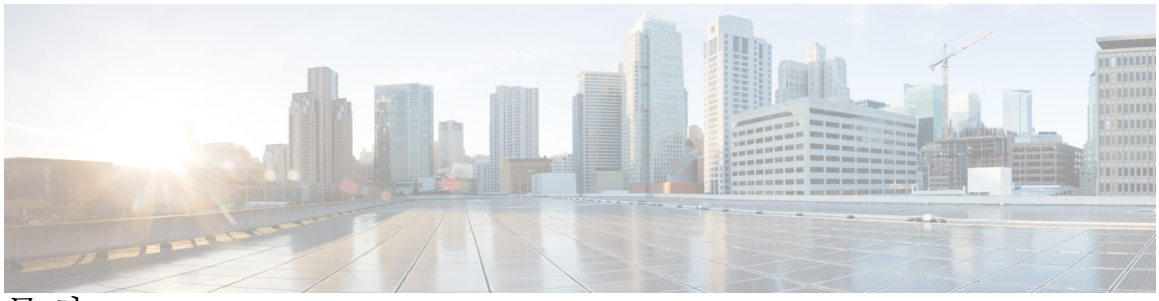
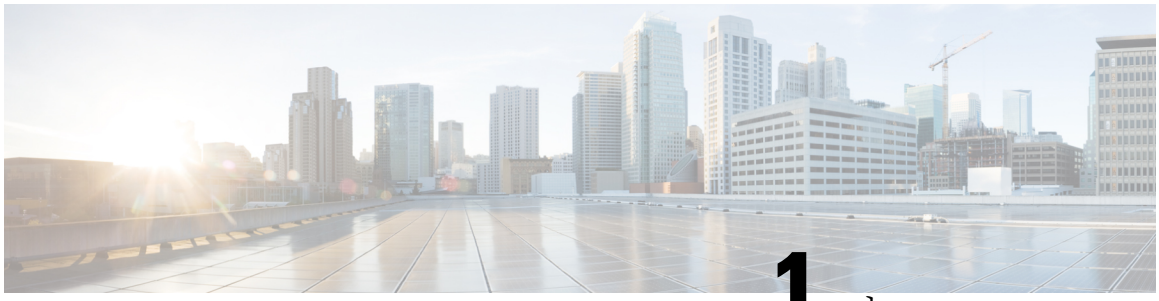
Cisco Secure Web Appliance S196, S396, S696 및 S696F 시작 가이드

초판: 2023년 12월 15일

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



목 차



1 장

Secure Web Appliance 소개

Secure Web Appliance 정보

Cisco Secure Web Appliance S196, S396, S696 및 S696F를 사용하면 조직에서 웹 트래픽을 보호하고 제어할 수 있습니다. 이 가이드에서는 어플라이언스를 설정하고 시스템 설정 마법사를 사용하여 어플라이언스의 기본 설정을 구성하는 방법을 설명합니다. 어플라이언스 설정을 구성하는 방법에 대한 자세한 내용은 Cisco Secure Web Appliances용 AsyncOS 사용자 가이드의 구축 장을 참조하십시오.

문서 네트워크 설정

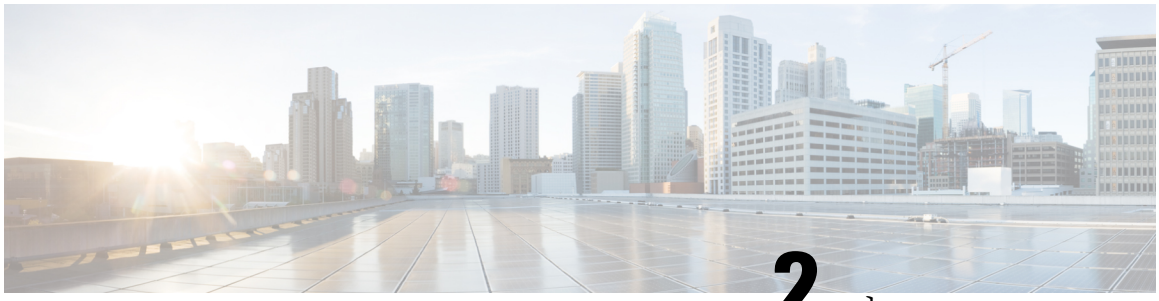
시작하기 전에 네트워크 및 관리자 설정에 대한 다음 정보를 적어 둡니다.

구축 옵션	
웹 프록시: • L4를 사용하는 투명 • WCCP 라우터를 사용하는 투명 스위치 • 명시적 전달 프록시	L4 트래픽 모니터: • 심플렉스 탭/스팬 포트 • 듀플렉스 탭/스팬 포트
네트워크 컨텍스트	
네트워크에 다른 웹 프록시가 있는 경우:	
다른 프록시 IP 주소:	
다른 프록시 포트:	

네트워크 설정	
기본 시스템 호스트 이름:	
DNS 서버:	인터넷 루트 DNS 서버 사용. DNS 서버 사용(최대 3개): 1. 2. 3.
NTP(Network Time Protocol) 서버:	
지역 표준 시간대:	
국가 표준 시간대:	
표준 시간대 GMT 오프셋:	
인터페이스 설정	
관리 포트	
IP 주소:	
네트워크 마스크:	
Hostname:	
데이터 포트(선택 사항, 참고 사항 참조)	
IP 주소:	
네트워크 마스크:	
Hostname:	
참고 웹 프록시는 관리 인터페이스를 공유할 수 있습니다. 별도로 구성하는 경우 데이터 인터페이스 IP 주소 및 관리 인터페이스 IP 주소는 동일한 서브넷을 공유할 수 없습니다.	
Routes	
관리를 위한 내부 경로	
기본 게이트웨이:	
정적 경로 이름:	
정적 경로 대상 네트워크:	
정적 경로 게이트웨이:	

데이터 내부 경로	
기본 게이트웨이:	
정적 경로 이름:	
정적 경로 대상 네트워크:	
정적 경로 게이트웨이:	
투명 라우팅 디바이스	
디바이스 유형:	• Layer 4 스위치 또는 디바이스 없음 • WCCP 라우터 - 표준 서비스 ID 활성화(웹 캐시). - 라우터 주소: _____ - 라우터 보안 활성화. Password: _____
참고 어플라이언스를 WCCP 라우터에 연결하는 경우, 시스템 설정 마법사를 실행한 후 WCCP 서비스를 생성하도록 Web Security 어플라이언스를 설정해야 할 수 있습니다.	
관리 설정	
관리자 비밀번호:	
다음 사용자에게 이메일로 시스템 경고문 보내기:	
SMTP 릴레이 호스트:	(선택 사항)
자동지원:	Enable
SenderBase 네트워크 참여:	Enable • 제한적 • 표준
보안 서비스	
L4 트래픽 모니터:	• 모니터링 전용 • 차단

허용 가능한 사용 제어:	Enable • Cisco IronPort 웹 사용 제어
웹 신뢰도 필터:	Enable
악성코드 및 스파이웨어 스캐닝:	• Webroot 사용 • McAfee 사용 • Sophos 사용
삭제된 악성코드에 대한 작업:	• 모니터링 전용 • 차단
IronPort 데이터 보안 필터:	Enable



2 장

설치 계획

설치 계획

네트워크 내에서 Cisco Web Security Appliance를 구성하는 방법을 결정합니다.

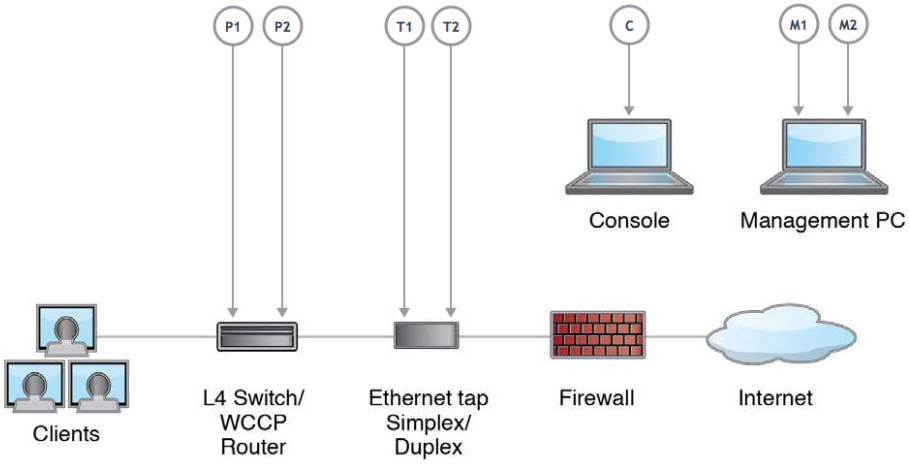
Cisco Web Security Appliance는 일반적으로 클라이언트와 인터넷 사이의 네트워크에 추가 계층으로 설치됩니다. 어플라이언스를 구축하는 방식에 따라 클라이언트 트래픽을 어플라이언스로 라우팅하기 위해 L4(레이어 4) 스위치 또는 WCCP 라우터가 필요할 수도 있고 필요하지 않을 수도 있습니다.

구축 옵션은 다음과 같습니다.

- 투명 프록시 - L4 스위치를 사용하는 웹 프록시
- 투명 프록시 - WCCP 라우터를 사용하는 웹 프록시
- 명시적 정방향 프록시 - 네트워크 스위치에 연결
- L4 트래픽 모니터 - 이더넷 탭(심플렉스 또는 듀플렉스)
  - 심플렉스 모드: 포트 T1이 모든 발신 트래픽을, 포트 T2가 모든 수신 트래픽을 받습니다.
  - 듀플렉스 모드: 포트 T1이 모든 수발신 트래픽을 받습니다.

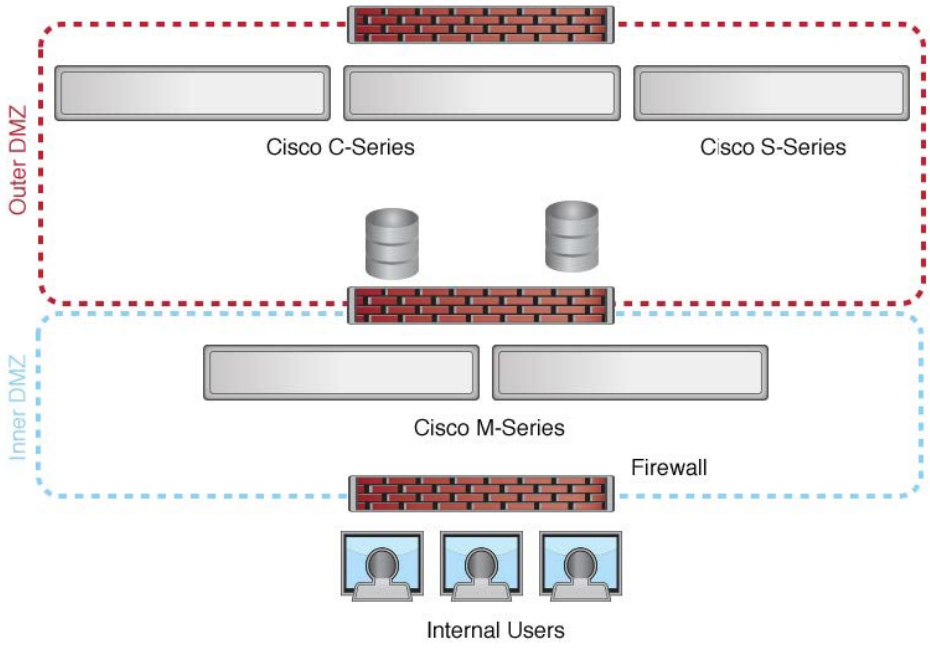
참고 어플라이언스의 개별 포트에 대한 자세한 내용은 어플라이언스에 연결 을 참조하십시오.

설치 계획



참고 실제 클라이언트 IP 주소를 모니터링하려면 L4 트래픽 모니터를 항상 방화벽 내부에서 그리고 NAT(Network Address Translation, 네트워크 주소 변환) 전에 구성해야 합니다.

설치에 여러 Cisco Web Security Appliance(S-Series) 또는 Cisco Email Security Appliance(C-Series)가 포함된 경우, 다음 네트워크 다이어그램에 표시된 것처럼 Cisco Content Security Management Appliance(M-Series)를 사용하여 관리할 수도 있습니다.



원격 액세스를 위해 일시적으로 IP 주소 변경

네트워크 연결을 사용하여 어플라이언스를 원격으로 구성하려면 일시적으로 컴퓨터의 IP 주소를 변경해야 합니다.

참고 구성을 완료한 후에 이 설정을 되돌려야 하므로 현재 IP 구성 설정을 적어둡니다.

또는 IP 주소를 변경하지 않고 시리얼 콘솔을 사용하여 어플라이언스를 구성할 수 있습니다. 시리얼 콘솔을 사용하는 경우 어플라이언스에 연결을 참조하십시오.

Windows에서 일시적으로 IP 주소 변경

참고 정확한 단계는 운영 체제의 버전에 따라 다릅니다.

단계 **1** 시스템 상자에 포함된 크로스 오버 또는 이더넷 케이블을 사용하여 노트북을 기본 관리 포트(M1)에 연결합니다. Cisco Web Security Appliance는 M1 관리 포트만 사용합니다. 설치 계획 참조하십시오.

단계 **2** 시작 메뉴로 이동하여 **Control Panel(**제어 패널**)**을 선택합니다.

단계 **3** **Network and Sharing Center(**네트워크 및 공유 센터**)**를 더블 클릭합니다.

단계 **4** **Local Area Connection(**로컬 영역 연결**)**을 클릭한 다음 **Properties(**속성**)**를 클릭합니다.

단계 **5** 인터넷 프로토콜**(TCP/IP)**을 선택하고 **Properties(**속성**)**를 클릭합니다.

단계 **6** **Use following IP Address(**다음 **IP** 주소 사용**)**를 선택합니다.

단계 **7** 다음 변경 사항을 입력합니다.

- IP 주소: **192.168.42.43**
- Subnet Mask(서브넷 마스크): **255.255.255.0**
- 기본 게이트웨이: **192.168.42.1**

단계 **8** **OK(**확인**)**를 클릭하여 대화 상자를 닫습니다**.**

Mac에서 일시적으로 IP 주소 변경

참고 정확한 단계는 운영 체제의 버전에 따라 다릅니다.

단계 **1** Apple 메뉴를 실행하고 **System Preferences(**시스템 환경 설정**)**을 선택합니다.

단계 **2** **Network(**네트워크**)**를 클릭합니다.

단계 **3** 변경을 허용하려면 잠금 아이콘을 클릭합니다.

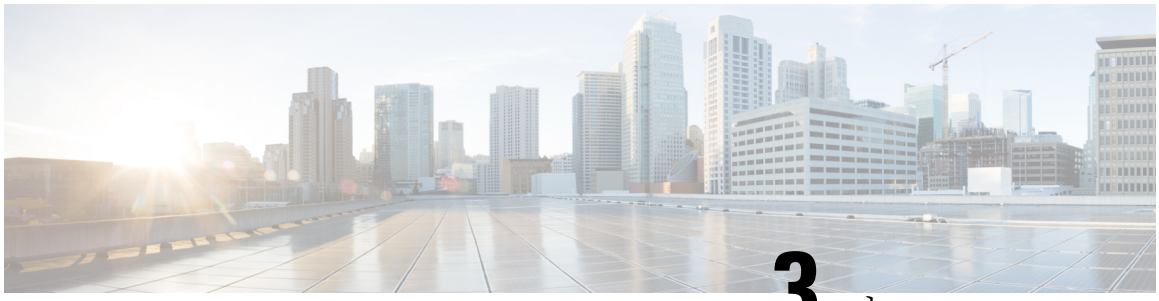
단계 **4** 녹색 아이콘을 사용하여 이더넷 네트워크 설정을 선택합니다. 이 연결이 활성 연결입니다. **Advanced(**고급**)**을 클릭합니다.

단계 **5** TCP/IP 탭을 클릭하고 이더넷 설정의 드롭다운 목록에서 **Manually(**수동**)**을 선택합니다.

단계 **6** 다음 변경 사항을 입력합니다.

- IP 주소: **192.168.42.43**
- Subnet Mask(서브넷 마스크): **255.255.255.0**
- 기본 게이트웨이: **192.168.42.1**

단계 **7** **OK(**확인**)**를 클릭합니다.



3 장

어플라이언스에 연결

어플라이언스를 랙에 장착한 후 다음 단계에 따라 케이블을 연결하고 전원을 켜서 연결을 확인합니다.

참고 각 항목의 연결 다이어그램은 프라이빗 네트워크에 연결된 관리 컴퓨터를 사용하는 기본 구성을 보여줍니다. 기본 논리적 네트워크 연결, 포트, 주소 지정 및 구성 요구 사항에 따라 구축이 달라질 수 있습니다.

Cisco S196 Secure Web Appliance

단계 **1** 직선 전원 케이블의 한쪽 끝을 어플라이언스의 후면 패널에 있는 전원 공급 장치에 연결합니다.

참고 선택 사항으로 별도의 전원 케이블을 주문하고 이중화를 위해 어플라이언스의 후면 패널에 있는 두 번째 전원 공급 장치에 연결합니다.

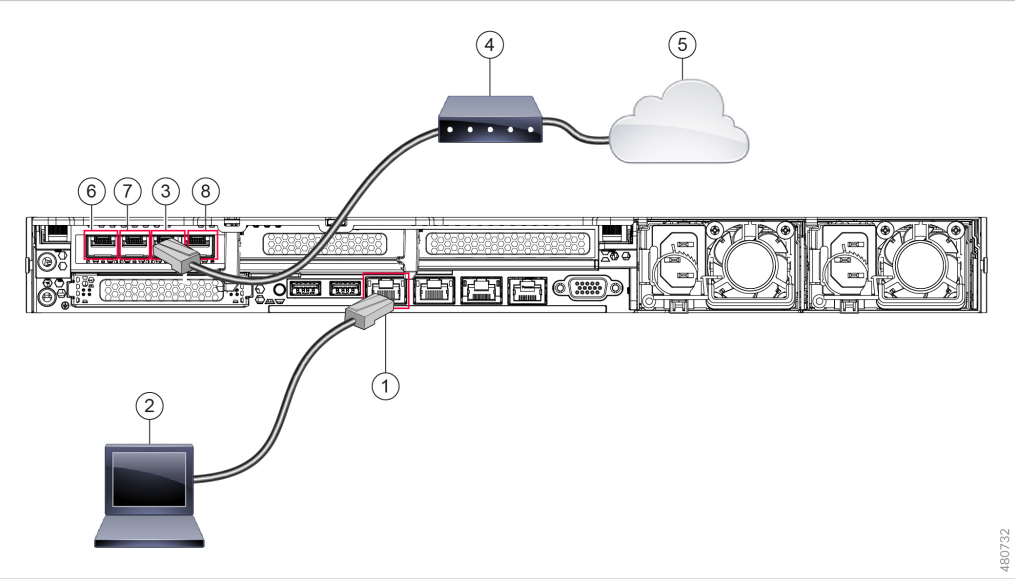
단계 **2** 다른 쪽 끝을 콘센트에 꽂습니다.

단계 **3** 이더넷 케이블을 어플라이언스 뒤쪽 패널의 해당 포트에 꽂습니다.

- 프록시 포트는 P1과 P2입니다.
  - P1만 활성: P1만 활성화된 경우 수발신 트래픽 모두를 위해 네트워크에 연결합니다.
  - P1 및 P2 활성: P1 및 P2 모두 활성화된 경우 P1은 내부 네트워크에, P2는 인터넷에 연결해야 합니다.
- 트래픽 모니터 포트는 T1 및 T2입니다.

- 심플렉스 탭: 포트 T1 및 T2. 케이블 하나는 인터넷으로 향하는 모든 패킷을 위한 것(T1)이고 다른 하나는 인터넷에서 오는 모든 패킷을 위한 것(T2)입니다.
- 듀플렉스 탭: 포트 T1. 단일 케이블에서 모든 수발신 트래픽을 담당합니다.

단계 **4** 시스템 박스에 포함된 이더넷 케이블을 사용하여 랩톱 노트북 컴퓨터를 관리 포트(M1)에 연결합니다.



1	관리 포트 (M1)~(192.168.42.42)	2	관리 컴퓨터(192.68.42.43)
3	트래픽 모니터 포트 1(T1)	4	WAN 모뎀
5	인터넷	6	프록시 포트 1(P1)
7	프록시 포트 2(P2)	8	트래픽 모니터 포트 2(T2)

단계 **5** 어플라이언스 앞쪽 패널의 전원 켜기/끄기 스위치를 눌러 어플라이언스 전원을 켭니다. 시스템 전원을 켤 때마다 시스템이 초기화될 때까지 10분간 기다려야 합니다. 어플라이언스 전원이 켜진 후 전면 패널에 녹색 표시등이 켜져 어플라이언스가 작동 중임을 나타냅니다.

주의 초기화가 완료되기 전에 전원을 끄면 어플라이언스가 작동 상태가 아니므로 시스코에 반환해야 합니다.

참고 어플라이언스에 전원을 연결한 후 빠르게 이 어플라이언스를 켜면 어플라이언스의 전원이 켜지고 팬이 회전하며 LED가 켜집니다. 30~60초 내에 팬이 중지되고 모든 LED가 꺼집니다. 31초 후에 어플라이언스의 전원이 켜집니다. 이 동작은 시스템 펌웨어와 컨트롤러의 동기화를 허용하기 위한 것입니다.

단계 **6** 추가 구성은 *Cisco Web Security Appliances*용 *AsyncOS* 사용 가이드를 참조하십시오.

Cisco S396 Secure Web Appliance

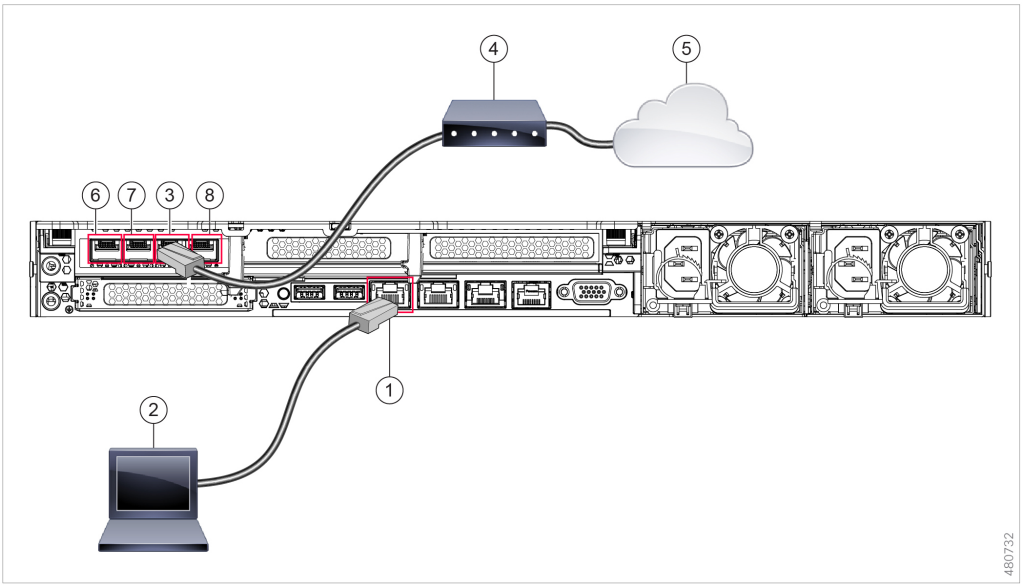
단계 **1** 각 직선 전원 케이블의 한쪽 끝을 기기 후면 패널의 예비 전원 공급 장치에 연결합니다.

단계 **2** 다른 쪽 끝을 콘센트에 꽂습니다.

단계 **3** 이더넷 케이블을 어플라이언스 뒤쪽 패널의 해당 포트에 꽂습니다.

- 프록시 포트는 P1과 P2입니다.
  - P1만 활성: P1만 활성화된 경우 수발신 트래픽 모두를 위해 네트워크에 연결합니다.
  - P1 및 P2 활성: P1 및 P2 모두 활성화된 경우 P1은 내부 네트워크에, P2는 인터넷에 연결해야 합니다.
- 트래픽 모니터 포트는 T1 및 T2입니다.
  - 심플렉스 탭: 포트 T1 및 T2. 케이블 하나는 인터넷으로 향하는 모든 패킷을 위한 것(T1)이고 다른 하나는 인터넷에서 오는 모든 패킷을 위한 것(T2)입니다.
  - 듀플렉스 탭: 포트 T1. 단일 케이블에서 모든 수발신 트래픽을 담당합니다.

단계 **4** 시스템 박스에 포함된 이더넷 케이블을 사용하여 랩톱 노트북 컴퓨터를 관리 포트에 연결합니다. S-Series 어플라이언스는 M1 관리 포트만 사용합니다.



1	관리 포트(M1)~(192.168.42.42)	2	관리 컴퓨터(192.168.42.43)
3	트래픽 모니터 포트 1(T1)	4	WAN 모뎀
5	인터넷	6	프록시 포트 1(P1)

7	프록시 포트 2(P2)	8	트래픽 모니터 포트 2(T2)

단계 **5** 어플라이언스 앞쪽 패널의 전원 켜기/끄기 스위치를 눌러 어플라이언스 전원을 켭니다. 시스템 전원을 켤 때마다 시스템이 초기화될 때까지 10분간 기다려야 합니다. 어플라이언스 전원이 켜진 후 전면 패널에 녹색 표시등이 켜져 어플라이언스가 작동 중임을 나타냅니다.

주의 초기화가 완료되기 전에 전원을 끄면 어플라이언스가 작동 상태가 아니므로 시스코에 반환해야 합니다.

참고 어플라이언스에 전원을 연결한 후 빠르게 이 어플라이언스를 켜면 어플라이언스의 전원이 켜지고 팬이 회전하며 LED가 켜집니다. 30~60초 내에 팬이 중지되고 모든 LED가 꺼집니다. 31초 후에 어플라이언스의 전원이 켜집니다. 이 동작은 시스템 펌웨어와 컨트롤러의 동기화를 허용하기 위한 것입니다.

단계 **6** 추가 구성은 *Cisco Web Security Appliances*용 *AsyncOS* 사용 가이드를 참조하십시오.

Cisco S696 Secure Web Appliance

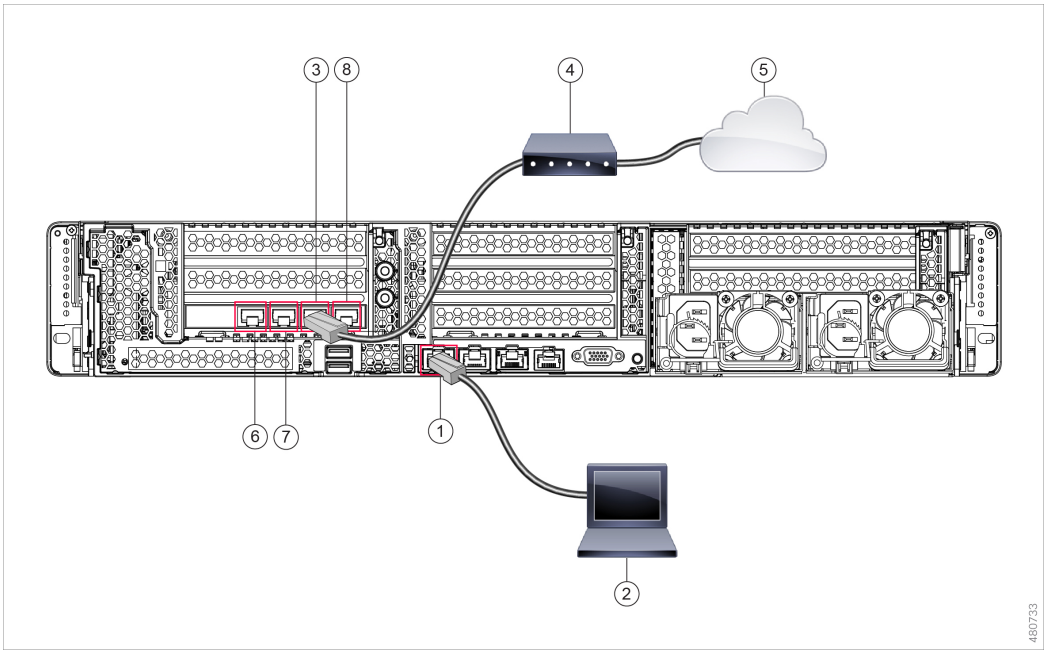
단계 **1** 각 직선 전원 케이블의 한쪽 끝을 기기 후면 패널의 예비 전원 공급 장치에 연결합니다.

단계 **2** 다른 쪽 끝을 콘센트에 꽂습니다.

단계 **3** 이더넷 케이블을 어플라이언스 뒤쪽 패널의 해당 포트에 꽂습니다.

- 프록시 포트는 P1과 P2입니다.
  - P1만 활성: P1만 활성화된 경우 수발신 트래픽 모두를 위해 네트워크에 연결합니다.
  - P1 및 P2 활성: P1 및 P2 모두 활성화된 경우 P1은 내부 네트워크에, P2는 인터넷에 연결해야 합니다.
- 트래픽 모니터 포트는 T1 및 T2입니다.
  - 심플렉스 탭: 포트 T1 및 T2. 케이블 하나는 인터넷으로 향하는 모든 패킷을 위한 것(T1)이고 다른 하나는 인터넷에서 오는 모든 패킷을 위한 것(T2)입니다.
  - 듀플렉스 탭: 포트 T1. 단일 케이블에서 모든 수발신 트래픽을 담당합니다.

단계 **4** 시스템 박스에 포함된 이더넷 케이블을 사용하여 랩톱 노트북 컴퓨터를 관리 포트에 연결합니다.



1	관리 포트 (M1)~(192.168.42.42)	2	관리 컴퓨터(192.168.42.43)
3	트래픽 모니터 포트(T1)	4	WAN 모뎀
5	인터넷	6	프록시 포트 1(P1)
7	프록시 포트 2(P2)	8	트래픽 모니터 포트 2(T2)

단계 **5** 어플라이언스 앞쪽 패널의 전원 켜기/끄기 스위치를 눌러 어플라이언스 전원을 켭니다. 시스템 전원을 켤 때마다 시스템이 초기화될 때까지 10분간 기다려야 합니다. 어플라이언스 전원이 켜진 후 전면 패널에 녹색 표시등이 켜져 어플라이언스가 작동 중임을 나타냅니다.

주의 시스템이 전원 켜기 시퀀스를 완료하고 LED가 녹색으로 바뀔 때까지 10분 이상 기다립니다. 초기화가 완료되기 전에 전원을 끄면 어플라이언스가 작동 상태가 아니므로 시스코에 반환해야 합니다.

참고 어플라이언스에 전원을 연결한 후 빠르게 이 어플라이언스를 켜면 어플라이언스의 전원이 켜지고 팬이 회전하며 LED가 켜집니다. 30~60초 내에 팬이 중지되고 모든 LED가 꺼집니다. 31초 후에 어플라이언스의 전원이 켜집니다. 이 동작은 시스템 펌웨어와 컨트롤러의 동기화를 허용하기 위한 것입니다.

단계 **6** 추가 구성은 *Cisco Web Security Appliances*용 *AsyncOS* 사용 가이드를 참조하십시오.

Cisco S696F Secure Web Appliance

다음 그림에는 광섬유 포트가 있는 Cisco S696F 모델이 나와 있습니다. 이러한 광섬유 포트는 그림의 이더넷 포트 위에 있으며 이더넷 포트는 없습니다. 자세한 내용은 *Cisco x96 Secure Web Appliance* 설치 및 유지 보수 가이드를 참조하십시오.

위쪽에 있는 2개의 광섬유 포트는 다음 표에서 설명하는 이더넷 프록시 포트와 동일한 방식으로 프록시 포트로 사용됩니다. 중간에 있는 2개의 광섬유 포트는 트래픽 포트로 사용됩니다. 아래쪽 2개의 광섬유 포트는 관리 포트로 사용됩니다.

단계 **1** 각 직선 전원 케이블의 한쪽 끝을 기기 후면 패널의 예비 전원 공급 장치에 연결합니다.

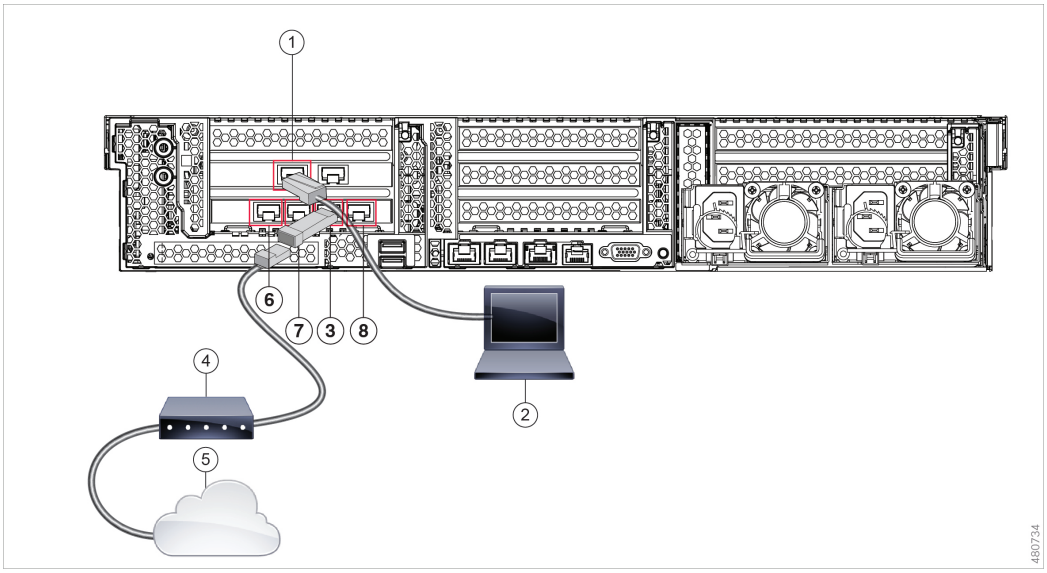
단계 **2** 다른 쪽 끝을 콘센트에 꽂습니다.

단계 **3** 이더넷 케이블을 어플라이언스 뒤쪽 패널의 해당 포트에 꽂습니다.

- 프록시 포트는 P1과 P2입니다.
  - P1만 활성: P1만 활성화된 경우 수발신 트래픽 모두를 위해 네트워크에 연결합니다.
  - P1 및 P2 활성: P1 및 P2 모두 활성화된 경우 P1은 내부 네트워크에, P2는 인터넷에 연결해야 합니다.
- 트래픽 모니터 포트는 T1 및 T2입니다.
  - 심플렉스 탭: 포트 T1 및 T2. 케이블 하나는 인터넷으로 향하는 모든 패킷을 위한 것(T1)이고 다른 하나는 인터넷에서 오는 모든 패킷을 위한 것(T2)입니다.
  - 듀플렉스 탭: 포트 T1. 단일 케이블에서 모든 수발신 트래픽을 담당합니다.

단계 **4** 시스템 박스에 포함된 이더넷 케이블을 사용하여 랩톱 노트북 컴퓨터를 관리 포트에 연결합니다.

주의 10기가비트 광섬유 인터페이스와 함께 제공된 트랜시버 모듈만 사용하십시오. 다른 트랜시버 모듈을 사용하면 광섬유 인터페이스 카드가 손상될 수 있습니다.



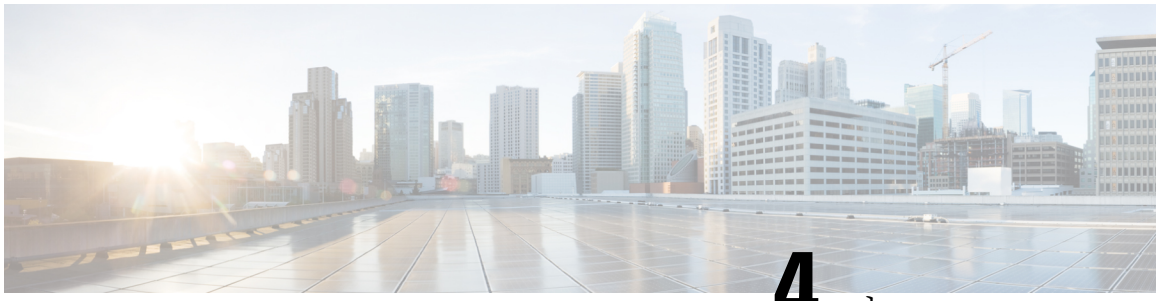
1	관리 포트 (M1)~(192.168.42.42)	2	관리 컴퓨터(192.168.42.43)
3	트래픽 모니터 포트(T1)	4	WAN 모뎀
5	인터넷	6	프록시 포트 1(P1)
7	프록시 포트 2(P2)	8	트래픽 모니터 포트 2(T2)

단계 **5** 어플라이언스 앞쪽 패널의 전원 켜기/끄기 스위치를 눌러 어플라이언스 전원을 켭니다. 시스템 전원을 켤 때마다 시스템이 초기화될 때까지 10분간 기다려야 합니다. 어플라이언스 전원이 켜진 후 전면 패널에 녹색 표시등이 켜져 어플라이언스가 작동 중임을 나타냅니다.

주의 시스템이 전원 켜기 시퀀스를 완료하고 LED가 녹색으로 바뀔 때까지 10분 이상 기다립니다. 초기화가 완료되기 전에 전원을 끄면 어플라이언스가 작동 상태가 아니므로 시스코에 반환해야 합니다.

참고 어플라이언스에 전원을 연결한 후 빠르게 이 어플라이언스를 켜면 어플라이언스의 전원이 켜지고 팬이 회전하며 LED가 켜집니다. 30~60초 내에 팬이 중지되고 모든 LED가 꺼집니다. 31초 후에 어플라이언스의 전원이 켜집니다. 이 동작은 시스템 펌웨어와 컨트롤러의 동기화를 허용하기 위한 것입니다.

단계 **6** 추가 구성은 *Cisco Web Security Appliances용 AsyncOS 사용 가이드*를 참조하십시오.



4 장

어플라이언스에 로그인

두 가지 인터페이스(웹 인터페이스 또는 CLI) 중 하나를 사용하여 Cisco Web Security Appliance에 로그인할 수 있습니다.

- 웹 인터페이스를 사용하여 어플라이언스에 로그인, 17 페이지
- CLI를 사용하여 어플라이언스에 로그인, 17 페이지

웹 인터페이스를 사용하여 어플라이언스에 로그인

단계 **1** 이더넷 포트를 통한 웹 브라우저 액세스의 경우(어플라이언스에 연결참조), 웹 브라우저에 다음 URL을 입력하여 어플라이언스 관리 인터페이스로 이동합니다.

https://10.10.193.32:8443/

단계 **2** 로그인 정보를 다음과 같이 입력합니다.

- 사용자 이름: **admin**
- 비밀번호: **ironport**

참고 hostname 매개변수는 시스템 설정 중에 할당됩니다. 호스트 이름(http://hostname:8443)을 사용하여 관리 인터페이스에 연결하려면 DNS 서버 데이터베이스에 어플라이언스 *hostname* 및 IP 주소를 추가해야 합니다.

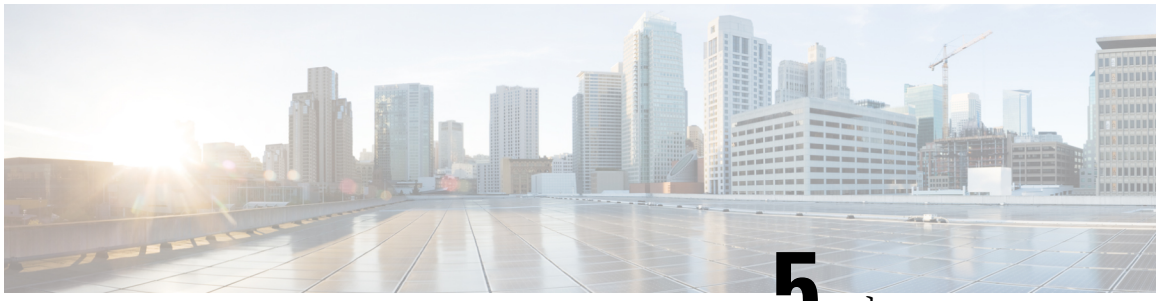
단계 **3** **Login(**로그인**)**을 클릭합니다.

CLI를 사용하여 어플라이언스에 로그인

단계 **1** 로컬 또는 원격으로 CLI에 액세스:

- CLI에 로컬로 액세스하려면 9600비트, 8비트, 패리티 없음, 1 정지 비트(**9600, 8, N, 1**), 하드웨어로 설정된 플로우 제어를 사용하여 시리얼 포트에 연결하도록 터미널을 설정합니다. 물리적으로 연결하려면 어플라이언스에 연결을 참조하십시오.
- 원격으로 CLI에 액세스하려면 IP 주소 **192.168.42.42**에 대해 SSH 세션을 시작합니다.

단계 **2** 비밀번호 **ironport**를 사용하여 관리자로 로그인합니다.



5 장

System Setup Wizard(시스템 설정 마법사) 실행

System Setup Wizard(시스템 설정 마법사) 실행

시작하기 전에:

- 시스템 설정 마법사를 실행하기 전에 Smart License를 활성화하고 등록합니다. 자세한 정보는 Smart Software Licensing을 참조하십시오.

System Setup Wizard(시스템 설정 마법사)를 실행하여 기본 설정을 구성하고 시스템 기본값 집합을 활성화합니다. 웹 기반 인터페이스를 통해 어플라이언스에 액세스하면 시스템 설정 마법사가 자동으로 시작되고 최종 사용자 라이선스 계약(EULA)을 표시합니다.

단계 **1** 최종 사용자 라이선스 계약을 읽고 동의합니다.

단계 **2** 문서 네트워크 설정의 정보를 입력합니다.

설정에 대한 추가 정보가 필요한 경우 도움말 및 지원 > 온라인 도움말을 선택합니다.

단계 **3** 구성 요약 페이지를 검토합니다.

단계 **4** **Install This Configuration(**이 구성 설치**)**을 클릭합니다.

단계 **5** 어플라이언스가 설정을 수락하지 않았거나 설치를 수행하지 않는 것으로 보일 수 있습니다. 이는 IP 주소를 변경했지만 설치가 진행 중이기 때문입니다.

단계 **6** 위의 설명과 같이 일시적으로 컴퓨터의 IP 주소를 변경한 경우, IP 주소 설정을 다시 원래 값으로 변경합니다.

단계 **7** 컴퓨터와 어플라이언스가 네트워크에 연결되어 있는지 확인합니다.

단계 **8** 설치 계획에서 확인한 호스트 이름 또는 IP 주소로 어플라이언스에 다시 로그인합니다. 사용자 이름 **admin** 과 마법사에서 입력한 새 비밀번호를 사용합니다.

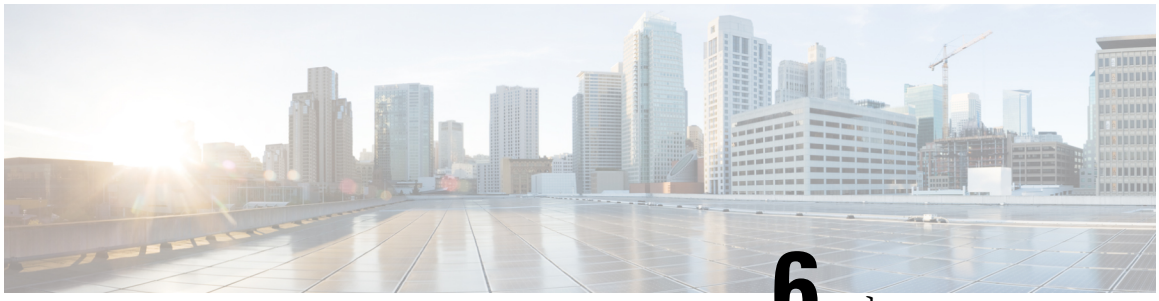
Cisco Web Security Appliance는 셀프 서명 인증서를 사용하므로 웹 브라우저에서 경고가 표시될 수 있습니다. 인증서를 수락하고 이 경고를 무시하십시오.

단계 **9** 새 관리자 비밀번호를 안전하게 보관하십시오.

사용 가능한 업그레이드 확인

어플라이언스에 로그인한 후 웹 브라우저 창 상단에서 업그레이드 알림(또는 CLI의 알림)을 확인합니다. 업그레이드가 사용 가능한 경우 해당 업그레이드를 설치해야 하는지 평가합니다.

각 릴리스에 대한 자세한 내용은 해당 Async OS 버전의 릴리스 노트에서 확인할 수 있습니다.



6 장

네트워크 설정 구성

네트워크 설정 구성

네트워크 구성에 따라 다음 포트를 사용하여 액세스를 허용하도록 방화벽을 구성해야 할 수도 있습니다. SMTP 및 DNS 서비스는 인터넷에 액세스해야 합니다.

Web Security Appliance는 다음 포트에서 수신 대기할 수 있어야 합니다.

- FTP: 포트 21, 데이터 포트 TCP 1024 이상
- HTTP(포트 80)
- HTTPS: 포트 443
- 관리 액세스: 포트 8443(HTTPS) 및 8080(HTTP)
- SSH: 포트 22

Web Security Appliance는 다음 포트에서 아웃바운드 연결을 설정할 수 있어야 합니다.

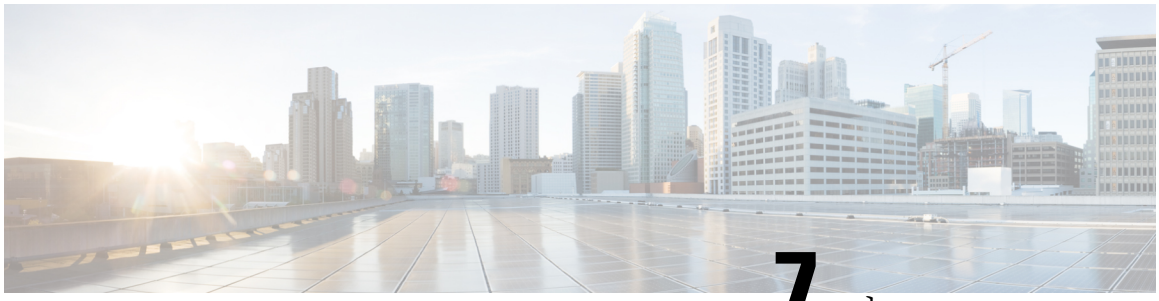
- DNS: 포트 53
- FTP: 포트 21, 데이터 포트 TCP 1024 이상
- HTTP(포트 80)
- HTTPS: 포트 443
- LDAP: 포트 389 또는 3268
- SSL을 통한 LDAP: 포트 636
- 글로벌 카탈로그 쿼리용 SSL을 사용하는 LDAP: 포트 3269
- NTP: 포트 123
- SMTP: 포트 25

참고 포트 80 및 443을 열지 않으면 기능 키를 다운로드할 수 없습니다.

자세한 내용은 사용 중인 버전에 대한 Cisco Web Security Appliances용 AsyncOS 사용 가이드에서 방화벽 정보를 참조하십시오.

구성 요약

항목	설명
관리	https://192.168.42.42:8443 을 입력하거나 시스템 설정 마법사를 완료한 후 관리 인터페이스에 할당된 IP 주소를 사용하여 관리 포트에서 Web Security Appliance를 관리할 수 있습니다. 구성을 공장 기본 설정으로 재설정하는 경우(예: 시스템 설정 마법사를 다시 실행), 관리 포트(https://192.168.42.42:8443)에서만 관리 인터페이스에 액세스할 수 있으므로 관리 포트에 연결되어 있는지 확인합니다. 또한, 관리 인터페이스의 방화벽 포트 80 및 443이 열려 있는지 확인합니다.
데이터	시스템 설정 마법사를 실행하면 네트워크의 클라이언트로부터 웹 트래픽을 수신하도록 어플라이언스의 포트가 하나 이상 구성됩니다(M1만, M1 및 P1, M1, P1 및 P2, P1만, 또는 P1 및 P2). 참고 웹 프록시를 명시적 전달 모드로 구성한 경우, 클라이언트 시스템의 애플리케이션이 데이터에 대해 구성된 IP 주소(M1 또는 P1)를 사용하여 웹 트래픽을 웹 보안 어플라이언스의 웹 프록시로 명시적으로 전달하도록 구성해야 합니다.
트래픽 모니터	시스템 설정 마법사를 실행한 다음, 하나 또는 두 개의 L4 트래픽 모니터 포트(T1만 또는 T1과 T2 모두)가 모든 TCP 포트에서 트래픽을 수신하도록 구성됩니다. L4 트래픽 모니터의 기본 설정은 모니터링 전용입니다. 설정 도중 또는 이후에 의심스러운 트래픽을 모니터링하고 차단하도록 L4 트래픽 모니터를 구성할 수 있습니다.
컴퓨터 주소	컴퓨터 IP 주소 원격 액세스를 위해 일시적으로 IP 주소 변경에 기록된 원래 설정으로 다시 변경해야 합니다. 참고 **System Administration**(시스템 관리) > **Configuration Summary**(구성 요약) 페이지에서 시스템 설정 요약을 검토할 수 있습니다.



7 장

추가 구성

다음 주제에서는 어플라이언스에서 구성할 수 있는 몇 가지 추가 기능에 대해 설명합니다. 자세한 내용은 해당 AsyncOS 릴리스의 온라인 도움말 또는 사용 가이드를 참조하십시오.

사용자 정책

웹 인터페이스를 사용하여 필요에 따라 어떤 사용자가 어떤 웹 리소스에 액세스할 수 있는지 정의하는 정책을 생성합니다.

- 사용자 식별 - **Web Security Manager(**웹 보안 관리자**)** > **Identities(ID)**를 선택하여, 인터넷에 액세스할 수 있는 사용자 그룹을 정의합니다.
- 액세스 정책 정의 - **Web Security Manager** > **Access Policies(**액세스 정책**)**을 선택하여, 허용하거나 차단할 개체 및 애플리케이션, 모니터링 또는 차단할 URL 범주, 웹 신뢰도 및 악성코드 차단 설정을 구성하여 인터넷에 대한 사용자 액세스를 제어합니다.

또한 인터넷에 대한 액세스를 제어하여 조직의 사용 제한 정책을 적용하는 몇 가지 다른 정책 유형을 정의할 수 있습니다. 예를 들어 HTTPS 트랜잭션의 암호 해독을 위한 정책과 업로드 요청을 제어하는 기타 정책을 정의할 수 있습니다.

Cisco Web Security Appliance 어플라이언스에서의 정책 구성에 대한 자세한 내용은 의 *Cisco Web Security Appliance*용 *AsyncOS* 사용 가이드의 "정책 사용" 장을 참조하십시오.

보고

웹 인터페이스에서 사용 가능한 보고서를 확인하여 네트워크에서 차단되고 모니터링된 웹 트래픽에 대한 통계를 볼 수 있습니다. 가장 많이 차단된 URL 범주, 클라이언트 활동, 시스템 상태 등에 대한 보고서를 볼 수 있습니다.

추가 정보

Cisco Web Security Appliance에 대해 구성할 수 있는 다른 기능이 있습니다. 기능 키, 최종 사용자 알림, 로깅 구성에 대한 자세한 내용 및 사용 가능한 다른 Web Security Appliance 기능에 대한 자세한 내용은 Cisco Web Security Appliance S196, S396, S696 및 S696F 설명서를 참조하십시오.

A 부록

추가 정보

관련 설명서

지원	
시스코 지원 포털	http://www.cisco.com/support
미국 및 캐나다 무료 번호	800-553-2447
국제 연락처	전 세계 전화번호
이메일:	tac@cisco.com
Cisco Web Security Appliance 지원 커뮤니티	https://supportforums.cisco.com/community/netpro/security/web
제품 설명서	
Cisco Secure Web Appliance 시작 가이드*(*이 문서*)*	https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html
Cisco Secure Web Appliance 설치 및 유지 보수 가이드 LED, 기술 사양 및 마운팅 옵션에 대한 정보가 포함됩니다.	https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html
Cisco Web Security Appliance 설명서 릴리스 노트, CLI 참조 및 설정 가이드를 포함합니다.	http://www.cisco.com/en/US/customer/products/ps10164/tsd_products_support_series_home.html

안전 및 규정 준수 가이드	https://www.cisco.com/c/en/us/support/security/web-security-appliance/products-installation-guides-list.html
MIB	
Cisco Web Security Appliance용 AsyncOS MIB(관련 툴 섹션)	http://www.cisco.com/en/US/products/ps10164/tsd_products_support_series_home.html

Cisco 알림 서비스

보안 자문, 현장 통지, 판매 중단 및 지원 종료 안내문, 소프트웨어 업데이트 및 알려진 문제에 대한 정보 등 Cisco Content Security Appliance와 관련된 알림을 수신하려면 신청하십시오.

알림 빈도, 수신할 정보 유형 등의 옵션을 지정할 수 있습니다. 사용하는 각 제품에 대한 알림을 받으려면 개별적으로 신청해야 합니다.

신청하려면 http://www.cisco.com/cisco/support/notifications.html 을 방문합니다.

Cisco.com 어카운트가 필요합니다. 어카운트가 없다면 https://identity.cisco.com/ui/tenants/global/v1.0/enrollment-ui 에서 등록합니다.