Secure Web Appliance에서 업스트림 프록시 구성

목차

소개

이 문서에서는 SWA(Secure Web Appliance)에서 업스트림 프록시를 구성하는 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
- SWA CLI(Command Line Interface)에 대한 관리 액세스

사용되는 구성 요소

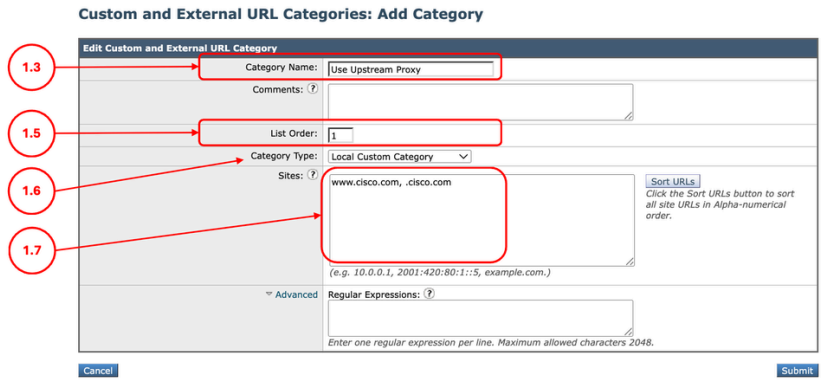
이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

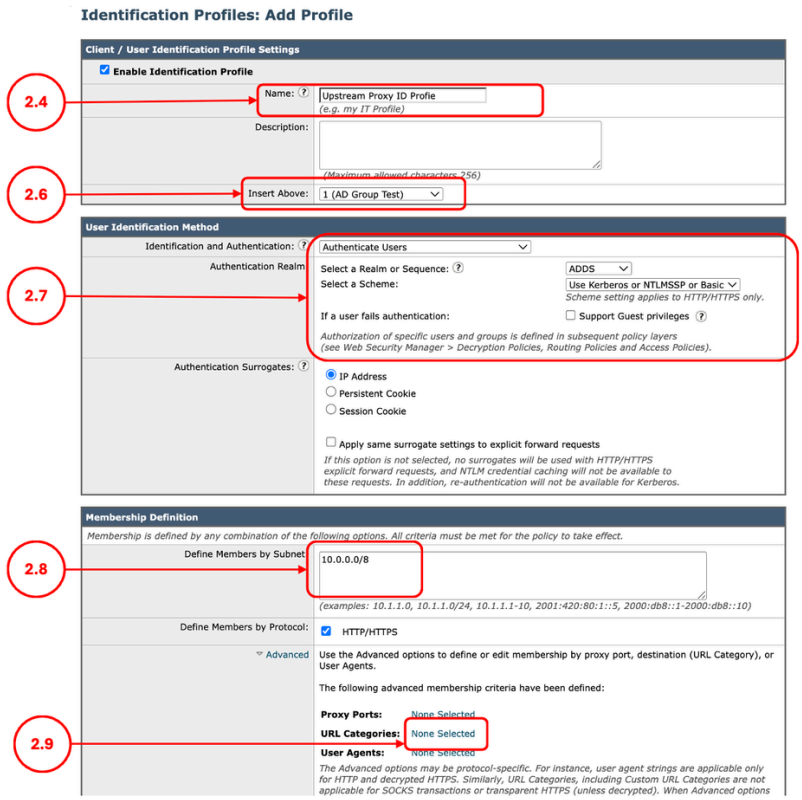
이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

업스트림 프록시 구성

SWA에서 업스트림 프록시를 구성하려면 다음 단계를 사용합니다.

단계	단계
1단계. (선택 사항) URL에 대한 맞춤형 URL 카테고리를 생성합니다 참고: 모든 트래픽에 대해 업스트림 프록시를 정의하려는 경우 이 단계를 건너뛸 수 있습니다.	1.1단계.GUI에서 Web Security Manager를 선택한 다음 Custom and External URL Categories(사용자 지정 및 외부 URL 범주)를 클릭합니다. 1.2단계.Add Categories(범주 추가)를 클릭하여 사용자 지정 URL 범주를 추가합니다. 1.3단계.고유한 CategoryName을 할당합니다. 1.4단계. (선택 사항) 설명을 추가합니다. 1.5단계. List Order(주문 목록)에서 맨 위에 배치할 첫 번째 범주를 선택합니다. 1.6단계. Category Type(카테고리 유형) 드롭다운 목록에서 Local Custom Category(로컬 맞춤형 카테고리)를 선택합니다. 1.7단계. Sites(사이트) 섹션에서 원하는 URL을 추가합니다. 1.8단계. 제출.

	 이미지 - 사용자 지정 URL 범주 만들기
2단계. (선택 사항) 업스트림 프록시를 사용할 식별 프로필을 생성합니다 참고: 모든 트래픽에 대해 업스트림 프록시를 정의하려는 경우 이 단계를 건너뛸 수 있습니다.	2.1단계.GUI에서 Web Security Manager를 선택한 다음 Identification Profiles(식별 프로필)를 클릭합니다. 2.2단계.프로파일 추가(Add Profile)를 클릭하여 프로파일을 추가합니다. 2.3단계.Enable Identification Profile(식별 프로필 활성화) 확인란을 사용하여 이 프로필을 활성화하거나 삭제하지 않고 신속하게 비활성화합니다. 2.4단계.고유한 profileName을 할당합니다. 2.5단계. (선택 사항) 설명을 추가합니다. 2.6단계.Insert Above(위에 삽입) 드롭다운 목록에서 이 프로파일을 테이블에 표시할 위치를 선택합니다. 2.7단계. 이 정책을 적중하는 사용자를 인증하지 않으려면 User Identification Method(사용자 식별 방법) 섹션에서 Exempt from authentication/identification(인증/식별에서 제외)을 선택하거나 인증 매개변수를 구성합니다. 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. 2.9단계(선택 사항: 특정 웹 사이트에 액세스하는 특정 사용자에 대해 업스트림 프록시를 사용해야 하는 경우 이 단계를 완료합니다.) Advanced(고급) 섹션에서 Custom URL Categories(맞춤형 URL 카테고리)를 선택하고 1단계에서 생성한 맞춤형 URL 카테고리를 추가합니다. 2.10단계. 제출.

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

이미지 - 식별 프로필 생성</td>
</tr>
<tr>
<td>3단계. 업스트림 프록시 생성</td>
<td>3.1단계.GUI에서 Network(네트워크)를 선택한 다음 Upstream Proxy(업스트림 프록시)를 클릭합니다.

3.2단계. 그룹 추가를 클릭합니다.

3.3단계.uniqueName을 할당합니다.
3.4단계. 프록시 주소 및 포트 번호를 정의합니다.
3.5단계(선택 사항) 업스트림 프록시가 두 개 이상인 경우 Add Row(행 추가)를 클릭하여 다음 프록시를 정의합니다.

3.6단계(선택 사항) 로드 밸런싱 섹션에서 둘 이상의 업스트림 프록시를 입력한 경우, 원하는 로드 밸런싱 방법을 정의합니다.

• 없음(장애 조치): 웹 프록시가 그룹에 있는 하나의 외부 프록시로 트랜잭션을 전달합니다. 나열된 순서대로 프록시에 연결을 시도합니다. 한 프록시에 연결할 수 없는 경우 웹 프록시가 목록의 다음 프록시에 연결을 시도합니다.
• 최소 연결: 웹 프록시는 그룹의 서로 다른 프록시에 있는 활성 요청 수를 추적하고 현재 최소 연결 수를 서비스하는 프록시에 트랜잭션을 전달합니다.
• 해시 기반:가장 최근에 사용되었습니다. 모든 프록시가 현재 활성 상태인 경우 웹 프록시는 가장 최근에 트랜잭션을 수신한 프록시에 트랜잭션을 전달합니다. 웹 프록</td>
</tr>
</table>

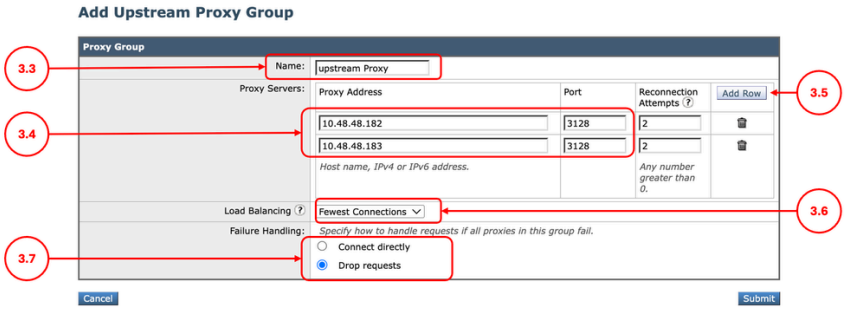
시가 다른 프록시 그룹의 구성원으로 프록시가 받은 트랜잭션도 고려한다는 점을 제외하면 이 설정은 라운드 로빈과 유사합니다. 즉, 프록시가 여러 프록시 그룹에 나열된 경우 "가장 최근 사용" 옵션은 해당 프록시에 부담을 덜 줍니다.

- 라운드 로빈: 웹 프록시는 나열된 순서대로 그룹의 모든 프록시 간에 트랜잭션을 동일하게 순환합니다.

3.7단계. 내부 정책에 따라 실패 처리 옵션을 선택합니다.

- 직접 연결: 요청을 대상 서버로 직접 전송합니다.
- 요청 삭제:전달하지 않고 요청을 삭제합니다.

3.8단계. 제출.



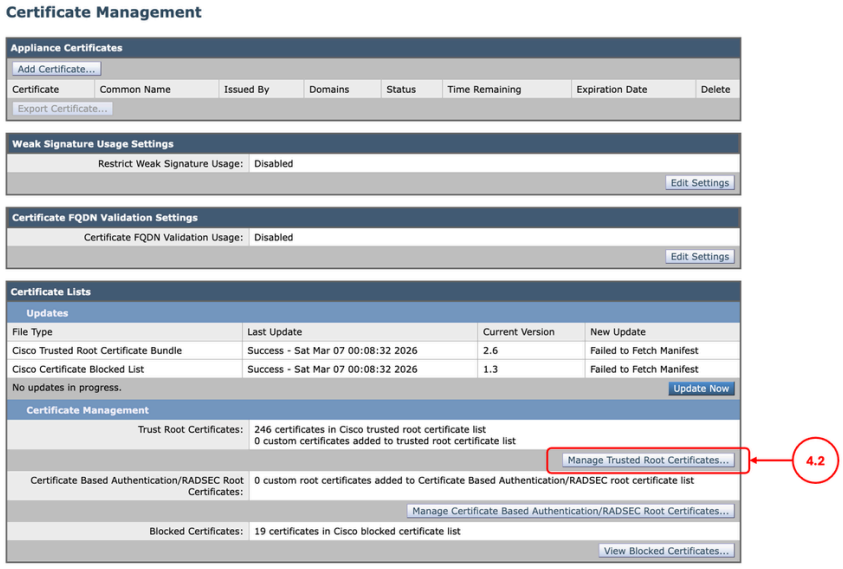
이미지 - 업스트림 프록시 그룹 추가

4단계. (선택 사항) 암호 해독 인증서를 업로드합니다

참고: 업스트림 프록시가 트래픽의 암호를 해독하지 않거나 해당 CA 서버가 SWA에서 이미 신뢰받는 경우 이 단계를 건너뛸 수 있습니다

4.1단계.GUI에서 Network(네트워크)를 선택한 다음 Certificate Management(인증서 관리)를 클릭합니다.

4.2단계. Certificate Management(인증서 관리) 섹션에서 Manage Trusted Root Certificates(신뢰할 수 있는 루트 인증서 관리)를 클릭합니다.



이미지 - 신뢰할 수 있는 루트 인증서 관리

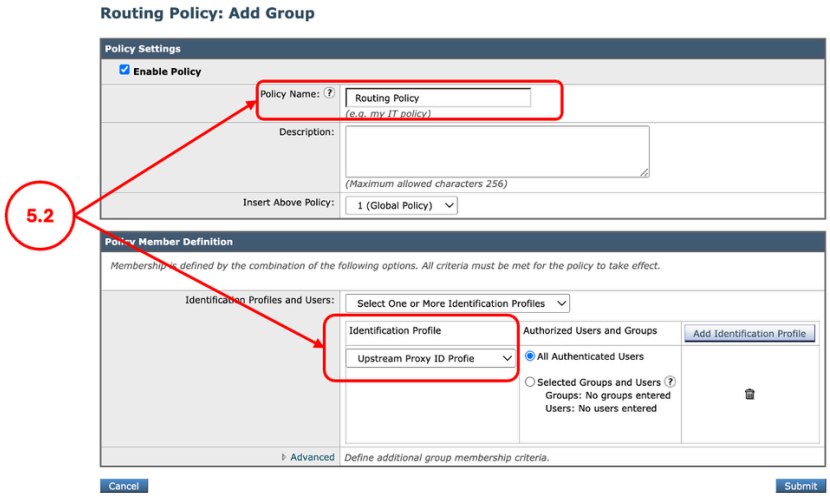
4.3단계. 변경 사항을 제출하고 커밋합니다.

⚠ 주의: 루트 및 중간 CA 인증서가 모두 필요한 경우 루트 CA 인증서를 먼저 업로드한 다음 Submit and Commit(제출 및 커밋)을 클릭합니다. 커밋이 완료되면 중간 CA 인증서를 가져오고 다시 변경 사항을 제출 및 커밋합니다.

5단계. 라우팅 정책 구성

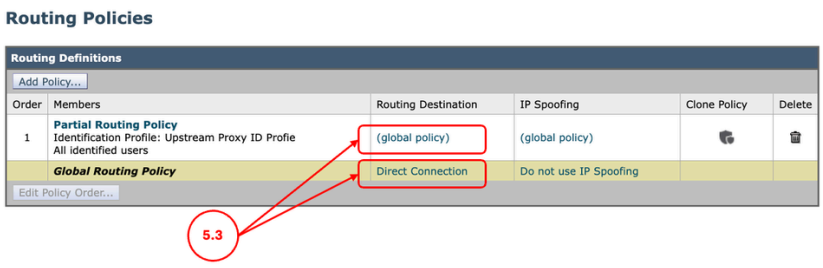
5.1단계. GUI에서 Web Security Manager를 선택한 다음 Routing Policy를 클릭합니다.

5.2단계(선택 사항) 특정 사용자 또는 웹 사이트에 대해 업스트림 프록시를 사용하려면 Add Policy(정책 추가)를 클릭하고 2단계에서 생성한 식별 프로필을 선택합니다.



이미지 - 라우팅 정책에 ID 프로필 추가

5.3단계. 업스트림 프록시를 사용하려는 원하는 조건의 경우 라우팅 대상 링크를 클릭하고 3단계에서 생성한 업스트림 프록시 그룹을 선택합니다.



이미지 - 라우팅 대상 구성

✎ 참고: 업스트림 프록시를 사용하는 모든 트래픽을 원하

	는 경우 글로벌 라우팅 정책에서 원하는 업스트림 프록시를 선택합니다. 5.4단계. 변경 사항을 제출하고 커밋합니다.
6단계. (선택 사항) 업스트림 프록시 무응답 시간 제한 설정 구성 팁: 이러한 값의 동작 및 잠재적 영향을 완전히 파악하지 않는 한 이 값을 수정하지 않는 것이 좋습니다.	6.1단계. CLI에 로그인하고 advancedproxyconfig를 실행합니다 6.2단계. 기타를 선택합니다. 6.3단계. Enter 키를 누르면 응답이 없는 업스트림 프록시를 확인하기 위한 최소 유휴 시간 제한 입력(초)이 표시됩니다. 최소 시간을 구성할 수 있습니다. SWA는 이전에 Sick으로 선언된 업스트림 프록시를 재시도하기 위해 대기합니다. 기본값은 10초입니다. 6.4단계. Enter를 눌러 다음 설정으로 진행합니다. 응답하지 않는 업스트림 프록시를 확인하기 위한 최대 유휴 시간 제한을 정의할 때 구성된 재연결 시도 횟수가 모두 소진되기 전에 이 시간 제한 값에 도달하면(3단계) SWA는 업스트림 프록시를 오프라인으로 간주합니다. 6.7단계. 마법사를 종료할 때까지 Enter 키를 계속 누르고 커밋을 실행하여 변경 사항을 저장합니다.

로깅

액세스 로그

액세스 로그에서 업스트림 프록시로 라우팅된 트래픽은 DEFAULT_PARENT로 표시되며 그 뒤에 업스트림 프록시의 이름이 표시됩니다. 예를 들면 다음과 같습니다.

```
1775659642.780 462 10.20.3.15 TCP_MISS_SSL/200 129 CONNECT tunnel://www.cisco.com:443/ "AMOJARRA\amojar
```

프록시 로그

proxylogs에서 업스트림 프록시의 상태를 확인할 수 있습니다.

팁: 업스트림 프록시와 관련된 로그를 검토하도록 피어에 대해 필터링할 수 있습니다.

다음은 몇 가지 예입니다. 3단계에서 재연결 시도를 두 번 구성했으므로 업스트림 프록시에 두 번 연결하지 못하면 업스트림 프록시가 dad로 선언되고 프록시 프로세스가 다시 시작될 때까지 SWA가 목록에서 이 업스트림 프록시를 제거합니다.

```
Thu Apr  2 13:52:35 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer-upstream 10.48.48.182:3128 was hea
Thu Apr  2 13:52:36 2026 Info: PROX_CONNTRACK : 940 : [15968:0] Peer 10.48.48.182:3128 was sick, now he
...
Thu Apr  2 13:59:37 2026 Info: PROX_CONNTRACK : 60 : [71197:0] Peer 10.48.48.183:3128 remains sick afte
Thu Apr  2 13:59:39 2026 Warning: PROX_CONNTRACK : 70 : [71197:0] Peer-upstream 10.48.48.183:3128 decla
```

참고: 업스트림 프록시가 TCP SYN 요청에 응답하지 않거나, HTTP 응답 코드를 반환하지 않거나, HTTP 504(게이트웨이 시간 제한) 응답을 반환하면, SWA는 업스트림 프록시를 사용할 수 없는 것으로 간주하고, 상태를 정상에서 병맛으로 변경합니다.

팁: SWA는 VIA 헤더를 반환할 경우 업스트림 프록시를 정상 프록시로 간주합니다.

관련 정보

- AsyncOS 15.0 for Cisco Secure Web Appliance 사용 설명서
- 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
- Secure Web Appliance에서 Microsoft 업데이트 트래픽 우회
- 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.