Secure Web Appliance와 Umbrella SWG 간의 프록시 체인 구성

목차

소개

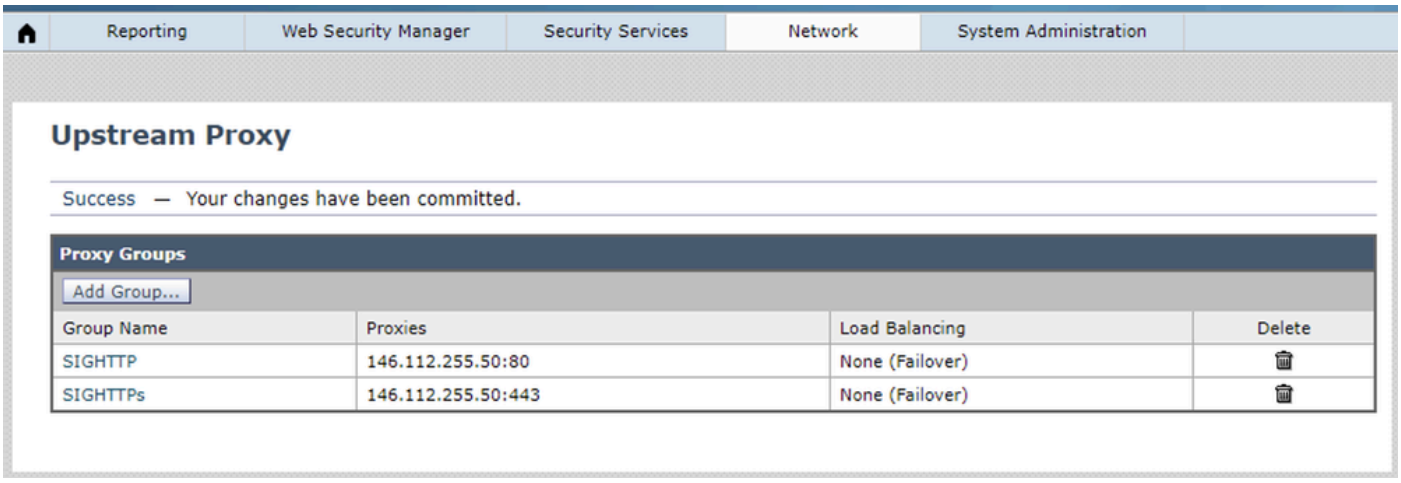
이 문서에서는 Secure Web Appliance와 Umbrella SWG(Secure Web Gateway) 간의 프록시 체인을 구성하는 방법에 대해 설명합니다.

개요

Umbrella SIG는 프록시 체인을 지원하며 다운스트림 프록시 서버의 모든 HTTP/HTTP 요청을 처리할 수 있습니다. Secure Web Appliance 및 SWG의 컨피그레이션을 포함하여 Cisco Secure Web Appliance(이전 Cisco WSA)와 Umbrella Secure Web Gateway(SWG) 간의 프록시 체인을 구현하기 위한 포괄적인 가이드입니다.

Secure Web Appliance 정책 컨피그레이션

1. SWG HTTP 및 HTTPs 링크를 네트워크>업스트림 프록시를 통해 업스트림 프록시로 구성합니다.

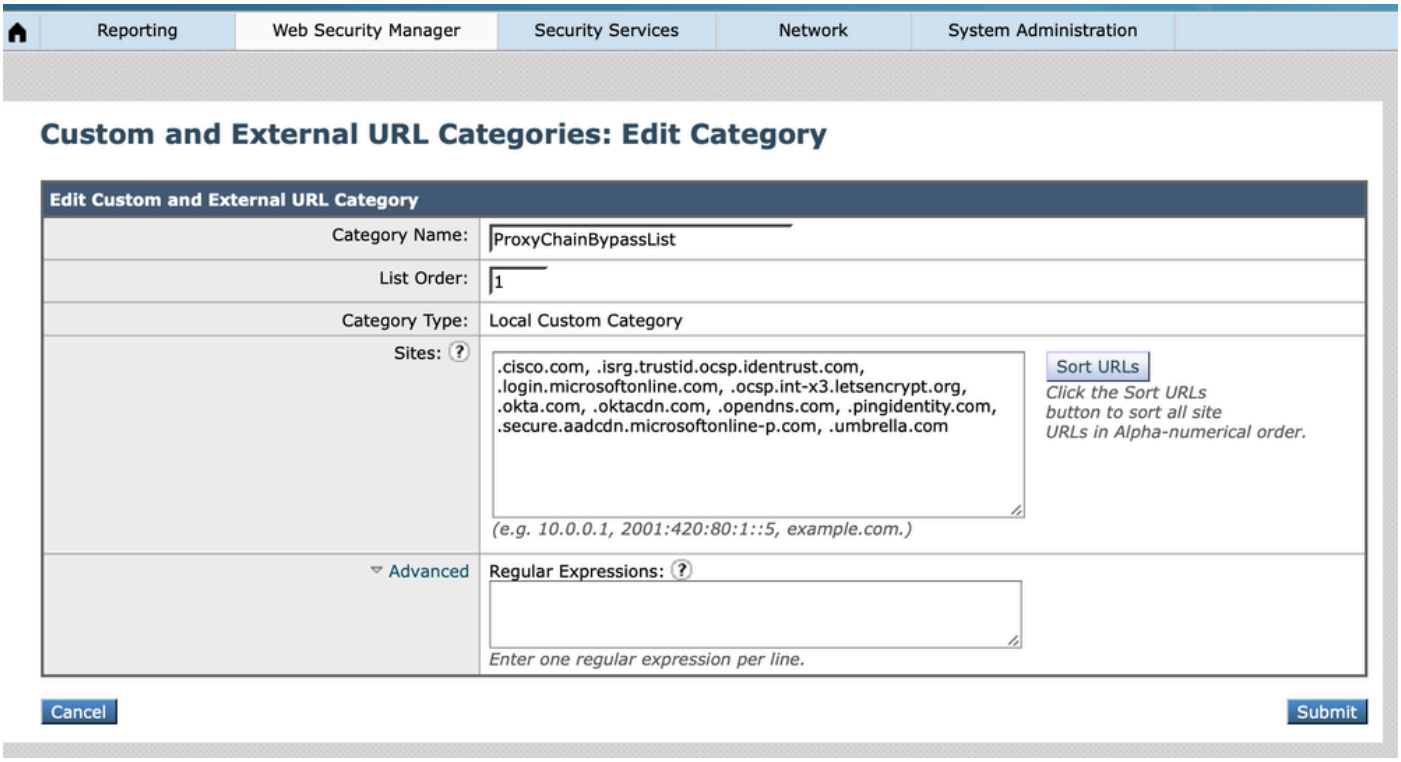


360079596451

2. Web Security Manager(웹 보안 관리자)>Routing Policy(라우팅 정책)를 통해 제안된 모든 URL을

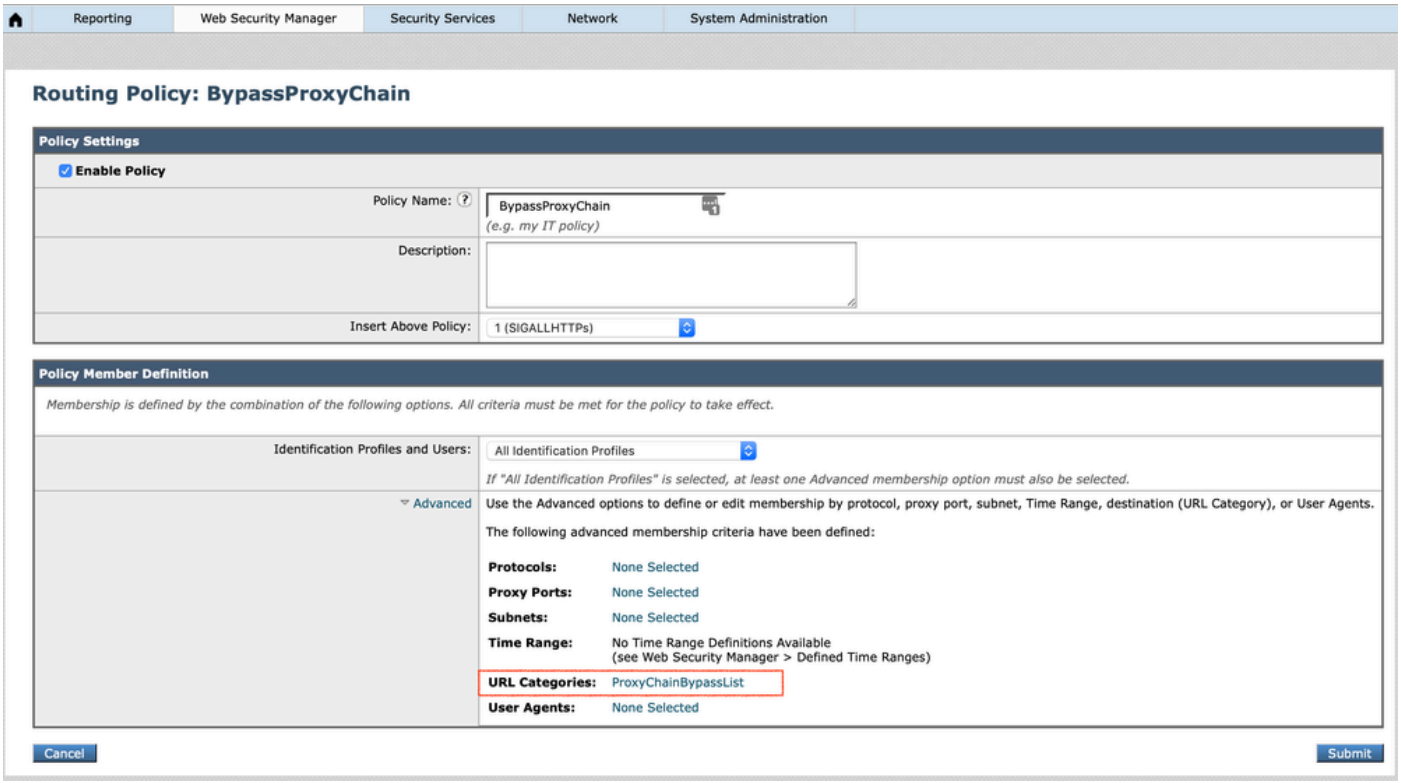
인터넷으로 직접 라우팅하는 우회 정책을 생성합니다. 우회된 모든 URL은 Cisco 문서에서 확인할 수 있습니다. [Cisco Umbrella SIG 사용 설명서: 프록시 연결 관리]

- 여기 표시된 대로 Web Security Manager>사용자 지정 및 외부 URL 범주로 이동하여 새 "사용자 지정 범주"를 만듭니다. 우회 정책은 "사용자 지정 범주"를 기반으로 합니다.



360050592552

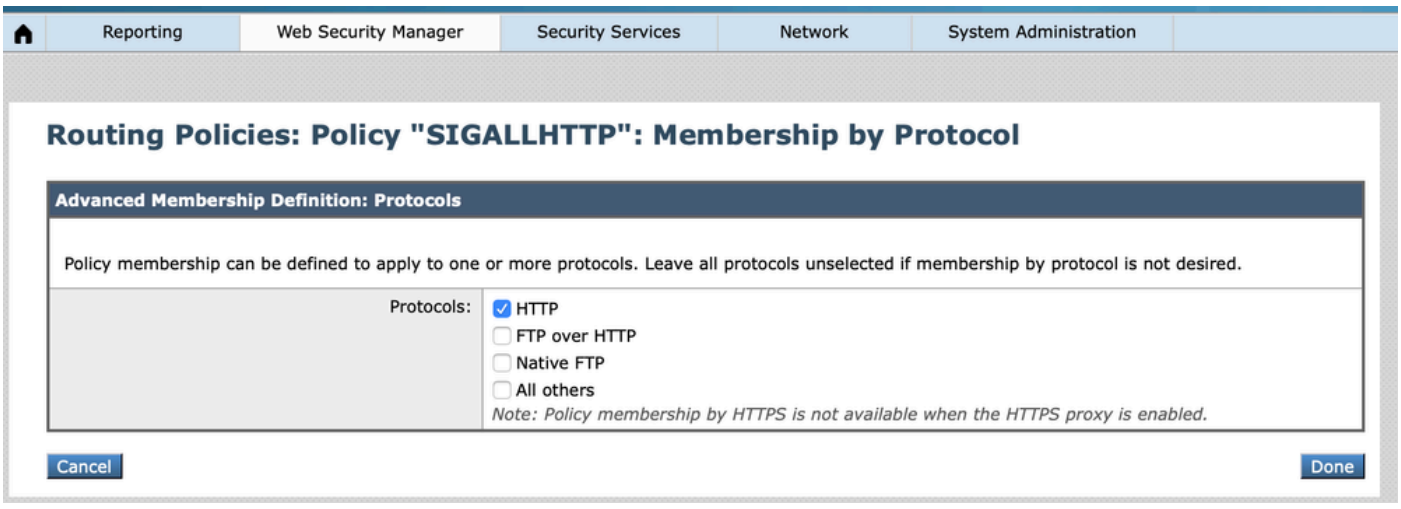
- 그런 다음 Web Security Manager(웹 보안 관리자)>Routing Policy(라우팅 정책)로 이동하여 새 우회 라우팅 정책을 생성합니다. Secure Web Appliance가 정책 순서에 따라 정책과 일치하므로 이 정책이 첫 번째인지 확인하십시오.



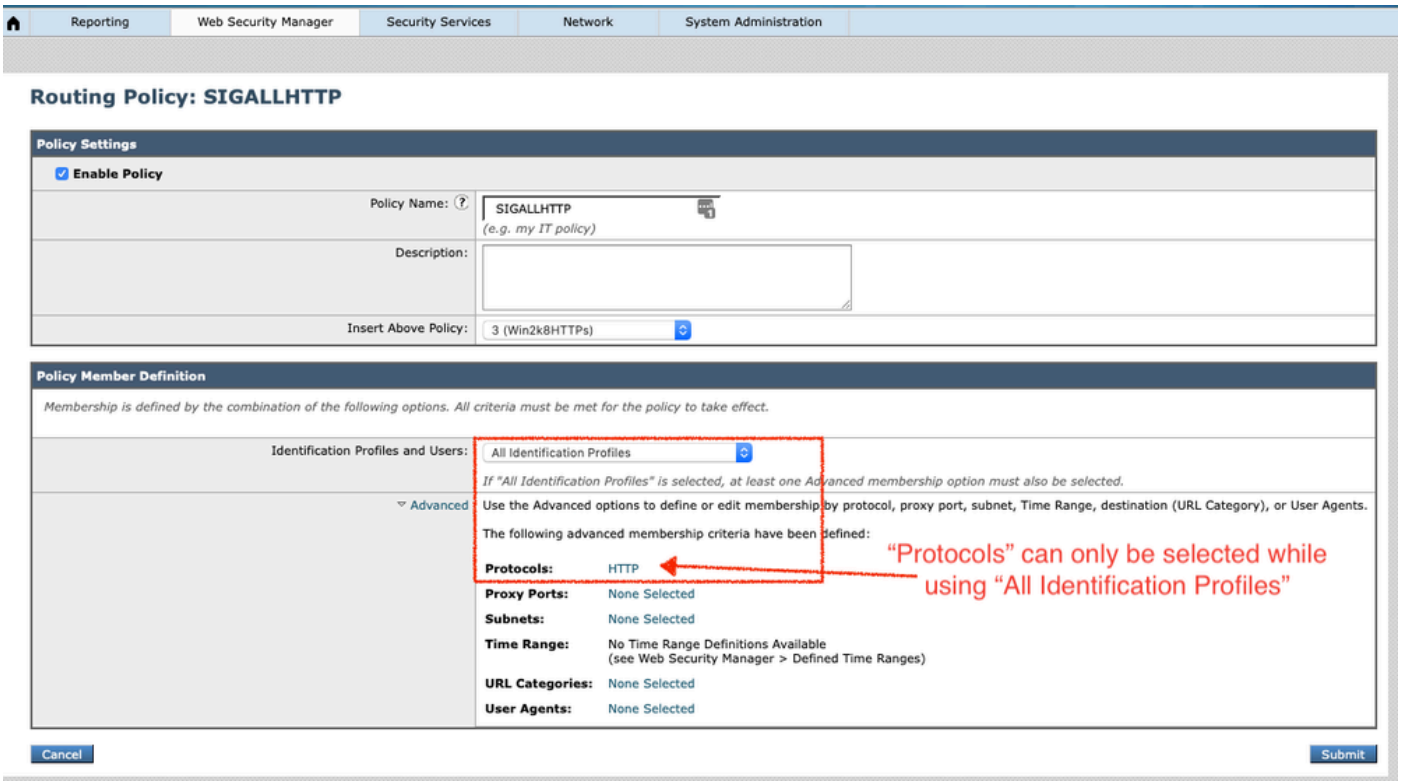
360050703131

3. 모든 HTTP 요청에 대해 새 라우팅 정책을 생성합니다.

- Secure Web Appliance 라우팅 정책 구성원 정의에서 프로토콜 옵션은 HTTP, FTP over HTTP, Native FTP 및 "All others"이며 "All Identification Profiles"가 선택됩니다. HTTP에 대한 옵션이 없으므로 모든 HTTP 요청에 대해 이 라우팅 정책을 구현한 후 HTTP 요청에 대한 라우팅 정책을 개별적으로 생성합니다.

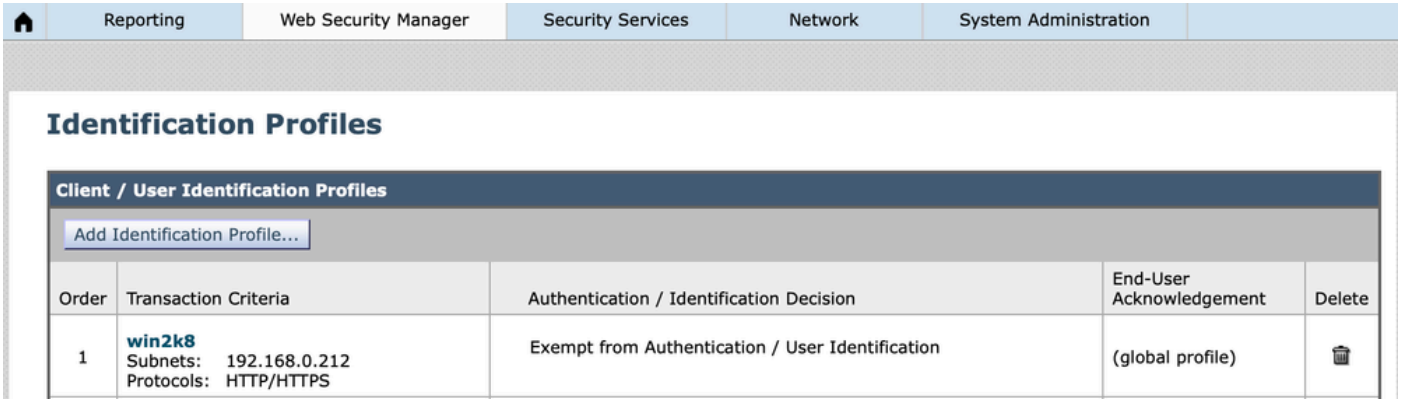


360050592772

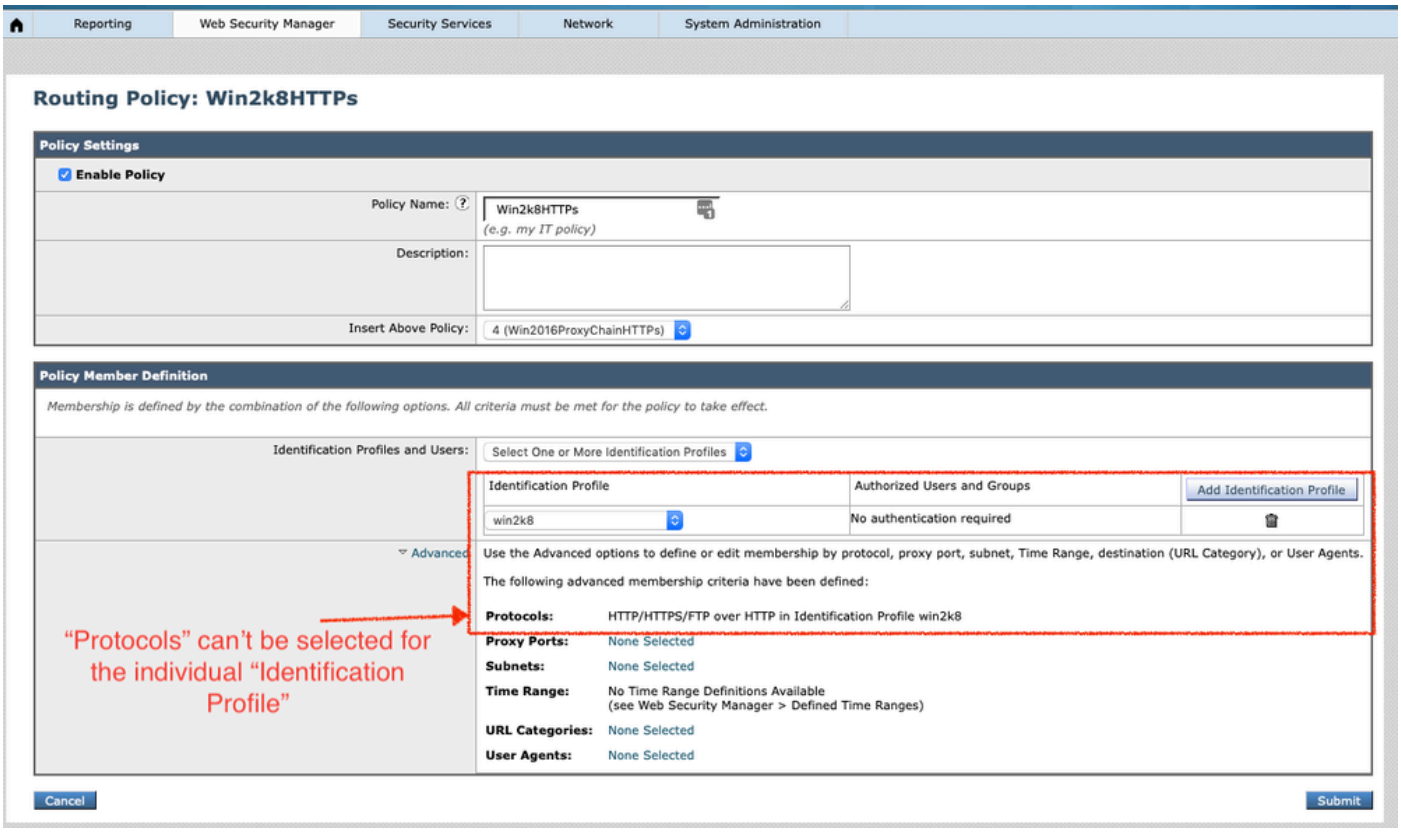


360050589572

4. "식별 프로필"을 기반으로 HTTP 요청에 대한 라우팅 정책을 만듭니다. Secure Web Appliance가 첫 번째 일치에 대한 "Identification"과 일치하므로 정의된 "Identification Profile"의 순서를 주의하십시오. 이 예에서 식별 프로필 "win2k8"은 내부 IP 기반 ID입니다.



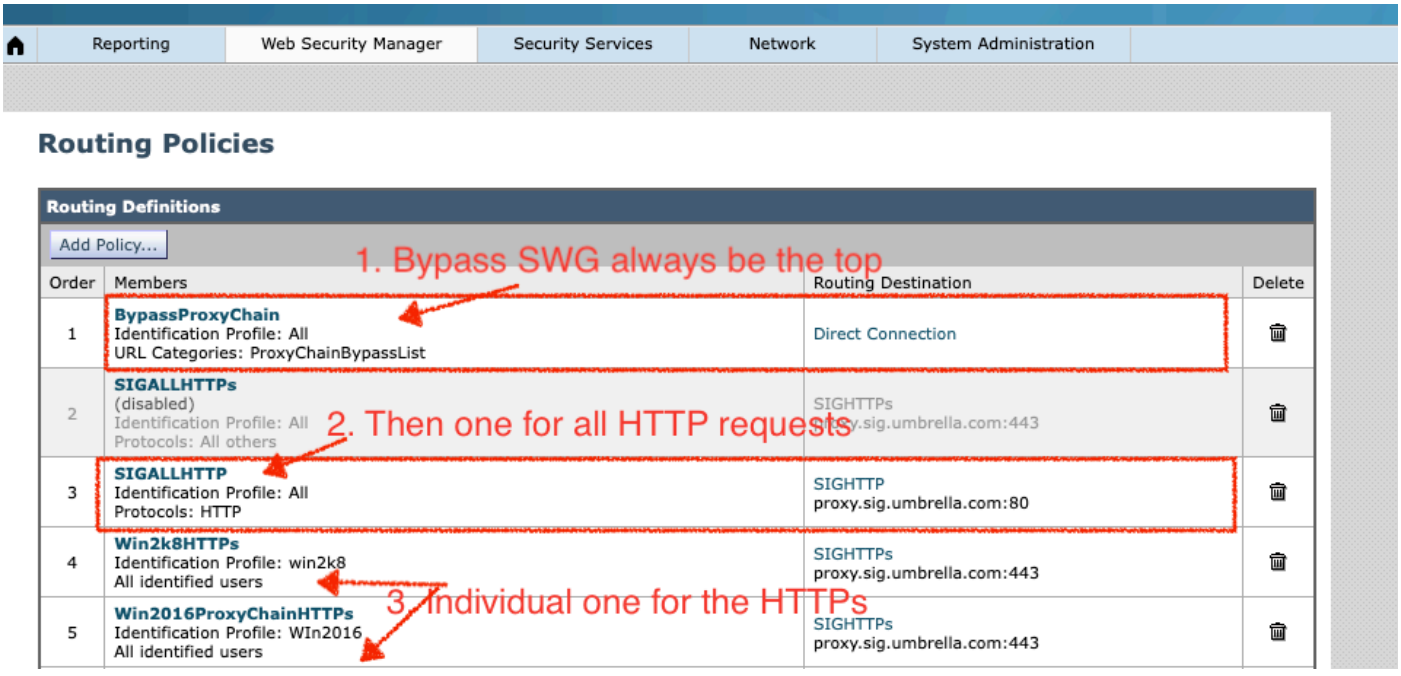
360050703971

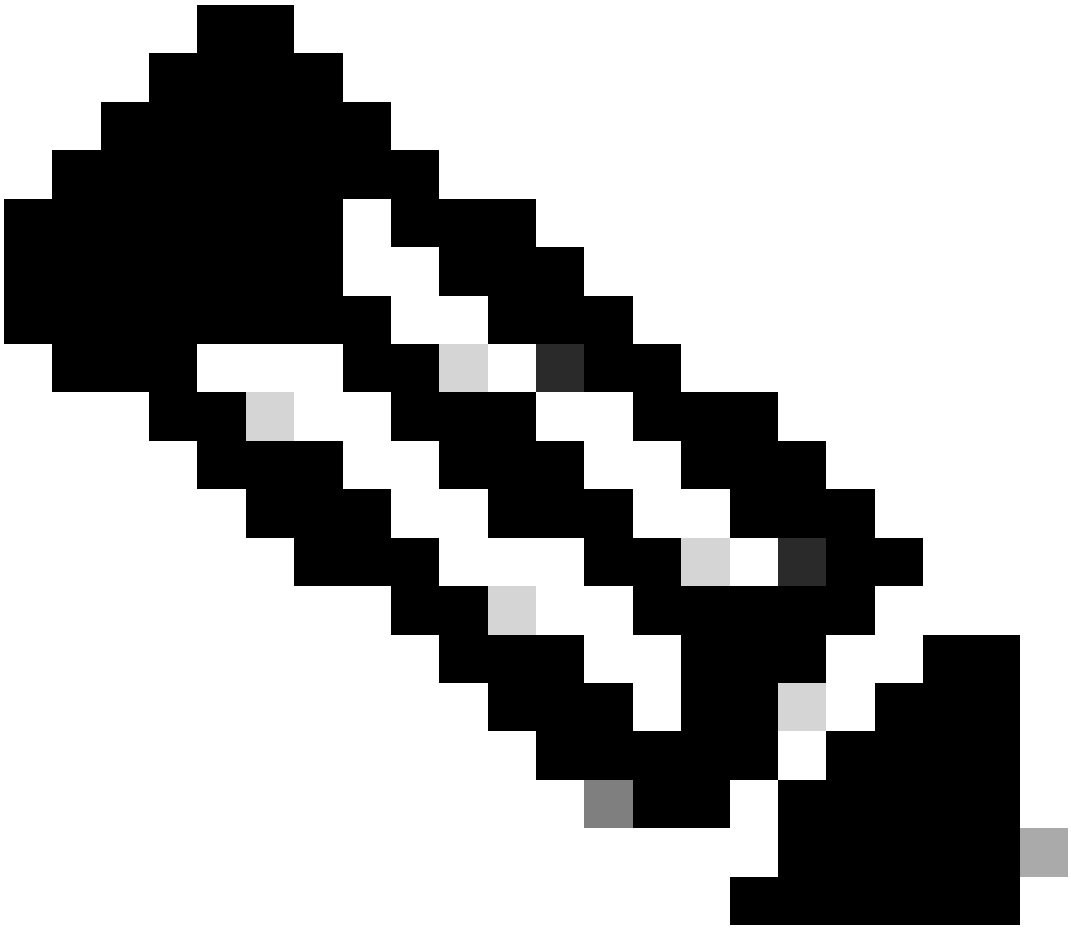


360050700091

5. Secure Web Appliance 라우팅 정책의 최종 구성

- Secure Web Appliance는 "하향식" 규칙 처리 방식을 사용하여 ID 및 액세스 정책을 평가합니다. 즉, 처리에서 임의의 시점에서 첫 번째 일치가 수행되면 Secure Web Appliance에서 수행한 작업이 결과로 이어집니다.
- 또한 ID를 먼저 평가합니다. 클라이언트의 액세스가 특정 ID와 일치하면 Secure Web Appliance는 클라이언트의 액세스와 일치하는 ID를 사용하도록 구성된 모든 액세스 정책을 확인합니다.





참고: 언급된 정책 컨피그레이션은 명시적 프록시 구축에만 적용됩니다.

투명 프록시 구축

투명 HTTPS의 경우 AsyncOS는 클라이언트 헤더의 정보에 액세스할 수 없습니다. 따라서 라우팅 정책 또는 식별 프로필이 클라이언트 헤더의 정보를 사용하는 경우 AsyncOS는 라우팅 정책을 적용할 수 없습니다.

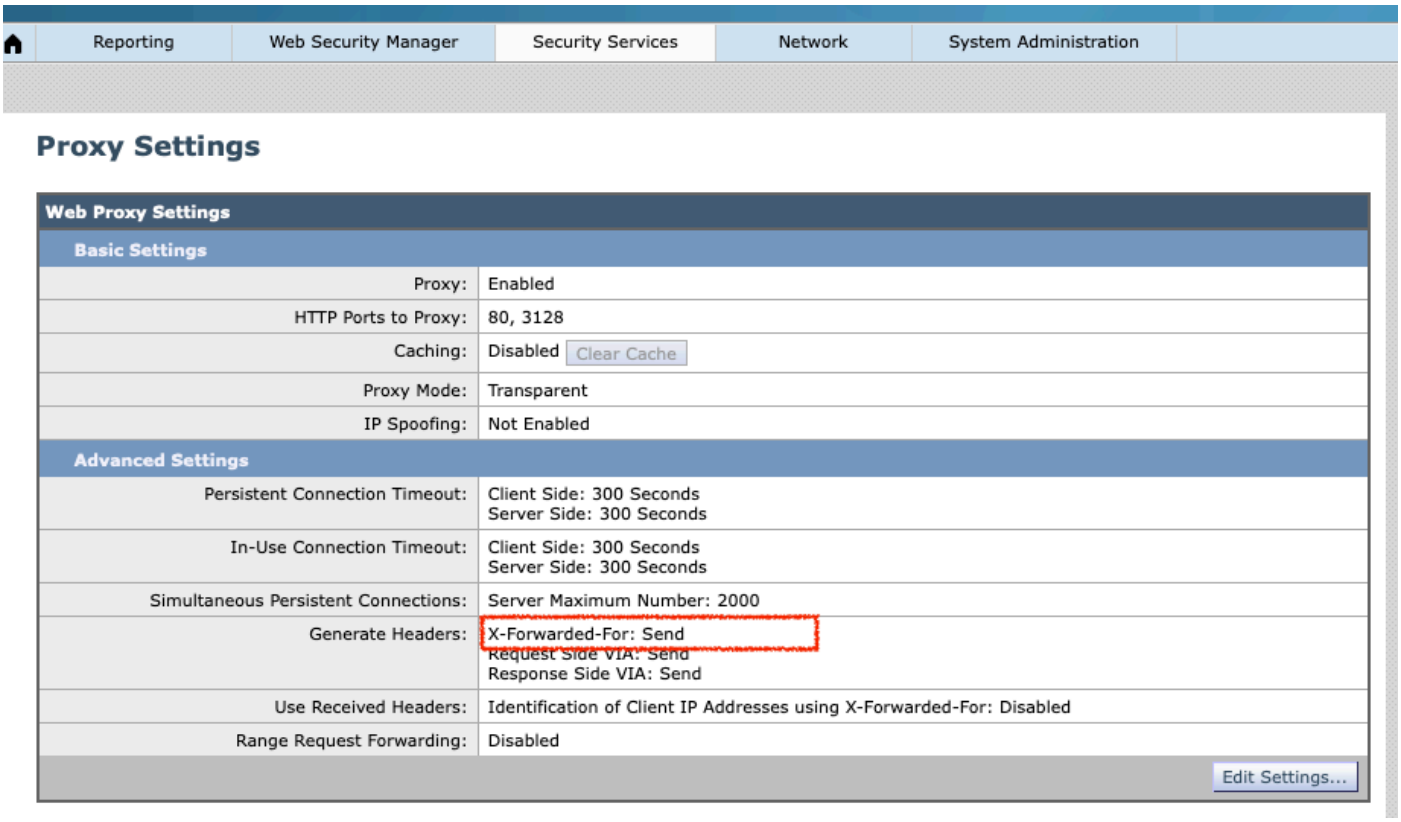
1. 다음과 같은 경우에만 투명하게 리디렉션된 HTTPS 트랜잭션이 라우팅 정책과 일치합니다.
   - 라우팅 정책 그룹에 URL 범주, 사용자 에이전트 등의 정책 구성원 자격 기준이 정의되어 있지 않습니다.
   - 식별 프로필에 URL 범주, 사용자 에이전트 등의 정책 구성원 자격 기준이 정의되어 있지 않습니다.
2. 식별 프로필 또는 라우팅 정책에 정의된 사용자 지정 URL 카테고리가 있는 경우 모든 투명

HTTPS 트랜잭션은 기본 라우팅 정책 그룹과 일치됩니다.

3. 투명 HTTPS 트랜잭션이 기본 라우팅 정책 그룹과 일치하게 될 수 있으므로 가능한 한 모든 식별 프로필로 라우팅 정책을 구성하지 마십시오.

1. X-Forwarded-For 헤더

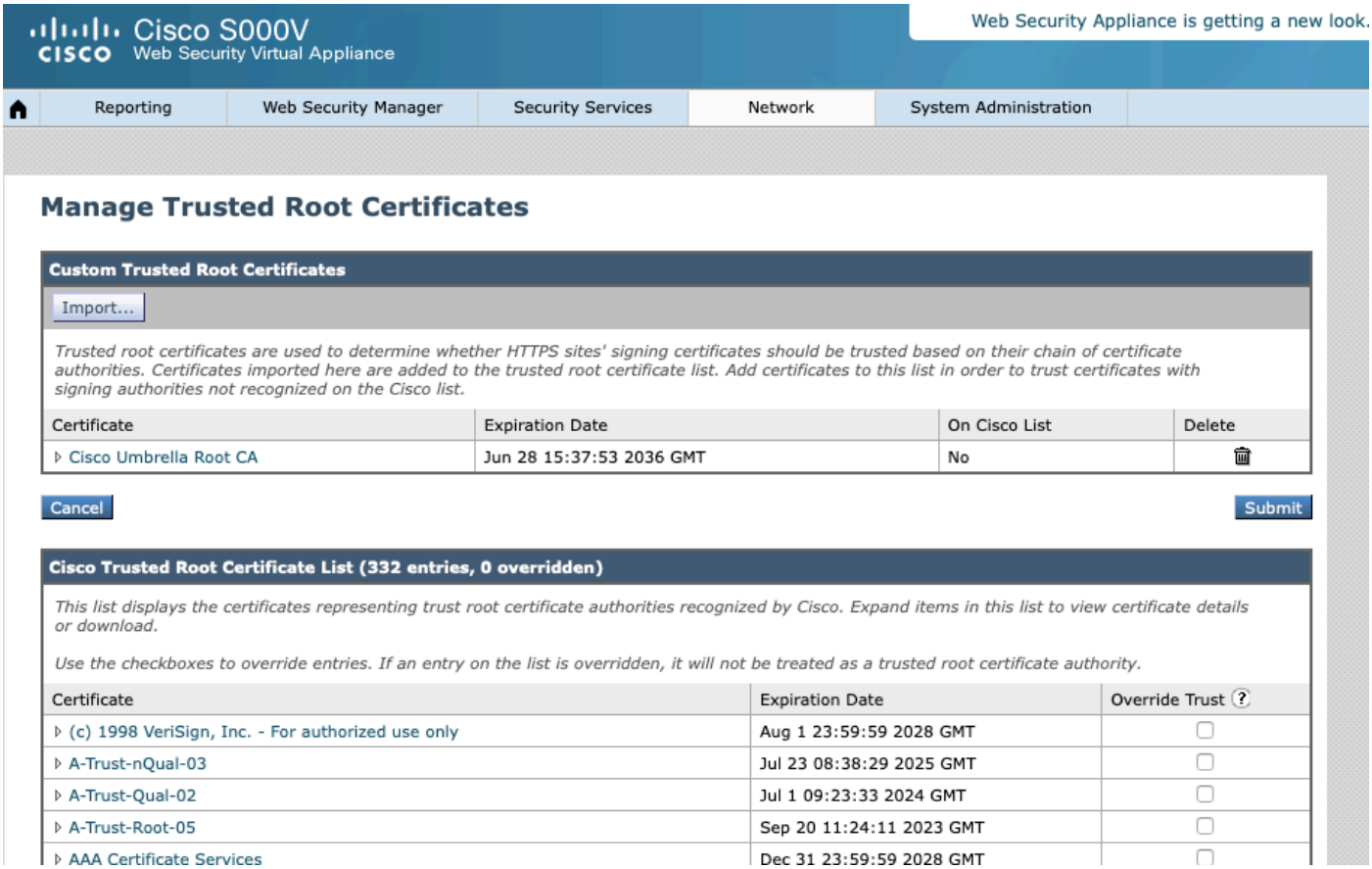
- swg에서 내부 IP 기반 웹 정책을 구현하려면 보안 서비스 > 프록시 설정을 통해 Secure Web Appliance에서 "X-Forwarded-For" 헤더를 활성화해야 합니다.



360050700111

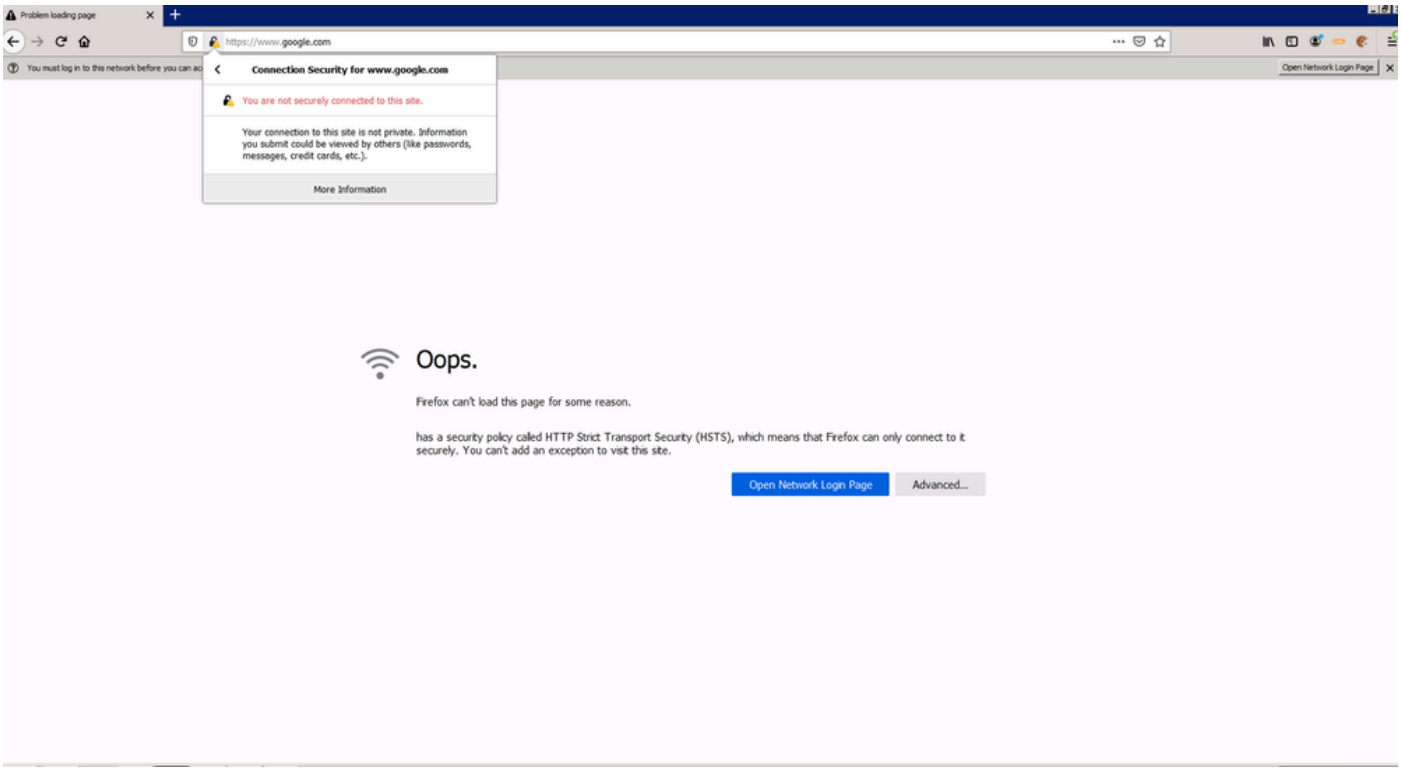
2. HTTP 암호 해독을 위한 신뢰할 수 있는 루트 인증서

- Umbrella 대시보드의 웹 정책에서 HTTP 암호 해독이 활성화된 경우 Umbrella 대시보드> Deployments(구축) > Configuration(컨피그레이션)에서 "Cisco Root Certificate(Cisco 루트 인증서)"를 다운로드하고 Secure Web Appliance의 신뢰할 수 있는 루트 인증서로 가져옵니다.



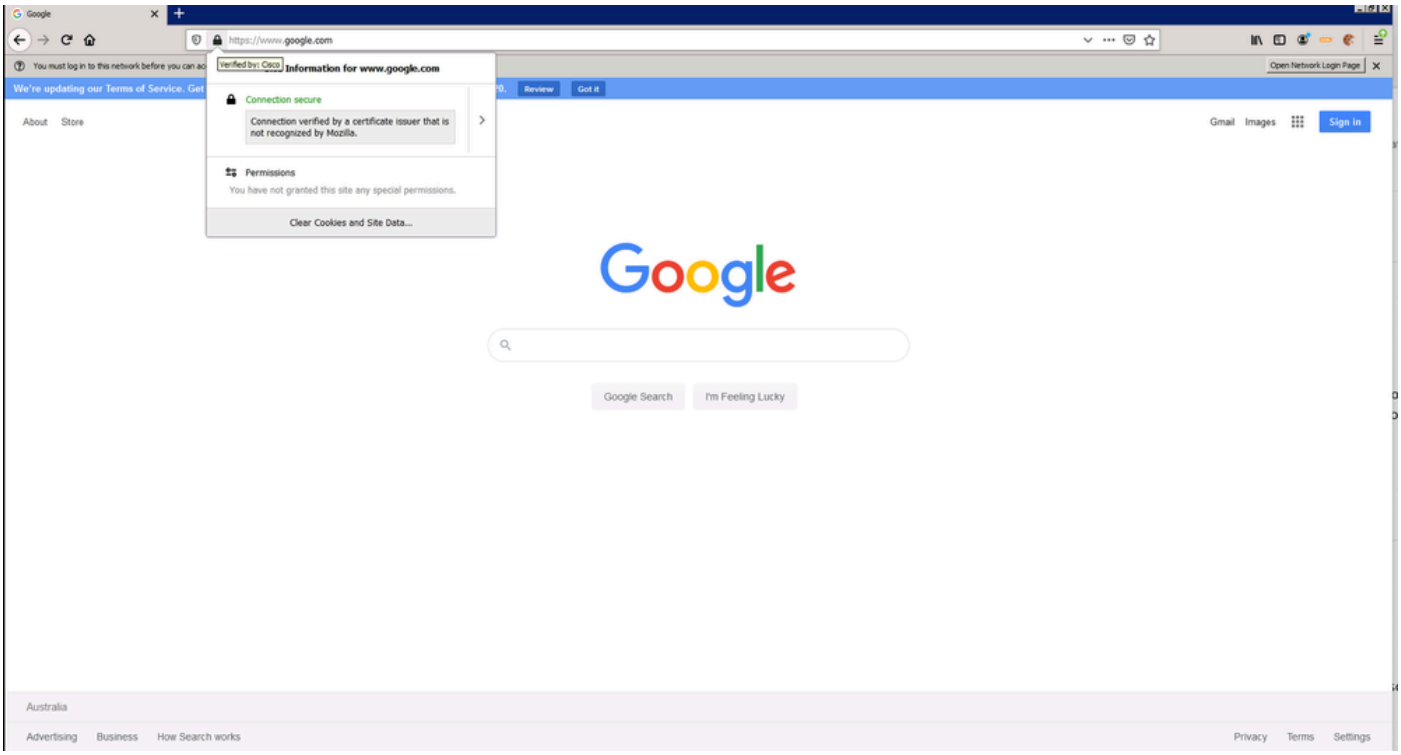
360050589612

- SWG 웹 정책에서 HTTP 암호 해독이 활성화된 상태에서 "Cisco 루트 인증서"를 Secure Web Appliance로 가져오지 않은 경우 최종 사용자에게 다음 예와 유사한 오류가 표시됩니다.
  - "이런. (브라우저)에서 어떤 이유로 이 페이지를 로드할 수 없습니다. 에는 HTTP HSTS(Strict Transport Security)라는 보안 정책이 있습니다. 즉 (브라우저)는 이 정책에 안전하게 연결할 수 있습니다. 이 사이트를 방문하는 예외를 추가할 수 없습니다."
  - "이 사이트에 안전하게 연결되지 않았습니다."



360050700171

- Umbrella SWG에서 해독된 HTTP의 예입니다. 인증서는 "Cisco Root Certificate"에서 확인합니다.



360050700191

Umbrella 대시보드의 SWG 웹 정책 컨피그레이션

내부 IP 기반 SWG 웹 정책:

- SWG는 내부 IP를 식별하기 위해 이를 사용하므로 Secure Web Appliance에서 "X-Forwarded-For" 헤더를 활성화해야 합니다.
- Deployment(구축) > Networks(네트워크)에서 Secure Web Appliance의 이그레스 IP를 등록합니다.
- Deployment(구축) > Configuration(컨피그레이션) > Internal Networks(내부 네트워크)에서 클라이언트 머신의 내부 IP를 생성합니다. "Show Networks(네트워크 표시)"를 선택/선택한 후 등록된 Secure Web Appliance 이그레스 IP(1단계)를 선택하십시오.
- 2단계에서 생성한 내부 IP를 기반으로 새 웹 정책을 생성합니다.
- 웹 정책에서 "SAML 사용" 옵션이 비활성화되어 있는지 확인합니다.

AD 사용자/그룹 기반 SWG 웹 정책:

- 모든 AD 사용자 및 그룹이 Umbrella 대시보드에 프로비저닝되었는지 확인합니다.
- "Enable SAML(SAML 활성화)" 옵션이 활성화된 Secure Web Appliance의 등록된 이그레스 IP를 기반으로 새 웹 정책을 생성합니다.
- "SAML 활성화" 옵션이 비활성화된 AD 사용자/그룹을 기반으로 다른 새 웹 정책을 생성합니다. 또한 이 웹 정책을 2단계에서 생성한 웹 정책보다 먼저 적용해야 합니다.

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.