Web Security Appliance에서 Webex 애플리케이션에 대한 추가 패스스루 설정을 구성하는 방법

소개

이 문서에서는 특수 구축 조건에서 적절한 Cisco Webex 애플리케이션 기능을 보장하기 위해 SWA/WSA(Secure Web Appliance) 우회 정책을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Async OS for Secure Web Appliance 14.x 이상
- Secure Web Appliance GUI(그래픽 사용자 인터페이스)에 대한 관리 사용자 액세스.
- Secure Web Appliance CLI(Command Line Interface)에 대한 관리 사용자 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.

문제

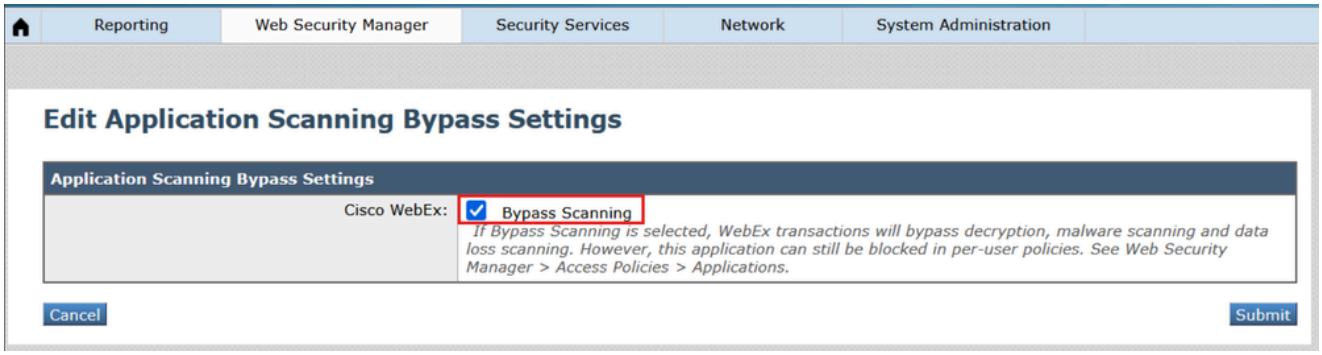
Webex Services에 대한 네트워크 요구 사항에 대한 Webex 공용 문서를 기반으로, Webex 시그널링 트래픽이 문서에 나열된 도메인/URL에 액세스할 수 있도록 프록시 서버를 구성해야 합니다. Secure Web Appliance는 우회 설정에서 Webex Application Bypass(Webex 애플리케이션 우회) 확인란을 활성화하여 대부분의 환경에 대한 요구 사항을 충족하지만, Webex 애플리케이션의 서비스 중단을 방지하기 위해 Secure Web Appliance에서 일부 추가 컨피그레이션이 필요할 수 있습니다. 다음 단계는 그러한 경우 시나리오에 권장됩니다.

Webex 애플리케이션 검사 바이패스

Cisco Webex: Bypass Scanning 기능은 Webex 애플리케이션 트래픽이 필터링되지 않은 상태로 Secure Web Appliance를 통과할 수 있도록 하는 첫 번째 단계입니다. Webex 데스크톱 또는 모바일 애플리케이션 사용자가 Secure Web Appliance를 통해 웹 트래픽을 프록시하는 모든 환경 및 구축 시나리오에서 활성화되어야 합니다.

Webex Application Scanning Bypass를 활성화하는 단계:

1. WSA GUI에서 Web Security Manager(웹 보안 관리자) > Bypass Settings(우회 설정) > Edit Application Bypass Settings(애플리케이션 우회 설정 편집)로 이동합니다.
2. "Cisco WebEx" 확인란을 선택합니다.



1_wsa_bypass_scanning_settings

3. 변경 내용을 제출하고 커밋합니다

이 설정을 사용하면 FQDN을 Secure Web Appliance의 우회 목록에 추가한 후 예상했던 대로 투명 트래픽을 우회하지 않습니다. 대신 Webex 애플리케이션 트래픽은 Secure Web Appliance를 통해 계속 프록시되지만, 암호 해독 시 "PASSTHRU_AVC" 결정 태그로 전달됩니다. 다음은 액세스 로그에 표시되는 방법의 예입니다.

```
1761695285.658 55398 192.168.100.100 TCP_MISS/200 4046848 TCP_CONNECT 3.161.225.70:443 - DIRECT/binarie
```

고유한 환경에 대한 고려 사항

트래픽이 Secure Web Appliance를 통해 프록시될 때 Webex 앱이 작동하려면 추가 컨피그레이션이 필요한 몇 가지 시나리오가 있습니다.

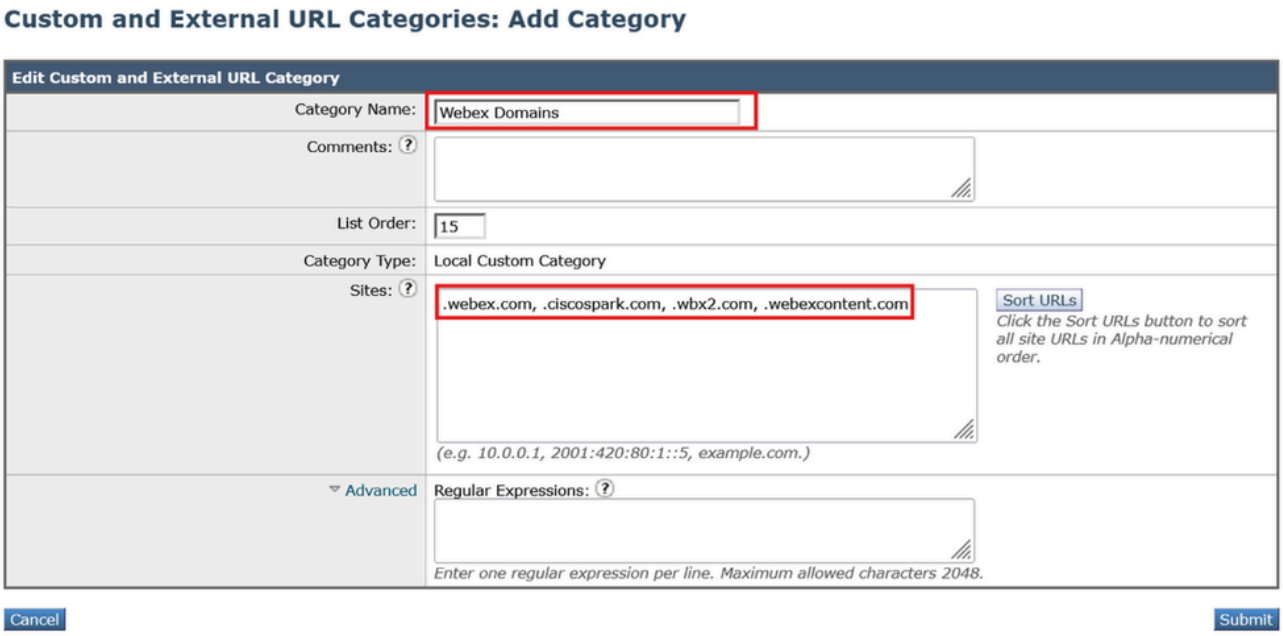
시나리오 1: Webex 도메인은 인증에서 제외되어야 합니다.

이는 IP 서로게이트가 ID 프로파일에서 활성화되지 않고 투명 리디렉션이 사용되는 환경에서 특히 두드러집니다. 기존 설명서를 기반으로 Webex 앱은 프록시가 명시적으로 정의된 도메인 가입 워크스테이션에서 NTLMSSP 인증을 수행할 수 있습니다. 그렇지 않으면 Webex 도메인에 대한 사용자 지정 카테고리를 구성하고 인증에서 제외하는 것이 좋습니다.

Webex 도메인을 인증에서 제외하는 단계:

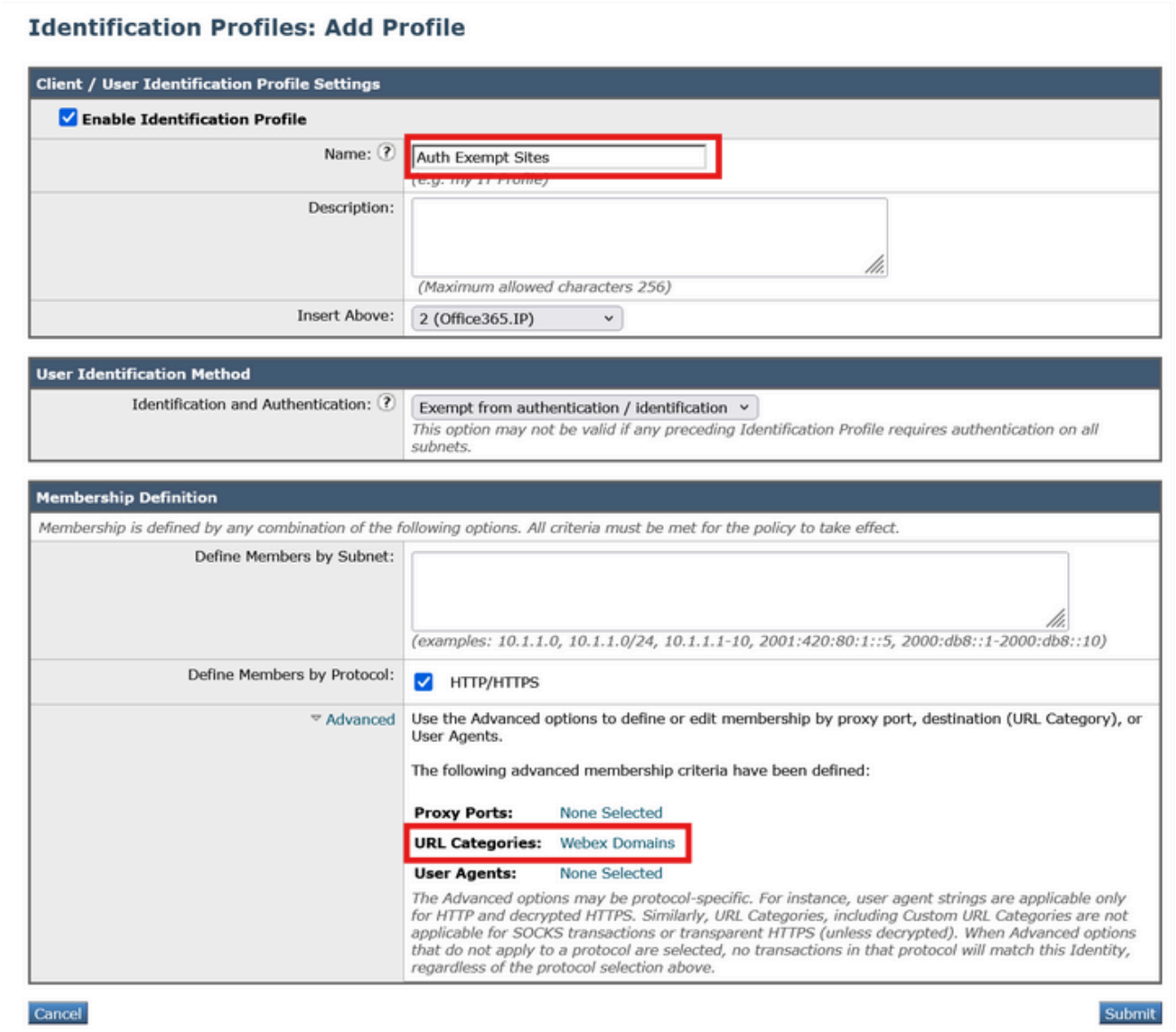
1. WSA GUI에서 Web Security Manager > Custom and External URL Categories(사용자 지정 및 외부 URL 범주) > Add Category(범주 추가)로 이동합니다.
2. 새 카테고리에 이름을 지정하고 사이트 섹션에 다음 도메인을 배치합니다.

```
.webex.com, .ciscospark.com, .wbx2.com, .webexcontent.com
```



2_wsa_custom_url_category

3. Submit(제출)을 클릭합니다. 그런 다음 Web Security Manager > Identification Profiles > Add Identification Profile로 이동합니다
4. 새 프로필에 이름을 지정하고 URL Categories(URL 카테고리)의 Advanced(고급) 섹션에서 #2단계에서 생성한 새 카테고리를 선택합니다



3_wsa_id_profile

5. 새 프로파일의 ID 및 인증이 인증/식별에서 제외로 설정되었는지 확인합니다.
6. 변경 사항을 제출하고 커밋합니다.

시나리오 2: Webex Content 도메인은 암호 해독 우회에 대해 완전히 인정되지 않습니다.

Webex Application Scanning Bypass가 사용하도록 설정된 경우 암호 해독 시 자동으로 전달되지 않는 webex.com 관련 하위 도메인이 몇 개 있습니다. Secure Web Appliance의 암호 해독 인증서가 디바이스의 신뢰할 수 있는 루트 인증서 저장소에 이미 추가되어 있거나 Webex 앱을 실행하는 디바이스에서 이미 신뢰하는 내부 인증 기관에서 서명한 경우, 이러한 도메인에서 제공되는 콘텐츠는 암호 해독 시 Webex 앱에서 신뢰됩니다. 그러나 장치가 관리되지 않고 Secure Web Appliance의 암호 해독 인증서를 신뢰할 수 없는 경우 이러한 도메인은 암호 해독 시 통과하도록 구성해야 합니다.

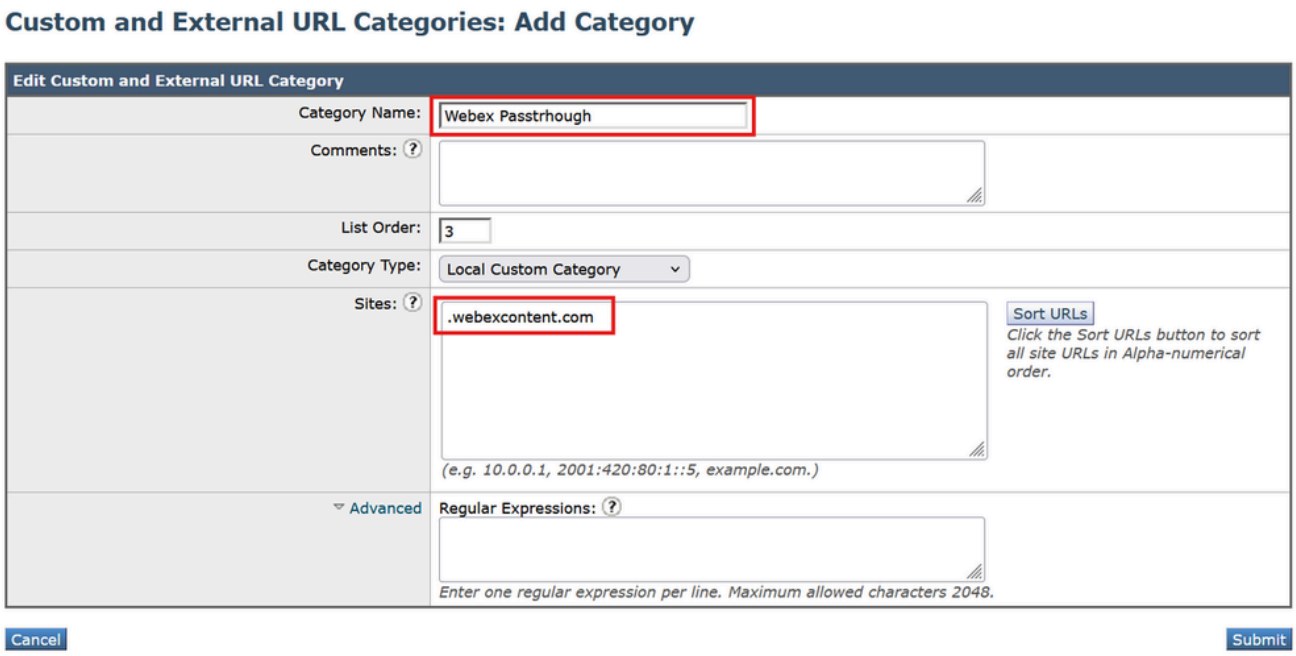
투명 리디렉션 구축이 진행되고 리디렉션 그룹에 대해 클라이언트 IP 스푸핑과 함께 둘 이상의 SWA가 사용되는 경우 대상 IP를 기반으로 보안 웹 어플라이언스에 리디렉션하도록 트래픽을 구성할 수 있으며, 마찬가지로 웹 서버의 반환 트래픽도 소스 주소를 기반으로 보안 웹 어플라이언스를

통해 다시 리디렉션하도록 구성됩니다. DNS 조회를 사용하여 확인되는 IP를 사용하여 웹 서버에 연결하도록 Secure Web Appliance가 구성된 경우 반환 트래픽이 실수로 다른 Secure Web Appliance로 리디렉션된 후 삭제될 수 있습니다. 이 문제는 Webex뿐만 아니라 다른 비디오 스트리밍 애플리케이션에도 영향을 미칩니다. 이는 웹 서버에서 회전하는 IP 주소를 사용하기 때문입니다.

모든 Webex 도메인에 대한 암호 해독 시 패스스루를 구성하는 단계:

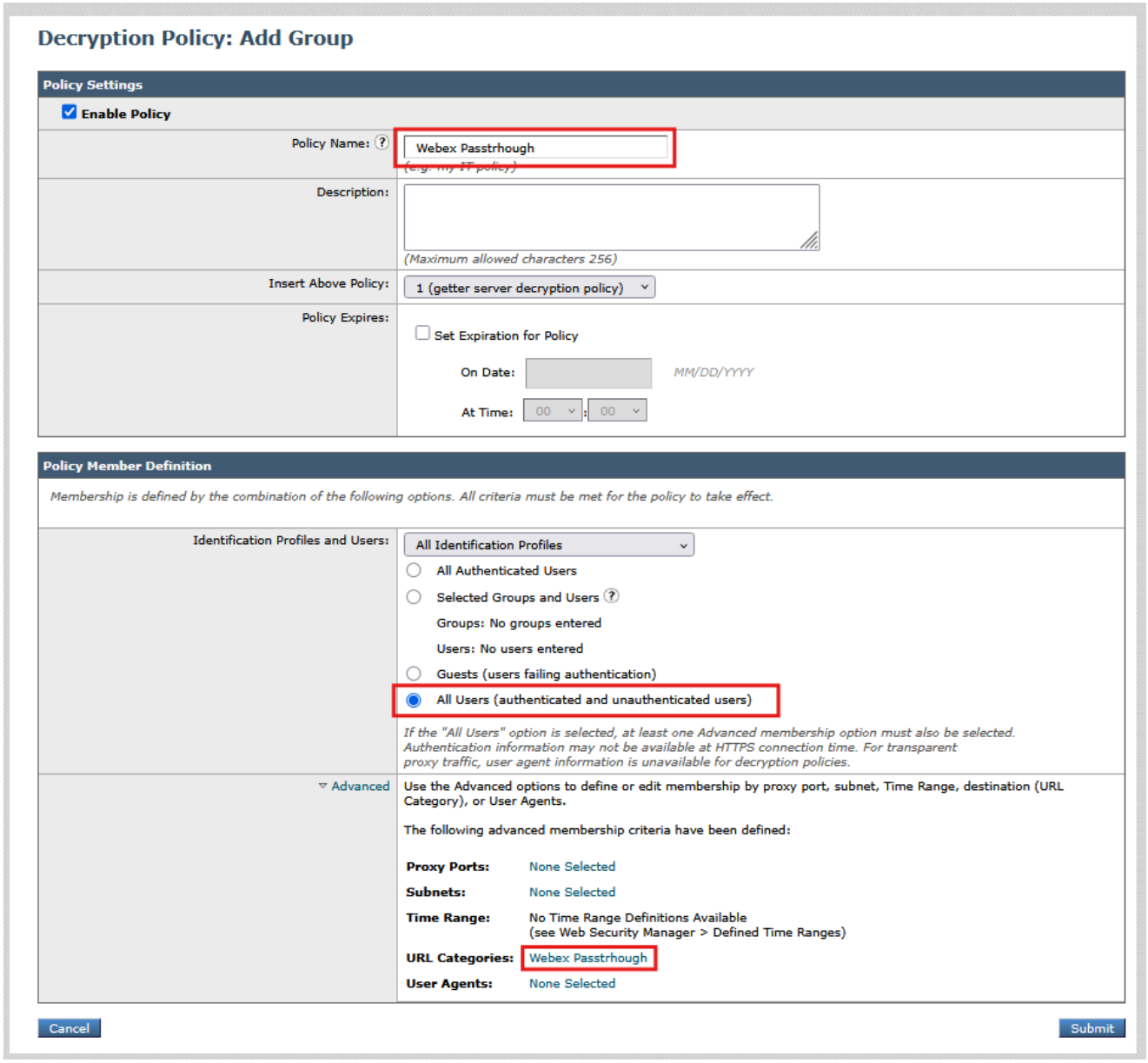
1. 위의 지침에 따라 Webex 애플리케이션 검사 우회가 활성화되었는지 확인합니다.
2. WSA GUI에서 Web Security Manager > Custom and External URL Categories(사용자 지정 및 외부 URL 범주) > Add Category(범주 추가)로 이동합니다.
3. 새 카테고리에 이름을 지정하고 다음 도메인을 사이트 섹션에 배치합니다.

```
.webexcontent.com
```



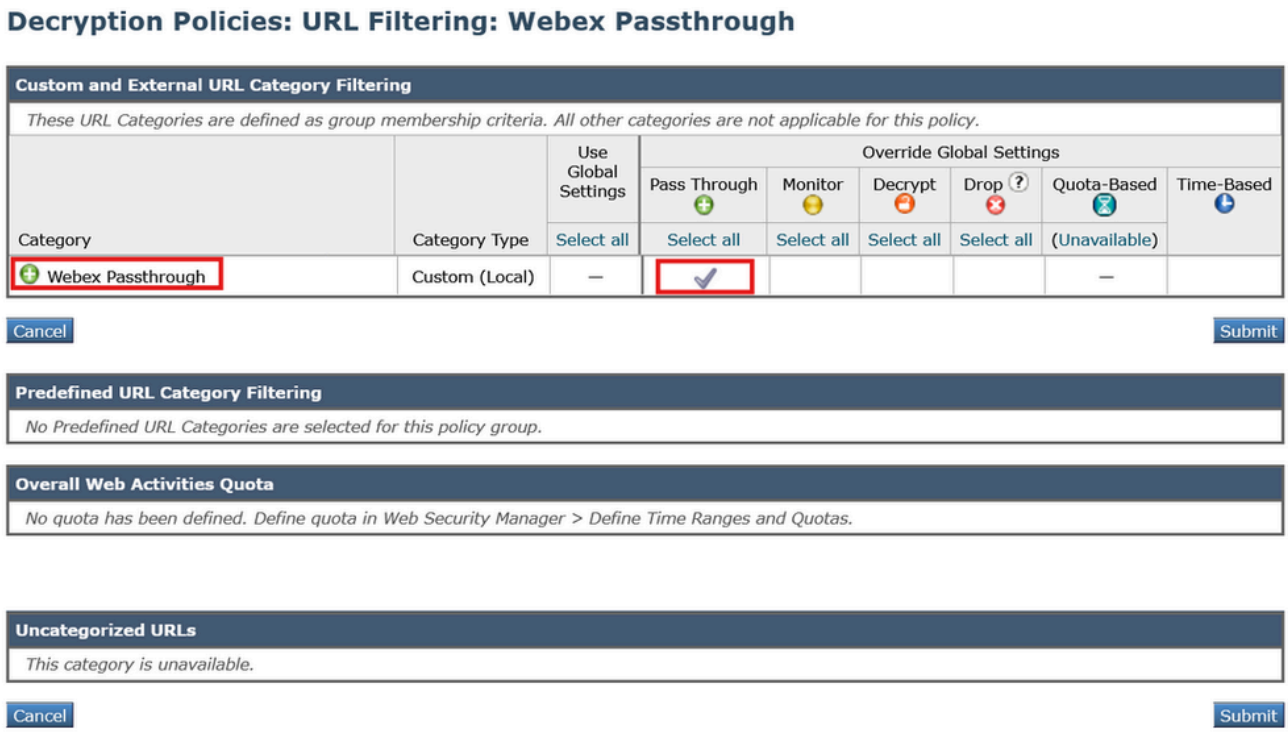
4_wsa_url_category

4. Submit(제출)을 클릭합니다. 이제 Web Security Manager(웹 보안 관리자) > Decryption Policies(암호 해독 정책) > Add Policy(정책 추가)로 이동합니다
5. 새 정책의 이름을 지정하고 Identification Profiles and Users(식별 프로필 및 사용자)를 "All Users(모든 사용자)"로 설정한 다음 URL Categories(URL 카테고리)의 Advanced(고급) 섹션에서 #3단계에서 생성한 새 카테고리를 선택합니다



5_wsa_decryption_policy

6. Submit(제출)을 클릭합니다. 그런 다음 URL Filtering(URL 필터링) 섹션을 클릭하고 #3단계에서 생성한 사용자 지정 카테고리를 "Pass Through"로 설정합니다.



6_wsa_url_필터링

7. 변경 사항을 제출하고 커밋합니다.

투명 리디렉션을 위해 여러 Secure Web Appliance가 구축되고 클라이언트 IP 스푸핑이 활성화된 경우 다음 두 가지 방법으로 해결할 수 있습니다.

1. 발신 및 반환 WCCP 서비스를 서버 주소가 아닌 클라이언트 주소를 기준으로 로드 밸런싱하도록 설정합니다.
2. WSA CLI에서 advancedproxyconfig > DNS > "Find web server by"를 설정하여 항상 웹 서버 연결에 클라이언트 제공 IP 주소를 사용합니다(옵션 2 및 3). 이 설정에 대한 자세한 내용은 Use Secure Web Appliance Best Practices(Secure Web Appliance 모범 사례 사용) 가이드의 DNS 섹션에서 확인할 수 있습니다.

확인

통과 설정이 완료되면 Webex 트래픽은 액세스 로그에서 정책에 따라 Pass through로 처리됩니다.

```
1763752739.797 457 192.168.100.100 TCP_MISS/200 6939 TCP_CONNECT 135.84.171.165:443 - DIRECT/da3-wxt08-
1763752853.942 109739 192.168.100.100 TCP_MISS/200 7709 TCP_CONNECT 170.72.245.220:443 - DIRECT/avatar-
1763752862.299 109943 192.168.100.100 TCP_MISS/200 8757 TCP_CONNECT 18.225.2.59:443 - DIRECT/highlights
1763752870.293 109949 192.168.100.100 TCP_MISS/200 8392 TCP_CONNECT 170.72.245.190:443 - DIRECT/retenti
```

Webex 애플리케이션을 검토 및 모니터링하여 속도 저하 또는 서비스 중단이 보고되면 액세스 로그를 한 번 더 검토하고 모든 webex 측 트래픽이 올바르게 처리되었는지 확인합니다.

관련 정보

- Webex 서비스의 네트워크 요구 사항
- Secure Web Appliance 모범 사례 사용

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.