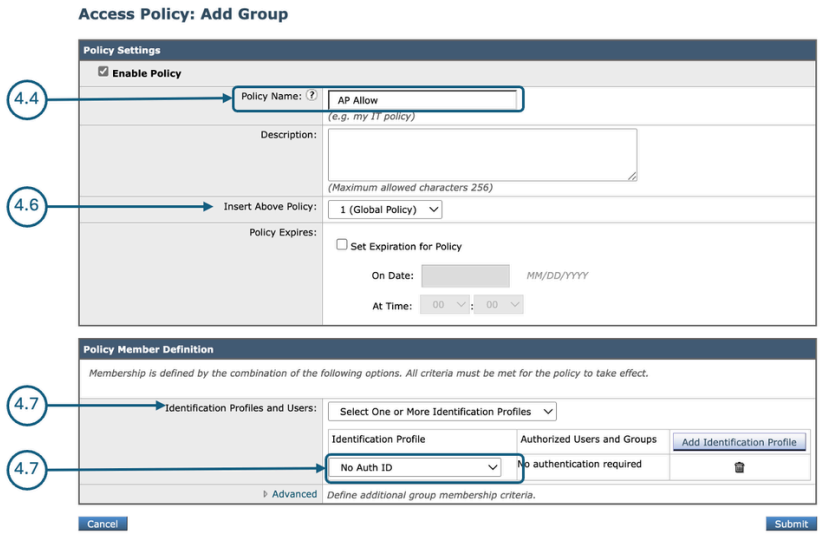
이미지 - 작업을 통과로 설정<br><br>
3.11단계. 제출.</td>
</tr>
<tr>
<td>4단계. Microsoft 업데이트 트래픽을 허용하는 액세스 정책을 만듭니다.</td>
<td>4.1단계.GUI에서 Web Security Manager를 선택한 다음 Access Policy(액세스 정책)를 클릭합니다.</td>
</tr>
</table>

4.2단계. Add Policy를 클릭하여 액세스 정책을 추가합니다.

4.3단계.Enable Policy(정책 활성화) 확인란을 사용하여 이 정책을 활성화합니다.
4.4단계.고유한 PolicyName을 할당합니다.
4.5단계. (선택 사항) 설명을 추가합니다.
4.6단계Insert Above Policy 드롭다운 목록에서 첫 번째 Policy를 선택합니다.

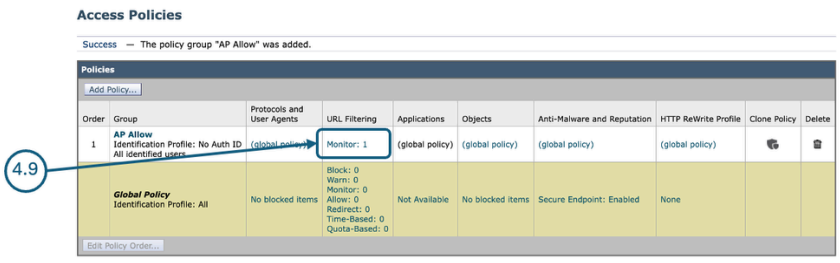
4.7단계.Identification Profiles and Users(식별 프로필 및 사용자)에서 2단계에서 생성한 식별 프로필을 선택합니다.

4.8단계. 제출.



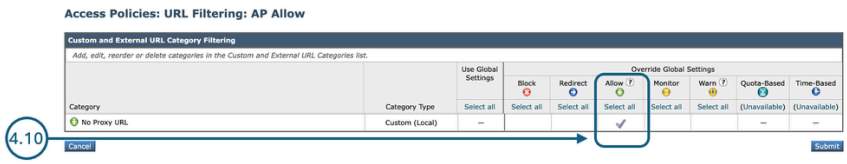

이미지 - 액세스 정책 생성

4.9단계. Access Policies(액세스 정책) 페이지의 URL Filtering(URL 필터링)에서 이 새 액세스 정책과 연결된 링크를 클릭합니다.




이미지 - URL 필터링 선택

4.10단계.Allow the Custom URL category created for the URL Category created for the URL Category created on the URL Category on the Step 1에서 생성한 URL 카테고리에 대해 Allow the action(맞춤형 URL 카테고리에 대한 작업 허용)을 선택합니다.




Image(이미지) - 작업을 Allow(허용)로 설정합니다.

4.11단계. 제출.

4.12단계. 변경 사항을 커밋합니다.

## 관련 정보

- Secure Web Appliance에서 Microsoft 업데이트 트래픽 우회
- Secure Web Appliance에서 인증 우회 - Cisco
- 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 트래픽 차단
- Secure Web Appliance에서 업로드 트래픽 차단
- SWA에서 실행 파일 다운로드 차단

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.