FireSIGHT 시스템 설치 가이드

버전 5.4.1
2015년 2월 9일 월요일

Cisco Systems, Inc.
www.cisco.com
Cisco는 전 세계에 200개가 넘는 지사를 운영하고 있습니다.
주소, 전화 번호 및 팩스 번호는
Cisco 웹사이트
www.cisco.com/go/offices.

동봉된 제품의 소프트웨어 라이센스 및 제한 보증은 제품과 함께 제공되는 정보 패킷에 설명되어 있으며 본 참조 문서에 통합되어 있습니다. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

목 차

FireSIGHT System 소개

Cisco FireSIGHT® System에서는 업계 최고 네트워크 침입 방지 시스템의 보안을 탐지된 애플리케이션, 사용자, URL을 기준으로 네트워크에 대한 액세스를 제어하는 기능과 결합합니다. 또한 FireSIGHT System 어플라이언스를 사용하여 스위치, 라우팅 또는 하이브리드(스위치 및 라우팅) 환경에서 서비스를 제공하거나, NAT(Network Address Translation)를 수행하거나, FirePOWER 관리되는 디바이스의 가상 라우터 사이에 보안 VPN(Virtual Private Network) 터널을 구축할 수 있습니다.

Cisco 방어 센터®는 FireSIGHT System에 대한 중앙 집중식 관리 콘솔과 데이터베이스 저장소를 제공합니다. 네트워크 세그먼트에 설치된 관리되는 디바이스는 분석을 위해 트래픽을 모니터링합니다.

수동으로 구축된 디바이스는 스위치 SPAN, 가상 스위치, 미러 포트 등을 사용하여 네트워크의 트래픽 흐름을 모니터링합니다. 수동 센싱 인터페이스는 모든 트래픽을 조건 없이 수신하며 이러한 인터페이스에서 수신된 트래픽은 재전송되지 않습니다.

인라인 방식으로 구축된 디바이스를 사용하면 네트워크 호스트의 가용성, 무결성 또는 기밀성에 영향을 미칠 수 있는 공격으로부터 네트워크를 보호할 수 있습니다. 인라인 인터페이스는 모든 트래픽을 조건 없이 수신하며 이러한 인터페이스에 수신된 트래픽은 구축의 일부 컨피그레이션에 의해 명시적으로 삭제되지 않는 이상 재전송됩니다. 인라인 디바이스는 간단한 침입 방지 시스템으로 구축할 수 있습니다. 또한 인라인 디바이스가 액세스 제어를 수행하고 다른 방식으로 네트워크 트래픽을 관리하도록 구성할 수 있습니다.

이 설치 가이드에서는 FireSIGHT System 어플라이언스(디바이스 및 방어 센터) 구축, 설치 및 설정에 대한 정보를 제공합니다. 또한 FireSIGHT System 어플라이언스의 하드웨어 사양, 안전 및 규정 정보가 들어 있습니다.

[이 소개의 상당 부분은 사용 설명서 및 가상 설치 가이드에 따라 조정해야 합니다. 릴리스할 때마다 다시 확인하십시오.]

정보 가상 방어 센터와 디바이스를 호스팅하여 물리적 어플라이언스를 관리하거나 그 반대로 관리를 받을 수 있습니다. 하지만 가상 어플라이언스는 이중화, 스위칭, 라우팅 등과 같은 시스템의 하드웨어 기반 기능을 지원하지 않습니다. 자세한 내용은 *FireSIGHT System 가상 설치 가이드*를 참조하십시오.

다음 주제에서는 FireSIGHT System을 소개하고 주요 구성 요소에 대해 설명합니다.

[개선 사항: 문서 리소스, 규칙, "시작 위치" 섹션을 추가하십시오.]

FireSIGHT System 어플라이언스

FireSIGHT System *어플라이언스*는 트래픽을 감지하는 관리되는 *디바이스*이거나 관리하는 *방어 센터*입니다.

물리적 디바이스는 다양한 처리량과 기능을 제공하는 맞춤형 폴트 톨러런트(fault-tolerant) 네트워크 어플라이언스입니다. 방어 센터는 이러한 디바이스에 대한 중앙 관리 지점의 역할을 하며 디바이스에서 생성한 이벤트를 자동으로 집계하고 상관 관계를 분석합니다. 각 물리적 어플라이언스 유형에는 여러 *모델*이 있으며 이러한 모델은 추가적으로 *Series*와 *제품군*으로 그룹화됩니다. 대부분의 FireSIGHT System 기능은 어플라이언스에 따라 다릅니다.

방어 센터

방어 센터에서는 FireSIGHT System 구축을 위해 중앙 집중식 관리 지점 및 이벤트 데이터베이스를 제공합니다. 방어 센터에서는 감염 지표를 사용하여 침입, 파일, 악성코드, 검색, 연결, 성능 데이터를 집계하고 상관 관계를 분석하며 이벤트가 특정 호스트와 태깅 호스트에 미치는 영향을 평가합니다. 이 기능을 활용하면 보유 디바이스에서 다른 디바이스와 관련하여 보고하는 정보를 모니터링하고 네트워크에서 발생하는 전반적인 활동을 평가 및 제어할 수 있습니다.

방어 센터의 핵심 기능은 다음과 같습니다.

- 디바이스, 라이센스, 정책 관리
- 표, 그래프, 차트를 사용하여 이벤트 및 상황별 정보 표시
- 상태 및 성능 모니터링
- 외부 알림 및 경고
- 실시간 위협 대응을 지원하는 상관 관계 분석, 보안 침해 지표 및 치료 기능
- 맞춤형 보고 및 템플릿 기반 보고

대부분의 물리적 방어 센터의 경우 고가용성(이중화) 기능으로 운영 연속성을 보장할 수 있습니다.

관리되는 디바이스

조직 내 네트워크 세그먼트에 구축된 디바이스는 분석용 트래픽을 모니터링합니다. 수동으로 구축된 디바이스를 사용하면 네트워크 트래픽에 대한 통찰력을 얻을 수 있습니다. 인라인 형태로 구축할 경우 FirePOWER 디바이스를 사용하여 여러 기준을 기반으로 트래픽 플로우에 영향을 미칠 수 있습니다. 디바이스는 모델 및 라이센스에 따라 다음을 수행합니다.

- 조직의 호스트, 운영 체제, 애플리케이션, 사용자, 파일, 네트워크, 취약점에 대한 세부 정보 수집
- 다양한 네트워크 기반의 기준은 물론 애플리케이션, 사용자, URL, IP 주소 평판, 침입이나 악성코드 검사의 결과와 같은 기타 기준에 따라 네트워크 트래픽을 차단 또는 허용
- 스위칭, 라우팅, DHCP, NAT 및 VPN 기능과 구성 가능한 바이패스 인터페이스, 빠른 경로 규칙 및 엄격한 TCP 적용 보유
- 클러스터링(이중화)을 통해 운영 연속성 및 여러 디바이스의 리소스를 결합하는 스태킹 보장

방어 센터를 사용하여 FirePOWER 디바이스를 **관리해야** 합니다.

어플라이언스 유형

FireSIGHT System은 Cisco에서 제공하는 맞춤형 폴트 톨러런트(fault-tolerant) *물리적* 네트워크 어플라이언스에서 실행할 수 있습니다. 각 방어 센터 및 관리되는 디바이스의 여러 *모델*이 있으며 이러한 모델은 *Series* 및 *제품군*으로 세부적으로 그룹화됩니다.

물리적 관리되는 디바이스는 다양한 처리량으로 제공되며 광범위한 기능을 보유하고 있습니다. 물리적 방어 센터에도 다양한 디바이스 관리, 이벤트 스토리지, 호스트 및 사용자 모니터링 기능이 있습니다.

또한 다음과 같은 소프트웨어 기반 어플라이언스를 구축할 수 있습니다.

- VMware vSphere Hypervisor 또는 vCloud Director 환경을 사용하여 64비트 *가상* 방어 센터 및 *가상*의 관리되는 디바이스를 ESXi 호스트로 구축할 수 있습니다.
- Blue Coat X-Series 플랫폼에 Cisco NGIPS for Blue Coat X-Series를 구축할 수 있습니다. 이것은 관리되는 디바이스로 작동합니다.

모든 유형의 방어 센터(물리적 또는 가상)는 물리적, 가상, Cisco ASA with FirePOWER Services 및 Cisco NGIPS for Blue Coat X-Series와 같은 모든 유형의 디바이스를 관리할 수 있습니다. 하지만 대부분의 FireSIGHT System 기능은 어플라이언스에 따라 다릅니다.

지원하는 기능을 포함하여 FireSIGHT System 어플라이언스에 대한 자세한 내용은 다음을 참조하십시오.

Series 2 어플라이언스

Series 2는 레거시 물리적 어플라이언스의 두 번째 시리즈입니다. 리소스 및 아키텍처 제한으로 인해, Series 2 디바이스는 FireSIGHT System의 제한된 기능 집합을 지원합니다.

Cisco에서는 더 이상 새로운 Series 2 어플라이언스를 출고하지 않지만, 이전 버전의 시스템을 실행하는 Series 2 디바이스와 방어 센터를 버전 5.4.1로 업데이트하거나 이미지로 다시 설치할 수 있습니다. 이미지로 다시 설치할 경우 어플라이언스의 거의 **모든** 컨피그레이션과 이벤트 데이터가 손실됩니다. 자세한 내용은 *FireSIGHT System 설치 가이드*를 참조하십시오.

정보 버전 4.10.3 구축에서 버전 5.2 구축으로 특정 컨피그레이션 및 이벤트 데이터를 마이그레이션한 다음 버전 5.4.1로 업데이트할 수 있습니다. 자세한 내용은 버전 5.2에 대한 *Cisco FireSIGHT 시스템 마이그레이션 가이드*를 참조하십시오.

Series 2 디바이스에는 보호 라이센스와 관련된 대부분의 기능, 즉, 침입 탐지 및 방지, 파일 제어, 기본적 액세스 제어가 탑재되어 있습니다. 하지만, Series 2 디바이스에서는 보안 인텔리전스 필터링, 고급 액세스 제어 또는 AMP(Advanced Malware Protection)를 수행할 수 없으며 아카이브된 파일의 콘텐츠를 검사할 수 없습니다. 또한 Series 2 디바이스에서 다른 라이센스가 있는 기능을 활성화할 수 없습니다. 빠른 경로 규칙, 스태킹, 탭 모드를 지원하는 3D9900을 제외하고, Series 2 디바이스는 Series 3 디바이스와 관련된 하드웨어 기반 기능(스위칭, 라우팅, NAT 등)을 지원하지 않습니다.

버전 5.4.1을 실행할 경우 DC1000 및 DC3000 Series 2 방어 센터에서는 FireSIGHT System의 모든 기능을 지원하며 DC500의 기능은 이보다 제한적입니다.

Series 3 어플라이언스

Series 3은 FirePOWER 물리적 어플라이언스의 세 번째 시리즈입니다. 모든 7000 Series 및 8000 Series 디바이스는 Series 3 어플라이언스입니다. 8000 Series 디바이스가 더 강력하며 7000 Series 디바이스에서 지원하지 않는 몇 가지 기능을 지원합니다.

가상 어플라이언스

VMware vSphere Hypervisor 또는 vCloud Director 환경을 사용하여 64비트 가상 방어 센터 및 관리되는 디바이스를 ESXi 호스트로 구축할 수 있습니다.

가상 어플라이언스는 설치 및 적용된 라이센스와 상관없이, 시스템의 하드웨어 기반 기능(이중화, 리소스 공유, 스위칭, 라우팅 등)을 지원하지 않습니다. 또한 가상 디바이스에는 웹 인터페이스가 없습니다. 가상 어플라이언스에 대한 자세한 내용은 *FireSIGHT System 가상 설치 가이드*를 참조하십시오.

Cisco NGIPS for Blue Coat X-Series

Blue Coat X-Series 플랫폼에서 Cisco NGIPS for Blue Coat X-Series를 설치할 수 있습니다. 이 소프트웨어 기반 어플라이언스는 가상의 관리되는 디바이스와 유사한 방식으로 작동합니다. 설치 및 적용된 라이센스와 상관없이 Cisco NGIPS for Blue Coat X-Series에서는 다음 기능을 지원하지 않습니다.

- Cisco NGIPS for Blue Coat X-Series에서는 클러스터링, 스태킹, 스위칭, 라우팅, VPN, NAT 등과 같은 시스템의 하드웨어 기반 기능을 지원하지 않습니다.
- Cisco NGIPS for Blue Coat X-Series를 사용하여 발송지 또는 대상지의 국가 또는 대륙을 기준으로 네트워크 트래픽을 필터링할 수 없습니다(위치 기반 액세스 제어).
- 방어 센터 웹 인터페이스를 사용하여 Cisco NGIPS for Blue Coat X-Series 인터페이스를 구성할 수 없습니다.
- 방어 센터를 사용하여 Cisco NGIPS for Blue Coat X-Series 프로세스를 종료하거나 다시 시작하거나 다른 방식으로 관리할 수 없습니다.
- 방어 센터를 사용하여 Cisco NGIPS for Blue Coat X-Series에서 백업을 생성하거나 여기로 백업을 복원할 수 없습니다.
- Cisco NGIPS for Blue Coat X-Series에 상태 또는 시스템 정책을 적용할 수 없습니다. 여기에는 시간 설정 관리가 포함됩니다.

Cisco NGIPS for Blue Coat X-Series에는 웹 인터페이스가 없습니다. 그러나 X-Series 플랫폼에 고유한 CLI(Command Line Interface)가 있습니다. 이 CLI를 사용하여 시스템을 설치하고 다음과 같이 다른 플랫폼별 관리 작업을 수행할 수 있습니다.

- X-Series 플랫폼의 로드 밸런싱 및 이중화 이점(Cisco 물리적 디바이스 클러스터링과 비교 가능)을 활용할 수 있는 VAP(Virtual Appliance Processor) 그룹 만들기
- 인터페이스의 MTU(Maximum Transmission Unit) 구성을 포함한 수동 및 인라인 센싱 인터페이스 구성
- 프로세스 관리
- NTP 설정을 포함한 시간 설정 관리

Cisco ASA with FirePOWER Services

Cisco ASA with FirePOWER Services(ASA FirePOWER 디바이스)는 관리되는 디바이스와 유사한 방식으로 작동합니다. 이러한 구축 환경에서 ASA 디바이스는 액세스 제어, 침입 탐지 및 방지, 검색, AMP(Advanced Malware Protection)를 위해 FireSIGHT System에 시스템 정책을 제공하고 트래픽을 전달합니다. 지원되는 ASA 모델 목록은 버전 5.4.1 FireSIGHT System 어플라이언스 표를 참조하십시오.

설치 및 적용된 라이센스와 상관없이 ASA FirePOWER 디바이스는 FireSIGHT System을 통해 다음 기능을 지원하지 않습니다.

- ASA FirePOWER 디바이스는 클러스터링, 스태킹, 스위칭, 라우팅, VPN, NAT 등과 같은 FireSIGHT System의 하드웨어 기반 기능을 지원하지 않습니다. 그러나 ASA 플랫폼은 이러한 기능을 제공하며, ASA CLI 및 ASDM을 사용하여 구성할 수 있습니다. 자세한 내용은 ASA 설명서를 참조하십시오.
- ASA FirePOWER 디바이스는 SSL 검사를 지원하지 않습니다.
- 방어 센터 웹 인터페이스를 사용하여 ASA FirePOWER 인터페이스를 구성할 수 없습니다.
- 방어 센터를 사용하여 ASA FirePOWER 프로세스를 종료하거나 다시 시작하거나 다른 방식으로 관리할 수 없습니다.
- 방어 센터를 사용하여 ASA FirePOWER 디바이스에서 백업을 생성하거나 해당 디바이스로 백업을 복원할 수 없습니다.
- VLAN 태그 조건을 사용하여 트래픽과 일치시키기 위한 액세스 제어 규칙을 작성할 수 없습니다.

ASA FirePOWER 디바이스에는 FireSIGHT 웹 인터페이스가 없습니다. 그러나 ASA 플랫폼에 고유한 소프트웨어와 CLI(Command Line Interface)가 있습니다. 이러한 ASA 특정 툴을 사용하여 시스템을 설치하고 다른 플랫폼별 관리 작업을 수행합니다. 자세한 내용은 ASA FirePOWER 모듈 설명서를 참조하십시오.

ASA5506-X, ASA5506H-X, 5506W-X, 5508-X, and 5518-X 디바이스를 독립형 디바이스 또는 관리되는 디바이스로 관리할 수 있습니다. 독립형 ASA FirePOWER 모듈은 ASDM으로 관리하고 관리되는 ASA FirePOWER 디바이스는 방어 센터로 관리합니다. 디바이스가 방어 센터에 등록된 경우에는 ASA FirePOWER 모듈을 ASDM으로 관리할 수 없습니다.

또한 ASA FirePOWER 모듈에는 FirePOWER 어플라이언스용 CLI가 포함됩니다. CLI를 사용하여 FireSIGHT System을 보고 구성하며 문제를 해결할 수 있습니다. 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

버전 5.4.1에 제공되는 어플라이언스

다음 표에는 Cisco에서 FireSIGHT System 버전 5.4.1에 제공하는 어플라이언스가 나열되어 있습니다.

표 1-1 버전 5.4.1 FireSIGHT System 어플라이언스

모델/제품군	시리즈	형식	유형
70xx 제품군: • 3D7010, 3D7020, 3D7030, 3D7050	Series 3 (7000 Series)	하드웨어	디바이스

표 1-1 버전 5.4.1 FireSIGHT System 어플라이언스(계속)

모델/제품군	시리즈	형식	유형
71xx 제품군: • 3D7110, 3D7120 • 3D7115, 3D7125 • AMP7150	Series 3 (7000 Series)	하드웨어	디바이스
80xx 제품군: • AMP8050	Series 3 (8000 Series)	하드웨어	디바이스
81xx 제품군: • 3D8120, 3D8130, 3D8140 • AMP8150	Series 3 (8000 Series)	하드웨어	디바이스
82xx 제품군: • 3D8250 • 3D8260, 3D8270, 3D8290	Series 3 (8000 Series)	하드웨어	디바이스
83xx 제품군: • 3D8350 • 3D8360, 3D8370, 3D8390 • AMP8350 • AMP8360, AMP8370, AMP8390	Series 3 (8000 Series)	하드웨어	디바이스
64비트 가상 디바이스	해당 없음	소프트웨어	디바이스
Cisco NGIPS for Blue Coat X-Series	해당 없음	소프트웨어	디바이스
ASA FirePOWER: • ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40, ASA5585-X-SSP-60	해당 없음	하드웨어	디바이스
ASA FirePOWER: • ASA5506-X ASA5506H-X, 5506W-X, 5508-X, ASA5512-X, ASA5515-X, 5518-XASA5525-X, ASA5545-X, ASA5555-X	해당 없음	소프트웨어	디바이스
Series 3 방어 센터: • DC750, DC1500, DC2000, DC3500, DC4000	Series 3	하드웨어	방어 센터
64비트 가상 방어 센터	해당 없음	소프트웨어	방어 센터

Cisco에서는 더 이상 새로운 Series 2 어플라이언스를 출시하지 않지만, 이전 버전의 시스템을 실행 중인 다음 Series 2 디바이스와 방어 센터를 버전 5.4.1로 업데이트하거나 이미지로 다시 설치할 수 있습니다.

- 3D500, 3D1000, 3D2000
- 3D2100, 3D2500, 3D3500, 3D4500
- 3D6500
- 3D9900
- DC500, DC1000, DC3000

이미지로 다시 설치할 경우 어플라이언스의 **모든** 컨피그레이션과 이벤트 데이터가 손실됩니다. 자세한 내용은 FireSIGHT System 어플라이언스를 출고 시 기본 설정으로 복원, 페이지 8-1을(를) 참조하십시오.

정보 버전 4.10.3 구축에서 버전 5.2 구축으로 특정 컨피그레이션 및 이벤트 데이터를 마이그레이션한 다음 버전 5.4.1로 업데이트할 수 있습니다. 자세한 내용은 버전 5.2에 대한 *FireSIGHT System 마이그레이션 가이드*를 참조하십시오.

방어 센터 모델별 지원되는 기능

버전 5.4.1을 실행 중인 경우 방어 센터에서는 몇 가지 모델 기반 제한 사항을 제외하고 유사한 기능을 제공합니다. 다음 표에는 시스템의 주요 기능과 이러한 기능을 지원하는 방어 센터가 연결되어 있습니다. 여기서는 이러한 기능을 지원하고 올바른 라이센스가 설치 및 적용된 디바이스를 관리 중인 것으로 가정합니다.

이 표에 나열된 기능 이외에, 방어 센터 모델은 관리할 수 있는 디바이스 수, 저장할 수 있는 이벤트 수, 모니터링할 수 있는 호스트 및 사용자 수에 따라 다양합니다. 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

또한 시스템의 버전 5.4.1을 실행하는 방어 센터 모델을 사용하여 버전 5.4.1 디바이스를 관리할 수 있는 경우에도 대부분의 시스템 기능은 디바이스 모델에 따라 제한됩니다. 예를 들어, Series 3 방어 센터가 있는 경우에도 구축에 Series 3 디바이스도 포함되어 있지 않으면 VPN을 구현할 수 없습니다. 자세한 내용은 관리되는 디바이스 모델별 지원되는 기능, 페이지 1-8을(를) 참고하십시오.

표 1-2 방어 센터 모델별 지원되는 기능

기능	Series 2 방어 센터	Series 3 방어 센터	가상 방어 센터
관리되는 디바이스가 보고하는 검색 데이터(호스트, 애플리케이션, 사용자) 수집 및 조직의 네트워크 맵 구축	예	예	예
네트워크 트래픽의 위치 데이터 보기	DC1000, DC3000	예	예
침입 탐지 및 방지(IPS) 구축 관리	예	예	예
보안 인텔리전스 필터링을 수행하는 디바이스 관리	DC1000, DC3000	예	예
위치 기반 필터링을 포함하여 간단한 네트워크 기반 제어를 수행하는 디바이스 관리	예	예	예
애플리케이션 제어를 수행하는 디바이스 관리	예	예	예
사용자 제어를 수행하는 디바이스 관리	DC1000, DC3000	예	예

표 1-2 방어 센터 모델별 지원되는 기능(계속)

기능	Series 2 방어 센터	Series 3 방어 센터	가상 방어 센터
리터럴 URL을 통해 네트워크 트래픽을 필터링하는 디바이스 관리	예	예	예
범주 및 평판별 URL 필터링을 수행하는 디바이스 관리	DC1000, DC3000	예	예
파일 유형별로 간단한 파일 제어를 수행하는 디바이스 관리	예	예	예
네트워크 기반 AMP(Advanced Malware Protection)를 수행하는 디바이스 관리	DC1000, DC3000	예	예
FireAMP 구축에서 엔드포인트 기반 악성코드(FireAMP) 이벤트 수신	예	예	예
디바이스 기반 하드웨어 기반 기능 관리: • 빠른 경로 규칙 • 엄격한 TCP 구현 • 구성 가능한 바이패스 인터페이스 • 탭 모드 • 스위칭 및 라우팅 • NAT 정책 • VPN	예	예	예
디바이스 기반 이중화 및 리소스 공유 관리: • 디바이스 스택 • 디바이스 클러스터 • Cisco NGIPS for Blue Coat X-Series VAP 그룹 • 클러스터링 스택	예	예	예
트래픽 채널을 사용하여 내부 및 외부 트래픽 구분 및 관리	아니요	예	예
복수 관리 인터페이스를 사용하여 서로 다른 네트워크에서 트래픽 격리 및 관리	아니요	예	예
고가용성 구현	DC1000, DC3000	DC1500, DC2000, DC3500, DC4000	아니요
악성코드 스토리지 팩 설치	DC1000, DC3000	예	아니요
eStreamer, 호스트 입력 또는 데이터베이스 클라이언트에 연결	예	예	예

관리되는 디바이스 모델별 지원되는 기능

디바이스는 네트워크 트래픽을 처리하는 어플라이언스이므로 대부분의 FireSIGHT System 기능은 관리되는 디바이스 모델에 따라 달라집니다.

다음 표에는 시스템의 주요 기능과 이러한 기능을 지원하는 디바이스가 연결되어 있습니다. 여기서는 방어 센터 관리에서 올바른 라이센스가 설치 및 적용된 것으로 가정합니다.

또한 시스템의 버전 5.4.1을 실행하는 방어 센터 모델을 사용하여 버전 5.4.1 디바이스를 관리할 수 있는 경우에도 몇 가지 시스템 기능은 방어 센터 모델에 따라 제한됩니다. 예를 들어, 디바이스가 보안 인텔리전스 필터링을 지원하는 경우에도 Series 2 DC500을 사용하여 이 기능을 지원하는 디바이스를 관리할 수 없습니다. 자세한 내용은 방어 센터 모델별 지원되는 기능, 페이지 1-7을(를) 참고하십시오.

표 1-3 관리되는 디바이스 모델별 지원되는 기능

기능	Series 2 디바이스	Series 3 디바이스	ASA FirePOWER	가상 디바이스	X-Series
네트워크 검색: 호스트, 애플리케이션, 사용자	예	예	예	예	예
침입 탐지 및 방지(IPS)	예	예	예	예	예
보안 인텔리전스 필터링	아니요	예	예	예	예
액세스 제어: 기본적인 네트워크 제어	예	예	예	예	예
액세스 제어: 위치 기반 필터링	아니요	예	예	예	아니요
액세스 제어: 애플리케이션 제어	아니요	예	예	예	예
액세스 제어: 사용자 제어	아니요	예	예	예	예
액세스 제어: 리터럴 URL	아니요	예	예	예	예
액세스 제어: 범주 및 평판별 URL 필터링	아니요	예	예	예	예
파일 제어: 파일 유형별	예	예	예	예	예
네트워크 기반 AMP(Advanced Malware Protection)	아니요	예	예	예	예
자동 애플리케이션 바이패스	예	예	아니요	예	아니요
빠른 경로(Fast-Path) 규칙	3D9900	8000 Series	아니요	아니요	아니요
엄격한 TCP 적용	아니요	예	아니요	아니요	아니요
구성 가능한 바이패스 인터페이스	예	하드웨어가 제한적인 경우 제외	아니요	아니요	아니요
탭 모드	3D9900	예	아니요	아니요	아니요
스위칭 및 라우팅	아니요	예	아니요	아니요	아니요
NAT 정책	아니요	예	아니요	아니요	아니요
VPN	아니요	예	아니요	아니요	아니요
디바이스 스태킹	3D9900	3D8140 82xx 제품군 83xx 제품군	아니요	아니요	아니요
디바이스 클러스터링	아니요	예	아니요	아니요	아니요
클러스터링 스택	아니요	3D8140 82xx 제품군 83xx 제품군	아니요	아니요	아니요
트래픽 채널	아니요	예	아니요	아니요	아니요
복수 관리 인터페이스	아니요	예	아니요	아니요	아니요
악성코드 스토리지 팩	아니요	예	아니요	아니요	아니요
제한된 CLI(Command Line Interface)	아니요	예	예	예	아니요

표 1-3 관리되는 디바이스 모델별 지원되는 기능(계속)

기능	Series 2 디바이스	Series 3 디바이스	ASA FirePOWER	가상 디바이스	X-Series
외부 인증	예	예	아니요	아니요	아니요
eStreamer 클라이언트에 연결	예	예	예	아니요	아니요

Series 3 디바이스 섀시 지정

다음 섹션에는 7000 Series 및 8000 Series 디바이스 및 각각의 섀시 하드웨어 코드가 나열되어 있습니다. 섀시 코드는 섀시 외부의 규정 레이블에 표시되며 하드웨어 인증 및 안전에 대한 공식 참조 코드입니다.

7000 Series 섀시 지정

다음 표에는 전 세계적으로 사용 가능한 7000 Series 모델의 섀시 지정이 나열되어 있습니다.

표 1-4 7000 Series 섀시 모델

3D 및 AMP 디바이스 모델	하드웨어 섀시 코드
3D7010, 3D7020, 3D7030	CHRY-1U-AC
3D7050	NEME-1U-AC
3D7110, 3D7120(구리)	GERY-1U-8-C-AC
3D7110, 3D7120(파이버)	GERY-1U-8-FM-AC
3D7115, 3D7125, AMP7150	GERY-1U-4C8S-AC

8000 Series 섀시 지정

다음 표에는 전 세계적으로 사용 가능한 Series 3 모델의 섀시 지정이 나열되어 있습니다.

표 1-5 8000 Series 섀시 모델

3D 및 AMP 디바이스 모델	하드웨어 섀시 코드
AMP8050(AC 또는 DC 전원)	CHAS-1U-AC/DC
3D8120, 3D8130, 3D8140, AMP8150 (AC 또는 DC 전원)	CHAS-1U-AC/DC
3D8250, 3D8260, 3D8270, 3D8290 (AC 또는 DC 전원)	CHAS-2U-AC/DC
3D8350, 3D8360, 3D8370, 3D8390 (AC 또는 DC 전원)	PG35-2U-AC/DC
AMP830, AMP8360, AMP8370, AMP8390 (AC 또는 DC 전원)	PG35-2U-AC/DC

FireSIGHT System 구성 요소

다음 섹션에서는 조직의 보안, 사용 정책 제어, 트래픽 관리 전략에 기여하는 FireSIGHT System의 몇 가지 주요 기능에 대해 설명합니다.

정보 대부분의 FireSIGHT System 기능은 어플라이언스 모델, 라이센스 및 사용자 역할에 따라 달라집니다. FireSIGHT System 설명서에는 필요에 따라 각 기능 및 작업의 요구 사항이 요약되어 있습니다.

이중화 및 리소스 공유

FireSIGHT System의 이중화 및 리소스 공유 기능을 이용하면 운영 연속성을 보장하고 복수 물리적 디바이스의 처리 리소스를 결합할 수 있습니다.

- 방어 센터 고가용성을 통해 이중화 DC1000, DC1500, DC2000, DC3000, DC3500 또는 DC4000 방어 센터를 지정하여 디바이스를 관리할 수 있습니다.
- 디바이스 스태킹을 이용하면 스택 컨피그레이션에서 2~4개의 물리적 디바이스를 연결하여 네트워크 세그먼트에서 검사하는 트래픽의 양을 늘릴 수 있습니다.
- 디바이스 클러스터링을 이용하면 2개 이상의 Series 3 디바이스 또는 스택 사이에서 네트워킹 기능 및 컨피그레이션 데이터의 이중화를 구현할 수 있습니다.

복수 관리 인터페이스

방어 센터, 디바이스 또는 둘 다에 대해 *복수 관리 인터페이스*를 사용하면 트래픽을 두 개의 트래픽 채널로 구분하여 성능을 향상할 수 있습니다. 즉, *관리 트래픽 채널*에서는 디바이스 간 통신이 이루어지며 *이벤트 트래픽 채널*에서는 침입 이벤트와 같은 높은 볼륨의 이벤트 트래픽이 전송됩니다. 두 트래픽 채널 모두 동일한 관리 인터페이스를 이용할 수도 있고, 각각 하나의 트래픽 채널을 전달하는 두 개의 관리 인터페이스로 분할할 수 있습니다.

또한 방어 센터의 특정 관리 인터페이스에서 다른 네트워크로 경로를 만들 수 있으므로 방어 센터를 통해 한 네트워크에 있는 디바이스 트래픽을 다른 네트워크에 있는 디바이스 트래픽과 격리하여 별도로 관리할 수 있습니다.

다음을 제외하고, 추가 관리 인터페이스에는 기본 관리 인터페이스와 동일한 여러 기능(예: 방어 센터 간 고가용성 이용)이 포함되어 있습니다.

- 기본(`eth0`) 관리 인터페이스에서만 DHCP를 구성할 수 있습니다. 추가(`eth1` 등) 인터페이스에는 고유한 고정 IP 주소 및 호스트 이름이 필요합니다.
- 방어 센터 및 관리되는 디바이스가 NAT 디바이스로 구분되어 있는 경우 기본이 아닌 동일한 관리 인터페이스를 사용하도록 두 트래픽 채널을 구성해야 합니다.
- 기본 관리 인터페이스에서만 Lights-Out 관리를 사용할 수 있습니다.
- 70xx 제품군에서는 트래픽을 두 개의 채널로 구분하고 해당 채널이 트래픽을 방어 센터에 있는 한 개 이상의 관리 인터페이스로 전송하도록 구성할 수 있습니다. 그러나 70xx 제품군에는 하나의 관리 인터페이스만 포함되어 있으므로 디바이스에서는 한 관리 인터페이스의 방어 센터에서 전송된 트래픽만 수신합니다.

어플라이언스를 설치한 후 웹 브라우저를 사용하여 복수 관리 인터페이스를 구성하십시오. 자세한 내용은 *FireSIGHT System 사용 설명서*에서 복수 관리 인터페이스를 참조하십시오.

네트워크 트래픽 관리

FireSIGHT System의 네트워크 트래픽 관리 기능을 사용하면 Series 3 디바이스를 조직의 네트워크 인프라 중 일부처럼 작동할 수 있습니다. 다음 작업을 수행할 수 있습니다.

- 레이어 2 구축을 구성하여 두 개 이상의 네트워크 세그먼트 사이에서 패킷 스위칭 수행

- 레이어 3 구축을 구성하여 두 개 이상의 인터페이스 사이에 트래픽 라우팅
- NAT(Network Address Translation) 수행
- 관리되는 디바이스의 가상 라우터에서 원격 디바이스 또는 다른 서드파티의 VPN 엔드포인트로 보안 VPN 터널 구축

FireSIGHT

FireSIGHT™는 네트워크에 대한 완전한 가시성을 제공하기 위해 호스트, 운영 체제, 애플리케이션, 사용자, 파일, 네트워크, 위치 정보, 취약성에 대한 정보를 수집하는 Cisco의 검색 및 인식 기술입니다.

방어 센터의 웹 인터페이스를 통해 FireSIGHT에서 수집한 데이터를 보고 분석할 수 있습니다. 또한 이 데이터를 사용하여 액세스 제어를 수행하고 침입 규칙 상태를 수정할 수도 있습니다. 뿐만 아니라, 호스트에 대한 상관관계 이벤트 데이터를 기준으로 네트워크의 호스트에 대한 감염지표를 생성 및 추적할 수 있습니다.

액세스 제어

액세스 제어는 네트워크를 통해 이동하는 트래픽을 지정, 검사 및 로깅할 수 있도록 하는 정책 기반 기능입니다. 보안 인텔리전스 기능은 액세스 제어에 포함되며, 트래픽을 자세히 분석하기 전에 특정 IP 주소를 블랙리스트에 추가합니다(트래픽의 수신 및 송신 거부).

보안 인텔리전스 필터링이 발생한 후 간단한 IP 주소 매핑부터 여러 사용자, 애플리케이션, 포트, URL이 관련된 복잡한 시나리오까지 대상 디바이스에서 처리할 트래픽과 처리 방식을 정의할 수 있습니다. 트래픽을 신뢰, 모니터링, 차단하거나 다음과 같은 추가 분석을 수행할 수 있습니다.

- 침입 탐지 및 방지
- 파일 제어
- 파일 추적 및 네트워크 기반 AMP(Advanced Malware Protection)

침입 탐지 및 방지

침입 탐지 및 방지는 액세스 제어에 통합된 정책 기반 기능으로, 이 기능을 통해 네트워크 트래픽을 모니터링하여 보안 위반을 찾아내고 인라인 구축의 경우 악성 트래픽을 차단 또는 수정할 수 있습니다. 침입 정책에는 다음과 같이 다양한 구성 요소가 포함되어 있습니다.

- 프로토콜 헤더 값, 페이로드 콘텐츠, 특정 패킷 크기 특성을 검사하는 규칙
- FireSIGHT 권장 사항을 기반으로 하는 규칙 상태 컨피그레이션
- 고급 설정(예: 프리프로세서), 기타 탐지 및 성능 기능
- 관련 프리프로세서 및 프리프로세서 옵션을 위한 이벤트를 생성할 수 있는 프리프로세서 규칙

파일 추적, 제어, 네트워크 기반 AMP(Advanced Malware Protection)

FireSIGHT System의 파일 제어, 네트워크 파일 전파 흔적 분석(File trajectory) 및 AMP 구성 요소는 악성코드의 효과를 식별하고 완화할 수 있도록 네트워크 트래픽의 파일(악성코드 파일 포함) 전송을 탐지, 추적, 캡처, 분석하고, 선택적으로 차단할 수 있습니다.

파일 제어는 액세스 제어에 통합된 정책 기반 기능으로, 이 기능을 사용하면 관리되는 디바이스가 특정 애플리케이션 프로토콜에서 특정 유형의 파일을 업로드(전송) 또는 다운로드(수신)하는 사용자를 감지 및 차단할 수 있습니다.

네트워크 기반 *AMP(Advanced Malware Protection)*를 사용하면 네트워크 트래픽에서 몇 가지 파일 유형의 악성코드를 검사할 수 있습니다. 어플라이언스는 감지된 파일을 추가 분석을 위해 하드 드라이브 또는 악성코드 스토리지 팩(일부 모델)에 저장할 수 있습니다.

감지된 파일의 저장 여부와 상관없이, 파일을 Cisco 클라우드에 제출하여 파일의 SHA-256 해시 값을 통해 알려진 속성 조회를 간단히 수행할 수 있습니다. 또한 위협 점수를 생성하는 *동적 분석*을 위해 파일을 제출할 수도 있습니다. 이러한 상황별 정보를 사용하여 특정 파일을 차단하거나 허용하도록 시스템을 구성할 수 있습니다.

FireAMP는 지능형 위협 발생, APT(Advanced Persistent Threat) 및 표적 공격을 발견하고 파악하여 차단하는 Cisco의 엔터프라이즈급 지능형 위협 분석 및 보호 솔루션입니다. 조직이 FireAMP에 가입된 경우 개별 사용자가 컴퓨터와 모바일 디바이스(엔드포인트라고도 함)에 FireAMP Connector를 설치할 수 있습니다. 이와 같이 경량 에이전트는 Cisco 클라우드와 통신하며, Cisco 클라우드는 방어 센터와 통신합니다.

클라우드에 연결하도록 방어 센터를 구성한 후 방어 센터 웹 인터페이스를 사용하여 조직의 엔드포인트에서 검사, 탐지, 격리의 결과로 생성된 엔드포인트 기반 악성코드 이벤트를 확인할 수 있습니다. 방어 센터는 또한 FireAMP 데이터를 사용하여 호스트에서 감염지표를 생성 및 추적하고 네트워크 파일 전파 흔적 분석을 표시합니다.

네트워크 파일 전파 흔적 분석 기능은 네트워크에서 파일의 전송 경로를 추적합니다. 시스템에서는 SHA256 해시 값을 사용하여 파일을 추적합니다. 각 파일에는 관련 전파 흔적 맵이 있으며, 여기에는 시간의 추이에 따른 파일의 전송 상태를 시각적으로 보여주는 자료 및 파일에 대한 추가 정보가 포함됩니다.

API(Application Programming Interface)

API(Application Programming Interface)를 사용하여 시스템과 상호 작용하는 몇 가지 방법이 있습니다.

- Event Streamer(eStreamer)를 사용하면 FireSIGHT System 어플라이언스에서 맞춤 개발된 클라이언트 애플리케이션으로 여러 종류의 이벤트 데이터를 스트리밍할 수 있습니다.
- 데이터베이스 액세스 기능을 사용하면 JDBC SSL 연결을 지원하는 서드파티 클라이언트를 사용하여 방어 센터의 여러 데이터베이스 테이블을 쿼리할 수 있습니다. [되돌아오는 경우 MDC.]
- 호스트 입력 기능은 스크립트 또는 커맨드 라인 파일을 사용하여 서드파티 소스에서 데이터를 가져오는 방법으로 네트워크 맵의 정보를 보강할 수 있습니다.
- 위협 요소 제거는 네트워크에서 특정 조건이 충족될 경우 방어 센터에서 자동으로 시작하는 프로그램입니다. 이 프로그램은 문제를 즉시 해결할 수 없을 때 공격을 자동으로 완화할 뿐만 아니라 시스템이 조직의 보안 정책을 준수함을 보장할 수 있습니다.

FireSIGHT System 라이센싱

다양한 기능의 라이센스를 취득하여 조직에 최적의 FireSIGHT System 구축을 조성할 수 있습니다. 방어 센터를 사용하여 자체 라이센스 및 여기에서 관리하는 디바이스의 라이센스를 제어해야 합니다.

조직에서 구매한 라이센스는 방어 센터의 초기 설정 과정에서 추가하는 것이 좋습니다. 그렇지 않을 경우 초기 설정 중 등록하는 디바이스는 방어 센터에 라이센스가 없는 상태로 추가됩니다. 초기 설정 프로세스를 마친 다음 각 디바이스에서 라이센스를 개별적으로 활성화해야 합니다. 자세한 내용은 FireSIGHT System 어플라이언스 설정, 페이지 5-1을(를) 참고하십시오.

FireSIGHT 라이센스는 구매한 각 방어 센터에 포함되어 있으며 호스트, 애플리케이션, 사용자 검색을 수행하는 데 필요합니다. 방어 센터의 FireSIGHT 라이센스에 따라, 방어 센터를 사용하여 모니터링할 수 있는 개별 호스트 및 사용자의 수, 관리되는 디바이스, 사용자 제어를 수행하는 데 사용할 수 있는 사용자 수가 결정됩니다. FireSIGHT 호스트 및 사용자 라이센스 한도는 아래 표와 같이 모델별로 다릅니다.

표 1-6 방어 센터 모델별 FireSIGHT 한도

방어 센터 모델	FireSIGHT 호스트 및 사용자 한도
DC500	1000(사용자 제어 없음)
DC750	2000
DC1000	20,000
DC1500	50,000
DC2000	100,000
DC3000	100,000
DC3500	300,000
DC4000	600,000

방어 센터에서 이전에 버전 4.10.x를 실행 중이었다면 FireSIGHT 라이센스 대신 레거시 RNA 호스트 및 RUA 사용자 라이센스를 사용할 수 있습니다. 자세한 내용은 레거시 RNA 호스트 및 RUA 사용자 라이센스 사용, 페이지 1-16을(를) 참고하십시오.

추가 모델별 라이센스를 사용하면 관리되는 디바이스로 다음과 같이 다양한 기능을 수행할 수 있습니다.

보호

보호 라이센스를 사용하면 관리되는 디바이스에서 침입 탐지 및 방지, 파일 제어, 보안 인텔리전스 필터링을 수행할 수 있습니다.

제어

제어 라이센스를 사용하면 관리되는 디바이스에서 사용자 및 애플리케이션 제어를 수행할 수 있습니다. 또한 디바이스에서 스위칭 및 라우팅(DHCP 릴레이 포함), NAT를 수행하고 디바이스와 스택을 클러스터링할 수 있습니다. [JUDY - NAT에 대해 업데이트된 텍스트는 Leon에게 확인하십시오.] 제어 라이센스에는 보호 라이센스가 필요합니다.

URL 필터링

URL 필터링 라이센스를 사용하면 관리되는 디바이스가 정기적으로 업데이트되는 클라우드 기반 카테고리 및 평판 데이터를 사용하여 모니터링되는 호스트에서 요청한 URL을 기준으로 네트워크를 이동할 수 있는 트래픽을 결정할 수 있습니다. URL 필터링 라이센스에는 보호 라이센스가 필요합니다.

악성코드

악성코드 라이센스를 사용하면 관리되는 디바이스가 네트워크에서 전송된 파일에서 악성코드를 감지 및 차단하는 네트워크 기반 AMP(Advanced Malware Protection)를 수행할 수 있습니다. 또한 네트워크에서 전송된 파일을 추적하는 전파 흔적 분석을 볼 수 있습니다. 악성코드 라이센스에는 보호 라이센스가 필요합니다.

VPN

VPN 라이센스를 사용하면 Cisco 관리되는 디바이스의 가상 라우터 사이 또는 관리되는 디바이스에서 원격 디바이스 또는 다른 서드파티 VPN 엔드포인트로 보안 VPN 터널을 구축할 수 있습니다. VPN 라이센스에는 보호 및 제어 라이센스가 필요합니다.

아키텍처 및 리소스 제한으로 인해, 모든 라이센스를 모든 관리되는 디바이스에 적용할 수는 없습니다. 일반적으로 디바이스에서 지원하지 않는 기능에 대해서는 라이센스를 취득할 수 없습니다. 관리되는 디바이스 모델별 지원되는 기능, 페이지 1-8을(를) 참조하십시오.

다음 표에는 방어 센터에 추가하고 각 디바이스 모델에 적용할 수 있는 라이센스가 요약되어 있습니다. 방어 센터 행(FireSIGHT를 제외한 모든 라이센스)은 해당 방어 센터에서 이러한 라이센스를 사용하여 디바이스를 관리할 수 있는지 여부를 나타냅니다. 예를 들어, Series 2 DC1000을 사용하면 Series 3 디바이스를 이용한 VPN 구축이 가능하지만, DC500을 사용할 경우 관리하는 디바이스와 상관없이 범주 및 평판 기반 URL 필터링을 수행할 수 없습니다. 해당 없음 표시는 관리되는 디바이스와 관련 없는 방어 센터 기반 라이센스를 나타냅니다.

표 1-7 모델별 지원되는 라이센스

모델	FireSIGHT	보호	제어	URL 필터링	악성코드	VPN
Series 2 디바이스: • 3D500, 3D1000, 3D2000 • 3D2100, 3D2500, 3D3500, 3D4500 • 3D6500 • 3D9900	해당 없음	자동, 보안 인텔리전스 없음	아니요	아니요	아니요	아니요
Series 3 디바이스: • 7000 Series • 8000 Series	해당 없음	예	예	예	예	예
가상 디바이스	해당 없음	예	예. 단, 하드웨어 기능에는 지원되지 않음	예	예	아니요
Cisco ASA with FirePOWER Services	해당 없음	예	예. 단, 하드웨어 기능에는 지원되지 않음	예	예	아니요
Cisco NGIPS for Blue Coat X-Series	해당 없음	예	예. 단, 하드웨어 기능에는 지원되지 않음	예	예	아니요
Series 2 방어 센터: • DC500	예	예. 단, 보안 인텔리전스 없음	예. 단, 사용자 제어 없음	아니요	아니요	예
Series 2 방어 센터: • DC1000, DC3000	예	예	예	예	예	예
Series 3 방어 센터: • DC750, DC1500, DC2000, DC3500, DC4000	예	예	예	예	예	예
가상 방어 센터	예	예	예	예	예	예

개선 사항: 이 표를 현재 위치에 배치하지 말고 사용 설명서의 라이센싱 장에 배치하되, 눈금 표시는 제거하십시오. 또는 스타일 설명서 논의가 완료될 때까지 기다리십시오.

표의 정보 이외에 다음을 참고하십시오.

- Series 2 디바이스는 보안 인텔리전스 필터링을 제외한 보호 기능을 자동으로 사용할 수 있습니다.
- 가상 디바이스에서 제어 라이센스를 활성화할 수 있지만 가상 디바이스는 스위칭이나 라우팅과 같이 해당 라이센스에서 부여되는 하드웨어 기반 기능을 지원하지 않습니다.
- DC500은 보호 및 제어 라이센스로 디바이스를 관리할 수 있지만, 보안 인텔리전스 필터링 또는 사용자 제어는 수행할 수 없습니다.

라이센싱에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*에서 FireSIGHT System 라이센싱 장을 참조하십시오.

레거시 RNA 호스트 및 RUA 사용자 라이센스 사용

FireSIGHT System 버전 4.10.x에서는 RNA 호스트 및 RUA 사용자 기능 라이센스에 따라 각각 모니터링되는 호스트와 사용자 한도가 결정됩니다. 방어 센터에서 이전에 버전 4.10.x를 실행 중이었다면 FireSIGHT 라이센스 대신 레거시 호스트 및 사용자 라이센스를 사용할 수 있습니다.

레거시 라이센스를 사용하는 버전 5.4.1 방어 센터에서는 FireSIGHT 호스트 한도로 RNA 호스트 한도를 사용하고 FireSIGHT 사용자 및 액세스 제어 사용자 한도로 RUA 사용자 한도를 사용합니다. FireSIGHT 호스트 라이센스 한도 상태 모듈은 라이센스 한도에 대해 적절한 경고를 표시합니다.

RNA 호스트와 RUA 사용자 한도는 누적됩니다. 즉, 각 유형의 복수 라이센스를 방어 센터에 추가하여 라이센스에서 허용하는 호스트 또는 사용자의 총 수를 모니터링할 수 있습니다.

나중에 FireSIGHT 라이센스를 추가하면 방어 센터에서 더 높은 한도를 사용합니다. 예를 들어, DC1500의 FireSIGHT 라이센스는 최대 50,000개의 호스트와 사용자를 지원합니다. 버전 4.10.x DC1500의 RNA 호스트 한도가 50,000보다 클 경우 버전 5.4.1을 실행하는 동일한 방어 센터에서 레거시 호스트 라이센스를 사용하면 한도가 더 높아집니다. 웹 인터페이스는 사용자 편의를 위해 더 높은 한도를 나타내는 라이센스만 표시합니다.

참고 FireSIGHT 라이센스 한도는 방어 센터의 하드웨어 용량과 일치하므로 Cisco에서는 레거시 라이센싱을 사용할 경우 해당 한도를 초과하지 **않도록** 권장합니다. 안내를 받으려면 고객 지원에 문의하십시오.

버전 4.10.x에서 버전 5.4.1로의 업데이트 경로가 없으므로 ISO 이미지를 사용하여 방어 센터를 "복원"해야 합니다. 이미지로 다시 설치할 경우 어플라이언스의 **모든** 컨피그레이션과 이벤트 데이터가 손실됩니다. 이미지로 다시 설치한 후에는 이 데이터를 어플라이언스로 가져올 수 **없습니다**. 자세한 내용은 FireSIGHT System 어플라이언스를 출고 시 기본 설정으로 복원, 페이지 8-1을(를) 참조하십시오.

참고 유지 보수 기간 중에만 어플라이언스를 이미지로 다시 설치하십시오. 이미지로 다시 설치하는 경우 인라인 구축의 디바이스가 바이패스하지 않는 컨피그레이션으로 재설정되고 바이패스 모드를 다시 구성할 때까지 네트워크 트래픽이 중단됩니다. 자세한 내용은 복원 프로세스 중 트래픽 흐름, 페이지 8-2을(를) 참고하십시오.

복원 과정에서 라이센스와 네트워크 설정을 삭제하라는 메시지가 표시됩니다. 실수로 삭제하는 경우 나중에 다시 추가할 수는 있지만 이러한 설정을 보관하십시오. 버전 5.4.1 방어 센터에서 버전 4.10.x 디바이스를 관리할 수 없습니다. 하지만 버전 4.10.x 디바이스를 최신 버전으로 복원 및 업데이트할 수 있습니다. 자세한 내용은 FireSIGHT System 어플라이언스를 출고 시 기본 설정으로 복원, 페이지 8-1을(를) 참고하십시오.

보안, 인터넷 액세스 및 통신 포트

방어 센터를 보호하려면 보호된 내부 네트워크에 설치해야 합니다. 방어 센터에서 필수 서비스와 사용 가능한 포트만 사용하도록 구성한 경우에도 방화벽 밖의 공격이 방어 센터(또는 관리되는 디바이스)에 도달할 수 없도록 해야 합니다.

방어 센터 및 관리되는 디바이스가 동일한 네트워크에 상주하는 경우 디바이스의 관리 인터페이스를 방어 센터와 동일한 보호된 내부 네트워크에 연결할 수 있습니다. 이렇게 하면 방어 센터에서 디바이스를 안전하게 제어할 수 있습니다. 또한 방어 센터에서 다른 네트워크에 있는 디바이스의 트래픽을 관리 및 격리할 수도 있도록 복수 관리 인터페이스를 구성할 수도 있습니다.

어플라이언스를 구축하는 방식과 상관없이 어플라이언스 간 통신은 암호화됩니다. 하지만 DDoS(Distributed Denial of Service) 또는 중간자(man-in-the-middle) 등의 공격으로 어플라이언스 간 통신이 중단, 차단, 변경되지 않도록 조치를 취해야 합니다.

또한 FireSIGHT System의 특정 기능에는 인터넷 연결이 필요합니다. 기본적으로 모든 어플라이언스는 인터넷에 직접 연결할 수 있도록 구성됩니다. 또한 특정 포트는 보안 어플라이언스 액세스를 제공하고 특정 시스템 기능이 올바르게 작동하는 데 필요한 로컬 또는 인터넷 리소스에 액세스할 수 있도록 개방하여 기본적인 어플라이언스 간 통신을 제공해야 합니다.

정보 Cisco NGIPS for Blue Coat X-Series 및 Cisco ASA with FirePOWER Services를 제외하고 FireSIGHT System 어플라이언스에서는 프록시 서버 사용을 지원합니다. 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

[개선 사항: 특정 FireAMP 프록시 방화벽 규칙을 포함합니다. 포트를 설정/해제하는 방법을 포함하시겠습니까? 보안과 어플라이언스에 대한 직접 인터넷 액세스 허용의 균형을 조정하기 위한 몇 가지 근거를 포함하시겠습니까?]

자세한 내용은 다음 링크를 참고하십시오.

- 인터넷 액세스 요구 사항, 페이지 1-17
- 통신 포트 요구 사항, 페이지 1-19

인터넷 액세스 요구 사항

FireSIGHT System 어플라이언스는 기본적으로 개방되는 포트 443/tcp(HTTPS) 및 80/tcp(HTTP)에서 인터넷에 직접 연결하도록 구성되었습니다. 통신 포트 요구 사항, 페이지 1-19을(를) 참조하십시오. 대부분의 FireSIGHT System 어플라이언스는 프록시 서버 사용을 지원합니다. *FireSIGHT System 사용 설명서*에서 네트워크 설정 구성 장을 참조하십시오. 프록시 서버는 whois 액세스에 사용할 수 없습니다.

운영 연속성을 보장하려면 고가용성 쌍의 두 방어 센터에 인터넷 액세스가 있어야 합니다. 특정 기능의 경우 기본 방어 센터에서 인터넷에 접속한 다음 동기화 프로세스 중에 보조 방어 센터와 정보를 공유합니다. 따라서 기본 방어 센터에 장애가 발생하면 *FireSIGHT System 사용 설명서*의 디바이스 관리 장에 설명된 대로 보조 방어 센터를 활성으로 승격해야 합니다.

다음 표에는 FireSIGHT System의 특정 기능에 대한 인터넷 액세스 요구 사항이 설명되어 있습니다.

표 1-8 FireSIGHT System 기능의 ?인터넷 액세스 요구 사항

기능	인터넷 액세스가 필요한 이유	어플라이언스	고가용성 고려 사항
동적 분석: 쿼리	이전에 동적 분석을 위해 제출한 파일의 위협 점수를 Collective Security Intelligence 클라우드에 쿼리	방어 센터	쌍으로 연결된 방어 센터에서는 위협 점수를 독립적으로 클라우드에 쿼리합니다.
동적 분석: 제출	동적 분석을 위해 Collective Security Intelligence 클라우드에 파일 제출	관리되는 장치	해당 없음
FireAMP 통합	Collective Security Intelligence 클라우드 클라우드에서 엔드포인트 기반 (FireAMP) 악성코드 이벤트 수신	방어 센터	클라우드 연결은 동기화되지 않습니다. 두 방어 센터 모두에 구성하십시오.
침입 규칙, VDB, GeoDB 업데이트	침입 규칙, GeoDB 또는 VDB 업데이트를 어플라이언스에 직접 다운로드하거나 다운로드 일정 예약	방어 센터	침입 규칙, GeoDB 및 VDB 업데이트가 동기화됩니다.
네트워크 기반 AMP	악성코드 클라우드 조회 수행	방어 센터	쌍으로 연결된 방어 센터에서 클라우드 조회를 독립적으로 수행합니다.
RSS 피드 대시보드 위젯	Cisco를 포함한 외부 소스에서 RSS 피드 데이터 다운로드	가상 디바이스, X-Series, ASA FirePOWER를 제외한 모든 디바이스	피드 데이터는 동기화되지 않습니다.
보안 인텔리전스 필터링	FireSIGHT System 인텔리전트 피드를 포함한 외부 소스에서 보안 인텔리전스 피드 데이터 다운로드	방어 센터	기본 방어 센터에서 피드 데이터를 다운로드한 후 보조 방어 센터와 공유합니다. 기본 방어 센터에 장애가 발생할 경우 보조 방어 센터를 활성으로 승격합니다.
시스템 소프트웨어 업데이트	시스템 업데이트를 어플라이언스에 직접 다운로드하거나 다운로드 예약	가상 디바이스, X-Series, ASA FirePOWER를 제외한 모든 디바이스	시스템 업데이트는 동기화되지 않습니다.
URL 필터링	액세스 제어를 위해 클라우드 기반 URL 범주 및 평판 데이터 다운로드, 분류되지 않은 URL에 대한 조회 수행	방어 센터	기본 방어 센터에서 URL 필터링 데이터를 다운로드한 후 보조 방어 센터와 공유합니다. 기본 방어 센터에 장애가 발생할 경우 보조 방어 센터를 활성으로 승격합니다.
whois	외부 호스트의 whois 정보 요청	가상 디바이스, X-Series, ASA FirePOWER를 제외한 모든 디바이스	whois 정보를 요청하는 어플라이언스는 인터넷에 액세스할 수 있어야 합니다.

통신 포트 요구 사항

FireSIGHT System 어플라이언스는 기본적으로 포트 8305/tcp를 사용하는 양방향 SSL-암호화 통신 채널을 사용하여 통신합니다. 이 포트는 기본적인 어플라이언스 간 통신을 위해 **반드시** 열려 있어야 합니다. 열린 다른 포트를 통해 다음과 같은 작업을 수행할 수 있습니다.

- 어플라이언스의 웹 인터페이스에 액세스
- 어플라이언스에 안전하게 원격 연결
- 시스템의 특정 기능이 올바르게 작동하는 데 필요한 로컬 또는 인터넷 리소스에 액세스

일반적으로 기능과 관련된 포트는 관련 기능을 활성화하거나 구성할 때까지 닫힌 상태를 유지해야 합니다. 예를 들어, 방어 센터를 사용자 에이전트에 연결할 때까지 에이전트 통신 포트(3306/tcp)는 닫혀 있습니다. 또 다른 예로, LOM을 활성화할 때까지 Series 3에서 623/udp 포트가 닫혀 있습니다.

주의 열려 있는 포트를 닫을 경우 구축에 어떤 영향을 미칠지 이해하기 전까지 열려 있는 포트를 **닫지 마십시오**.

예를 들어, 관리되는 디바이스에서 아웃바운드로 25/tcp(SMTP) 포트를 닫으면 디바이스가 개별 침입 이벤트에 대한 이메일 알림을 전송하지 못하도록 차단됩니다(*FireSIGHT System 사용 설명서* 참조). 다른 예를 들어, 포트 443/tcp(HTTPS)를 닫아 물리적 관리되는 디바이스의 웹 인터페이스에 대한 액세스를 비활성화할 수 있지만, 그럴 경우 디바이스가 의심되는 악성코드 파일을 동적 분석을 위해 클라우드로 제출하지 못하게 됩니다.

사용자는 시스템에서 일부 통신 포트를 변경할 수 있습니다.

- 시스템과 인증 서버 간 연결을 구성할 때 LDAP 및 RADIUS 인증에 대해 사용자 정의 포트를 지정할 수 있습니다. *FireSIGHT System 사용 설명서*를 참조하십시오.
- 관리 포트(8305/tcp)를 변경할 수 있습니다. *FireSIGHT System 사용 설명서*를 참조할 수 있습니다. 그러나 기본 설정을 유지하는 것이 **좋습니다**. 관리 포트를 변경할 경우, 구축 과정에서 서로 통신해야 하는 모든 어플라이언스의 설정을 변경해야 합니다.
- 포트 32137/tcp를 사용하면 업그레이드된 방어 센터에서 Collective Security Intelligence 클라우드 클라우드와 통신할 수 있습니다. 그러나 Cisco에서는 버전 5.4.1 이상의 신규 설치에 대한 기본 설정인 포트 443으로 전환하도록 권장합니다. 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

다음 표에는 FireSIGHT System 기능을 충분히 활용할 수 있는 각 어플라이언스 유형에 필요한 열린 포트가 나와 있습니다.

표 1-9 FireSIGHT System 기능 및 작동을 위한 기본 통신 포트

포트	설명	방향	열리는 디바이스	수행하는 작업
22/tcp	SSH/SSL	양방향	모든	어플라이언스에 대한 안전한 원격 연결 허용
25/tcp	SMTP	아웃바운드	모든	어플라이언스에서 이메일 알림 및 경고 전송
53/tcp	DNS	아웃바운드	모든	DNS 사용
67/udp 68/udp	DHCP	아웃바운드	X-Series를 제외한 모든 디바이스	DHCP 사용 **참고** 이러한 포트는 기본적으로 **닫혀** 있습니다.

표 1-9 FireSIGHT System 기능 및 작동을 위한 기본 통신 포트(계속)

포트	설명	방향	열리는 디바이스	수행하는 작업
80/tcp	HTTP	아웃바운드	가상 디바이스, X-Series, ASA FirePOWER를 제외한 모든 디바이스	RSS 피드 대시보드 위젯에서 원격 웹 서버에 연결
		양방향	방어 센터	HTTP를 통해 맞춤형 및 서드파티 보안 인텔리전스 피드 업데이트 URL 범주 및 평판 데이터 다운로드(포트 443도 필요)
161/udp	SNMP	양방향	가상 디바이스, X-Series, ASA FirePOWER를 제외한 모든 디바이스	SNMP 폴링을 통해 어플라이언스의 MIB에 대한 액세스 허용
162/udp	SNMP	아웃바운드	모든	SNMP 경고를 원격 트랩 서버로 전송
389/tcp 636/tcp	LDAP	아웃바운드	가상 디바이스 및 X-Series를 제외한 모든 디바이스	외부 인증을 위해 LDAP 서버와 통신
389/tcp 636/tcp	LDAP	아웃바운드	방어 센터	탐지된 LDAP 사용자의 메타데이터 가져오기
443/tcp	HTTPS	인바운드	가상 디바이스, X-Series, ASA FirePOWER를 제외한 모든 디바이스	어플라이언스의 웹 인터페이스에 액세스
443/tcp	HTTPS AMQP 클라우드 통신	양방향	방어 센터	보기: • 소프트웨어, 침입 규칙, VDB, GeoDB 업데이트 • URL 범주 및 평판 데이터(포트 80도 필요) • Cisco 인텔리전스 피드 및 기타 안전한 보안 인텔리전스 피드 • 엔드포인트 기반(FireAMP) 악성코드 이벤트 • 네트워크 트래픽에서 탐지된 파일의 악성코드 처리 • 전송된 파일에 대한 동적 분석 정보
			Series 2 및 Series 3 디바이스	디바이스의 로컬 웹 인터페이스를 사용하여 소프트웨어 업데이트 다운로드
			Series 3, 가상 디바이스, X-Series, ASA FirePOWER	동적 분석을 위해 Cisco 클라우드에 파일 제출
514/udp	syslog	아웃바운드	모든	원격 syslog 서버에 경고 전송
623/udp	SOL/LOM	양방향	Series 3	SOL(Serial Over LAN) 연결을 사용하여 Lights-Out 관리를 수행하도록 허용

표 1-9 FireSIGHT System 기능 및 작동을 위한 기본 통신 포트(계속)

포트	설명	방향	열리는 디바이스	수행하는 작업
1500/tcp 2000/tcp	데이터베이스 액세스	인바운드	방어 센터 및 마스터 방어 센터	서드파티 클라이언트의 데이터베이스에 대한 읽기 전용 액세스 허용
1812/udp 1813/udp	RADIUS	양방향	가상 디바이스, X-Series, ASA FirePOWER를 제외한 모든 디바이스	외부 인증 및 계정 관리를 위해 RADIUS 서버와 통신
3306/tcp	사용자 에이전트	인바운드	방어 센터	사용자 에이전트와 통신
8302/tcp	eStreamer	양방향	가상 디바이스 및 X-Series를 제외한 모든 디바이스	eStreamer 클라이언트와 통신
8305/tcp	어플라이언스 통신	양방향	모든	구축 과정에서 어플라이언스 간에 안전하게 통신. **필수입니다.**
8307/tcp	호스트 입력 클라이언트	양방향	방어 센터	호스트 입력 클라이언트와 통신
32137/tcp	클라우드 통신	양방향	방어 센터	업그레이드된 방어 센터와 Cisco 클라우드의 통신 허용

어플라이언스 사전 구성

나중에 다른 사이트에서 구축할 수 있도록 중앙 위치에서 여러 디바이스와 방어 센터를 사전 구성할 수 있습니다. 어플라이언스를 사전 구성할 경우 고려 사항은 FireSIGHT System 어플라이언스 사전 구성, 페이지 E-1을(를) 참조하십시오.

관리 네트워크에서 구축

FireSIGHT System은 각각의 고유한 네트워크 아키텍처의 요구 사항에 맞게 구축할 수 있습니다. 방어 센터에서는 FireSIGHT System을 위한 중앙 집중식 관리 콘솔 및 데이터베이스 저장소를 제공합니다. 디바이스는 분석용 트래픽 연결을 수집하기 위해 네트워크 세그먼트에 설치됩니다.

방어 센터에서는 관리 인터페이스를 사용하여 *신뢰하는 관리 네트워크*(즉, 외부 트래픽에 노출되지 않는 안전한 내부 네트워크)에 연결합니다. 디바이스는 관리 인터페이스를 사용하여 방어 센터에 연결합니다.

그런 다음 디바이스가 트래픽을 모니터링하기 위해 센싱 인터페이스를 사용하여 외부 네트워크에 연결됩니다. 구축 과정에서 센싱 인터페이스를 사용하는 방법에 대한 자세한 내용은 관리되는 디바이스 구축, 페이지 3-1을(를) 참조하십시오.

참고 ASA FirePOWER 디바이스의 구축 시나리오에 대한 자세한 내용은 ASA 설명서를 참조하십시오.

인터페이스 옵션에 대한 자세한 내용은 다음 섹션을 참조하십시오.

관리 구축 고려 사항

관리 구축 의사 결정은 다양한 요인을 기반으로 합니다. 다음 질문에 대한 답변을 알고 있을 경우 가장 효율적이고 효과적인 시스템을 구성하기 위한 구축 옵션을 파악하는 데 도움이 될 수 있습니다.

- 기본 단일 관리 인터페이스를 사용하여 디바이스를 방어 센터에 연결할 것입니까? 성능을 향상하거나 서로 다른 네트워크에 있는 방어 센터에서 수신된 트래픽을 격리하기 위해 추가 관리 인터페이스를 활성화할 것입니까? 자세한 내용은 관리 인터페이스 이해, 페이지 2-2을(를) 참조하십시오.
- 트래픽 채널을 활성화하여 방어 센터와 관리되는 디바이스 간의 연결을 생성하는 방법을 통해 성능을 향상하고자 합니까? 복수 관리 인터페이스를 사용하여 방어 센터와 관리되는 디바이스 간의 처리 용량을 더욱 늘리고자 합니까? 자세한 내용은 트래픽 채널로 구축, 페이지 2-3을(를) 참조하십시오.
- 하나의 방어 센터를 사용하여 다른 네트워크에 있는 디바이스의 트래픽을 관리 및 격리하고자 합니까? 자세한 내용은 네트워크 경로로 구축, 페이지 2-5을(를) 참조하십시오.

- 보호된 환경에서 관리 인터페이스를 구축하고 있습니까? 어플라이언스 액세스가 특정 워크스테이션 IP 주소로 제한되어 있습니까? 보안 문제, 페이지 2-5에서는 관리 인터페이스를 안전하게 구축하기 위한 몇 가지 고려 사항에 대해 설명합니다.
- 8000 Series 디바이스를 구축 중입니까? 자세한 내용은 특별 고려 사항: 8000 Series 디바이스 연결, 페이지 2-6을(를) 참조하십시오.

관리 인터페이스 이해

관리 인터페이스에서는 방어 센터 및 여기서 관리하는 모든 디바이스 간의 통신 수단을 제공합니다. 어플라이언스 간 트래픽 제어를 올바르게 유지하는 것은 성공적인 구축을 위한 필수 조건입니다.

Series 3 어플라이언스 및 가상 방어 센터의 경우 방어 센터, 디바이스 또는 둘 모두에서 관리 인터페이스를 활성화하여 어플라이언스 간 트래픽을 별도의 두 트래픽 채널로 분류할 수 있습니다. *관리 트래픽 채널*은 모든 내부 트래픽(즉, 어플라이언스 및 시스템의 관리에 한정된 디바이스 간 트래픽)을 전달하고, *이벤트 트래픽 채널*은 모든 이벤트 트래픽(즉, 침입 및 악성코드 이벤트와 같은 높은 볼륨의 이벤트 트래픽)을 전달합니다. 트래픽을 두 개의 채널로 분리하면 어플라이언스 간 연결 지점이 두 개가 생성되므로 처리량이 증가하여 성능이 향상됩니다. 또한 *복수 관리 인터페이스*를 활성화하여 어플라이언스 간에 더욱 방대한 처리량을 제공하거나, 서로 다른 네트워크에 있는 디바이스 간 트래픽을 관리 및 격리할 수 있습니다.

방어 센터에 디바이스를 등록한 후에는 각 어플라이언스의 웹 브라우저를 사용하여 기본 컨피그레이션을 변경함으로써 트래픽 채널 및 복수 관리 인터페이스를 활성화할 수 있습니다. 컨피그레이션 정보에 대한 내용은 *FireSIGHT System 사용 설명서*의 어플라이언스 설정 구성을 참조하십시오.

관리 인터페이스는 종종 어플라이언스의 뒷면에 있습니다. 자세한 내용은 관리 인터페이스 식별, 페이지 4-2을(를) 참조하십시오. 관리 인터페이스에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- 단일 관리 인터페이스, 페이지 2-2
- 복수 관리 인터페이스, 페이지 2-3

단일 관리 인터페이스

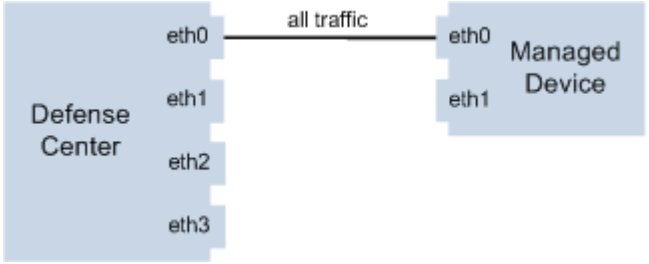
라이센스: 모두

지원되는 방어 센터: 모두

지원되는 디바이스: 모두

바이스를 방어 센터에 등록하면 방어 센터의 관리 인터페이스와 디바이스의 관리 인터페이스 간에 모든 트래픽을 전달하는 단일 통신 채널이 설정됩니다.

다음 그래픽에는 기본 단일 통신 채널이 나와 있습니다. 단일 인터페이스는 관리 및 이벤트 트래픽을 모두 포함하는 단일 통신 채널을 전달합니다.



복수 관리 인터페이스

라이센스: 모두

지원되는 방어 센터: Series 3, 가상

지원되는 디바이스: Series 3

각각의 IPv4 또는 IPv6 주소 및 호스트 이름(선택 사항)이 있는 복수 관리 인터페이스를 활성화하고 구성하면 각 트래픽 채널을 서로 다른 관리 인터페이스로 전송하여 더 많은 트래픽 처리량을 제공할 수 있습니다. 가벼운 관리 트래픽을 전달하려면 소형 인터페이스를 구성하고, 무거운 이벤트 트래픽 로드를 전달하려면 대형 인터페이스를 구성합니다. 디바이스를 등록하여 관리 인터페이스를 분리하고 동일한 인터페이스에 대해 두 트래픽 채널을 모두 구성하거나, 전용 관리 인터페이스를 사용하여 방어 센터에서 관리하는 모든 디바이스의 이벤트 트래픽 채널을 전달할 수 있습니다.

또한 방어 센터의 특정 관리 인터페이스에서 다른 네트워크로 경로를 만들 수 있으므로 방어 센터를 통해 한 네트워크에 있는 디바이스 트래픽을 다른 네트워크에 있는 디바이스 트래픽과 격리하여 별도로 관리할 수 있습니다.

다음을 제외하고, 추가 관리 인터페이스에는 기본 관리 인터페이스와 동일한 기능(예: 방어 센터 간 고가용성 이용)이 포함되어 있습니다.

- 기본(`eth0`) 관리 인터페이스에서만 DHCP를 구성할 수 있습니다. 추가(`eth1` 등) 인터페이스에는 고유한 고정 IP 주소 및 호스트 이름이 필요합니다. Cisco에서는 추가 관리 인터페이스에 대한 DNS 항목을 설정하지 말고,대신 이러한 인터페이스 전용으로 IP 주소별 방어 센터 및 디바이스를 등록하도록 권장합니다.
- 기본이 아닌 관리 인터페이스를 사용하여 방어 센터 및 관리되는 디바이스를 연결할 경우, 해당 어플라이언스가 NAT 디바이스로 분리되어 있으면 두 트래픽 채널을 모두 구성하여 동일한 관리 인터페이스를 사용해야 합니다.
- 기본 관리 인터페이스에서만 LOM(Lights-Out Management)을 사용할 수 있습니다.
- 70xx 제품군에서는 트래픽을 두 개의 채널로 구분하고 해당 채널이 트래픽을 방어 센터에 있는 한 개 이상의 관리 인터페이스로 전송하도록 구성할 수 있습니다. 그러나 70xx 제품군에는 단일 관리 인터페이스만 포함되어 있으므로 디바이스에서는 단일 관리 인터페이스의 방어 센터에서 전송된 트래픽만 수신합니다.

구축 옵션

하나 이상의 관리 인터페이스를 사용하여 시스템의 성능을 향상하려면 트래픽 채널을 사용하여 트래픽 플로우를 관리할 수 있습니다. 또한 방어 센터 및 관리되는 디바이스에서 특정 관리 인터페이스를 사용하는 서로 다른 네트워크에 경로를 생성하면 다른 네트워크에 있는 디바이스 간에 트래픽을 격리할 수 있습니다. 자세한 내용은 다음 섹션을 참조하십시오.

트래픽 채널로 구축

라이센스: 모두

지원되는 방어 센터: Series 3, 가상

지원되는 디바이스: Series 3

단일 관리 인터페이스에서 트래픽 채널을 2개 사용할 경우 방어 센터와 관리되는 디바이스 간에 연결을 생성할 수 있습니다. 한 채널은 관리 트래픽을 전달하며, 또 다른 채널은 동일한 인터페이스에서 별도로 이벤트 트래픽을 전달합니다.

다음 예에는 동일한 인터페이스에서 별도의 트래픽 채널 2개를 사용하는 통신 채널이 나와 있습니다.

복수 관리 인터페이스를 사용할 경우, 2개의 관리 인터페이스를 통해 트래픽 채널을 분할하여 성능을 향상할 수 있으며 이 경우 결과적으로 두 인터페이스 모두의 용량이 추가되므로 트래픽 플로우가 증대됩니다. 한 인터페이스는 관리 트래픽 채널을 전달하고 다른 하나는 이벤트 트래픽 채널을 전달합니다. 두 인터페이스 중 하나에 오류가 발생하면, 모든 트래픽이 활성 인터페이스로 다시 라우팅되며 연결이 유지됩니다.

다음 그래픽에는 2개의 관리 인터페이스에서 사용되는 관리 트래픽 채널 및 이벤트 트래픽 채널이 나와 있습니다.

전용 관리 인터페이스를 사용하여 여러 개의 디바이스에서 이벤트 트래픽만 전달할 수 있습니다. 이 컨피그레이션에서 각 디바이스는 관리 트래픽 채널을 전달하기 위해 다른 관리 인터페이스에 등록되어 있으며, 방어 센터의 한 관리 인터페이스는 모든 디바이스의 모든 이벤트 트래픽 채널을 전달합니다. 인터페이스에 오류가 발생하면 트래픽은 활성 인터페이스로 다시 라우팅되며 연결이 유지됩니다. 모든 디바이스의 이벤트 트래픽이 동일한 인터페이스에서 전달되므로, 네트워크 간에 트래픽이 격리되지 않습니다.

다음 표에는 이벤트 트래픽 채널에 대해 동일한 전용 인터페이스를 공유하는 서로 다른 관리 채널 트래픽 인터페이스를 사용하는 두 개의 디바이스가 나와 있습니다.

네트워크 경로로 구축

라이센스: 모두

지원되는 방어 센터: Series 3, 가상

지원되는 디바이스: Series 3

방어 센터의 특정 관리 인터페이스에서 다른 네트워크에 대한 경로를 생성할 수 있습니다. 해당 네트워크의 디바이스를 방어 센터에서 지정된 관리 인터페이스에 등록하면 서로 다른 네트워크에 있는 방어 센터와 디바이스 간에 격리된 연결을 제공하게 됩니다. 동일한 관리 인터페이스를 사용하여 두 트래픽 채널을 모두 구성하면 해당 디바이스의 해당 트래픽이 다른 네트워크의 디바이스 트래픽과 격리된 상태를 유지하도록 할 수 있습니다. 라우팅된 인터페이스가 방어 센터의 다른 모든 인터페이스와 격리되므로, 라우팅된 관리 인터페이스에 오류가 발생할 경우 연결이 손실됩니다.

정보 기본(`eth0`) 관리 인터페이스 이외의 모든 관리 인터페이스의 고정 IP 주소에 디바이스를 등록해야 합니다. DHCP는 기본 관리 인터페이스에서만 지원됩니다.

방어 센터를 설치한 후 웹 인터페이스를 사용하여 복수 관리 인터페이스를 구성합니다. 자세한 내용은 *FireSIGHT System 사용 설명서*의 어플라이언스 설정 구성을 참조하십시오.

다음 그래픽에는 모든 트래픽에 별도의 관리 인터페이스를 사용하여 네트워크 트래픽을 격리하는 두 개의 디바이스가 나와 있습니다. 관리 인터페이스를 추가하여 각 디바이스에 별도의 관리 및 이벤트 트래픽 채널 인터페이스를 구성할 수 있습니다.

보안 문제

안전한 환경에서 관리 인터페이스를 구축하기 위해 Cisco에서 권장하는 사항은 다음과 같습니다.

- 관리 인터페이스를 항상 무단 액세스로부터 보호되는 신뢰하는 내부 관리 네트워크에 연결하십시오.
- 어플라이언스에 대한 액세스를 허용할 수 있는 특정 워크스테이션 IP 주소를 식별하십시오. 어플라이언스 시스템 정책 내의 액세스 목록을 이용하여 특정 호스트만 어플라이언스에 액세스할 수 있도록 제한하십시오. 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

특별 고려 사항: 8000 Series 디바이스 연결

라이센스: 모두

지원되는 디바이스: 8000 Series

8000 Series 관리되는 디바이스를 방어 센터에 등록할 경우, 안정적인 네트워크 링크를 보장하려면 연결 양측에서 자동 협상을 사용하거나 양측을 동일한 고정 속도로 설정해야 합니다. 8000 Series 관리되는 디바이스는 반이중 네트워크 링크를 지원하지 않으며 속도 차이 또는 연결 반대쪽의 이중 컨피그레이션도 지원하지 않습니다.

3장 관리되는 디바이스 구축

디바이스를 방어 센터에 등록한 후 침입 탐지 시스템을 사용하여 트래픽을 모니터링하거나 침입 방지 시스템을 사용하여 네트워크를 위협으로부터 보호할 수 있도록 네트워크 세그먼트에 관리되는 디바이스의 센싱 인터페이스를 구축합니다.

센싱 구축에 대한 자세한 내용은 다음 섹션을 참조하십시오.

참고 ASA FirePOWER 디바이스의 구축 시나리오에 대한 자세한 내용은 ASA 설명서를 참조하십시오.

구축에 대한 자세한 내용은 Cisco 영업부에서 제공하는 *모범 사례 가이드*를 참조하십시오.

센싱 구축 고려 사항

센싱 구축 의사 결정은 다양한 요인을 기반으로 합니다. 다음 질문에 답변하여 네트워크의 취약한 영역을 이해하고 침입 탐지 및 방지 요구 사항을 명확히 확인할 수 있습니다.

- 관리되는 디바이스를 수동 인터페이스 또는 인라인 인터페이스 중 어떤 인터페이스로 구축하시겠습니까? 디바이스가 일부는 수동이고 일부는 인라인인 혼합 인터페이스를 지원합니까? 자세한 내용은 센싱 인터페이스 이해, 페이지 3-2을(를) 참조하십시오.
- 관리되는 디바이스를 네트워크에 어떤 방식으로 연결하시겠습니까? 허브? 탭? 스위치의 스패닝 포트? 가상 스위치? 자세한 내용은 네트워크에 디바이스 연결, 페이지 3-5을(를) 참조하십시오.
- 네트워크에서 모든 공격을 감지하시겠습니까, 아니면 방화벽을 침투하는 공격만 확인하시겠습니까? 네트워크에 재무, 회계, 개인 기록, 운영 코드 또는 특별 보안 정책이 필요한 기타 보호되는 민감한 정보와 같은 특정 자산이 있습니까? 자세한 내용은 구축 옵션, 페이지 3-8을(를) 참조하십시오.

- 관리되는 디바이스에서 복수의 센싱 인터페이스를 사용하여 네트워크 탭에서 개별 연결을 재결합하거나 다른 네트워크의 트래픽을 캡처 및 평가하시겠습니까? 복수의 센싱 인터페이스를 사용하여 가상 라우터 또는 가상 스위치로 실행하시겠습니까? 자세한 내용은 관리되는 디바이스에서 멀티 센싱 인터페이스 사용, 페이지 3-17을(를) 참조하십시오.
- 원격 근무자를 위한 VPN 또는 모뎀 접속을 제공합니까? 침입 방지 구축이 필요한 원격사무실이 있습니까? 외주업체 또는 다른 임시 직원을 고용하고 있습니까? 이러한 직원이 특정 네트워크 세그먼트만 사용해야 합니까? 회사의 네트워크가 고객, 공급업체 또는 비즈니스 파트너와 같은 다른 조직의 네트워크와 통합되어 있습니까? 자세한 내용은 복잡한 네트워크 구축, 페이지 3-19을(를) 참조하십시오.

센싱 인터페이스 이해

다음 섹션에서는 여러 센싱 인터페이스가 FireSIGHT System의 기능에 미치는 영향에 대해 설명합니다. 수동 및 인라인 인터페이스 이외에, 라우팅, 스위치 및 하이브리드 인터페이스를 구축할 수 있습니다.

센싱 인터페이스는 디바이스의 전면에 있습니다. 센싱 인터페이스를 식별하려면 센싱 인터페이스 식별, 페이지 4-5을(를) 참조하십시오. 센싱 인터페이스에 대한 자세한 내용은 다음 섹션을 참조하십시오.

수동 인터페이스

라이센스: 모두

지원되는 디바이스: 모두

스위치 SPAN, 가상 스위치 또는 미러 포트를 사용하여 네트워크를 이동하는 트래픽을 모니터링하고 스위치에 있는 다른 포트의 트래픽을 복사하도록 수동 구축을 구성할 수 있습니다. 수동 인터페이스를 사용하면 네트워크 트래픽 흐름에 있지 않아도 네트워크 내의 트래픽을 검사할 수 있습니다. 수동 구축으로 구성된 시스템에서는 트래픽 차단 또는 형성과 같은 특정 작업을 할 수 없습니다. 수동 인터페이스에서는 모든 트래픽을 조건 없이 수신하고 수신된 트래픽을 다시 전송하지 않습니다.

관리되는 디바이스에서 하나 이상의 물리적 포트를 수동 인터페이스로 구성할 수 있습니다. 자세한 내용은 네트워크에 디바이스 연결, 페이지 3-5을(를) 참고하십시오. ASA FirePOWER 디바이스를 수동 모드로 구성하는 데 대한 자세한 내용은 ASA 설명서를 참조하십시오.

인라인 인터페이스

라이센스: 모두

지원되는 디바이스: 모두

두 개의 포트를 결합하여 네트워크 세그먼트에서 투명하게 인라인 구축을 구성할 수 있습니다. 인라인 인터페이스를 사용하면 인접 네트워크 디바이스를 구성하지 않고도 모든 네트워크 컨피그레이션에서 디바이스를 설치할 수 있습니다. 인라인 인터페이스에서는 모든 트래픽을 조건 없이 수신한 다음 명시적으로 삭제된 트래픽을 제외한 모든 트래픽을 다시 전송합니다.

관리되는 디바이스에서 하나 이상의 물리적 포트를 인라인 인터페이스로 구성할 수 있습니다. 인라인 세트에 할당된 인라인 인터페이스 쌍에서만 인라인 구축의 트래픽을 처리할 수 있습니다.

참고 인터페이스를 인라인 인터페이스로 구성하는 경우 해당 NetMod의 인접 포트가 자동으로 인라인 인터페이스가 되어 쌍을 완성합니다.

구성 가능한 바이패스 인라인 세트를 사용하면 하드웨어에 전체 장애가 발생하는 경우(예: 디바이스 전원 유실) 트래픽이 처리되는 방법을 선택할 수 있습니다. 한 네트워크 세그먼트의 연결이 위험한지를 판별할 수 있으며, 이러한 경우 다른 네트워크 세그먼트에서 검사되지 않은 트래픽을 허용할 수 없습니다. 구성 가능한 바이패스 인라인 세트를 사용하여 다음 중 한 가지 방식으로 네트워크 트래픽의 트래픽 흐름을 관리할 수 있습니다.

- *바이패스*: 바이패스로 구성된 인터페이스 쌍을 사용하면 디바이스에 장애가 발생할 경우 모든 트래픽이 이동할 수 있습니다. 트래픽이 디바이스와 디바이스에서 수행하는 모든 검사 또는 기타 처리를 바이패스합니다. 바이패스를 이용하면 네트워크 세그먼트 전반에서 검사되지 않은 트래픽이 이동할 수 있지만 네트워크 연결성이 보장됩니다.
- *비 바이패스*: 비 바이패스로 구성된 인터페이스 쌍은 디바이스 장애가 발생할 경우 모든 트래픽을 중단합니다. 장애가 발생한 디바이스에 도달하는 트래픽이 디바이스에 진입하지 못합니다. 비 바이패스에서는 트래픽이 검사되지 않은 상태로 통과하도록 허용하지 않지만, 디바이스에 장애가 발생하는 경우 네트워크 세그먼트의 연결이 끊어집니다. 네트워크 보안이 트래픽 손실보다 더 중요한 구축 상황에서는 비 바이패스 인터페이스를 사용하십시오.

디바이스에 장애가 발생한 경우 트래픽이 계속 이동하도록 하려면 인라인 세트를 바이패스로 구성하십시오. 디바이스에 장애가 발생한 경우 트래픽을 중지하려면 인라인 세트를 비 바이패스로 구성하십시오. 이미지로 다시 설치할 경우 바이패스 모드의 어플라이언스가 비 바이패스 컨피그레이션으로 재설정되고 바이패스 모드를 다시 구성할 때까지 네트워크의 트래픽이 중단됩니다. 자세한 내용은 복원 프로세스 중 트래픽 흐름, 페이지 8-2을(를) 참고하십시오.

모든 어플라이언스에 구성 가능한 바이패스 인터페이스가 탑재될 수 있습니다. 또한 8000 Series 어플라이언스에는 바이패스로 구성할 수 없는 인터페이스가 포함된 NetMod도 탑재될 수 있습니다. NetMod에 대한 자세한 내용은 8000 Series 모듈, 페이지 7-50을(를) 참조하십시오.

고급 옵션은 어플라이언스별로 다르며 탭 모드, 전파 링크 상태, 투명한 인라인 모드 및 엄격한 TCP 모드를 포함할 수 있습니다. 인라인 인터페이스 세트를 구성하는 방법에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오. 인라인 인터페이스 사용에 대한 자세한 내용은 네트워크에 디바이스 연결, 페이지 3-5을(를) 참조하십시오.

FireSIGHT System을 사용하여 ASA FirePOWER 디바이스에 바이패스 인터페이스를 구성할 수 없습니다. ASA FirePOWER 디바이스를 인라인 모드로 구성하는 데 대한 자세한 내용은 ASA 설명서를 참조하십시오.

스위치 인터페이스

라이센스: 제어

지원되는 디바이스: Series 3

레이어 2 구축에서 관리되는 디바이스에 스위치 인터페이스를 구성하여 두 개 이상의 네트워크 사이에서 패킷 스위칭을 제공할 수 있습니다. 또한 관리되는 디바이스에서 가상 스위치가 독립 브로드캐스트 도메인으로 작동하도록 구성하여 네트워크를 논리적 세그먼트로 구분할 수 있습니다. 가상 스위치는 호스트의 MAC(Media Access Control) 주소를 사용하여 패킷을 보낼 대상을 결정합니다.

다음과 같이 스위치 인터페이스에 물리적 또는 논리적 컨피그레이션이 가능합니다.

- *물리적 스위치 인터페이스*는 스위칭이 구성된 물리적 인터페이스입니다. 태그가 지정되지 않은 VLAN 트래픽을 처리하려면 물리적 스위치 인터페이스를 사용합니다.
- *논리적 스위치 인터페이스*는 물리적 인터페이스와 VLAN 태그 사이의 연결입니다. 지정된 VLAN 태그가 있는 트래픽을 처리하려면 논리적 인터페이스를 사용합니다.

가상 스위치는 독립 브로드캐스트 도메인으로 작동하여 네트워크를 논리적 세그먼트로 구분할 수 있습니다. 가상 스위치는 호스트의 MAC(Media Access Control) 주소를 사용하여 패킷을 보낼 대상을 결정합니다. 가상 스위치를 구성할 경우 이 스위치는 처음에 스위치에서 사용 가능한 모든 포트를 통해 패킷을 브로드캐스트합니다. 시간이 경과함에 따라 이 스위치는 태그가 지정된 반환 트래픽을 사용하여 각 포트에 연결된 네트워크에 상주하는 호스트를 알아냅니다.

디바이스를 가상 스위치로 구성하고 나머지 인터페이스를 사용하여 모니터링하려는 네트워크 세그먼트에 연결할 수 있습니다. 디바이스에서 가상 스위치를 사용하려면 물리적 스위치 인터페이스를 생성한 다음 *FireSIGHT System 사용 설명서*의 가상 스위치 설정에 대한 지침을 따릅니다.

라우팅 인터페이스

라이센스: 제어

지원되는 디바이스: Series 3

레이어 3 구축에서 관리되는 디바이스에 라우팅 인터페이스를 구성하여 두 개 이상의 인터페이스 간에 트래픽을 라우팅하도록 할 수 있습니다. 트래픽을 라우팅하려면 각 인터페이스에 IP 주소를 할당하고 인터페이스를 가상 라우터에 할당해야 합니다.

라우팅 인터페이스를 게이트웨이 VPN(Virtual Private Network) 또는 NAT(Network Address Translation)에 사용하도록 구성할 수 있습니다. 자세한 내용은 게이트웨이 VPN 구축, 페이지 3-12 및 정책 기반 NAT로 구축, 페이지 3-13을(를) 참조하십시오.

또한 수신 주소에 따라 패킷 전달을 결정하여 패킷을 라우팅하도록 구성할 수 있습니다. 라우팅 인터페이스로 구성된 인터페이스는 레이어 3 트래픽을 수신 및 전달할 수 있습니다. 라우터는 전달 기준에 따라 발신 인터페이스에서 대상을 확인하며, 액세스 제어 규칙을 통해 적용될 보안 정책이 지정됩니다.

다음과 같이 라우팅 인터페이스에 물리적 또는 논리적 컨피그레이션이 가능합니다.

- *물리적 라우팅 인터페이스*는 라우팅이 구성된 물리적 인터페이스입니다. 태그가 지정되지 않은 VLAN 트래픽을 처리하려면 물리적 라우팅 인터페이스를 사용합니다.
- *논리적 스위치 인터페이스*는 물리적 인터페이스와 VLAN 태그 사이의 연결입니다. 지정된 VLAN 태그가 있는 트래픽을 처리하려면 논리적 인터페이스를 사용합니다.

레이어 3 구축에서 라우팅 인터페이스를 사용하려면 가상 라우터를 구성하고 여기에 라우팅된 인터페이스를 할당해야 합니다. 가상 라우터는 레이어 3 트래픽을 라우팅하는 라우팅 인터페이스의 그룹입니다.

디바이스를 가상 라우터로 구성하고 나머지 인터페이스를 사용하여 모니터링하려는 네트워크 세그먼트에 연결할 수 있습니다. 또한 엄격한 TCP를 적용하여 TCP 보안을 극대화할 수 있습니다. 디바이스에서 가상 스위치를 사용하려면 디바이스에 물리적 라우팅 인터페이스를 생성한 다음 *FireSIGHT System 사용 설명서*의 가상 라우터 설정에 대한 지침을 따릅니다.

하이브리드 인터페이스

라이센스: 제어

지원되는 디바이스: Series 3

관리되는 디바이스에 논리적 하이브리드 인터페이스를 구성하여 FireSIGHT System에서 가상 라우터와 가상 스위치 사이의 트래픽을 연결하도록 지정할 수 있습니다. 가상 스위치의 인터페이스에 수신된 IP 트래픽의 주소가 연결된 하이브리드 논리적 인터페이스의 MAC 주소로 지정된 경우, 레이어 3 트래픽으로 처리되고 대상 IP 주소에 따라 트래픽을 라우팅하거나 다른 방식으로 응답합니다. 시스템에서 다른 트래픽을 수신하면 레이어 2 트래픽으로 처리하고 적절히 스위칭합니다.

하이브리드 인터페이스를 생성하려면 우선 가상 스위치와 가상 라우터를 구성한 다음 가상 스위치와 가상 라우터를 하이브리드 인터페이스에 추가합니다. 가상 스위치 및 가상 라우터와 연결되지 않은 하이브리드 인터페이스는 라우팅에 사용할 수 없으며 트래픽을 생성하거나 트래픽에 응답하지 않습니다.

NAT(Network Address Translation)로 하이브리드 인터페이스를 구성하여 네트워크 간에 트래픽을 전달할 수 있습니다. 자세한 내용은 정책 기반 NAT로 구축, 페이지 3-13을(를) 참고하십시오.

디바이스에서 하이브리드 인터페이스를 사용하려면 디바이스에 하이브리드 인터페이스를 정의한 다음 *FireSIGHT System 사용 설명서*의 하이브리드 인터페이스 설정에 대한 지침을 따릅니다.

네트워크에 디바이스 연결

여러 가지 방법으로 관리되는 디바이스의 센싱 인터페이스를 네트워크에 연결할 수 있습니다. 수동 또는 인라인 인터페이스를 사용하여 허브 또는 네트워크 탭을 구성하거나 수동 인터페이스를 사용하여 Span 포트를 구성합니다. 다음 섹션에서는 지원되는 연결 방법과 케이블 작업 시 고려할 사항에 대해 설명합니다.

허브 사용

외부 디렉토리는 관리되는 디바이스가 네트워크 세그먼트의 모든 트래픽을 볼 수 있도록 보장하는 간단한 방법입니다. 이 유형의 허브 대부분은 세그먼트의 모든 호스트로 전달할 수 있는 IP 트래픽을 수신하여 허브에 연결된 모든 디바이스로 브로드캐스트합니다. 세그먼트에서 수신 및 발송되는 모든 트래픽을 모니터링하려면 인터페이스 세트를 허브에 연결합니다. 허브를 사용할 경우 패킷 충돌 가능성으로 인해 탐지 엔진이 높은 볼륨의 네트워크에서 모든 패킷을 확인하지 못할 수 있습니다. 트래픽이 적은 단순한 네트워크에서는 이러한 문제가 발생할 가능성이 적습니다. 트래픽이 많은 네트워크에서는 다른 옵션이 더 나은 결과를 제공할 수 있습니다. 허브에 장애 또는 정전이 발생할 경우 네트워크 연결이 끊어집니다. 단순한 네트워크에서는 네트워크가 다운될 수 있습니다.

일부 디바이스는 허브로 판매되고 있지만 실제로 스위치로 작동하며 각 패킷을 모든 포트로 브로드캐스트하지 않습니다. 관리되는 디바이스를 허브에 연결했지만 모든 트래픽을 볼 수 없는 경우 다른 허브를 구매하거나 Span 포트가 있는 스위치를 사용해야 할 수 있습니다.

Span 포트 사용

대부분의 네트워크 스위치에는 하나 이상의 포트의 트래픽을 미러링하는 Span 포트가 포함되어 있습니다. 인터페이스 세트를 Span 포트에 연결하면 모든 포트(일반적으로 수신 및 발송)의 결합된 트래픽을 모니터링할 수 있습니다. 네트워크에 이 기능이 포함된 스위치가 올바른 위치에 이미 설치되어 있는 경우 관리되는 디바이스 비용에 약간의 장비 비용을 추가하면 복수 세그먼트에 탐지를 구축할 수 있습니다. 트래픽이 많은 네트워크에서 이 솔루션에는 제약 사항이 있습니다. Span 포트가 200Mbps를 처리할 수 있고 세 개의 미러링된 포트가 최대 100Mbps까지 처리할 수 있는 경우 Span 포트가 초과 가입되어 패킷을 삭제할 가능성이 높아지므로 관리되는 디바이스의 효과가 감소합니다.

네트워크 탭 사용

네트워크 탭에서는 네트워크 흐름을 중단하거나 네트워크 토폴로지를 변경하지 않고 트래픽을 수동적으로 모니터링할 수 있습니다. 탭은 다른 대역폭에 손쉽게 사용 가능하며 네트워크 세그먼트에서 수신 및 발송되는 패킷을 분석할 수 있습니다. 대부분의 탭에서는 단일 네트워크 세그먼트만 모니터링할 수 있으므로 스위치의 8개 포트 중 2개의 트래픽을 모니터링하려는 경우에는 적합한 솔루션이 아닙니다. 대신, 라우터와 스위치 사이에 탭을 설치하고 스위치에 대한 전체 IP 스트림에 액세스하는 것이 좋습니다.

네트워크 탭은 수신 및 발송 트래픽을 두 개의 다른 케이블의 두 개의 다른 스트림으로 나누도록 설계되었습니다. 관리되는 디바이스는 전체 트래픽 스트림을 디코더, 프리프로세서 및 탐지 엔진에서 평가할 수 있도록 대화의 양측을 재결합하는 멀티 센싱 인터페이스 옵션을 제공합니다.

구리 인터페이스의 인라인 구축 케이블링

디바이스를 네트워크에서 인라인으로 구축하고 디바이스에 장애가 발생할 경우 디바이스의 바이패스 기능을 사용하여 네트워크 연결성을 유지하려는 경우 연결 케이블링 방법에 특히 주의해야 합니다.

바이패스가 지원되는 파이버 인터페이스로 디바이스를 구축할 경우에는 연결이 단단하게 고정되어 있고 케이블이 꼬이지 않도록 주의하는 것 이외에 특별한 케이블링 문제가 없습니다. 하지만 파이버 네트워크 인터페이스가 아닌 구리로 디바이스를 구축할 경우에는 디바이스 모델별로 다른 네트워크 카드를 사용하기 때문에 사용 중인 디바이스 모델을 알아야 합니다. 일부 8000 Series NetMod에서는 바이패스 컨피그레이션이 허용되지 않습니다.

디바이스의 NIC(Network Interface Cards)는 다른 네트워크 디바이스에 연결하는 데 사용하는 이더넷 케이블(straight-through 또는 crossover)과 상관없이 네트워크 인터페이스가 자동으로 구성되도록 하는 Auto-MDI-X(Auto-Medium Dependent Interface Crossover) 기능을 지원합니다. 다음 표는 다양한 디바이스와 각 디바이스의 바이패스 방법(straight-through 또는 crossover 연결)을 보여줍니다.

표 3-1 디바이스 및 바이패스 특성

디바이스	장애 시 개방 방식
3D500, 3D1000, 3D2000	straight-through
7000 Series	crossover
8000 Series	crossover

straight-through 연결로 바이패스하는 관리되는 디바이스의 경우 일반적으로 네트워크에서 활성화된 디바이스에 대해 수행되는 방식과 마찬가지로 디바이스를 연결합니다. 대부분의 경우에는 하나의 straight-through 케이블과 하나의 crossover 케이블을 사용하여 디바이스를 두 개의 엔드포인트에 연결해야 합니다.

그림 3-1 straight-Through 바이패스 연결 케이블링

crossover 연결로 바이패스하는 관리되는 디바이스의 경우 일반적으로 디바이스를 구축하지 않고 디바이스를 연결하는 방식과 마찬가지로 디바이스를 연결합니다. 제거된 디바이스에 전원을 연결하면 링크가 작동해야 합니다. 대부분의 경우에는 두 개의 straight-through 케이블을 사용하여 디바이스를 두 개의 엔드포인트에 연결해야 합니다.

그림 3-2 crossover 바이패스 연결 케이블링

다음 표는 하드웨어 바이패스 컨피그레이션에서 crossover 또는 straight-through 케이블을 사용해야 하는 경우를 보여줍니다. 레이어 2 포트는 구축에서 straight-through(MDI) 엔드포인트로 작동하며 레이어 3 포트는 구축에서 crossover(MDIX) 엔드포인트로 작동합니다. 바이패스가 올바르게 작동하려면 전체 crossover(케이블 및 어플라이언스)가 홀수여야 합니다.

표 3-2 유효한 하드웨어 바이패스 컨피그레이션

엔드포인트 1	케이블	관리되는 디바이스	케이블	엔드포인트 2
MDIX	straight-through	straight-through	straight-through	MDI
MDI	crossover	straight-through	straight-through	MDI
MDI	straight-through	straight-through	crossover	MDI
MDI	straight-through	straight-through	straight-through	MDIX
MDIX	straight-through	crossover	straight-through	MDIX
MDI	straight-through	crossover	straight-through	MDI
MDI	crossover	crossover	crossover	MDI
MDIX	crossover	crossover	straight-through	MDI

Auto-MDI-X에 대한 여러 조합의 지원이 있는 엔드포인트를 사용하면 모든 네트워크 환경이 고유하게 될 수 있습니다. 디바이스를 올바른 케이블링으로 설치하는지 확인하는 가장 쉬운 방법은 먼저 디바이스의 전원을 끈 상태에서 하나의 crossover 케이블과 하나의 straight-through 케이블을 사용하여 디바이스를 두 엔드포인트에 연결하는 것입니다. 두 엔드포인트가 통신할 수 있는지 확인합니다. 서로 통신할 수 없는 경우에는 케이블 중 하나가 올바른 유형이 아닙니다. 케이블 중 하나만 다른 유형(straight-through 또는 crossover)으로 교체합니다.

인라인 디바이스의 전원을 끈 상태에서 두 엔드포인트가 성공적으로 통신하면 디바이스의 전원을 켭니다. Auto-MDI-X 기능은 두 엔드포인트가 계속 통신하도록 보장합니다. 인라인 디바이스를 교체해야 하는 경우 원래 디바이스와 교체한 디바이스가 다른 바이패스 특성을 가진 경우로부터 보호할 수 있도록 새 디바이스의 전원을 끈 상태에서 엔드포인트가 통신하는지 확인하는 과정을 반복해야 합니다.

Auto-MDI-X 설정은 네트워크 인터페이스에 자동 협상을 허용하는 경우에만 올바르게 작동합니다. Network Interface(네트워크 인터페이스) 페이지의 Auto Negotiate(자동 협상) 옵션을 해제해야 하는 네트워크 환경에서는 인라인 네트워크 인터페이스에 대해 올바른 MDI/MDIX 옵션을 지정해야 합니다. 자세한 내용은 *FireSIGHT System 사용 설명서*의 인라인 인터페이스 구성을 참조하십시오.

특별 고려 사항: 8000 Series 디바이스 연결

8000 Series 관리되는 디바이스를 방어 센터에 등록하는 경우 안정적인 네트워크 링크를 보장하기 위해 연결 양측에서 자동 협상을 사용하거나 양측을 동일한 정적 속도로 설정해야 합니다. 8000 Series 관리되는 디바이스는 반이중 네트워크 링크를 지원하지 않으며 속도 차이 또는 연결 반대쪽의 이중 컨피그레이션도 지원하지 않습니다.

구축 옵션

관리되는 디바이스를 네트워크 세그먼트에 배치할 경우 침입 탐지 시스템을 사용하여 트래픽을 모니터링하거나 침입 방지 시스템을 사용하여 네트워크를 위협으로부터 보호할 수 있습니다.

관리되는 디바이스가 가상 스위치, 가상 라우터 또는 게이트웨이 VPN으로 작동하도록 구축할 수도 있습니다. 또한 정책을 사용하여 트래픽을 라우팅하거나 네트워크의 트래픽에 대한 액세스를 제어할 수 있습니다. 자세한 내용은 다음 섹션을 참조하십시오.

- 가상 스위치로 구축, 페이지 3-8
- 가상 라우터로 구축, 페이지 3-10
- 하이브리드 인터페이스로 구축, 페이지 3-11
- 게이트웨이 VPN 구축, 페이지 3-12
- 정책 기반 NAT로 구축, 페이지 3-13
- 액세스 제어로 구축, 페이지 3-13

가상 스위치로 구축

라이센스: 제어

지원되는 디바이스: Series 3

인라인 인터페이스를 스위치 인터페이스로 구성하여 관리되는 디바이스에 *가상 스위치*를 생성할 수 있습니다. 가상 스위치는 구축 중에 레이어 2 패킷 스위칭을 제공합니다. 고급 옵션에는 고정 MAC 주소 설정, STP(Spanning Tree Protocol) 활성화, 엄격한 TCP 적용, 도메인 레벨에서 BPDU(Bridge Protocol Data Unit) 삭제 등이 있습니다. 스위치 인터페이스에 대한 자세한 내용은 스위치 인터페이스, 페이지 3-4을(를) 참조하십시오.

가상 스위치에는 트래픽을 처리할 수 있도록 두 개 이상의 스위치 인터페이스가 포함되어야 합니다. 각 가상 스위치의 경우 시스템에서 스위치 인터페이스로 구성된 포트 집합으로만 트래픽이 스위칭됩니다. 예를 들어, 네 개의 스위치 인터페이스가 포함된 가상 스위치를 구성하는 경우 시스템에서 하나의 포트를 통해 트래픽 패킷을 수신하면 스위치의 나머지 세 개 포트로만 이러한 패킷을 브로드캐스트합니다.

트래픽을 허용하도록 가상 스위치를 구성하려면 물리적 포트에 두 개 이상의 스위치 인터페이스를 구성하고 가상 스위치를 추가 및 구성한 다음 가상 스위치를 스위치 인터페이스로 할당합니다. 시스템에서는 트래픽을 기다리는 스위치 인터페이스가 없는 외부 물리적 인터페이스에 수신된 트래픽을 삭제합니다. 시스템에서 VLAN 태그가 없는 패킷을 수신하고 해당 포트에 대한 물리적 스위치 인터페이스를 구성하지 않은 경우에는 시스템에서 패킷을 삭제합니다. 시스템에서 VLAN 태그가 있는 패킷을 수신하고 논리적 스위치 인터페이스를 구성하지 않은 경우에도 시스템에서 패킷을 삭제합니다.

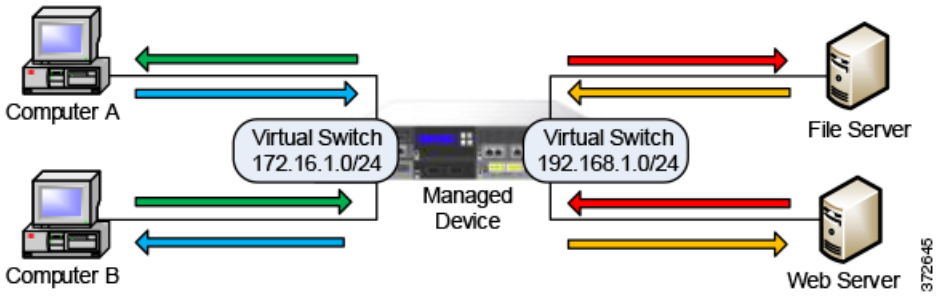
필요에 따라 물리적 포트에서 논리적 스위치 인터페이스를 추가로 정의할 수 있지만 트래픽을 처리하려면 논리적 스위치 인터페이스를 가상 스위치로 할당해야 합니다.

가상 스위치에는 확장성의 이점이 있습니다. 물리적 스위치를 사용할 경우 스위치에서 사용 가능한 포트 수에 따라 제한됩니다. 물리적 스위치를 가상 스위치로 교체하는 경우에는 구축에 도입하려는 복잡도 수준과 대역폭에 따라서만 제한됩니다.

레이어 2 스위치를 사용하려는 경우 작업 그룹 연결 및 네트워크 세그먼테이션과 같은 가상 스위치를 사용합니다. 레이어 2 스위치는 작업자가 대부분의 시간 동안 로컬 세그먼트에 있는 경우에 특히 효과적입니다. 대규모 구축(예: 브로드캐스트 트래픽, VoIP(Voice-over-IP) 또는 복수 네트워크가 포함된 구축)은 구축의 더 작은 네트워크 세그먼트에서 가상 스위치를 사용할 수 있습니다.

동일한 관리되는 디바이스에 복수의 가상 스위치를 구축할 경우 각 네트워크의 요구 사항에 따라 별도의 보안 수준을 유지할 수 있습니다.

그림 3-3 관리되는 디바이스의 가상 스위치



이 예제에서는 관리되는 디바이스가 두 개의 별도 네트워크(172.16.1.0/20 및 192.168.1.0/24)의 트래픽을 모니터링합니다. 두 네트워크 모두 동일한 관리되는 디바이스에서 모니터링되지만 가상 스위치는 동일한 네트워크에 있는 컴퓨터 또는 서버로만 트래픽을 전달합니다. 트래픽은 172.16.1.0/24 가상 스위치를 통해 컴퓨터 A에서 컴퓨터 B로 전달될 수 있으며(파란색 선) 동일한 가상 스위치를 통해 컴퓨터 B에서 컴퓨터 A로 전달될 수 있습니다(녹색 선). 마찬가지로, 트래픽은 192.168.1.0/24 가상 스위치를 통해 파일과 웹 서버 간에 전달될 수 있습니다(녹색 및 주황색 선). 그러나 컴퓨터가 서버와 동일한 가상 스위치에 없기 때문에 컴퓨터와 웹 또는 파일 서버 간에는 트래픽이 전달될 수 없습니다.

스위치 인터페이스 및 가상 스위치 구성에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*의 가상 스위치 설정을 참조하십시오.

가상 라우터로 구축

라이센스: 제어

지원되는 디바이스: Series 3

관리되는 디바이스에 *가상 라우터*를 생성하여 두 개 이상의 네트워크 간에 트래픽을 라우팅하거나 사설 네트워크를 공용 네트워크(예: 인터넷)에 연결할 수 있습니다. 가상 라우터는 두 개의 라우팅 인터페이스를 연결하여 수신 주소에 따라 구축을 위한 레이어 3 패킷 전달 의사 결정을 제공합니다. 선택적으로 가상 라우터에 엄격한 TCP를 적용할 수 있습니다. 라우팅 인터페이스 사용에 대한 자세한 내용은 라우팅 인터페이스, 페이지 3-4을(를) 참조하십시오. 가상 라우터는 게이트웨이 VPN과 함께 사용해야 합니다. 자세한 내용은 게이트웨이 VPN 구축, 페이지 3-12을(를) 참고하십시오.

가상 라우터는 동일한 브로드캐스트 도메인 내에 하나 이상의 개별 디바이스의 물리적 또는 논리적 라우팅 컨피그레이션을 포함할 수 있습니다. 물리적 인터페이스에서 VLAN 태그와 함께 수신된 트래픽을 처리하려면 각 논리적 인터페이스를 해당 특정 태그와 연결해야 합니다. 트래픽을 라우팅하려면 가상 라우터에 논리적 라우팅 인터페이스를 지정해야 합니다.

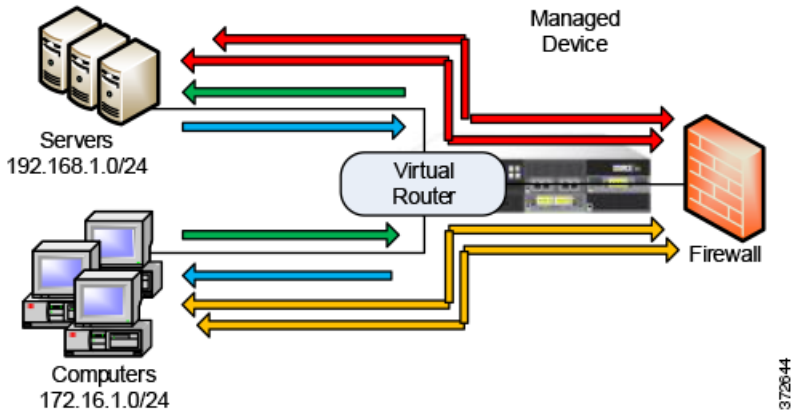
가상 라우터를 구성하려면 물리적 또는 논리적 컨피그레이션으로 라우팅 인터페이스를 설정합니다. 태그가 지정되지 않은 VLAN 트래픽을 처리하기 위한 물리적 라우팅 인터페이스를 구성할 수 있습니다. 또한 지정된 VLAN 태그가 포함된 트래픽을 처리하기 위해 논리적 라우팅 인터페이스를 생성할 수 있습니다. 시스템에서는 트래픽을 기다리는 라우팅 인터페이스가 없는 외부 물리적 인터페이스에 수신된 트래픽을 삭제합니다. 시스템에서 VLAN 태그가 없는 패킷을 수신하고 해당 포트에 대한 물리적 라우팅 인터페이스를 구성하지 않은 경우에는 시스템에서 패킷을 삭제합니다. 시스템에서 VLAN 태그가 지정된 패킷을 수신하고 논리적 라우팅 인터페이스를 구성하지 않은 경우에도 시스템에서 패킷을 삭제합니다.

가상 라우터에는 확장성의 이점이 있습니다. 물리적 라우터에 따라 연결할 수 있는 네트워크 수가 제한되는 경우 동일한 관리되는 디바이스에 여러 가상 라우터를 구성할 수 있습니다. 여러 라우터를 동일한 디바이스에 배치할 경우 구축의 물리적 복잡도가 감소하여 하나의 디바이스에서 여러 라우터를 모니터링하고 관리할 수 있습니다.

레이어 3 물리적 라우터를 사용하여 구축의 여러 네트워크 간에 트래픽을 전달하거나 사설 네트워크를 공용 네트워크에 연결하려는 경우 가상 라우터를 사용합니다. 가상 라우터는 보안 요구 사항이 다른 네트워크 또는 네트워크 세그먼트가 많은 대규모 구축에서 특히 효과적입니다.

관리되는 디바이스에 가상 라우터를 구축할 경우 하나의 어플라이언스를 사용하여 여러 네트워크를 서로 연결하고 인터넷에도 연결할 수 있습니다.

그림 3-4 관리되는 디바이스의 가상 라우터



이 예제에서는 172.16.1.0/20 네트워크에 있는 컴퓨터와 192.168.1.0/24 네트워크에 있는 서버 간에 트래픽을 이동하도록 허용하는 가상 라우터가 관리되는 디바이스에 포함되어 있습니다(파란색 및 녹색 선). 가상 라우터의 세 번째 인터페이스를 사용하여 각 네트워크의 트래픽을 방화벽으로 전달하거나 그 반대 방향으로 전달할 수 있습니다(빨간색 및 주황색 선).

자세한 내용은 *FireSIGHT System 사용 설명서*의 가상 라우터 설정을 참조하십시오.

하이브리드 인터페이스로 구축

라이센스: 제어

지원되는 디바이스: Series 3

가상 스위치와 가상 라우터를 사용하여 레이어 2 및 레이어 3 네트워크 간에 트래픽을 라우팅하기 위해 관리되는 디바이스에 *하이브리드 인터페이스*를 생성할 수 있습니다. 이 경우 하나의 인터페이스로 스위치의 로컬 트래픽을 라우팅하고 외부 네트워크와 트래픽을 상호 라우팅할 수 있습니다. 가장 좋은 방법은 인터페이스에 정책 기반 NAT를 구성하여 하이브리드 인터페이스에 네트워크 주소 변환을 제공하는 것입니다. 정책 기반 NAT로 구축, 페이지 3-13을(를) 참조하십시오.

하이브리드 인터페이스에는 하나 이상의 스위치 인터페이스와 하나 이상의 라우팅 인터페이스가 포함되어야 합니다. 일반적인 구축은 로컬 네트워크의 트래픽을 전달하기 위해 가상 스위치로 구성된 두 개의 스위치 인터페이스와 트래픽을 사설 또는 공용 네트워크로 라우팅하는 가상 라우터로 구성됩니다.

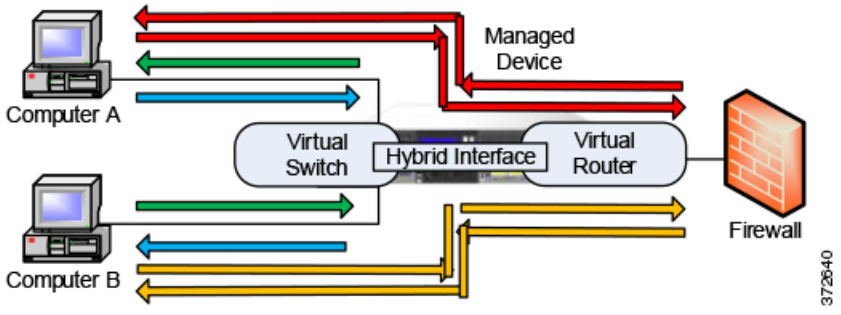
하이브리드 인터페이스를 생성하려면 우선 가상 스위치와 가상 라우터를 구성한 다음 가상 스위치와 가상 라우터를 하이브리드 인터페이스에 추가합니다. 가상 스위치 및 가상 라우터와 연결되지 않은 하이브리드 인터페이스는 라우팅에 사용할 수 없으며 트래픽을 생성하거나 트래픽에 응답하지 않습니다.

하이브리드 인터페이스는 차지하는 공간이 작고 확장 가능한 이점이 있습니다. 단일 하이브리드 인터페이스를 사용할 경우 레이어 2 및 레이어 3 트래픽 라우팅 기능이 단일 인터페이스에 결합되어 구축에서 물리적 어플라이언스의 수를 줄이고 트래픽에 대해 단일 관리 인터페이스를 제공합니다.

레이어 2 및 레이어 3 라우팅 기능이 모두 필요할 경우 하이브리드 인터페이스를 사용합니다. 이 구축은 공간과 리소스가 제한적인 구축의 작은 세그먼트에 적합할 수 있습니다.

하이브리드 인터페이스를 구축할 경우 트래픽이 로컬 네트워크에서 외부 또는 공용 네트워크(예: 인터넷)로 전달되도록 허용하는 동시에, 하이브리드 인터페이스의 가상 스위치와 가상 라우터에 대한 별도의 보안 고려 사항을 해결할 수 있습니다.

그림 3-5 관리되는 디바이스의 하이브리드 인터페이스



이 예제에서 컴퓨터 A와 컴퓨터 B는 동일한 네트워크에 있으며 관리되는 디바이스에 구성된 레이어 2 가상 스위치를 사용하여 통신합니다(파란색 및 녹색 선). 관리되는 디바이스에 구성된 가상 라우터는 방화벽에 대한 레이어 3 액세스를 제공합니다. 하이브리드 인터페이스는 가상 스위치와 가상 라우터의 레이어 2 및 레이어 3 기능을 결합하여 각 컴퓨터의 트래픽이 하이브리드 인터페이스를 통해 방화벽으로 전달될 수 있도록 허용합니다(빨간색 및 주황색 선).

자세한 내용은 *FireSIGHT System 사용 설명서*의 하이브리드 인터페이스 설정을 참조하십시오.

게이트웨이 **VPN** 구축

라이센스: VPN

지원되는 디바이스: Series 3

게이트웨이 VPN(*Virtual Private Network*) 연결을 생성하여 로컬 게이트웨이와 원격 게이트웨이 사이에 보안 터널을 설정할 수 있습니다. 게이트웨이 사이의 보안 터널은 게이트웨이 간 통신을 보호합니다.

IPSec(Internet Protocol Security) 프로토콜군을 사용하여 Cisco 관리되는 디바이스의 가상 라우터에서 원격 디바이스 또는 다른 서드파티 VPN 엔드포인트로의 보안 VPN 터널을 구축하도록 FireSIGHT System을 구성할 수 있습니다. VPN 연결이 설정된 후 보안 VPN 터널을 통해 로컬 게이트웨이 뒤에 있는 호스트에서 원격 게이트 뒤에 있는 호스트에 연결할 수 있습니다. VPN 엔드포인트는 IKE(Internet Key Exchange) 버전 1 또는 버전 2 프로토콜로 상호 인증하여 터널에 대한 보안 연결을 생성합니다. 시스템은 IPSec AH(Authentication Header) 모드 또는 IPSec ESP(Encapsulating Security Payload) 모드에서 실행됩니다. AH와 ESP 모두 인증을 제공하며 ESP는 암호화도 제공합니다.

게이트웨이 VPN은 포인트투포인트(point-to-point), 스타 또는 메시 구축에서 사용될 수 있습니다.

- 포인트투포인트 구축은 두 엔드포인트를 직접적인 일대일 관계로 연결합니다. 두 엔드포인트가 쌍 디바이스로 구성되며, 각 디바이스가 보안 연결을 시작할 수 있습니다. 하나 이상의 디바이스가 VPN을 지원하는 관리되는 디바이스여야 합니다.

  원격 위치의 호스트가 공용 네트워크를 사용하여 회사 네트워크의 호스트에 연결할 경우 포인트 투 포인트 구축을 사용하여 네트워크 보안을 유지합니다.

- 스타 구축은 허브와 복수의 원격 엔드포인트(리프 노드) 사이에 보안 연결을 구축합니다. 허브 노드와 개별 리프 노드 사이의 각 연결은 별도의 VPN 터널입니다. 일반적으로 허브 노드는 본사에 있으며 VPN을 지원하는 관리되는 디바이스입니다. 리프 노드는 지사에 있으며 대부분의 트래픽을 시작합니다.

  인터넷 또는 서드파티의 다른 네트워크의 보안 연결을 사용하여 조직의 본사 및 지사에 연결하고 모든 직원에게 조직 네트워크에 대한 제어된 액세스를 제공하려면 스타 구축을 사용합니다.

- 메시 구축은 VPN 터널을 사용하여 모든 엔드포인트를 연결합니다. 이 구축에서는 한 엔드포인트에 장애가 발생할 경우에도 나머지 엔드포인트는 여전히 서로 통신할 수 있다는 점에서 이중화를 제공합니다.

  분산된 지사 위치 그룹을 연결하여 하나 이상의 VPN 터널에서 장애가 발생할 경우 트래픽이 이동할 수 있도록 하려면 메시 구축을 사용합니다. 이 컨피그레이션에서 VPN을 지원하는 관리되는 디바이스를 몇 개 구축하는가에 따라 이중화 수준이 결정됩니다.

게이트웨이 VPN 컨피그레이션 및 구축에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*의 게이트웨이 VPN을 참조하십시오.

정책 기반 NAT로 구축

라이센스: 제어

지원되는 디바이스: ASA FirePOWER를 제외한 모든 디바이스

정책 기반 NAT(Network Address Translation)를 사용하여 NAT 수행 방법을 지정하는 정책을 정의할 수 있습니다. 정책의 대상을 단일 인터페이스, 하나 이상의 디바이스 또는 전체 네트워크로 지정할 수 있습니다.

정적(일대일) 또는 동적(일대다) 변환을 구성할 수 있습니다. 동적 변환은 순서에 따라 다릅니다. 즉, 첫 번째 일치하는 규칙이 적용될 때까지 규칙이 순서대로 검색됩니다.

정책 기반 NAT는 일반적으로 다음과 같은 구축에서 작동합니다.

- 사설 네트워크 주소를 숨길 경우

  사설 네트워크에서 공용 네트워크에 액세스할 경우 NAT가 사설 네트워크 주소를 공용 네트워크 주소로 변환합니다. 특정 사설 네트워크 주소는 공용 네트워크에서 숨겨집니다.

- 사설 네트워크 서비스에 대한 액세스를 허용하는 경우

  공용 네트워크가 사설 네트워크에 액세스하는 경우 NAT는 공용 주소를 사설 네트워크 주소로 변환합니다. 공용 네트워크가 특정 사설 네트워크 주소에 액세스할 수 있습니다.

- 여러 사설 네트워크 간에 트래픽을 리디렉션하는 경우

  사설 네트워크의 서버가 연결된 사설 네트워크의 서버에 액세스할 경우 NAT는 두 사설 네트워크 사이의 사설 주소를 변환하여 사설 주소가 중복되지 않는지와 이러한 사설 네트워크 사이에 트래픽이 이동할 수 있는지를 확인합니다.

정책 기반 NAT를 사용할 경우 추가 하드웨어가 필요하지 않으며 침입 탐지 또는 방지 시스템과 NAT의 컨피그레이션이 단일 사용자 인터페이스로 통합됩니다. 자세한 내용은 *FireSIGHT System 사용 설명서*의 NAT 정책 사용을 참조하십시오.

액세스 제어로 구축

라이센스: 모두

지원되는 디바이스: 모두

액세스 제어는 네트워크를 들어오고 나가며 네트워크 안에서 이동하는 트래픽을 지정, 검사, 로깅할 수 있는 정책 기반 기능입니다. 다음 섹션은 구축에서 액세스 제어가 작동하는 방식에 대해 설명합니다. 이 기능에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

액세스 제어 정책에 따라 시스템이 네트워크의 트래픽을 처리하는 방식이 결정됩니다. 정책에 액세스 제어 규칙을 추가하여 네트워크 트래픽을 처리 및 로깅하는 방식을 더 자세히 제어할 수 있습니다.

액세스 제어 규칙이 포함되지 않은 액세스 제어 정책은 트래픽을 처리하기 위해 다음 중 한 가지 기본 동작을 사용합니다.

- 네트워크에 진입하는 모든 트래픽 차단
- 추가 검사 없이 네트워크에 진입하려는 모든 트래픽 신뢰
- 네트워크에 진입하려는 모든 트래픽을 허용하고, 네트워크 검색 정책만 사용하여 트래픽 검사
- 네트워크에 진입하려는 모든 트래픽을 허용하고, 침입 및 네트워크 검색 정책을 사용하여 트래픽 검사

액세스 제어 규칙은 간단한 IP 주소 매칭부터 다른 사용자, 애플리케이션, 포트, URL이 포함된 복잡한 시나리오까지, 대상 디바이스가 트래픽을 처리하는 방식을 더 자세히 정의합니다. 각 규칙에 대해 규칙 동작, 즉, 침입 또는 파일 정책을 사용하여 일치하는 트래픽을 신뢰, 모니터링, 차단 또는 검사할지를 지정합니다.

액세스 제어는 액세스 제어 정책에 따라 소스 또는 대상 IP 주소를 기반으로 네트워크를 이동할 수 있는 트래픽을 지정하는 기능인 보안 인텔리전스 데이터를 기준으로 트래픽을 필터링할 수 있습니다. 이 기능은 허용되지 않는 IP 주소의 블랙리스트를 만들 수 있습니다. 이러한 IP 주소의 트래픽은 차단되며 검사되지 않습니다.

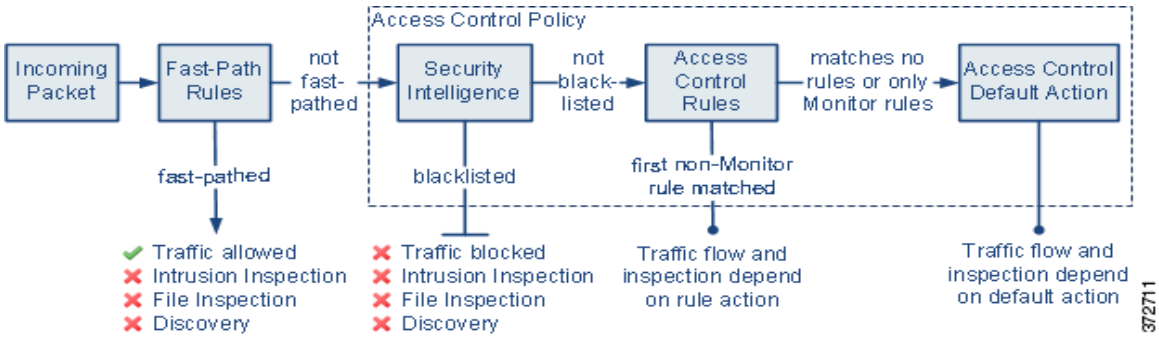
예제 구축에서는 일반 네트워크 세그먼트를 보여줍니다. 이러한 각 위치에 관리되는 디바이스를 구축함으로써 다른 목적을 충족할 수 있습니다. 다음 섹션에서는 일반적인 위치 권장사항에 대해 설명합니다.

- 방화벽 내부, 페이지 3-14에서는 방화벽을 통과하는 트래픽에서 액세스 제어의 작동 방식에 대해 설명합니다.
- DMZ에서, 페이지 3-15에서는 DMZ 내의 액세스 제어로 외부로 연결된 서버를 보호하는 방법에 대해 설명합니다.
- 내부 네트워크에서, 페이지 3-15에서는 액세스 제어가 내부 네트워크를 고의적 또는 우연한 공격으로부터 보호하는 방법에 대해 설명합니다.
- 핵심 네트워크에서, 페이지 3-16에서는 엄격한 규칙의 액세스 제어 정책이 중요 자산을 보호하는 방법에 대해 설명합니다.
- 원격 또는 모바일 네트워크에서, 페이지 3-16에서는 액세스 제어가 원격 위치 또는 모바일 디바이스의 트래픽으로부터 네트워크를 모니터링 및 보호하는 방법에 대해 설명합니다.

방화벽 내부

방화벽 내의 관리되는 디바이스는 방화벽에서 허용하는 인바운드 트래픽과 컨피그레이션 오류로 인해 방화벽을 통과하는 트래픽을 모니터링합니다. 일반 네트워크 세그먼트에는 DMZ, 내부 네트워크, 코어, 모바일 액세스 및 원격 네트워크가 포함됩니다.

아래 다이어그램은 FireSIGHT System을 통한 트래픽 흐름을 나타내며 이러한 트래픽에서 수행되는 검사 유형에 대해 몇 가지 정보를 제공합니다. 시스템에서 빠른 경로 또는 블랙리스트의 트래픽은 검사하지 않습니다. 액세스 제어 규칙 또는 기본 동작에서 처리되는 트래픽의 경우 흐름 및 검사는 규칙 동작에 따라 다릅니다. 다이어그램을 간단히 표시하기 위해 규칙 동작은 생략되어 있지만 신뢰하거나 차단된 트래픽에는 어떤 종류의 검사도 수행하지 않습니다. 또한 기본 동작에서는 파일 검사가 지원되지 않습니다.



인커밍 패킷은 먼저 빠른 경로 규칙에 대해 검사됩니다. 일치하는 항목이 있는 경우 트래픽이 빠른 경로로 이동합니다. 일치하는 항목이 없는 경우 보안 인텔리전스 기반 필터링에서 패킷이 블랙리스트인지 여부를 확인합니다. 블랙리스트가 아닌 경우 액세스 제어 규칙이 적용됩니다. 패킷이 규칙 조건을 충족하는 경우 트래픽 흐름과 검사는 규칙 동작에 따라 달라집니다. 패킷과 일치하는 규칙이 없을 경우 트래픽 흐름과 검사는 기본 정책 동작에 따라 달라집니다. (트래픽을 계속 평가할 수 있는 모니터 규칙에서는 예외가 발생합니다.) 각 액세스 제어 정책의 기본 동작은 빠른 경로에 없거나 블랙리스트가 아닌 트래픽 또는 모니터 이외의 규칙에서 일치하는 트래픽을 관리합니다. 빠른 경로는 8000 Series 및 3D9900 디바이스에만 사용할 수 있습니다.

액세스 제어 규칙을 생성하여 네트워크 트래픽을 처리 및 로깅하는 방식을 더 자세히 제어할 수 있습니다. 각 규칙에 대해 특정 기준을 충족하는 트래픽에 적용할 동작(신뢰, 모니터링, 차단 또는 검사)을 지정합니다.

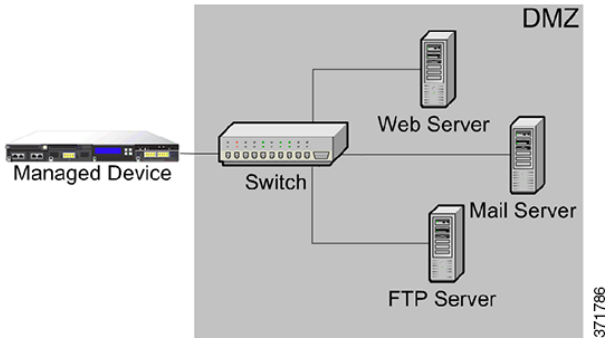
DMZ에서

DMZ에는 외부로 향하는 서버(예: 웹, FTP, DNS, 메일)가 포함되며 내부 네트워크의 사용자에게 메일 릴레이, 웹 프록시 등의 서비스를 제공할 수 있습니다.

DMZ에 저장된 콘텐츠는 정적이며 변경 사항은 명확한 커뮤니케이션과 사전 알림으로 계획 및 실행됩니다. DMZ의 서버에는 계획된 변경 사항만 발생하므로 이 세그먼트의 공격은 일반적으로 인바운드이며 즉시 확실해집니다. 이 세그먼트에 대한 효과적인 액세스 제어 정책을 통해 서비스에 대한 액세스를 긴밀히 제어하며 새로운 네트워크 이벤트를 검색합니다.

DMZ의 서버에는 DMZ에서 네트워크를 통해 쿼리할 수 있는 데이터베이스가 포함될 수 있습니다. DMZ와 마찬가지로, 예기치 않은 변경 사항이 없어야 하지만 데이터베이스 콘텐츠는 더 민감하며 웹사이트 또는 다른 DMZ 서비스보다 더 강력한 보호가 필요합니다. DMZ 액세스 제어 정책 이외에도 강력한 침입 정책이 효과적인 전략입니다.

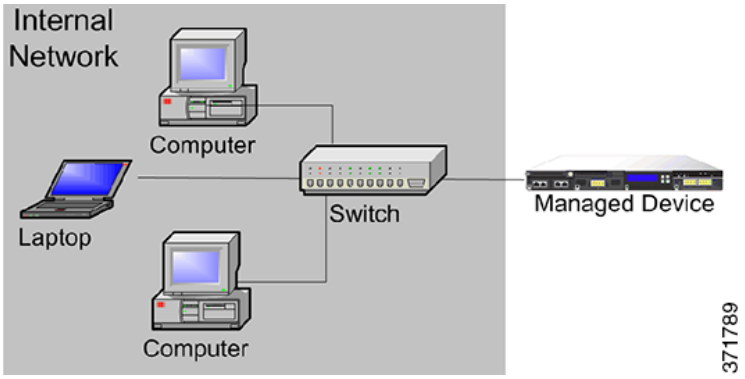
이 세그먼트에 구축하는 관리되는 디바이스는 DMZ에 있는 감염 서버에서 시작되어 인터넷으로 향하는 공격을 감지할 수 있습니다. 네트워크 검색을 사용하여 네트워크 트래픽을 모니터링하면 변경 사항(예: 예기치 않은 서비스가 갑자기 나타남)에 노출된 서버를 모니터링할 수 있습니다. 이러한 변경 사항은 DMZ의 서버가 감염되었음을 의미할 수 있습니다.



내부 네트워크에서

악의적 공격은 내부 네트워크에 있는 컴퓨터에서 시작될 수 있습니다. 고의적 행동(예: 네트워크에 알 수 없는 컴퓨터가 예기치 않게 나타남)이나 우연한 감염(예: 오프사이트에서 감염된 업무용 노트북 컴퓨터가 네트워크에 연결되고 바이러스를 퍼뜨림)이 이러한 공격에 해당합니다. 내부 네트워크의 위험은 아웃바운드일 수도 있습니다(예: 컴퓨터가 의심스러운 외부 IP 주소로 정보를 발송).

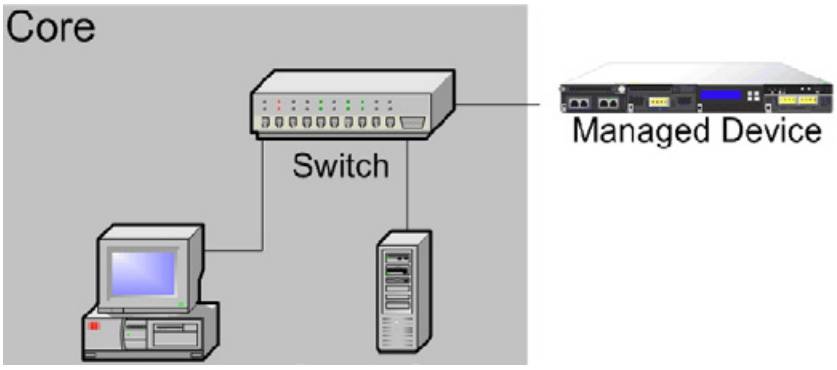
이러한 동적 네트워크에는 아웃바운드 트래픽 이외에 내부 트래픽에 대한 엄격한 액세스 제어 정책이 필요합니다. 사용자와 애플리케이션 사이의 트래픽을 엄격히 제어할 수 있도록 액세스 제어 규칙을 추가하십시오.



핵심 네트워크에서

핵심 자산이란 비즈니스 성공에 중요하며 어떤 방법으로도 반드시 보호해야 하는 자산입니다. 핵심 자산은 비즈니스 특성에 따라 다르지만, 일반적인 핵심 자산으로는 재무 및 관리 센터 또는 지적 재산권 저장소 등이 있습니다. 핵심 자산의 보안이 침해될 경우 비즈니스가 파괴될 수 있습니다.

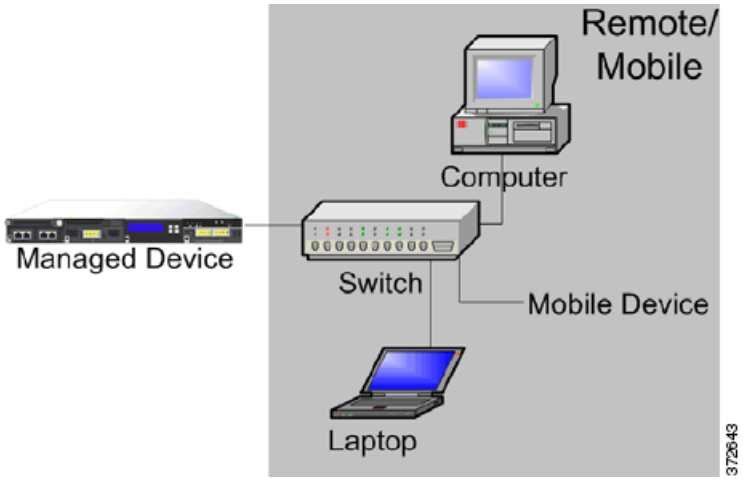
이 세그먼트는 비즈니스 운영에 쉽게 사용할 수 있어야 하지만 반드시 엄격히 제어해야 합니다. 액세스 제어는 원격 네트워크나 모바일 디바이스와 같이 위험도가 높은 네트워크 세그먼트에서 이러한 자산에 도달할 수 없도록 보장해야 합니다. 이 세그먼트에는 사용자와 애플리케이션 액세스에 대한 엄격한 규칙을 적용하여 항상 가장 공격적인 제어를 사용하십시오.



원격 또는 모바일 네트워크에서

오프 사이트에 위치한 원격 네트워크는 일반적으로 VPN(Virtual Private Network)을 사용하여 기본 네트워크에 대한 액세스를 제공합니다. 비즈니스 목적을 위해 모바일 디바이스와 개인 디바이스를 사용하는 사례(예: "스마트폰"을 사용하여 기업 이메일 액세스)가 점점 보편화되고 있습니다.

이러한 네트워크는 빠르고 지속적인 변경이 있는 매우 동적인 환경일 수 있습니다. 전용 모바일 또는 원격 네트워크에 관리되는 디바이스를 구축할 경우 알려지지 않은 외부 소스와 송수신하는 트래픽을 모니터링 및 관리하는 엄격한 액세스 제어 정책을 생성할 수 있습니다. 정책은 사용자, 네트워크 및 애플리케이션이 핵심 리소스에 액세스하는 방식을 엄격히 제한함으로써 위험을 줄일 수 있습니다.



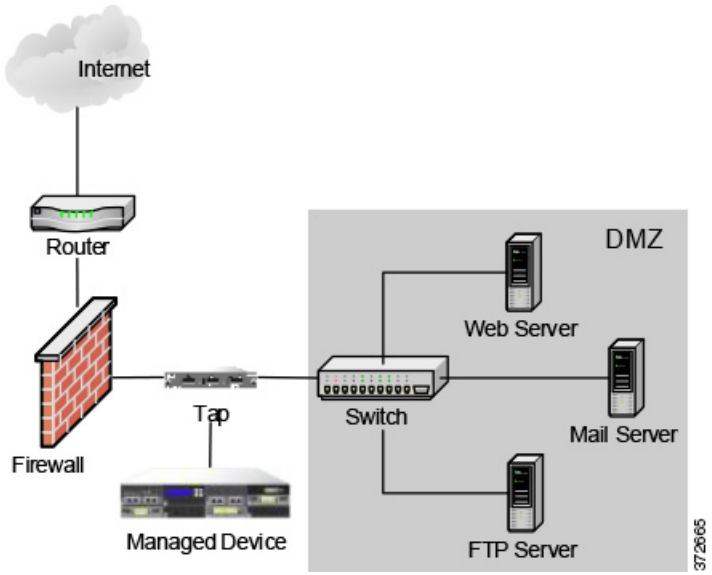
관리되는 디바이스에서 멀티 센싱 인터페이스 사용

관리되는 디바이스는 네트워크 모듈에 멀티 센싱 포트인터페이스를 제공합니다. 관리되는 디바이스에서 멀티 센싱 인터페이스를 사용하여 다음을 수행할 수 있습니다.

- 네트워크 탭에서 개별 연결 재결합
- 다른 네트워크의 트래픽 캡처 및 평가
- 가상 라우터로 실행
- 가상 스위치로 실행

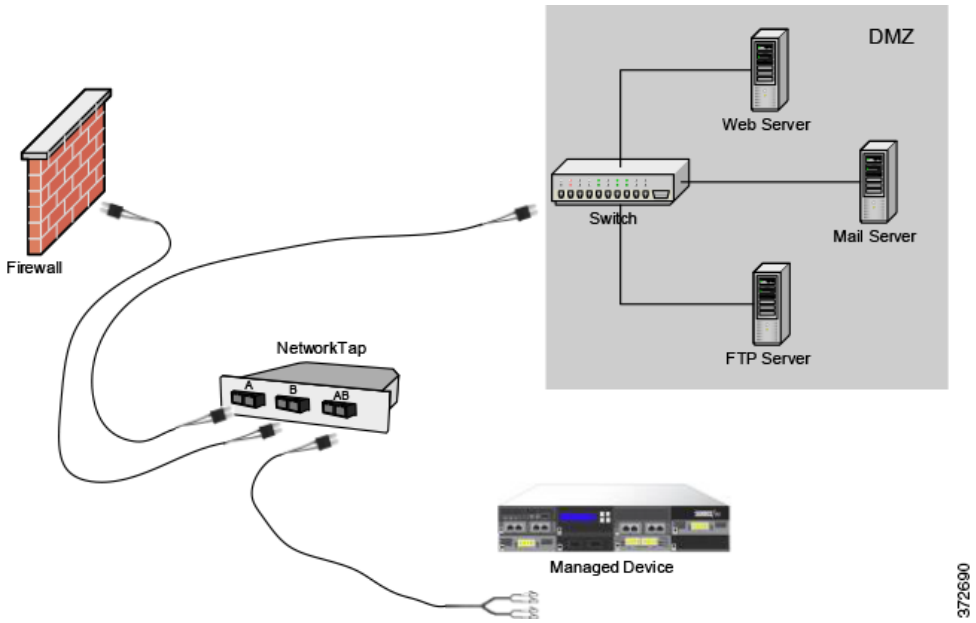
참고 각 센싱 인터페이스는 디바이스의 최대 정격 처리량을 수신할 수 있지만, 관리되는 디바이스의 총 트래픽은 패킷 손실 없이 대역폭 한도를 초과할 수 없습니다.

네트워크 탭을 사용하여 관리되는 디바이스에 멀티 센싱 인터페이스를 구축하는 과정은 간단합니다. 다음 다이어그램은 트래픽이 많은 네트워크 세그먼트에 설치한 네트워크 탭입니다.

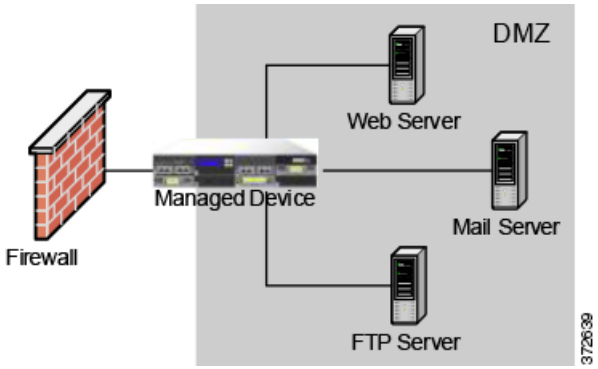


이 시나리오에서는 탭이 별도의 센싱 인터페이스를 통해 수신 및 발송 트래픽을 전송합니다. 관리되는 디바이스의 멀티 센싱 인터페이스 어댑터 카드를 탭에 연결할 경우 관리되는 디바이스가 트래픽 분석을 위해 트래픽을 단일 데이터 스트림에 결합합니다.

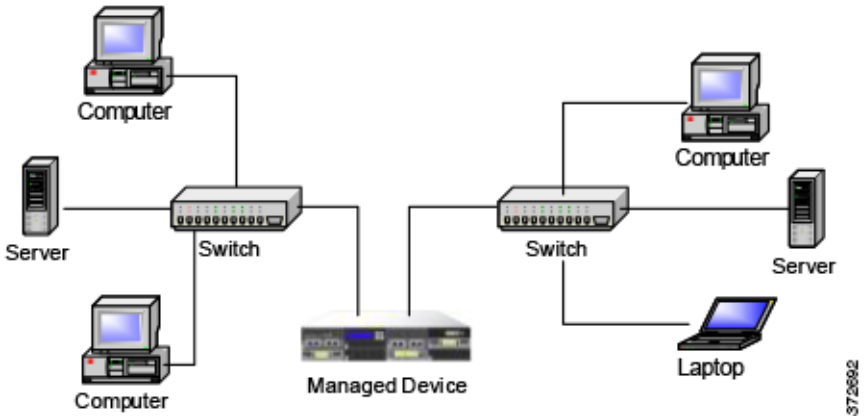
아래 그림과 같이 기가비트 옵티컬 탭의 경우 탭의 커넥터에서 관리되는 디바이스의 센싱 인터페이스 세트를 둘 다 사용합니다.



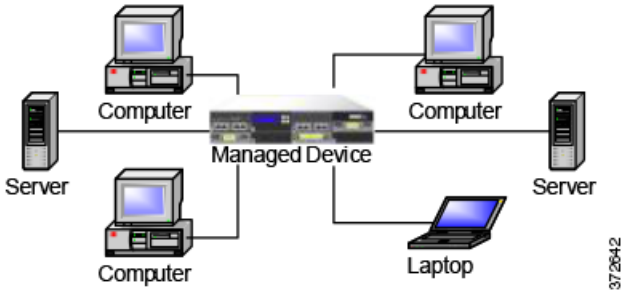
가상 스위치를 사용하여 구축의 탭과 스위치를 모두 교체할 수 있습니다. 탭을 가상 스위치로 교체할 경우 탭 패킷 전달을 보장할 수 없게 됩니다.



또한 별도 네트워크에서 데이터를 캡처하는 인터페이스를 생성할 수 있습니다. 다음 다이어그램은 듀얼 센싱 인터페이스 어댑터와 두 개 네트워크에 연결된 두 개의 인터페이스가 있는 단일 디바이스를 보여줍니다.



하나의 디바이스를 사용하여 두 네트워크 세그먼트를 모두 모니터링하는 것 이외에도, 디바이스의 가상 스위치 기능을 사용하여 구축된 두 스위치를 교체할 수 있습니다.



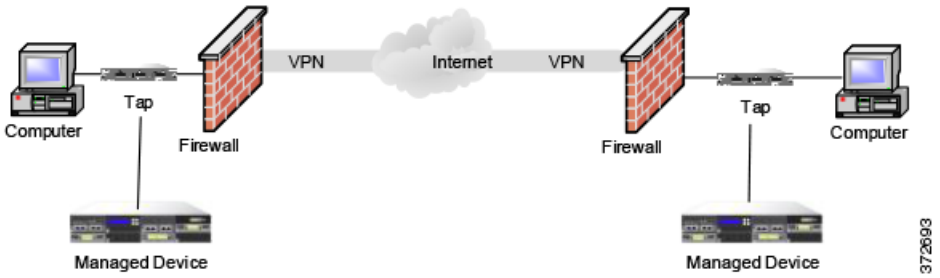
복잡한 네트워크 구축

엔터프라이즈 네트워크에는 VPN 사용과 같은 원격 접속이 필요하거나 비즈니스 파트너 또는 뱅크 연결과 같은 여러 진입점이 있을 수 있습니다. 다음 섹션에서는 이러한 구축과 관련된 몇 가지 문제에 대해 설명합니다.

VPN과 통합

가상 사설 네트워크 또는 VPN에서는 IP 터널링 기법을 사용하여 인터넷에서 원격 사용자에게 로컬 네트워크의 보안을 제공합니다. 일반적으로 VPN 솔루션은 데이터 페이로드를 IP 패킷으로 암호화합니다. IP 헤더는 다른 패킷과 거의 동일한 방식으로 공용 네트워크를 통해 전송될 수 있도록 암호화되지 않습니다. 패킷이 대상 네트워크에 도달하면 페이로드의 암호가 해독되고 패킷이 올바른 호스트로 전달됩니다.

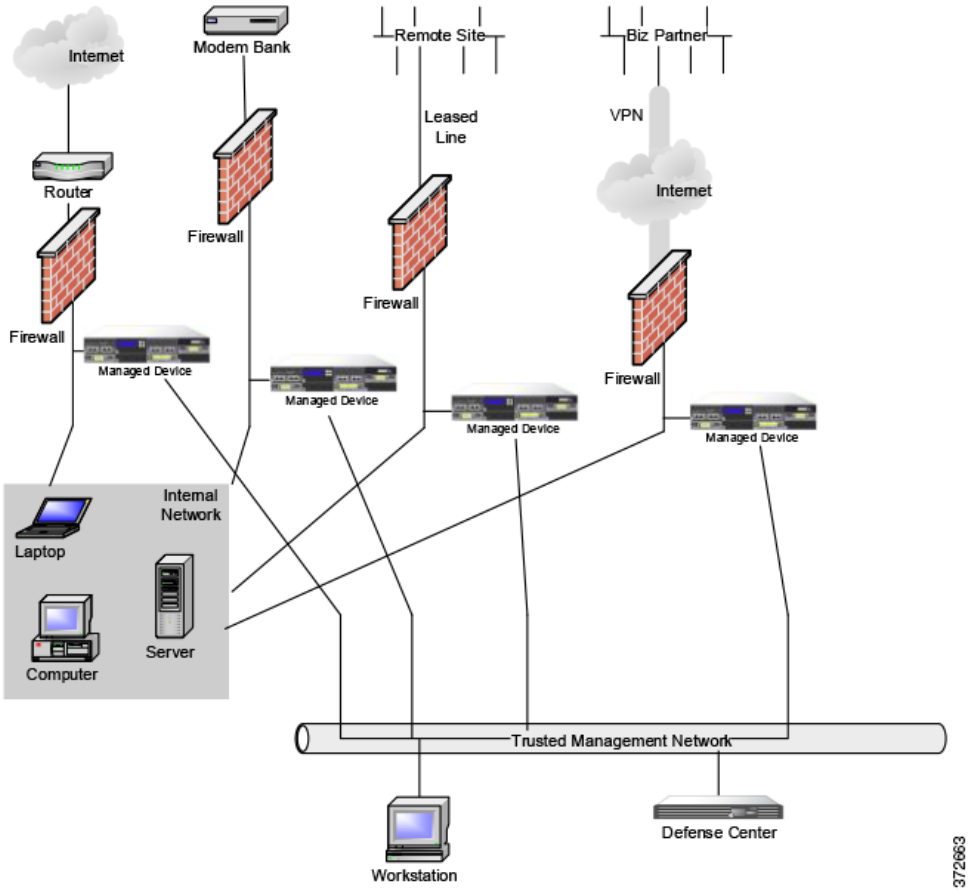
네트워크 어플라이언스는 VPN 패킷의 암호화된 페이로드를 분석할 수 없으므로 관리되는 디바이스를 VPN 연결의 터미네이션 엔드포인트 밖에 배치할 경우 모든 패킷 정보에 액세스할 수 있습니다. 다음 다이어그램은 관리되는 디바이스를 VPN 환경에 구축하는 방법을 보여줍니다.



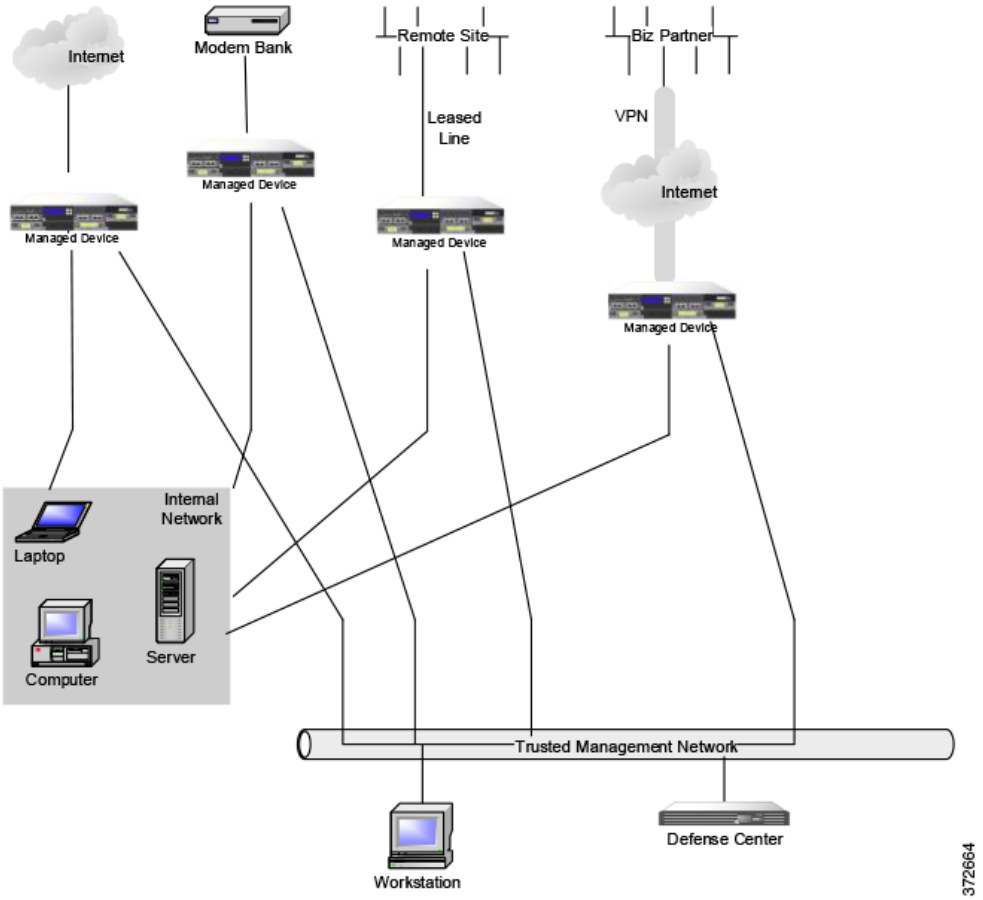
VPN 연결의 어느 한쪽에 있는 탭과 방화벽을 관리되는 디바이스로 교체할 수 있습니다. 탭을 관리되는 디바이스로 교체할 경우 탭 패킷 전달을 보장할 수 없게 됩니다.

다른 진입점의 침입 감지

대부분의 네트워크에는 둘 이상의 액세스 포인트가 있습니다. 일부 엔터프라이즈는 인터넷에 연결되는 단일 경계 라우터를 사용하는 대신 인터넷, 모뎀 뱅크 및 비즈니스 파트너 네트워크에 대한 직접 링크를 결합하여 사용합니다. 일반적으로, 관리되는 디바이스는 방화벽과 근처에(방화벽 내부, 방화벽 외부 또는 둘 다) 구축하고 비즈니스 데이터의 무결성 및 기밀성에 중요한 네트워크 세그먼트에 구축해야 합니다. 다음 다이어그램은 진입점이 여러 개인 복잡한 네트워크의 주요 위치에 관리되는 디바이스를 설치하는 방법을 보여줍니다.

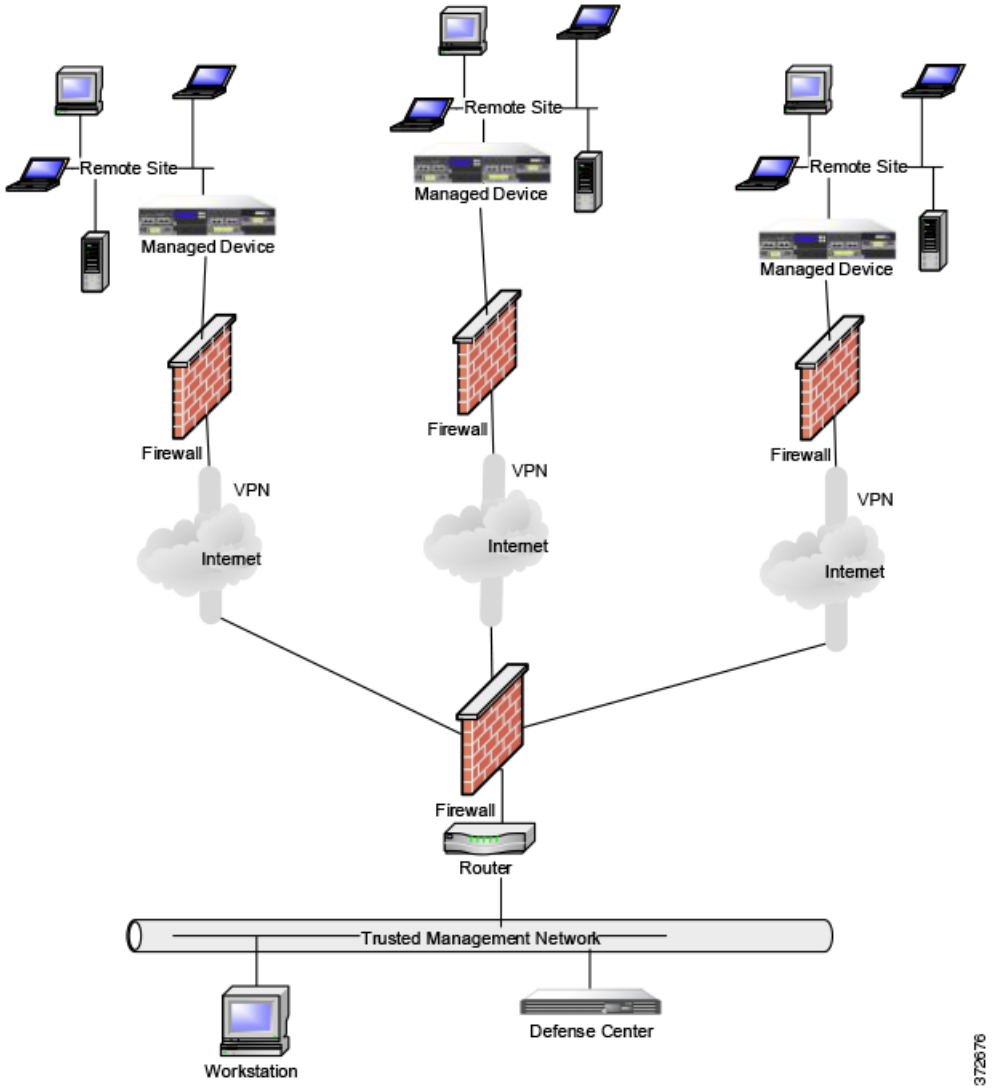


방화벽과 라우터 대신 해당 네트워크 세그먼트에 관리되는 디바이스를 구축할 수 있습니다.

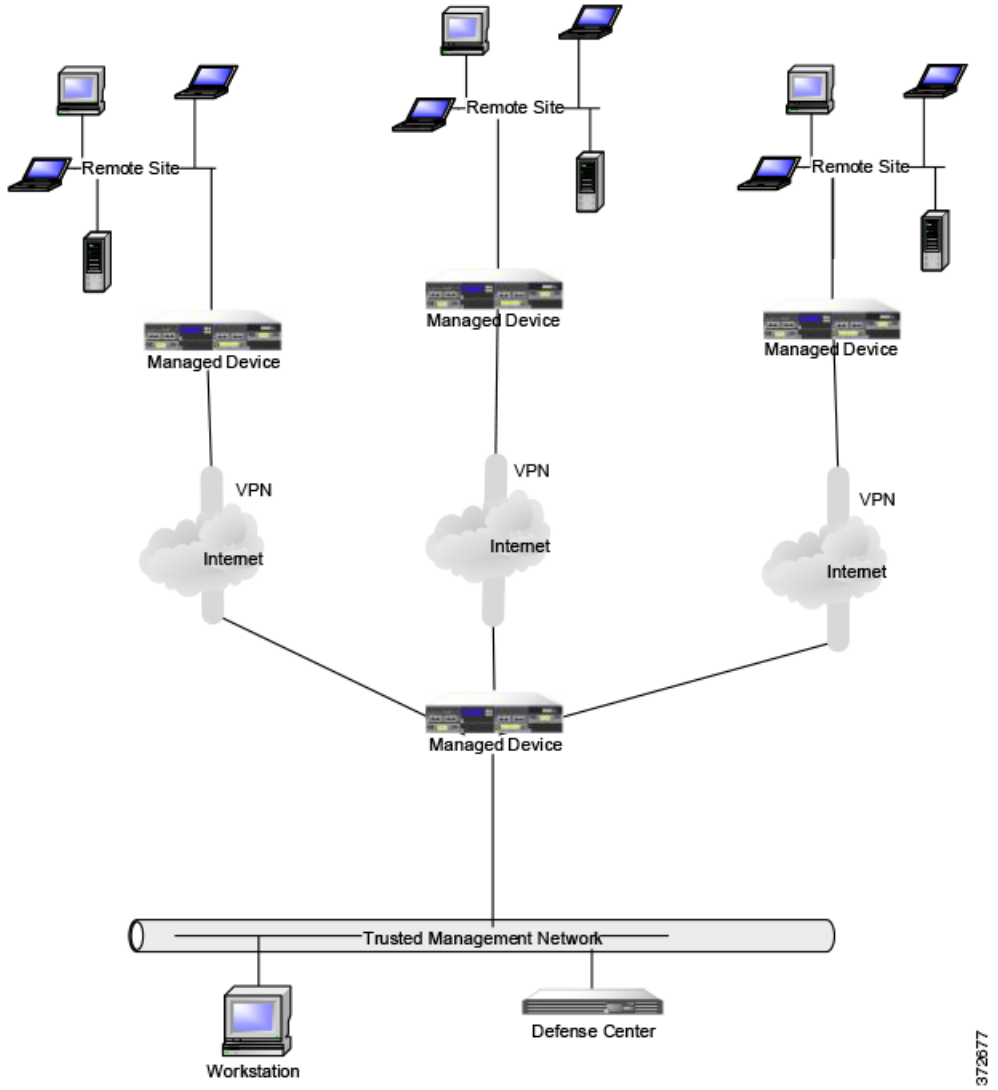


멀티 사이트 환경에 구축

대부분의 조직에서는 다른 지리적 위치의 엔터프라이즈에서 침입 탐지를 확장한 후 한 위치에서 모든 데이터를 분석하려고 합니다. FireSIGHT System에서는 조직의 여러 위치에 구축된 관리되는 디바이스에서 이벤트를 집계하고 상관 관계를 분석하는 방어 센터를 제공하여 이러한 기능을 지원합니다. 동일한 네트워크의 동일한 지리적 위치에서 복수의 관리되는 디바이스와 방어 센터를 구축하는 경우와 달리, 관리되는 디바이스를 여러 위치에 구축할 때에는 관리되는 디바이스와 데이터 스트림의 보안을 보장하기 위한 예방 조치를 수행해야 합니다. 데이터를 보호하려면 관리되는 디바이스와 방어 센터를 보호되지 않은 네트워크로부터 격리해야 합니다. 다음 다이어그램에 표시된 대로 VPN을 통하거나 다른 보안 터널링 프로토콜을 사용하여 관리되는 디바이스에서 데이터 스트림을 전송하여 이를 수행할 수 있습니다.



방화벽 및 라우터를 각 네트워크 세그먼트에 구축된 관리되는 디바이스로 교체할 수 있습니다.



복잡한 네트워크 내에서 복수 관리 인터페이스 통합

모든 구축에서 복수 관리 인터페이스를 구성하여 여러 네트워크를 모니터링하고 동일한 방어 센터에서 관리되는 디바이스의 트래픽을 격리할 수 있습니다. 복수 관리 인터페이스를 사용하면 고유한 IP 주소(IPv4 또는 IPv6)를 사용하는 관리 인터페이스를 방어 센터에 추가하고 해당 관리 인터페이스에서 관리하려는 디바이스가 포함된 네트워크로의 경로를 생성할 수 있습니다. 디바이스를 새 관리 인터페이스에 등록할 경우 해당 디바이스의 트래픽이 방어 센터의 기본 관리 인터페이스에 등록된 디바이스의 트래픽으로부터 격리됩니다.

정보 기본(`eth0`) 관리 인터페이스 이외의 모든 관리 인터페이스의 고정 IP 주소에 디바이스를 등록해야 합니다. DHCP는 기본 관리 인터페이스에서만 지원됩니다.

복수 관리 인터페이스는 트래픽 채널에 별도의 관리 인터페이스를 사용하지 않는 경우에 한해 NAT 환경에서 지원됩니다. 자세한 내용은 관리 네트워크에서 구축, 페이지 2-1을(를) 참조하십시오. LOM(Lights-Out Management)은 기본 관리 인터페이스에서만 지원되며, 추가 관리 인터페이스에서는 지원되지 않습니다.

방어 센터를 설치한 후 웹 인터페이스를 사용하여 복수 관리 인터페이스를 구성합니다. 자세한 내용은 *FireSIGHT System 사용 설명서*의 어플라이언스 설정 구성을 참조하십시오.

복잡한 네트워크 내에서 관리되는 디바이스 통합

단순한 다중 섹터 네트워크보다 더 복잡한 네트워크 토폴로지에서 관리되는 디바이스를 구축할 수 있습니다. 이 섹션에서는 방어 센터를 사용하여 여러 관리되는 디바이스를 관리하는 방법과 다중 사이트 환경에서 관리되는 디바이스를 구축 및 관리하는 방법에 대한 정보뿐만 아니라, 프록시 서버, NAT 디바이스 및 VPN이 있는 환경에서 구축할 경우 네트워크 검색 및 취약성 분석에 관한 문제에 대해 설명합니다.

프록시 서버 및 NAT와 통합

내부 호스트의 IP 주소를 방화벽 뒤에 효과적으로 숨겨서 방화벽에 걸쳐 NAT(Network Address Translation) 디바이스 또는 소프트웨어를 사용할 수 있습니다. 관리되는 디바이스를 이러한 디바이스 또는 소프트웨어와 모니터링되는 호스트 사이에 배치하는 경우 시스템에서 프록시 또는 NAT 디바이스 뒤에 있는 호스트를 올바르게 식별하지 않을 수도 있습니다. 이 경우, Cisco에서는 호스트가 올바르게 감지될 수 있도록 관리되는 디바이스를 프록시 또는 NAT 디바이스로 보호되는 네트워크 세그먼트 내에 배치하도록 권장합니다.

로드 밸런싱 방법을 사용하여 통합

일부 네트워크 환경에서는 "서버 팜" 컨피그레이션을 사용하여 웹 호스팅, FTP 스토리지 사이트 등의 서비스에 대한 네트워크 로드 밸런싱을 수행합니다. 로드 밸런싱 환경에서는 고유한 운영 체제를 사용하는 둘 이상의 호스트 간에 IP 주소를 공유합니다. 이 경우, 시스템에서 운영 체제 변경 사항을 감지하지만 높은 신뢰도로 운영 체제 식별을 제공할 수는 없습니다. 영향을 받는 호스트의 여러 운영 체제 수에 따라, 시스템에서 많은 수의 운영 체제 변경 이벤트를 생성하거나 낮은 신뢰도로 정적 운영 체제 식별을 표시할 수 있습니다.

기타 탐지 고려사항

식별하는 호스트의 TCP/IP 스택이 수정된 경우 시스템에서 호스트 운영 체제를 정확하게 식별하지 못할 수 있습니다. 이로 인해 성능이 향상되는 경우도 있습니다. 예를 들어, IIS(Internet Information Services) 웹 서버를 실행 중인 Windows 호스트의 관리자는 많은 양의 데이터를 수신하여 성능을 향상시킬 수 있도록 TCP 윈도우 크기를 늘리는 것이 좋습니다. 다른 예를 들면, TCP/IP 스택 변경을 이용하면 진정한 운영 체제를 확인할 수 없도록 하여 정확한 식별을 방해하고 표적 공격을 방지할 수 있습니다. 여기서 해결하려는 시나리오는 공격자가 네트워크를 정찰하여 특정 운영 체제가 설치된 호스트를 식별한 다음 해당 운영 체제에만 해당하는 공격용 악성코드로 해당 호스트에 대해 표적 공격을 실시하는 경우입니다.

FireSIGHT System 어플라이언스 설치

FireSIGHT System 어플라이언스는 대규모 FireSIGHT System 구축의 일부로 네트워크에 쉽게 설치할 수 있습니다. 네트워크 세그먼트에 디바이스를 설치하여 트래픽을 검사하고 적용된 침입 정책을 기준으로 침입 이벤트를 생성합니다. 이 데이터는 전체 구축에서 데이터의 상관 관계를 분석하고 보안에 대한 위협을 조정하여 이에 대응하기 위해 하나 이상의 디바이스를 관리하는 방어 센터로 전송됩니다.

여러 관리 인터페이스를 사용하여 성능을 향상하거나 두 개의 다른 네트워크에서 트래픽을 격리 및 관리할 수 있습니다. 초기 설치 중에 기본 관리 인터페이스(`eth0`)를 구성합니다. 설치 후 사용자 인터페이스에서 추가 관리 인터페이스를 구성할 수 있습니다. 자세한 내용은 *FireSIGHT System 사용 설명서*을(를) 참조하십시오.

다양한 구축 위치에서 사용될 여러 개의 어플라이언스를 한 위치에서 사전 구성할 수 있습니다. 사전 구성에 대한 지침은 FireSIGHT System 어플라이언스 사전 구성, 페이지 E-1을(를) 참조하십시오.

참고 ASA FirePOWER 디바이스 설치에 대한 자세한 내용은 ASA 설명서를 참조하십시오.

FireSIGHT System 어플라이언스 설치에 대한 자세한 내용은 다음 섹션을 참조하십시오.

포함된 항목

다음은 FireSIGHT System 어플라이언스에 제공되는 구성 요소 목록입니다. 시스템과 관련 액세서리의 포장을 풀면서 패키지 내용물에 다음 품목이 모두 포함되었는지 확인하십시오.

- FireSIGHT System 어플라이언스 1대
- 전원 코드(예비 전원 공급 장치가 포함된 어플라이언스에 2개의 전원 코드가 포함됨)

- 카테고리 5e 이더넷 straight-through 케이블: 방어 센터용 1개, 관리되는 디바이스용 2개
- 랙 마운팅 키트(3D7010, 3D7020, 3D7030 및 3D7050의 경우 필수 트레이 및 랙 마운팅 키트 별도 구매 가능)

보안 문제

Cisco에서는 어플라이언스를 설치하기 전에 다음 사항을 고려하도록 권장합니다.

- 안전한 위치에 있어 무단 접근이 불가능하고 잠글 수 있는 랙에 FireSIGHT System 어플라이언스를 배치하십시오.
- 교육을 받고 자격을 갖춘 담당자만 FireSIGHT System 어플라이언스를 설치, 교체, 관리 또는 서비스하도록 하십시오.
- 항상 무단 액세스로부터 보호된 내부의 보안 관리 네트워크에 관리 인터페이스를 연결하십시오.
- 어플라이언스에 대한 액세스를 허용할 수 있는 특정 워크스테이션 IP 주소를 식별하십시오. 어플라이언스 시스템 정책 내의 액세스 목록을 이용하여 특정 호스트만 어플라이언스에 액세스할 수 있도록 제한하십시오. 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

관리 인터페이스 식별

관리 인터페이스를 사용하여 구축의 각 어플라이언스를 네트워크에 연결합니다. 이렇게 하면 방어 센터에서 관리하는 디바이스와 통신하고 해당 디바이스를 관리할 수 있습니다.

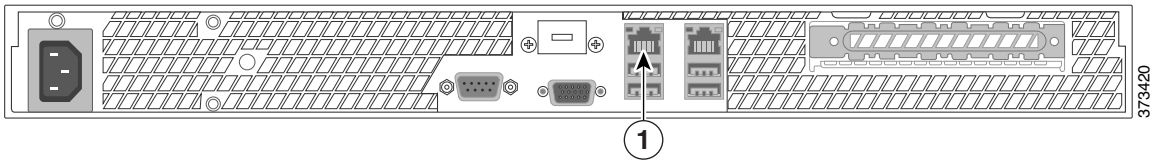
FireSIGHT System 어플라이언스는 다양한 하드웨어 플랫폼에 제공됩니다. 설치 절차를 수행할 때는 어플라이언스에 해당하는 그림을 참조하십시오.

- 방어 센터 750, 페이지 4-2
- 방어 센터 1500, 페이지 4-3
- 방어 센터 3500, 페이지 4-3
- 방어 센터 2000 및 4000, 페이지 4-3
- FirePOWER 7000 Series, 페이지 4-3
- FirePOWER 8000 Series, 페이지 4-4

방어 센터 750

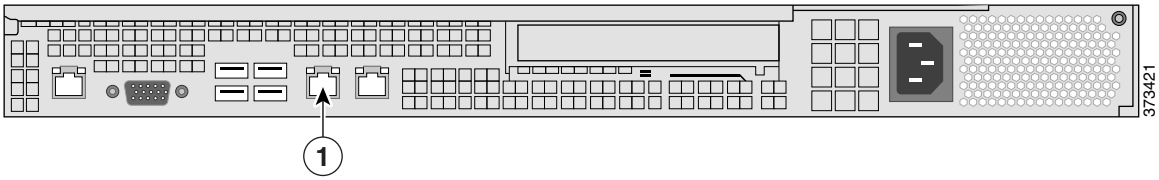
DC750은 1U 어플라이언스로 사용 가능합니다. 다음의 섀시 후면 그림은 DC750의 기본 관리 인터페이스(1) 위치를 나타냅니다.

그림 4-1 DC750



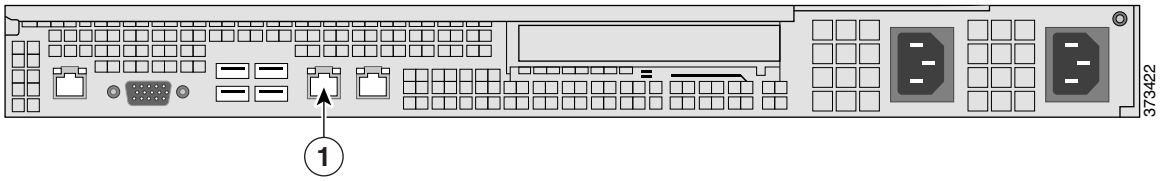
방어 센터 **1500**

DC1500은 1U 어플라이언스로 사용 가능합니다. 다음의 섀시 후면 그림은 DC1500의 기본 관리 인터페이스(1) 위치를 나타냅니다.



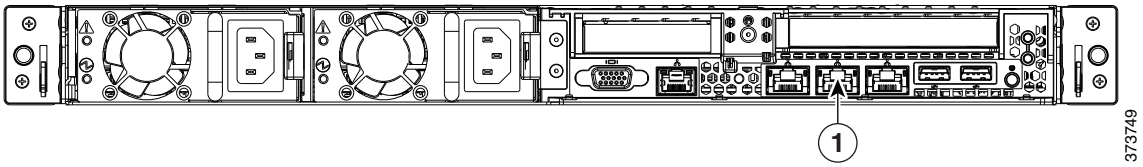
방어 센터 **3500**

DC3500은 1U 어플라이언스로 사용 가능합니다. 다음의 섀시 후면 그림은 DC3500의 기본 관리 인터페이스(1) 위치를 나타냅니다.



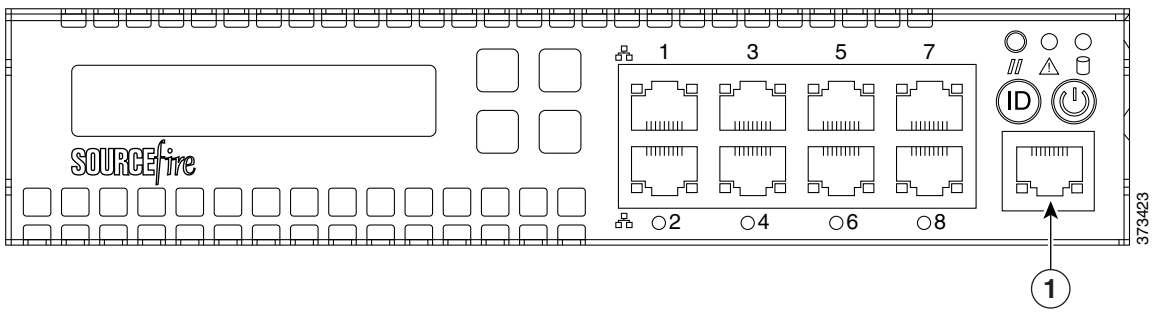
방어 센터 **2000** 및 **4000**

DC2000 및 DC4000은 1U 어플라이언스로 사용 가능합니다. 다음의 섀시 후면 그림은 DC2000 및 DC4000의 기본 관리 인터페이스(1) 위치를 나타냅니다.

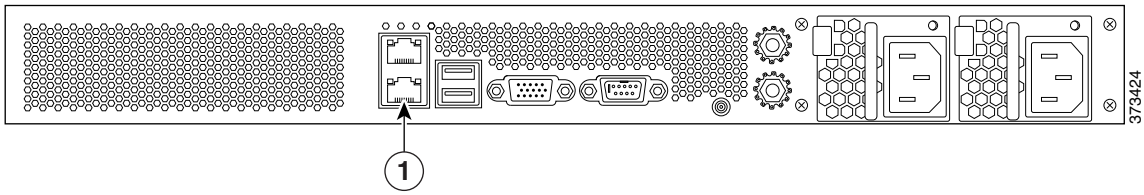


FirePOWER 7000 Series

3D7010, 3D7020, 3D7030 및 3D7050은 섀시 트레이의 절반 폭인 1U 어플라이언스입니다. 다음의 섀시 전면 그림은 기본 관리 인터페이스의 위치(1)를 나타냅니다.

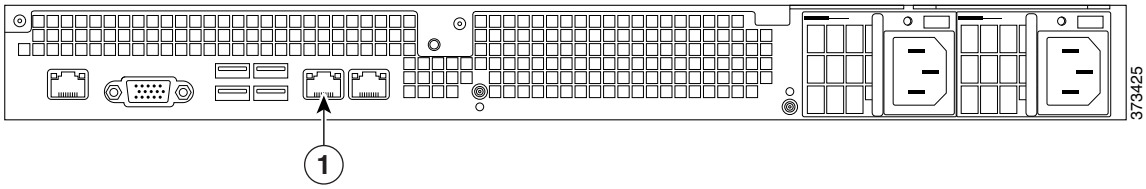


3D7110/7120, 3D7115/7125 및 AMP7150은 1U 어플라이언스로 사용 가능합니다. 다음의 섀시 후면 그림은 기본 관리 인터페이스의 위치(1)를 나타냅니다.

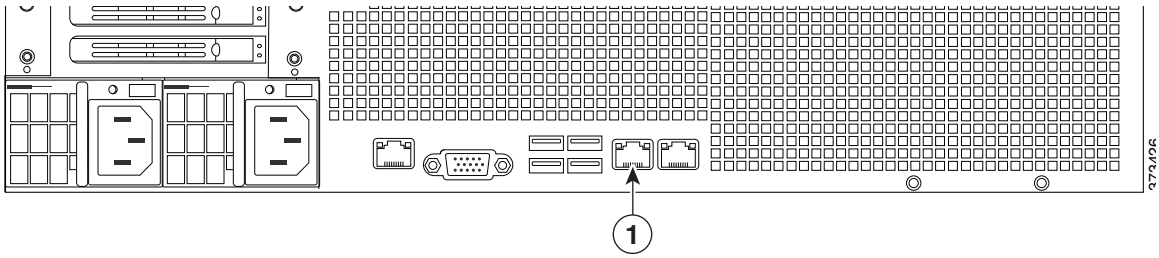


FirePOWER 8000 Series

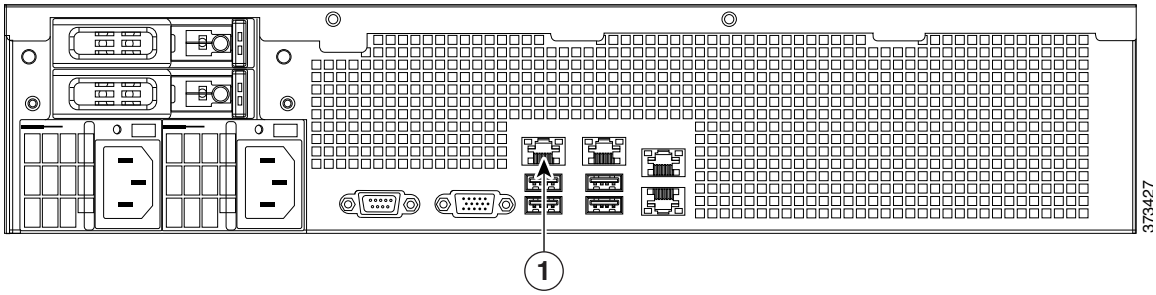
AMP8050, 3D8120, 3D8130, 3D8140 및 AMP8150은 1U 어플라이언스로 사용 가능합니다. 다음의 섀시 후면 그림은 기본 관리 인터페이스의 위치(1)를 나타냅니다.



3D8250은 2U 어플라이언스로 사용 가능합니다. 3D8260, 3D8270 및 3D8290은 1, 2 또는 3개의 보조 2U 어플라이언스를 포함하는 2U 어플라이언스로 사용 가능합니다. 다음의 섀시 후면 그림은 각 2U 어플라이언스의 기본 관리 인터페이스 위치(1)를 나타냅니다.



3D8350 및 AMP8350은 2U 어플라이언스로 사용 가능합니다. 3D8360, 3D8370, 3D8390, AMP8360, AMP8370 및 AMP8390은 1, 2 또는 3개의 보조 2U 어플라이언스를 포함하는 2U 어플라이언스로 사용 가능합니다. 다음의 섀시 후면 그림은 각 2U 어플라이언스의 기본 관리 인터페이스(1) 위치를 나타냅니다.



센싱 인터페이스 식별

관리되는 디바이스는 센싱 인터페이스를 사용하여 네트워크 세그먼트에 연결됩니다. 각 디바이스가 모니터링할 수 있는 세그먼트 수는 디바이스의 센싱 인터페이스 수와 네트워크 세그먼트에서 사용하려는 연결 유형(수동, 인라인, 라우팅, 스위치)에 따라 달라집니다.

다음 섹션에서는 각각의 관리되는 디바이스의 센싱 인터페이스에 대해 설명합니다.

- 7000 Series의 센싱 인터페이스를 확인하려면 FirePOWER 7000 Series, 페이지 4-5을(를) 참조하십시오.
- 8000 Series의 모듈 슬롯을 확인하려면 FirePOWER 8000 Series, 페이지 4-10을(를) 참조하십시오.
- 8000 Series NetMod의 센싱 인터페이스를 확인하려면 8000 Series 모듈, 페이지 4-11을(를) 참조하십시오.

연결 유형에 대한 자세한 내용은 센싱 인터페이스 이해, 페이지 3-2을(를) 참조하십시오.

FirePOWER 7000 Series

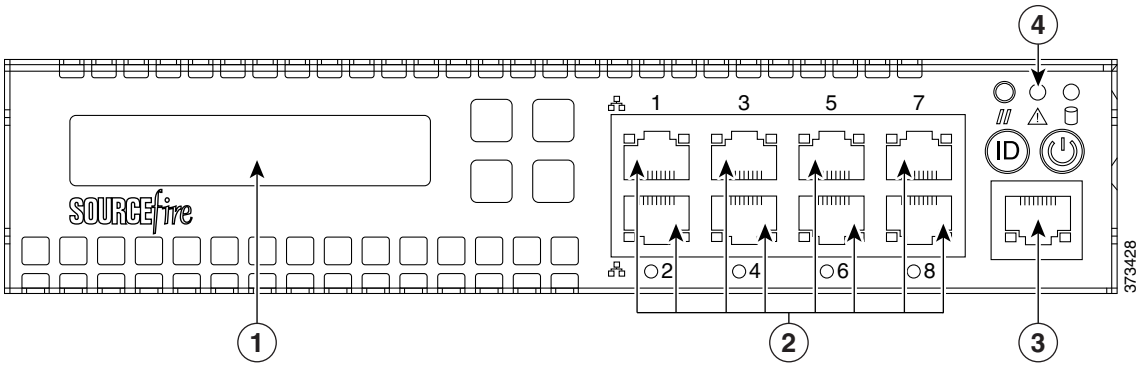
7000 Series는 다음 컨피그레이션으로 사용 가능합니다.

- 구리 인터페이스 8개(각각 바이패스 기능 구성 가능)가 포함되고 랙 트레이의 절반 폭인 1U 디바이스
- 구리 인터페이스 8개 또는 파이버 인터페이스 8개(각각 바이패스 기능 구성 가능)가 포함된 1U 디바이스
- 구리 인터페이스 4개(바이패스 기능 구성 가능) 및 SFP(Small Form-Factor Pluggable) 포트 8개(바이패스 기능 없음)가 포함된 1U 디바이스

3D7010, 3D7020, 3D7030 및 3D7050

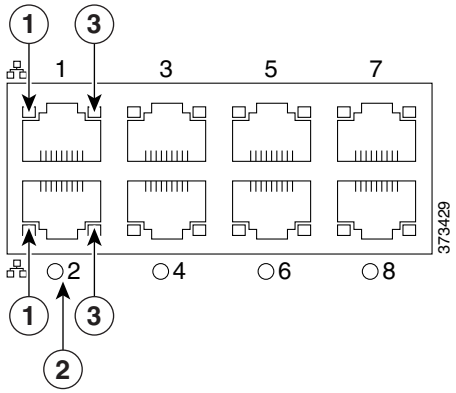
3D7010, 3D7020, 3D7030 및 3D7050에는 각각 바이패스 기능을 구성할 수 있는 8개의 카퍼(copper) 포트 센싱 인터페이스가 제공됩니다. 다음의 섀시 전면 그림은 센싱 인터페이스의 위치를 나타냅니다.

그림 4-2 8포트 1000BASE-T 바이패스 구성 가능 구리 인터페이스



1	LCD 패널	3	관리 포트
2	센싱 인터페이스	4	전면 패널

이러한 연결을 사용하여 최대 8개의 개별 네트워크 세그먼트를 수동적으로 모니터링할 수 있습니다. 또한 쌍으로 연결된 인터페이스를 인라인 또는 바이패스 모드가 포함된 인라인으로 사용하여 최대 4개 네트워크에서 디바이스를 침입 방지 시스템으로 구축할 수 있습니다.



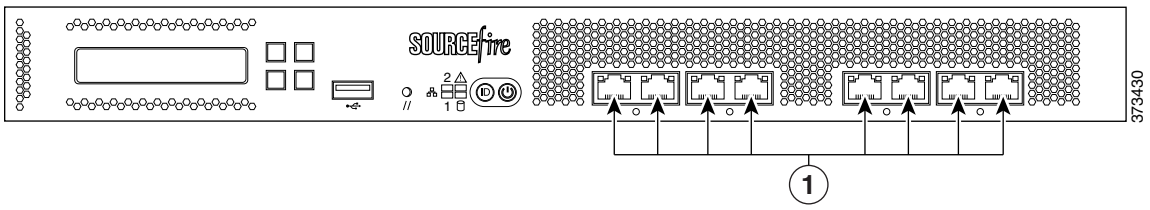
1	링크 LED	**3**	활동 LED
2	바이패스 LED	**—**	—

디바이스의 자동 바이패스 기능을 활용하려는 경우 2개의 인터페이스를 네트워크 세그먼트에 수직으로 연결해야 합니다(인터페이스 1/2, 3/4, 5/6, 7/8). 자동 바이패스 기능을 사용하면 디바이스에 장애 또는 정전이 발생하는 경우에도 트래픽이 이동할 수 있습니다. 인터페이스에 케이블을 연결한 다음에는 웹 인터페이스를 사용하여 인터페이스 쌍을 인라인 세트로 구성하고 인라인 세트에 바이패스 모드를 활성화합니다.

3D7110 및 3D7120

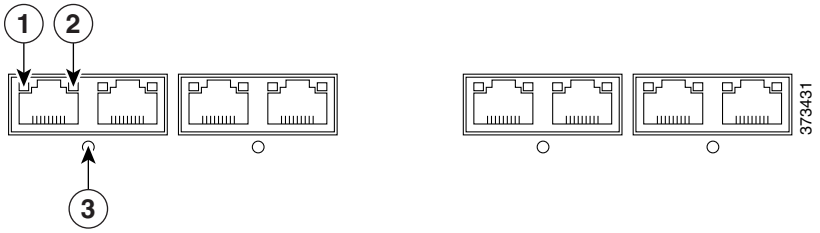
3D7110 및 3D7120에는 각각 바이패스 기능을 구성할 수 있는 8개의 카퍼(copper) 포트 센싱 인터페이스(그림 4-3 참조) 또는 8개의 파이버 포트 센싱 인터페이스(그림 4-5 참조)가 제공됩니다. 다음의 섀시 전면 그림은 센싱 인터페이스의 위치(1)와 LED 설명을 나타냅니다.

그림 4-3 3D7110 및 3D7120 구리 인터페이스



1	구리 센싱 인터페이스	**—**	—

그림 4-4 8포트 1000BASE-T 구리 인터페이스 LED

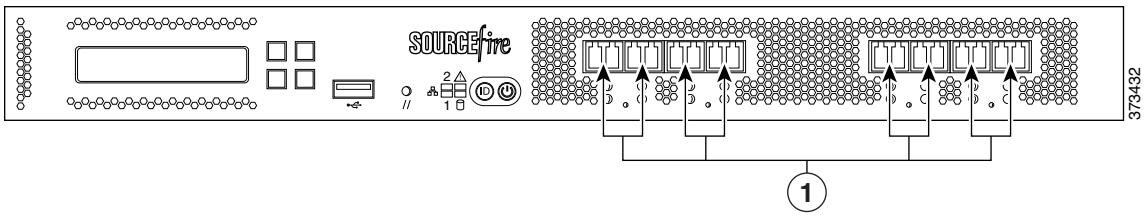


1	링크 LED	3	바이패스 LED
2	활동 LED	—	—

이러한 연결을 사용하여 최대 8개의 개별 네트워크 세그먼트를 수동적으로 모니터링할 수 있습니다. 또한 쌍으로 연결된 인터페이스를 인라인 또는 바이패스 모드가 포함된 인라인으로 사용하여 최대 4개 네트워크에서 디바이스를 침입 방지 시스템으로 구축할 수 있습니다.

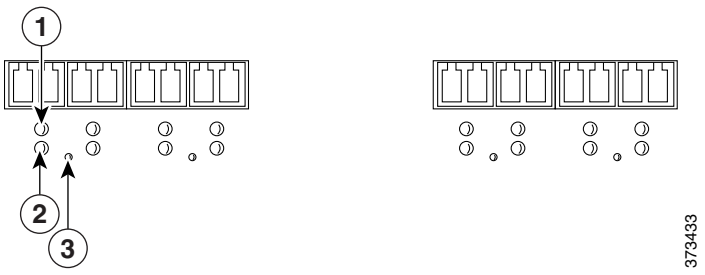
디바이스의 자동 바이패스 기능을 활용하려면 왼쪽에 있는 2개의 인터페이스 또는 오른쪽에 있는 2개의 인터페이스를 네트워크 세그먼트에 연결해야 합니다. 자동 바이패스 기능을 사용하면 디바이스에 장애 또는 정전이 발생하는 경우에도 트래픽이 이동할 수 있습니다. 인터페이스에 케이블을 연결한 다음에는 웹 인터페이스를 사용하여 인터페이스 쌍을 인라인 세트로 구성하고 인라인 세트에 바이패스 모드를 활성화합니다.

그림 4-5 3D7110 및 3D7120 파이버 인터페이스



1	파이버 센싱 인터페이스	—	—

그림 4-6 8포트 1000BASE-SX 파이버 바이패스 구성 가능 LED



1	활동 LED	3	바이패스 LED
2	링크 LED	—	—

8포트 1000BASE-SX 파이버 바이패스 구성 가능 컨피그레이션에서는 LC 유형(로컬 커넥터)의 옵티컬 트렌시버를 사용합니다.

이러한 연결을 사용하여 최대 8개의 개별 네트워크 세그먼트를 수동적으로 모니터링할 수 있습니다. 또한 쌍으로 연결된 인터페이스를 인라인 또는 바이패스 모드가 포함된 인라인으로 사용하여 최대 4개 네트워크에서 디바이스를 침입 방지 시스템으로 구축할 수 있습니다.

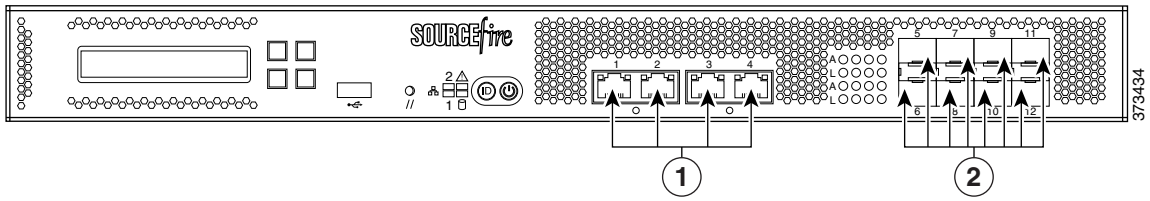
정보 최고의 성능을 위해서는 인터페이스 세트를 연속적으로 사용합니다. 인터페이스를 생략할 경우 성능이 저하될 수 있습니다.

디바이스의 자동 바이패스 기능을 활용하려면 왼쪽에 있는 2개의 인터페이스 또는 오른쪽에 있는 2개의 인터페이스를 네트워크 세그먼트에 연결해야 합니다. 자동 바이패스 기능을 사용하면 디바이스에 장애 또는 정전이 발생하는 경우에도 트래픽이 이동할 수 있습니다. 인터페이스에 케이블을 연결한 다음에는 웹 인터페이스를 사용하여 인터페이스 쌍을 인라인 세트로 구성하고 인라인 세트에 바이패스 모드를 활성화합니다.

3D7115, 3D7125 및 AMP7150

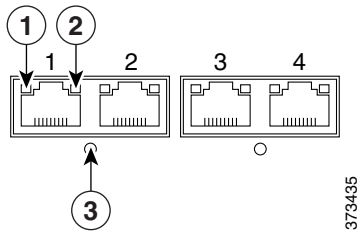
3D7115, 3D7125 및 AMP7150 디바이스는 구성 가능한 바이패스 기능이 있는 4포트 구리 인터페이스와 바이패스 기능이 없고 운영 중 교체 가능한 SFP(Small Form-Factor Pluggable) 포트 8개와 함께 제공됩니다. 다음의 섀시 전면 그림은 센싱 인터페이스의 위치를 나타냅니다.

그림 4-7 3D7115, 3D7125 및 AMP7150 구리 및 SFP 인터페이스



1	구리 센싱 인터페이스	**2**	SFP 소켓

그림 4-8 4개의 1000BASE-T 구리 인터페이스 LED



1	링크 LED	**3**	바이패스 LED
2	활동 LED	**—**	—

구리 인터페이스를 사용하여 최대 4개의 개별 네트워크 세그먼트를 수동적으로 모니터링할 수 있습니다. 또한 쌍으로 연결된 인터페이스를 인라인 또는 바이패스 모드가 포함된 인라인으로 사용하여 최대 2개 네트워크에서 디바이스를 침입 방지 시스템으로 구축할 수 있습니다.

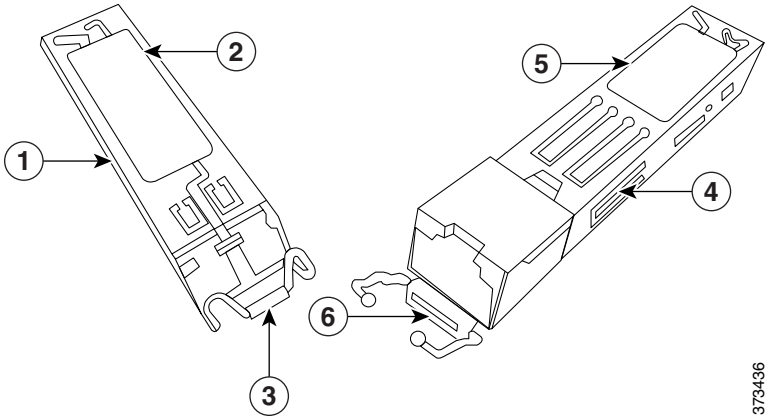
디바이스의 자동 바이패스 기능을 활용하려면 왼쪽에 있는 2개의 인터페이스 또는 오른쪽에 있는 2개의 인터페이스를 네트워크 세그먼트에 연결해야 합니다. 자동 바이패스 기능을 사용하면 디바이스에 장애 또는 정전이 발생하는 경우에도 트래픽이 이동할 수 있습니다. 인터페이스에 케이블을 연결한 다음에는 웹 인터페이스를 사용하여 인터페이스 쌍을 인라인 세트로 구성하고 인라인 세트에 바이패스 모드를 활성화합니다.

SFP 인터페이스

Cisco SFP 트렌시버를 SFP 소켓에 설치할 경우 최대 8개의 개별 네트워크 세그먼트를 수동적으로 모니터링할 수 있습니다. 또한 쌍으로 연결된 인터페이스를 비 바이패스 모드의 인라인으로 사용하여 최대 4개 네트워크에서 디바이스를 침입 탐지 시스템으로 구축할 수 있습니다.

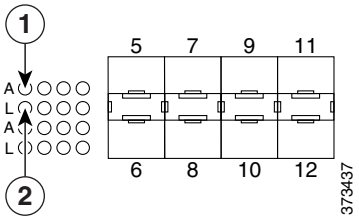
Cisco SFP 트렌시버는 1G 구리, 1G 단거리 파이버 또는 1G 장거리 파이버로 사용 가능하며 운영 중 교체할 수 없습니다. 수동 또는 인라인 컨피그레이션의 디바이스에 구리 또는 파이버 트렌시버를 임의로 조합하여 사용할 수 있습니다. SFP 트렌시버에는 바이패스 기능이 없으며 침입 방지 구축에 사용할 수 없습니다. 호환성을 보장하기 위해 Cisco의 SFP 트렌시버만 사용하십시오. 자세한 내용은 3D71x5 및 AMP7150 디바이스에서 SFP 트렌시버 사용, 페이지 B-1을(를) 참조하십시오.

그림 4-9 샘플 SFP 트렌시버



1	파이버 SFP 샘플	4	구리 SFP 샘플
2	접점이 있는 파이버 후면	5	접점이 있는 구리 후면
3	베일이 있는 파이버 전면	6	베일이 있는 구리 전면

그림 4-10 SFP 소켓



1	활동 LED	2	링크 LED

FirePOWER 8000 Series

8000 Series는 10G 네트워크 스위치가 포함된 1U 디바이스 또는 10G 또는 40G 네트워크 스위치가 포함된 2U 디바이스로 사용할 수 있습니다. 이 디바이스는 완전히 조립된 상태로 출고 가능하며 센싱 인터페이스가 포함된 네트워크 모듈(NetMod)을 설치할 수도 있습니다.

참고 디바이스의 호환되지 않는 슬롯에 NetMod를 설치할 경우(예: 40G NetMod를 3D8250 또는 3D8350의 슬롯 1 및 4에 삽입) 또는 NetMod가 다른 이유로 시스템과 호환되지 않는 경우 NetMod 구성을 시도하면 방어 센터 관리 웹 인터페이스에 오류 또는 경고 메시지가 나타납니다. 도움을 받으려면 고객 지원에 문의하십시오.

다음 모듈에는 바이패스 기능을 구성할 수 있는 센싱 인터페이스가 포함되어 있습니다.

- 구성 가능한 바이패스 기능이 포함된 쿼드 포트 1000BASE-T 구리 인터페이스
- 구성 가능한 바이패스 기능이 포함된 쿼드 포트 1000BASE-SX 파이버 인터페이스
- 구성 가능한 바이패스 기능이 포함된 듀얼 포트 10GBASE(MMSR 또는 SMLR) 파이버 인터페이스
- 구성 가능한 바이패스 기능이 포함된 듀얼 포트 40GBASE-SR4 파이버 인터페이스(2U 디바이스만 해당)

다음 모듈에는 비 바이패스 센싱 인터페이스가 포함되어 있습니다.

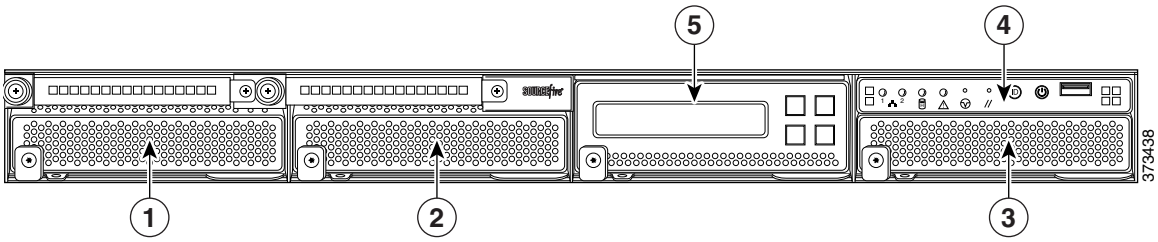
- 바이패스 기능이 없는 쿼드 포트 1000BASE-T 구리 인터페이스
- 바이패스 기능이 없는 쿼드 포트 1000BASE-SX 파이버 인터페이스
- 바이패스 기능이 없는 듀얼 포트 10GBASE(MMSR 또는 SMLR) 파이버 인터페이스

또한 스태킹 모듈은 2개 이상의 동일하게 구성된 어플라이언스의 리소스를 결합합니다. 스태킹 모듈은 3D8140, 3D8250 및 3D8350에서는 선택 사항이며 3D8260, 3D8270, 3D8290, 3D8360, 3D8370, 3D8390 및 AMP8350, AMP8360, AMP8370, AMP8390 스태킹 컨피그레이션에는 기본 제공됩니다.

주의 모듈은 운영 중 교체할 수 **없습니다**. 자세한 내용은 8000 Series 모듈 삽입 및 제거, 페이지 C-1을(를) 참조하십시오.

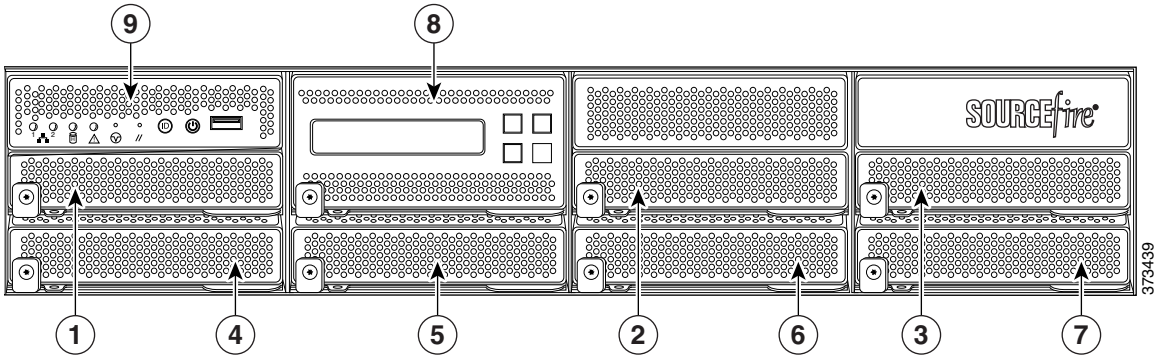
다음의 섀시 전면 그림은 센싱 인터페이스가 포함된 모듈 슬롯의 위치를 나타냅니다.

그림 4-11 81xx 제품군 섀시 전면 보기



1	모듈 슬롯 1	**4**	전면 패널
2	모듈 슬롯 2	**5**	LCD 패널
3	모듈 슬롯 3	**—**	—

그림 4-12 82xx 제품군 및 83xx 제품군 섀시 전면 보기



1	모듈 슬롯 1	**6**	모듈 슬롯 6
2	모듈 슬롯 2	**7**	모듈 슬롯 7
3	모듈 슬롯 3	**8**	LCD 패널
4	모듈 슬롯 4	**9**	전면 패널
5	모듈 슬롯 5	—	—

8000 Series 모듈

8000 Series에서는 구성 가능한 바이패스 기능을 포함하는 다음과 같은 모듈로 제공될 수 있습니다.

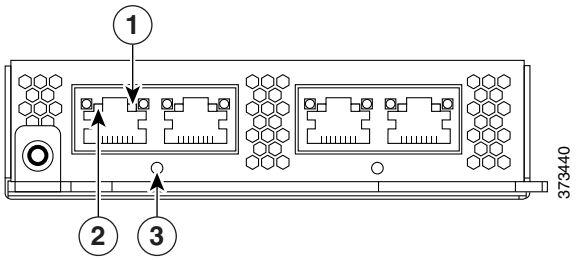
- 구성 가능한 바이패스 기능이 포함된 쿼드 포트 1000BASE-T 구리 인터페이스. 자세한 내용은 그림 4-13쿼드 포트 1000BASE-T 구리 바이패스 구성 가능 NetMod LED, 페이지 4-12을(를) 참조하십시오.
- 구성 가능한 바이패스 기능이 포함된 쿼드 포트 1000BASE-SX 파이버 인터페이스. 자세한 내용은 그림 4-14쿼드 포트 1000BASE-SX 파이버 바이패스 구성 가능 NetMod, 페이지 4-12을(를) 참조하십시오.
- 구성 가능한 바이패스 기능이 포함된 듀얼 포트 10GBASE(MMSR 또는 SMLR) 파이버 인터페이스. 자세한 내용은 그림 4-15듀얼 포트 10GBASE(MMSR 또는 SMLR) 파이버 바이패스 구성 가능 NetMod, 페이지 4-13을(를) 참조하십시오.
- 구성 가능한 바이패스 기능이 포함된 듀얼 포트 40GBASE-SR4 파이버 인터페이스. 자세한 내용은 그림 4-16듀얼 포트 40GBASE-SR4 파이버 바이패스 구성 가능 NetMod, 페이지 4-13을(를) 참조하십시오.

8000 Series는 구성 가능한 바이패스 기능이 없는 다음과 같은 모듈로 제공될 수 있습니다.

- 바이패스 기능이 없는 쿼드 포트 1000BASE-T 구리 인터페이스 자세한 내용은 그림 4-18쿼드 포트 1000BASE-T 구리 비 바이패스 NetMod LED, 페이지 4-14을(를) 참조하십시오.
- 바이패스 기능이 없는 쿼드 포트 1000BASE-SX 파이버 인터페이스. 자세한 내용은 그림 4-19 쿼드 포트 1000BASE-SX 파이버 비 바이패스 NetMod LED, 페이지 4-15을(를) 참조하십시오.
- 바이패스 기능이 없는 쿼드 포트 10GBASE(MMSR 또는 SMLR) 파이버 인터페이스. 자세한 내용은 그림 4-20쿼드 포트 10GBASE(MMSR 또는 SMLR) 파이버 비- 바이패스 NetMod, 페이지 4-15을(를) 참조하십시오.

스태킹 모듈은 3D8140, 3D8250 및 3D8350에서는 선택 사항이며 3D8260, 3D8270, 3D8290, 3D8360, 3D8370, 3D8390 및 AMP8350, AMP8360, AMP8370, AMP8390 스태킹 컨피그레이션에는 기본 제공됩니다. 자세한 내용은 8000 Series 스태킹 모듈, 페이지 4-16을(를) 참조하십시오.

그림 4-13 쿼드 포트 1000BASE-T 구리 바이패스 구성 가능 NetMod LED

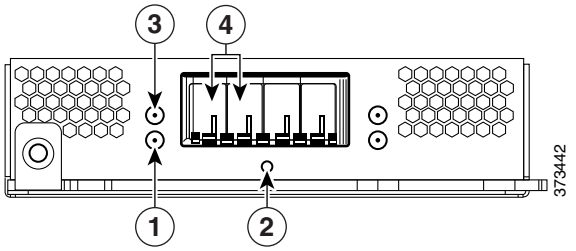


1	활동 LED	3	바이패스 LED
2	링크 LED	—	—

이러한 연결을 사용하여 최대 4개의 개별 네트워크 세그먼트를 수동적으로 모니터링할 수 있습니다. 또한 쌍으로 연결된 인터페이스를 인라인 또는 바이패스 모드가 포함된 인라인으로 사용하여 최대 2개 네트워크에서 디바이스를 침입 방지 시스템으로 구축할 수 있습니다.

디바이스의 자동 바이패스 기능을 활용하려면 왼쪽에 있는 2개의 인터페이스 또는 오른쪽에 있는 2개의 인터페이스를 네트워크 세그먼트에 연결해야 합니다. 이렇게 하면 디바이스에 장애 또는 정전이 발생하는 경우에도 트래픽이 이동할 수 있습니다. 또한 웹 인터페이스를 사용하여 인터페이스 쌍을 인라인 세트로 구성하고 인라인 세트에서 바이패스 모드를 활성화해야 합니다.

그림 4-14 쿼드 포트 1000BASE-SX 파이버 바이패스 구성 가능 NetMod



1	활동 LED	3	링크 LED
2	바이패스 LED	4	포트

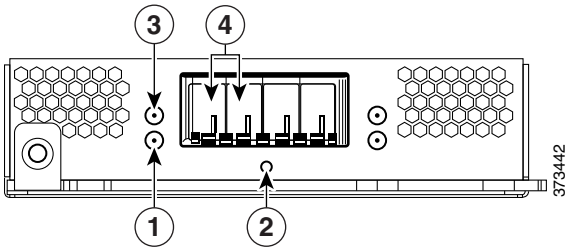
쿼드 포트 1000BASE-SX 파이버 바이패스 구성 가능 컨피그레이션은 LC 유형(로컬 커넥터)의 옵티컬 트렌시버를 사용합니다.

이 컨피그레이션을 사용하여 최대 4개의 개별 네트워크 세그먼트를 모니터링할 수 있습니다. 또한 쌍으로 연결된 인터페이스를 인라인 또는 바이패스 모드가 포함된 인라인으로 사용하여 최대 2개의 개별 네트워크에서 관리되는 디바이스를 침입 방지 시스템으로 구축할 수 있습니다.

정보 최고의 성능을 위해서는 인터페이스 세트를 연속적으로 사용합니다. 인터페이스를 생략할 경우 성능이 저하될 수 있습니다.

디바이스의 자동 바이패스 기능을 활용하려면 왼쪽에 있는 2개의 인터페이스 또는 오른쪽에 있는 2개의 인터페이스를 네트워크 세그먼트에 연결해야 합니다. 이렇게 하면 디바이스에 장애 또는 정전이 발생하는 경우에도 트래픽이 이동할 수 있습니다. 또한 웹 인터페이스를 사용하여 인터페이스 쌍을 인라인 세트로 구성하고 인라인 세트에서 바이패스 모드를 활성화해야 합니다.

그림 4-15 듀얼 포트 10GBASE(MMSR 또는 SMLR) 파이버 바이패스 구성 가능 NetMod



1	활동 LED	3	링크 LED
2	바이패스 LED	4	포트

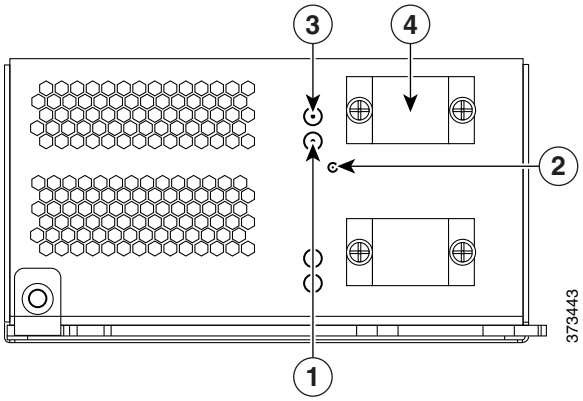
듀얼 포트 10GBASE 파이버 바이패스 구성 가능 컨피그레이션은 LC 유형(로컬 커넥터)의 옵티컬 트렌시버를 사용합니다. 이러한 컨피그레이션에서는 MMSR 또는 SMLR 인터페이스를 사용합니다.

이 컨피그레이션을 사용하여 최대 2개의 개별 네트워크 세그먼트를 수동적으로 모니터링할 수 있습니다. 또한 쌍으로 연결된 인터페이스를 인라인 또는 바이패스 모드가 포함된 인라인으로 사용하여 단일 네트워크에서 관리되는 디바이스를 침입 방지 시스템으로 구축할 수 있습니다.

정보 최고의 성능을 위해서는 인터페이스 세트를 연속적으로 사용합니다. 인터페이스를 생략할 경우 성능이 저하될 수 있습니다.

디바이스의 자동 바이패스 기능을 활용하려면 2개의 인터페이스를 네트워크 세그먼트에 연결해야 합니다. 이렇게 하면 디바이스에 장애 또는 정전이 발생하는 경우에도 트래픽이 이동할 수 있습니다. 또한 웹 인터페이스를 사용하여 인터페이스 쌍을 인라인 세트로 구성하고 인라인 세트에서 바이패스 모드를 활성화해야 합니다.

그림 4-16 듀얼 포트 40GBASE-SR4 파이버 바이패스 구성 가능 NetMod



1	링크 LED	3	활동 LED
2	바이패스 LED	4	포트

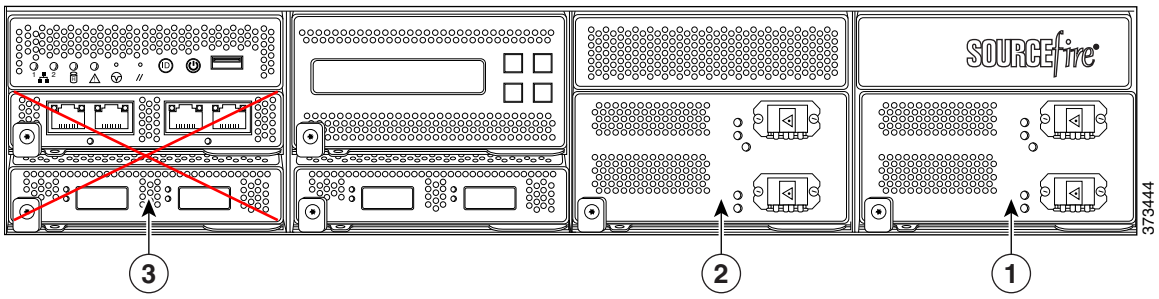
듀얼 포트 40GBASE-SR4 파이버 바이패스 구성 가능 컨피그레이션에서는 MPO(Multiple-Fiber Push On) 커넥터 옵티컬 트렌시버를 사용합니다.

40G NetMod는 3D8270, 3D8290, 3D8360, 3D8370, 3D8390 또는 40G 지원 3D8250, 3D8260, 3D8350에서만 사용할 수 있습니다. 40G를 지원하지 않는 디바이스에 40G 인터페이스를 생성하려고 시도하면 관리 방어 센터 웹 인터페이스의 40G 인터페이스 화면이 빨간색으로 표시됩니다. 40G를 지원하는 3D8250의 경우 LCD 패널에 "3D 8250-40G"가 표시되고 40G를 지원하는 3D8350의 경우에는 LCD 패널에 "3D 8350-40G"가 표시됩니다.

이 컨피그레이션을 사용하여 최대 2개의 개별 네트워크 세그먼트를 수동적으로 모니터링할 수 있습니다. 또한 쌍으로 연결된 인터페이스를 인라인 또는 바이패스 모드가 포함된 인라인으로 사용하여 단일 네트워크에서 디바이스를 침입 방지 시스템으로 구축할 수 있습니다.

최대 2개의 40G NetMod를 사용할 수 있습니다. 첫 번째 40G NetMod를 슬롯 3 및 7에 설치하고 두 번째는 슬롯 2 및 6에 설치합니다. 슬롯 1 및 4에서는 40G NetMod를 사용할 수 없습니다.

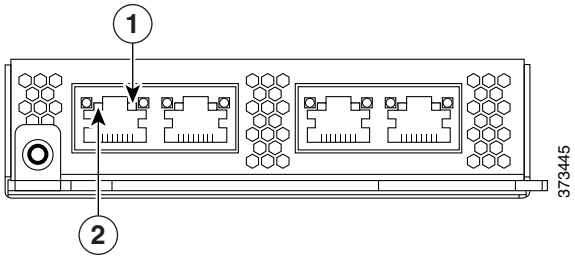
그림 4-17 40G NetMod 배치



1	첫 번째 40G NetMod	3	40G NetMod에 사용할 수 없음
2	두 번째 40G NetMod	—	—

디바이스의 자동 바이패스 기능을 활용하려면 웹 인터페이스를 사용하여 인터페이스 쌍을 인라인 세트로 구성하고 인라인 세트에서 바이패스 모드를 활성화해야 합니다.

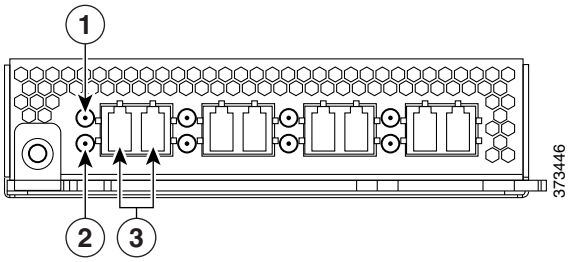
그림 4-18 쿼드 포트 1000BASE-T 구리 비 바이패스 NetMod LED



1	활동 LED	2	링크 LED

이러한 연결을 사용하여 최대 4개의 개별 네트워크 세그먼트를 수동적으로 모니터링할 수 있습니다. 또한 최대 2개의 네트워크 세그먼트에서 쌍으로 연결된 인터페이스를 인라인 컨피그레이션으로 사용할 수 있습니다.

그림 4-19 쿼드 포트 1000BASE-SX 파이버 비 바이패스 NetMod LED



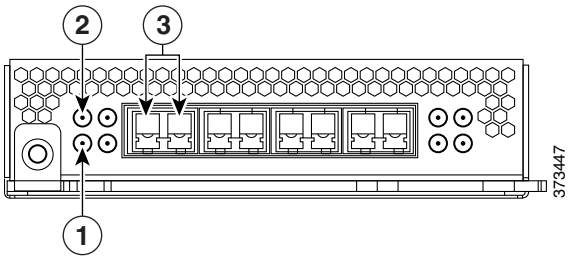
1	활동 LED	3	포트
2	링크 LED	—	—

쿼드 포트 1000BASE-SX 파이버 비 바이패스 컨피그레이션에서는 LC 유형(로컬 커넥터)의 옵티컬 트렌시버를 사용합니다.

이러한 연결을 사용하여 최대 4개의 개별 네트워크 세그먼트를 수동적으로 모니터링할 수 있습니다. 또한 최대 2개의 네트워크 세그먼트에서 쌍으로 연결된 인터페이스를 인라인 컨피그레이션으로 사용할 수 있습니다.

정보 최고의 성능을 위해서는 인터페이스 세트를 연속적으로 사용합니다. 인터페이스를 생략할 경우 성능이 저하될 수 있습니다.

그림 4-20 쿼드 포트 10GBASE(MMSR 또는 SMLR) 파이버 비- 바이패스 NetMod



1	활동 LED	3	포트
2	링크 LED	—	—

쿼드 포트 10GBASE 파이버 비 바이패스 컨피그레이션에서는 MMSR 또는 SMLR 인터페이스로 LC 유형(로컬 커넥터)의 옵티컬 트렌시버를 사용합니다.

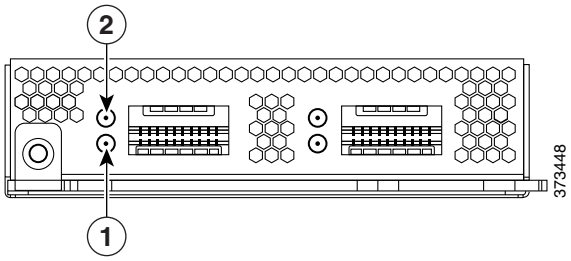
주의 쿼드 포트 10G BASE 비 바이패스 NetMod에는 제거할 수 없는 SFP(Small Form-Factor Pluggable) 트렌시버가 포함되어 있습니다. SFP 제거를 시도할 경우 모듈이 손상될 수 있습니다.

이러한 연결을 사용하여 최대 4개의 개별 네트워크 세그먼트를 수동적으로 모니터링할 수 있습니다. 또한 최대 2개의 네트워크 세그먼트에서 쌍으로 연결된 인터페이스를 인라인 컨피그레이션으로 사용할 수 있습니다.

정보 최고의 성능을 위해서는 인터페이스 세트를 연속적으로 사용합니다. 인터페이스를 생략할 경우 성능이 저하될 수 있습니다.

8000 Series 스태킹 모듈

스태킹 모듈은 2개 이상의 동일하게 구성된 어플라이언스의 리소스를 결합합니다. 스태킹 모듈은 3D8140, 3D8250 및 3D8350에서는 선택 사항이며 3D8260, 3D8270, 3D8290, 3D8360, 3D8370, 3D8390 및 AMP8350, AMP8360, AMP8370, AMP8390 스태킹 컨피그레이션에는 기본 제공됩니다.



1	링크 LED	2	활동 LED

스태킹 모듈에서는 하나는 기본 디바이스를 사용하고 다른 하나는 보조 디바이스로 사용하여 두 디바이스의 리소스를 결합할 수 있습니다. 기본 디바이스에만 센싱 인터페이스가 있습니다. 다음 디바이스는 스태킹 모듈을 사용할 수 있습니다.

- 3D8140, 3D8250, 3D8350 및 AMP8350은 스태킹 모듈과 함께 제공될 수 있습니다.
- 3D8260, 3D8360 및 AMP8360의 경우에는 기본 디바이스에 하나의 스태킹 모듈이 있고 보조 디바이스에 하나의 스태킹 모듈이 있습니다.
- 3D8270, 3D8370 및 AMP8370의 경우에는 기본 디바이스에 2개의 스태킹 모듈이 있고 2개의 보조 디바이스 각각에 하나의 스태킹 모듈이 있습니다.
- 3D8290, 3D8390 및 AMP8390의 경우에는 기본 디바이스에 3개의 스태킹 모듈이 있고 3개의 보조 디바이스 각각에 하나의 스태킹 모듈이 있습니다.

스태킹된 디바이스 사용에 대한 자세한 내용은 스태킹 컨피그레이션에서 디바이스 사용을 참조하십시오.

스태킹 컨피그레이션에서 디바이스 사용

스태킹 컨피그레이션에서 동일하게 구성된 디바이스의 리소스를 결합하여 네트워크 세그먼트에서 검사되는 트래픽의 양을 늘릴 수 있습니다. 하나의 디바이스는 기본 디바이스로 지정되며 네트워크 세그먼트에 연결됩니다. 나머지 다른 디바이스는 보조 디바이스로 지정되며 기본 디바이스에 추가 리소스를 제공하는 데 사용됩니다. 방어 센터에서는 스태킹 컨피그레이션을 만들고 편집 및 관리합니다.

기본 디바이스에는 센싱 인터페이스가 있으며 여기에 연결된 각 보조 디바이스마다 하나의 스태킹 인터페이스 세트가 있습니다. 기본 디바이스의 센싱 인터페이스를 스태킹되지 않은 디바이스와 동일한 방법으로 모니터링하려는 네트워크 세그먼트에 연결합니다. 스태킹 케이블을 사용하여 기본 디바이스의 스태킹 인터페이스를 보조 디바이스의 스태킹 인터페이스에 연결합니다. 각 보조 디바이스는 스태킹 인터페이스를 사용하여 기본 디바이스에 직접 연결됩니다. 조 디바이스에 센싱 인터페이스가 포함된 경우 해당 인터페이스는 사용되지 않습니다.

다음 컨피그레이션으로 디바이스를 스태킹할 수 있습니다.

- 2개의 3D8140
- 최대 4개의 3D8250
- 3D8260(하나의 10G 지원 기본 디바이스 및 하나의 보조 디바이스)

- 3D8270(하나의 40G 지원 기본 디바이스 및 2개의 보조 디바이스)
- 3D8290(하나의 40G 지원 기본 디바이스 및 3개의 보조 디바이스)
- 최대 4개의 3D8350
- 최대 4개의 AMP8350
- 3D8360(하나의 40G 지원 기본 디바이스 및 하나의 보조 디바이스)
- AMP8360(하나의 40G 지원 기본 디바이스 및 하나의 보조 디바이스)
- 3D8370(하나의 40G 지원 기본 디바이스 및 2개의 보조 디바이스)
- AMP8370(하나의 40G 지원 기본 디바이스 및 2개의 보조 디바이스)
- 3D8390(하나의 40G 지원 기본 디바이스 및 3개의 보조 디바이스)
- AMP8390(하나의 40G 지원 기본 디바이스 및 3개의 보조 디바이스)

3D8260, 3D8270, 3D8360, 3D8370, AMP8360, AMP8370의 경우 스택에서 총 4개의 디바이스까지 추가로 디바이스를 스태킹할 수 있습니다.

하나의 디바이스가 기본 디바이스로 지정되며 방어 센터의 웹 인터페이스에 기본 역할과 함께 표시됩니다. 스태킹 컨피그레이션의 나머지 다른 디바이스는 보조 디바이스로 보조 역할과 함께 웹 인터페이스에 표시됩니다. 스태킹된 디바이스의 정보를 보는 경우를 제외하고, 결합된 리소스를 단일 엔티티로 사용합니다.

기본 디바이스를 단일 3D8140, 3D8250, 3D8350 또는 AMP8350을 연결할 때와 동일한 방식으로 분석하려는 네트워크 세그먼트에 연결합니다. 보조 디바이스를 스택 케이블링 다이어그램에 따라 기본 디바이스에 연결합니다.

주의 **반드시** 관리 인터페이스가 구성되고 모든 디바이스 스택 멤버에 대해 작동 중이어야 합니다. 모든 디바이스를 단일 디바이스로 등록하고 스태킹한 후 스태킹된 보조 디바이스에 대한 관리 인터페이스를 제거하거나 비활성화지 마십시오. 이렇게 하면 각 스택 멤버가 상태를 보고하고 컨피그레이션 정보를 교환할 수 있습니다.

디바이스를 네트워크 세그먼트 및 디바이스 상호 간에 물리적으로 연결한 다음 방어 센터를 사용하여 스택을 구축 및 관리합니다.

다음 섹션에서는 스태킹된 디바이스를 연결 및 관리하는 방법에 대해 자세히 설명합니다.

- 3D8140 연결, 페이지 4-17
- 82xx 제품군 및 83xx 제품군 연결, 페이지 4-18
- 8000 Series 스태킹 케이블 사용, 페이지 4-22
- 스태킹된 디바이스 관리, 페이지 4-22

3D8140 연결

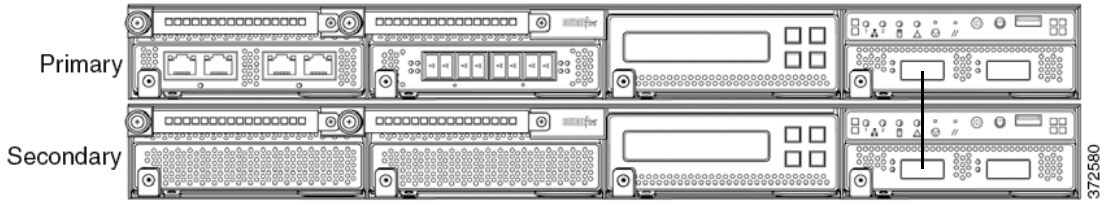
스태킹 컨피그레이션에서 2개의 3D8140을 연결할 수 있습니다. 하나의 8000 Series 스태킹 케이블을 사용하여 기본 디바이스와 보조 디바이스를 물리적으로 연결해야 합니다. 스태킹 케이블 사용에 대한 자세한 내용은 8000 Series 스태킹 케이블 사용, 페이지 4-22을(를) 참조하십시오.

스태킹 모듈 간에 케이블을 쉽게 연결할 수 있도록 디바이스를 랙에 설치합니다. 기본 디바이스의 위 또는 아래에 보조 디바이스를 설치할 수 있습니다.

기본 디바이스를 단일 3D8140을 연결할 때와 동일한 방식으로 분석하려는 네트워크 세그먼트에 연결합니다. 보조 디바이스를 기본 디바이스에 직접 연결합니다.

주의 **반드시** 관리 인터페이스가 구성되고 모든 디바이스 스택 멤버에 대해 작동 중이어야 합니다. 모든 디바이스를 단일 디바이스로 등록하고 스태킹한 후 스태킹된 보조 디바이스에 대한 관리 인터페이스를 제거하거나 비활성화지 마십시오. 이렇게 하면 각 스택 멤버가 상태를 보고하고 컨피그레이션 정보를 교환할 수 있습니다.

다음 그림은 기본 디바이스와 기본 디바이스 아래 설치된 보조 디바이스를 보여줍니다.



3D8140 보조 디바이스를 연결하려면 다음을 수행합니다.

단계 1 8000 Series 스태킹 케이블을 사용하여 기본 디바이스의 스태킹 인터페이스를 보조 디바이스의 왼쪽 스태킹 인터페이스에 연결한 다음 디바이스를 관리하는 방어 센터를 사용하여 시스템에 스태킹된 디바이스 관계를 구축합니다. 오른쪽 스태킹 인터페이스는 연결하지 않습니다. 스태킹된 디바이스 관리, 페이지 4-22을(를) 참조하십시오.

참고 **반드시** 관리 인터페이스가 구성되고 모든 디바이스 스택 멤버에 대해 작동 중이어야 합니다. 모든 디바이스를 단일 디바이스로 등록하고 스태킹한 후 스태킹된 보조 디바이스에 대한 관리 인터페이스를 제거하거나 비활성화지 마십시오. 이렇게 하면 각 스택 멤버가 상태를 보고하고 컨피그레이션 정보를 교환할 수 있습니다.

82xx 제품군 및 83xx 제품군 연결

다음 컨피그레이션을 연결할 수 있습니다.

- 최대 4개의 3D8250
- 최대 4개의 3D8350 또는 4개의 AMP8350
- 3D8260(하나의 10G 지원 기본 디바이스 및 하나의 보조 디바이스)
- 3D8360 또는 AMP8360(하나의 40G 지원 기본 디바이스 및 하나의 보조 디바이스)
- 3D8270(하나의 40G 지원 기본 디바이스 및 2개의 보조 디바이스)
- 3D8370 또는 AMP8370(하나의 40G 지원 기본 디바이스 및 2개의 보조 디바이스)
- 3D8290(하나의 40G 지원 기본 디바이스 및 3개의 보조 디바이스)
- 3D8390 또는 AMP8390(하나의 40G 지원 기본 디바이스 및 3개의 보조 디바이스)

3D8260, 3D8270, 3D8360, 3D8370, AMP8360 및 AMP8370의 경우 스택에서 총 4개의 디바이스까지 추가로 디바이스를 스태킹할 수 있습니다.

기본 디바이스에 연결하려는 각각의 보조 디바이스에 2개의 8000 Series 스태킹 케이블을 사용해야 합니다. 스태킹 케이블 사용에 대한 자세한 내용은 8000 Series 스태킹 케이블 사용, 페이지 4-22을(를) 참조하십시오.

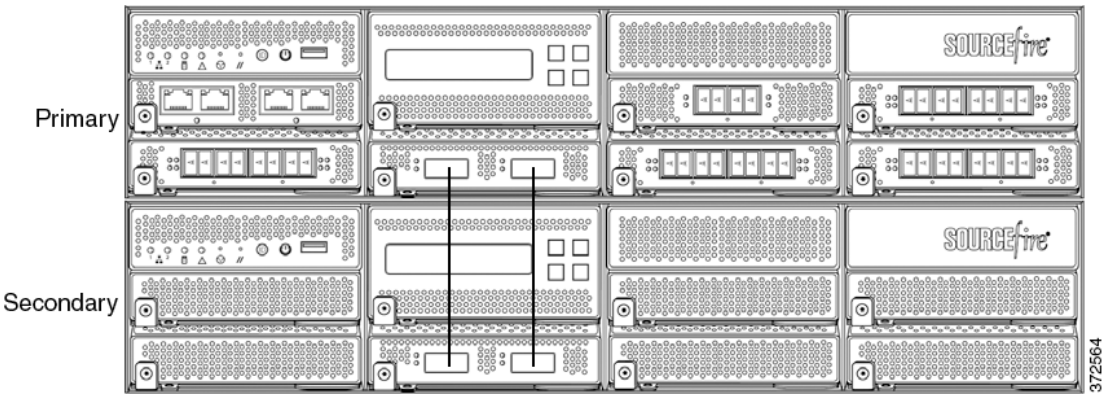
스태킹 모듈 간에 케이블을 쉽게 연결할 수 있도록 디바이스를 랙에 설치합니다. 기본 디바이스의 위 또는 아래에 보조 디바이스를 설치할 수 있습니다.

기본 디바이스를 단일 3D8250, 3D8350 또는 AMP8350을 연결할 때와 동일한 방식으로 분석하려는 네트워크 세그먼트에 연결합니다. 컨피그레이션의 보조 디바이스 수에 필요한 대로 각 보조 디바이스를 기본 디바이스에 직접 연결합니다.

주의 **반드시** 관리 인터페이스가 구성되고 모든 디바이스 스택 멤버에 대해 작동 중이어야 합니다. 모든 디바이스를 단일 디바이스로 등록하고 스태킹한 후 스태킹된 보조 디바이스에 대한 관리 인터페이스를 제거하거나 비활성화지 마십시오. 이렇게 하면 각 스택 멤버가 상태를 보고하고 컨피그레이션 정보를 교환할 수 있습니다.

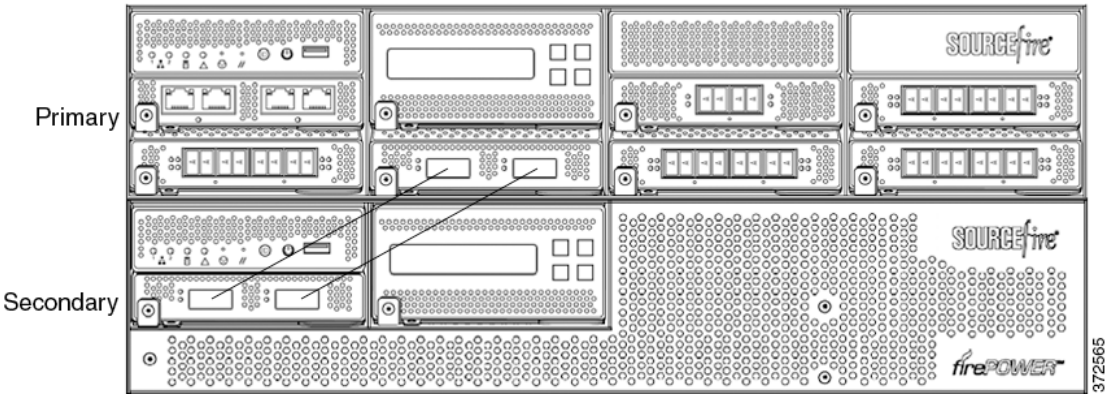
3D8250, 3D8350 또는 AMP8350 기본 디바이스 및 하나의 보조 디바이스

다음 예는 3D8250, 3D8350 또는 AMP8350 기본 디바이스와 하나의 보조 디바이스를 보여줍니다. 보조 디바이스는 기본 디바이스 아래에 설치됩니다. 보조 디바이스에는 센싱 인터페이스가 없습니다.



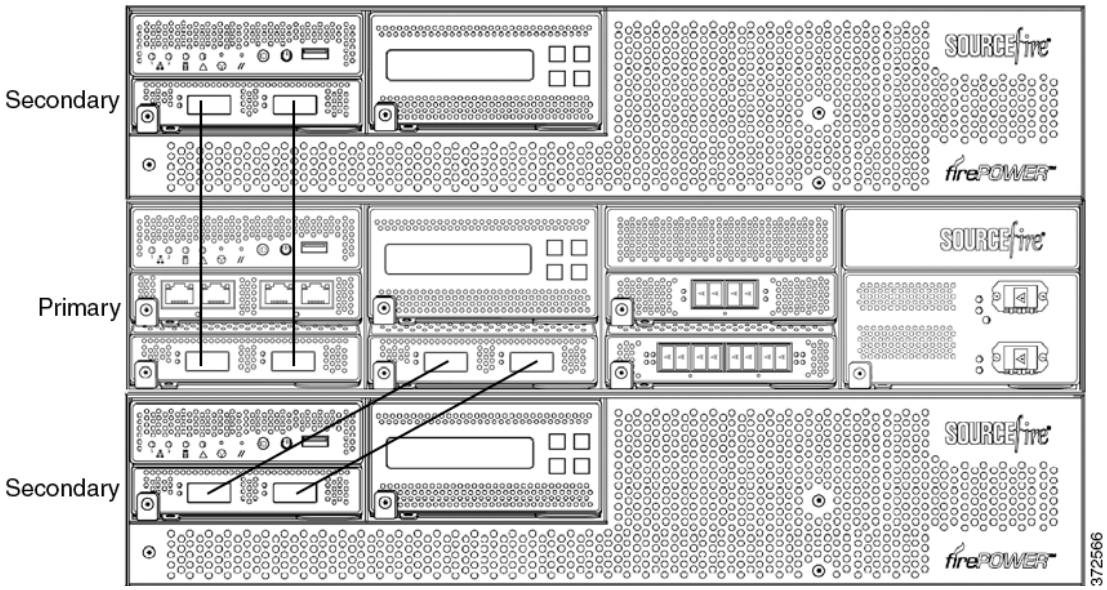
3D8260, 3D8360 또는 AMP8360 기본 디바이스 및 하나의 보조 디바이스

다음 예는 3D8260, 3D8360 또는 AMP8360 컨피그레이션을 보여줍니다. 3D8260에는 하나의 10G 지원 3D8250 기본 디바이스와 하나의 전용 보조 디바이스가 포함됩니다. AMP8360에는 하나의 40G 지원 AMP8350 기본 디바이스와 하나의 전용 보조 디바이스가 포함됩니다. 각 컨피그레이션(3D8260, 3D8360 또는 AMP8360)에서 보조 디바이스는 기본 디바이스 아래에 설치됩니다.



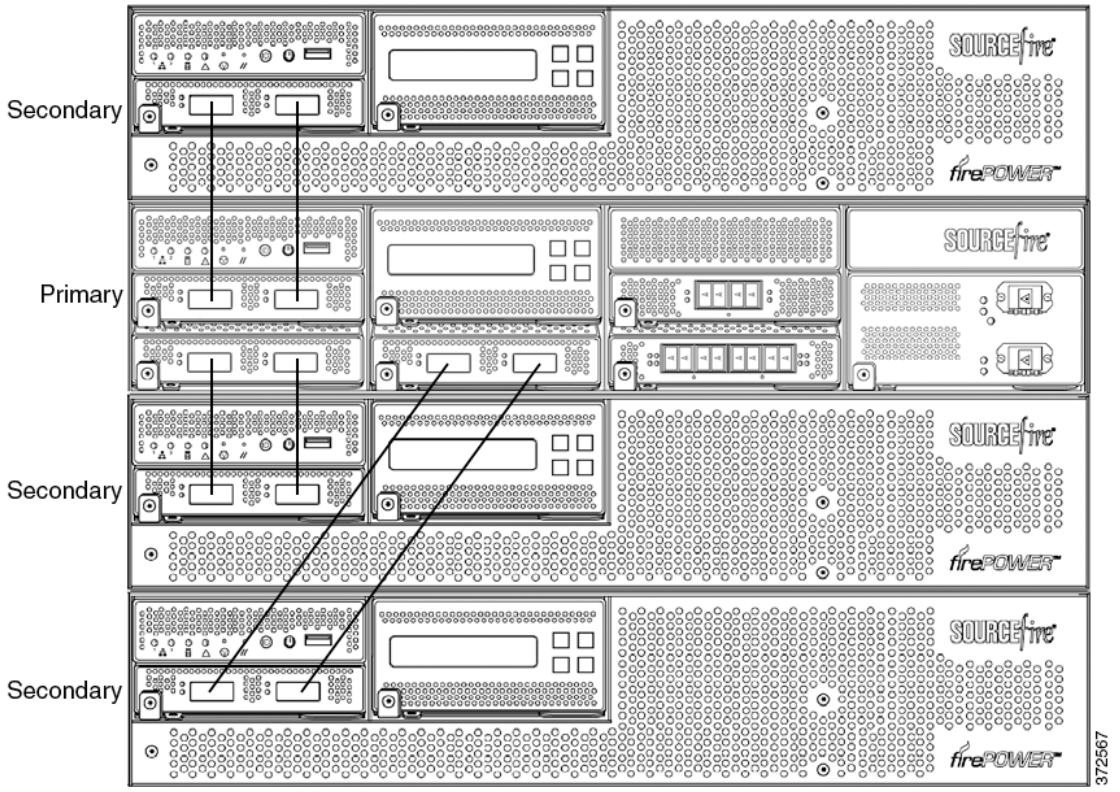
3D8270, 3D8370 또는 AMP8370 기본 디바이스(40G) 및 2개의 보조 디바이스

다음 예는 3D8270, 3D8370 또는 AMP8370 컨피그레이션을 보여줍니다. 3D8270에는 하나의 40G 지원 3D8250 기본 디바이스와 2개의 전용 보조 디바이스가 포함됩니다. 3D8370에는 하나의 40G 지원 3D8350 기본 디바이스와 2개의 전용 보조 디바이스가 포함됩니다. AMP8370에는 하나의 40G 지원 AMP8350 기본 디바이스와 2개의 전용 보조 디바이스가 포함됩니다. 각 컨피그레이션(3D8270, 3D8370 또는 AMP8370)에서 하나의 보조 디바이스가 기본 디바이스 위에 설치되고 나머지는 기본 디바이스 아래에 설치됩니다.



3D8290, 3D8390 또는 AMP8390 기본 디바이스(40G) 및 3개의 보조 디바이스

다음 예는 3D8290, 3D8390 또는 AMP8390 컨피그레이션을 보여줍니다. 3D8290에는 하나의 40G 지원 3D8250 기본 디바이스와 3개의 전용 보조 디바이스가 포함됩니다. 3D8370에는 하나의 40G 지원 3D8350 기본 디바이스와 2개의 전용 보조 디바이스가 포함됩니다. AMP8370에는 하나의 40G 지원 AMP8350 기본 디바이스와 2개의 전용 보조 디바이스가 포함됩니다. 각 컨피그레이션(3D8290, 3D8390 또는 AMP8390)에서 하나의 보조 디바이스가 기본 디바이스 위에 설치되고 2개의 보조 디바이스는 기본 디바이스 아래에 설치됩니다.



3D8250, 3D8350 또는 AMP8350 보조 디바이스를 연결하려면 다음을 수행합니다.

단계 1 8000 Series 스태킹 케이블을 사용하여 기본 디바이스의 스태킹 모듈에 있는 왼쪽 인터페이스를 보조 디바이스의 스태킹 모듈에 있는 왼쪽 인터페이스에 연결합니다.

단계 2 두 번째 8000 Series 스태킹 케이블을 사용하여 기본 디바이스의 스태킹 모듈에 있는 오른쪽 인터페이스를 보조 디바이스의 스태킹 모듈에 있는 오른쪽 인터페이스에 연결합니다.

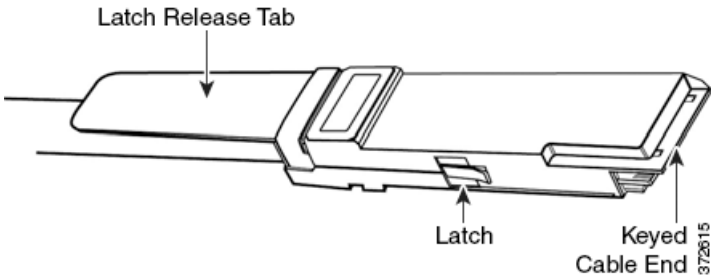
단계 3 연결하려는 각 보조 디바이스에 대해 1단계 및 2단계를 반복합니다.

단계 4 디바이스를 관리하는 방어 센터를 사용하여 스태킹된 디바이스 관계를 구축하고 결합 리소스를 관리합니다. 스태킹된 디바이스 관리, 페이지 4-22을(를) 참조하십시오.

참고 **반드시** 관리 인터페이스가 구성되고 모든 디바이스 스택 멤버에 대해 작동 중이어야 합니다. 모든 디바이스를 단일 디바이스로 등록하고 스태킹한 후 스태킹된 보조 디바이스에 대한 관리 인터페이스를 제거하거나 비활성화지 마십시오. 이렇게 하면 각 스택 멤버가 상태를 보고하고 컨피그레이션 정보를 교환할 수 있습니다.

8000 Series 스태킹 케이블 사용

8000 Series 스태킹 케이블의 끝부분은 동일한 모양의 돌출부로 되어 있으며 각각에는 디바이스의 케이블을 고정하기 위한 래치와 래치 해제 탭이 있습니다.



8000 Series 스태킹 케이블을 사용하여 각 디바이스 컨피그레이션에 필요한 대로 기본 디바이스와 각 보조 디바이스를 물리적으로 연결합니다.

- 3D8140에는 하나의 케이블이 필요함
- 3D8250, 3D8260, 3D8270 및 3D8290에는 연결당 2개의 케이블이 필요함
- 3D8350, 3D8360, 3D8370 및 3D8390에는 연결당 2개의 케이블이 필요함
- AMP8350, AMP8360, AMP8370 및 AMP8390에는 연결당 2개의 케이블이 필요함

스태킹 케이블을 삽입 또는 제거하기 위해 디바이스 전원을 끄지 않아도 됩니다.

주의 디바이스에 케이블을 연결할 때는 Cisco 8000 Series 스태킹 케이블만 사용합니다. 지원되지 않는 케이블을 사용할 경우 예측할 수 없는 오류가 발생할 수 있습니다.

디바이스를 물리적으로 연결한 다음 방어 센터를 사용하여 스태킹된 디바이스를 관리합니다.

8000 Series 스태킹 케이블을 삽입하려면 다음을 수행합니다.

단계 1 케이블을 삽입하려면 릴리스 탭을 위로 한 상태에서 케이블 끝부분을 손으로 잡은 다음 래치가 딸각 소리가 나며 제자리에 고정될 때까지 돌출된 끝부분을 스태킹 모듈의 포트에 삽입합니다.

8000 Series 스태킹 케이블을 제거하려면 다음을 수행합니다.

단계 1 케이블을 제거하려면 릴리스 탭을 당겨 래치를 해제한 다음 케이블 끝부분을 제거합니다.

스태킹된 디바이스 관리

방어 센터에서는 디바이스 간 스태킹 관계를 구축하고 기본 디바이스의 인터페이스 세트를 제어하며 스택의 결합된 리소스를 관리합니다. 스태킹된 디바이스의 로컬 웹 인터페이스에서 인터페이스 세트를 관리할 수 없습니다.

스태킹 관계가 구축되면 각 디바이스에서 하나의 공유된 탐지 컨피그레이션을 사용하여 트래픽을 개별적으로 검사합니다. 기본 디바이스에 장애가 발생할 경우 트래픽은 기본 디바이스의 컨피그레이션에 따라 처리됩니다(즉, 스태킹 관계가 없는 것처럼). 보조 디바이스에 장애가 발생할 경우 기본 디바이스가 계속해서 트래픽을 감지하고 경고를 발생하며 트래픽이 삭제된 위치에서 장애가 발생한 보조 디바이스로 트래픽을 전송합니다.

주의 **반드시** 관리 인터페이스가 구성되고 모든 디바이스 스택 멤버에 대해 작동 중이어야 합니다. 모든 디바이스를 단일 디바이스로 등록하고 스태킹한 후 스태킹된 보조 디바이스에 대한 관리 인터페이스를 제거하거나 비활성화지 마십시오. 이렇게 하면 각 스택 멤버가 상태를 보고하고 컨피그레이션 정보를 교환할 수 있습니다.

스태킹된 디바이스의 구축 및 관리에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*의 스태킹된 디바이스 관리를 참조하십시오.

랙에 어플라이언스 설치

FireSIGHT System은 다른 하드웨어 플랫폼에 제공됩니다. 모든 FireSIGHT System 어플라이언스를 랙에 장착할 수 있습니다(3D7010, 3D7020, 3D7030 및 3D7050용 1U 마운팅 키트 구매 시). 어플라이언스를 설치할 때는 어플라이언스 콘솔에 액세스할 수 있는지 확인해야 합니다. 초기 설정을 위해 콘솔에 액세스하려면 다음 중 한 가지 방법으로 FireSIGHT System에 연결합니다.

키보드 및 모니터/KVM

USB 키보드와 VGA 모니터를 FireSIGHT System 어플라이언스에 연결할 수 있습니다. 이는 키보드, 비디오 및 마우스(KVM) 스위치에 연결된 랙 마운트 어플라이언스에 유용합니다.

주의 어플라이언스에서 대용량 스토리지 디바이스를 부팅 디바이스로 사용하려고 시도할 수 있으므로 초기 설정을 위해 어플라이언스에 액세스하는 데 USB 대용량 스토리지가 있는 KVM 콘솔을 사용하지 **마십시오**.

관리 인터페이스에 대한 이더넷 연결

다음 네트워크 설정을 사용하여 로컬 컴퓨터를 구성합니다. 이 컴퓨터는 인터넷에 연결되어서는 안 됩니다.

- IP 주소: `192.168.45.2`
- 넷마스크: `255.255.255.0`
- 기본 게이트웨이: `192.168.45.1`

이더넷 케이블을 사용하여 로컬 컴퓨터의 네트워크 인터페이스를 어플라이언스의 관리 인터페이스에 연결합니다. 어플라이언스와 상호 작용하려면 HyperTerminal이나 XModem 등의 터미널 에뮬레이션 소프트웨어를 사용합니다. 이 소프트웨어에 대한 설정은 다음과 같습니다.

- 9600보드
- 8 데이터 비트
- 패리티 검사 없음
- 1 스톱 비트
- 흐름 제어 없음

물리적 FireSIGHT System 어플라이언스의 관리 인터페이스는 기본 IPv4 주소로 사전 구성됩니다. 하지만 설정 프로세스의 일부로 관리 인터페이스를 IPv6 주소로 다시 구성할 수 있습니다.

초기 설정 후에는 다음과 같은 추가 방법으로 콘솔에 액세스할 수 있습니다.

시리얼 연결/노트북 컴퓨터

물리적 시리얼 포트를 사용하여 3D2100/2500/3500/4500 디바이스를 제외한 모든 FireSIGHT System 어플라이언스에 컴퓨터를 연결할 수 있습니다. 언제든지 적절한 롤오버 시리얼 케이블(NULL 모뎀 케이블 또는 Cisco 콘솔 케이블이라고도 함)을 연결한 다음 원격 관리 콘솔에서 기본 VGA 출력을 시리얼 포트로 리디렉션하도록 구성합니다. 어플라이언스와 상호 작용하려면 위의 설명과 같이 터미널 에뮬레이션 소프트웨어를 사용합니다.

시리얼 포트에는 어플라이언스에 따라 RJ-45 연결 또는 DB-9 연결이 가능합니다. 어플라이언스별 커넥터는 다음 표를 참조하십시오.

표 4-1 모델별 시리얼 커넥터

어플라이언스	커넥터
3D500, 3D1000, 3D2000	DB-9(암)
3D6500	RJ-45
Series 3 방어 센터	RJ-45
3D70xx 제품군	RJ-45
3D71xx 제품군	DB-9(암)
3D8000 Series 및 AMP8000 Series	RJ-45
3D9900	RJ-45

적절한 롤오버 케이블을 디바이스에 연결한 다음 콘솔 출력 리디렉션, 페이지 4-26의 설명에 따라 콘솔 출력을 리디렉션합니다. 각 어플라이언스의 시리얼 포트를 찾으려면 하드웨어 사양, 페이지 7-1의 다이어그램을 사용합니다.

SOL(Serial over LAN)을 사용한 LOM(Lights-Out Management)

LOM 기능을 사용하면 SOL 연결을 사용하여 Series 3 어플라이언스에 대해 제한적인 작업을 실행할 수 있습니다. LOM 지원 어플라이언스를 출고 시 기본값으로 복원해야 하고 어플라이언스에 대한 물리적 액세스가 없는 경우 LOM을 사용하여 복원 프로세스를 수행할 수 있습니다. LOM을 사용하여 어플라이언스에 연결한 다음 물리적 시리얼 연결을 사용하는 것처럼 복원 유틸리티에 명령을 실행합니다. 자세한 내용은 LOM(Lights-Out Management) 설정, 페이지 8-18을(를) 참고하십시오.

참고 기본(`eth0`) 관리 인터페이스에서만 LOM(Lights-Out Management) 관리를 사용할 수 있습니다.

LOM을 사용하여 어플라이언스를 출고 시 설정으로 복원하려면 네트워크 설정을 삭제하지 **마십시오**. 네트워크 설정을 삭제할 경우 LOM 연결도 끊어집니다. 자세한 내용은 FireSIGHT System 어플라이언스를 출고 시 기본 설정으로 복원, 페이지 8-1을(를) 참고하십시오.

어플라이언스를 설치하려면 다음을 수행합니다.

단계 1 마운팅 키트를 사용하고 제공된 지침에 따라 어플라이언스를 랙에 장착합니다.

단계 2 키보드와 모니터 또는 이더넷 연결을 사용하여 어플라이언스를 연결합니다.

단계 3 키보드와 모니터를 사용하여 어플라이언스를 설정하는 경우 이제 이더넷 케이블을 사용하여 관리 인터페이스를 보호된 네트워크 세그먼트에 연결합니다.

컴퓨터를 어플라이언스의 물리적 관리 인터페이스에 직접 연결하여 초기 설정 프로세스를 수행하려는 경우 설정을 마친 다음 관리 인터페이스를 보호된 네트워크에 연결합니다.

단계 4 관리되는 디바이스의 경우 인터페이스에 적절한 케이블을 사용하여 센싱 인터페이스를 분석하려는 네트워크 세그먼트에 연결합니다.

- 구리 센싱 인터페이스: 디바이스에 구리 센싱 인터페이스가 포함된 경우 적절한 케이블을 사용하여 네트워크에 연결합니다. 구리 인터페이스의 인라인 구축 케이블링, 페이지 3-6을(를) 참조하십시오.
- 파이버 어댑터 카드: 파이버 어댑터 카드가 있는 디바이스의 경우 선택적인 멀티 모드 파이버 케이블의 LC 커넥터를 어댑터 카드에 있는 2개의 포트에 임의 순서로 연결합니다. SC 플러그를 분석하려는 네트워크 세그먼트에 연결합니다.
- 파이버 탭: 선택적인 파이버 옵틱 탭이 있는 디바이스를 구축하는 경우 선택적인 멀티 모드 파이버 케이블에 있는 SC 플러그를 탭의 "분석기" 포트에 연결합니다. 분석하려는 네트워크 세그먼트에 탭을 연결합니다.
- 구리 탭: 선택적 구리 탭이 있는 디바이스를 구축하는 경우 탭 왼쪽에 있는 A 및 B 포트를 분석하려는 네트워크 세그먼트에 연결합니다. 탭 오른쪽에 있는 A 및 B 포트("분석기" 포트)를 어댑터 카드의 카퍼(copper) 포트 2개에 연결합니다.

관리되는 디바이스 구축 옵션에 대한 자세한 내용은 관리되는 디바이스 구축, 페이지 3-1을(를) 참조하십시오.

바이패스 인터페이스가 있는 디바이스를 구축하는 경우 디바이스에 장애가 발생하는 경우에도 디바이스의 네트워크 연결성을 유지할 수 있습니다. 설치 및 레이턴시 테스트에 대한 자세한 내용은 인라인 바이패스 인터페이스 설치 테스트, 페이지 4-26을(를) 참조하십시오.

단계 5 전원 코드를 어플라이언스에 연결하고 전원에 꽂습니다.

어플라이언스에 예비 전원 공급 장치가 있는 경우 전원 코드를 두 전원 공급 장치에 연결하고 별도의 전원에 꽂습니다.

단계 6 어플라이언스 전원을 켭니다.

어플라이언스를 설정하기 위해 직접적인 이더넷 연결을 사용하는 경우 로컬 컴퓨터의 네트워크 인터페이스와 어플라이언스의 관리 인터페이스에 대한 링크 LED가 켜지는지 확인합니다. 관리 인터페이스 및 네트워크 인터페이스 LED가 켜지지 않는 경우 crossover 케이블을 사용해보십시오. 자세한 내용은 구리 인터페이스의 인라인 구축 케이블링, 페이지 3-6을(를) 참고하십시오.

단계 7 다음 장 FireSIGHT System 어플라이언스 설정, 페이지 5-1을(를) 계속 진행하십시오.

콘솔 출력 리디렉션

기본적으로, FireSIGHT System 어플라이언스는 초기화 상태 또는 *init* 메시지를 VGA 포트로 보냅니다. 어플라이언스를 출고 시 기본값으로 복원하고 라이센스 및 네트워크 설정을 삭제할 경우 복원 유틸리티도 콘솔 출력을 VGA로 재설정합니다. 물리적 시리얼 포트 또는 SOL을 사용하여 콘솔에 액세스하려는 경우 Cisco에서는 초기 설정을 마친 후 콘솔 출력을 시리얼 포트로 리디렉션하도록 권장합니다.

셸을 사용하여 콘솔 출력을 리디렉션하려면 어플라이언스 셸에서 스크립트를 실행합니다. 모든 Series 3 어플라이언스가 LOM을 지원하지만 7000 Series 디바이스는 LOM과 물리적 시리얼 액세스를 동시에 지원하지 않습니다. 하지만 콘솔 설정은 사용하려는 액세스 방식과 상관없이 동일합니다.

셸을 사용하여 콘솔 출력을 리디렉션하려면 다음을 수행합니다.

액세스: Admin

단계 1 키보드/모니터 또는 시리얼 연결을 사용하여 관리자 권한의 계정으로 어플라이언스 셸에 로그인합니다. 비밀번호는 어플라이언스의 웹 인터페이스 비밀번호와 동일합니다.

Series 3 또는 가상의 관리되는 디바이스에서는 셸 프롬프트를 표시하려면 `expert`를 입력해야 합니다.

어플라이언스에 대한 프롬프트가 나타납니다.

단계 2 프롬프트에서 다음 명령 중 하나를 입력하여 콘솔 출력을 설정합니다.

VGA 포트를 사용하여 어플라이언스에 액세스하려면 다음을 실행합니다.

```
sudo /usr/local/sf/bin/configure_console.sh vga
```

물리적 시리얼 포트를 사용하여 어플라이언스에 액세스하려면 다음을 실행합니다.

```
sudo /usr/local/sf/bin/configure_console.sh serial
```

SOL을 통한 LOM을 사용하여 어플라이언스에 액세스하려면 다음을 실행합니다.

```
sudo /usr/local/sf/bin/configure_console.sh sol
```

단계 3 변경 사항을 구현하려면 `sudo reboot`를 입력하여 어플라이언스를 재부팅합니다.

어플라이언스가 재부팅됩니다.

인라인 바이패스 인터페이스 설치 테스트

바이패스 인터페이스가 포함된 관리되는 디바이스는 디바이스 전원이 꺼져 있거나 작동하지 않을 때에도 네트워크 연결을 유지하는 기능을 제공합니다. 이러한 디바이스를 올바르게 설치하고 설치 시 발생하는 레이턴시를 수량화하는 것이 중요합니다.

참고 스위치의 스패닝 트리 검색 프로토콜로 인해 30초의 트래픽 지연이 발생할 수 있습니다. Cisco에서는 다음 절차 중에 스패닝 트리를 비활성화하도록 권장합니다.

다음 절차는 구리 인터페이스에만 해당하며 인라인 바이패스 인터페이스의 설치를 테스트하고 레이턴시를 ping하는 방법에 대해 설명합니다. ping 테스트를 수행하고 관리되는 디바이스 콘솔에 연결하려면 네트워크에 연결해야 합니다.

인라인 바이패스 인터페이스 설치로 디바이스를 테스트하려면 다음을 수행합니다.

액세스: Admin

단계 1 어플라이언스의 인터페이스 세트 유형이 인라인 바이패스 모드로 구성되었는지 확인하십시오.

인터페이스 세트를 인라인 바이패스 모드로 구성하는 방법에 대한 지침은 *FireSIGHT System 사용 설명서*의 인라인 세트 구성을 참조하십시오.

단계 2 스위치, 방화벽 및 디바이스 센싱 인터페이스의 모든 인터페이스를 자동 협상으로 설정합니다.

참고 Cisco 디바이스에서는 디바이스에서 자동 MDIX를 사용할 때 자동 협상이 필요합니다.

단계 3 디바이스의 전원을 끄고 모든 네트워크 케이블을 분리합니다.

디바이스를 다시 연결하고 올바른 네트워크 연결이 있는지 확인하십시오. 케이블링 지침에서 디바이스에서 스위치 및 방화벽까지 crossover로 연결하는 방법과 straight-through로 연결하는 방법을 비교 확인하십시오. 구리 인터페이스의 인라인 구축 케이블링, 페이지 3-6을(를) 참조하십시오.

단계 4 디바이스의 전원을 끈 상태에서 디바이스를 통해 방화벽에서 스위치로 ping할 수 있는지 확인하십시오.

ping이 실패할 경우 네트워크 케이블을 올바르게 연결하십시오.

단계 5 10단계를 완료할 때까지 지속적인 ping을 실행합니다.

단계 6 디바이스의 전원을 다시 켭니다.

단계 7 키보드/모니터 또는 시리얼 연결을 사용하여 관리자 권한의 계정으로 디바이스에 로그인합니다. 비밀번호는 디바이스의 웹 인터페이스 비밀번호와 동일합니다.

디바이스에 대한 프롬프트가 나타납니다.

단계 8 `system shutdown`을 입력하여 디바이스의 전원을 끕니다.

또한 웹 인터페이스를 사용하여 디바이스를 종료할 수 있습니다. *FireSIGHT System 사용 설명서*에서 디바이스 관리 장을 참조하십시오. 대부분의 디바이스는 전원이 꺼질 때 딸각 소리가 납니다. 이 딸각 소리는 릴레이가 스위칭되고 디바이스가 하드웨어 바이패스로 전환되는 소리입니다.

단계 9 30초 동안 기다립니다.

ping 트래픽이 다시 시작되는지 확인합니다.

단계 10 디바이스의 전원을 다시 켜고 ping 트래픽이 계속 전달되는지 확인합니다.

단계 11 탭 모드를 지원하는 어플라이언스의 경우 다음과 같은 조건 집합에서 ping 레이턴시 결과를 테스트하고 기록할 수 있습니다.

- 디바이스 전원이 꺼짐
- 디바이스 전원이 켜짐, 규칙이 없는 정책 적용, 인라인 침입 정책 보호 모드
- 디바이스 전원이 켜짐, 규칙이 없는 정책 적용, 인라인 침입 정책 보호 탭 모드
- 디바이스 전원이 켜짐, 규칙이 있는 정책 적용, 인라인 침입 정책 보호 모드

설치에 레이턴시 기간이 허용되는지 확인합니다. 과도한 레이턴시 문제의 해결에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*에서 패킷 대기 시간 임계값 구성 및 규칙 대기 시간 임계값 이해를 참조하십시오.

FireSIGHT System 어플라이언스 설정

어플라이언스를 구축 및 설치한 다음 새로운 어플라이언스가 신뢰할 수 있는 관리 네트워크와 통신할 수 있도록 설정 프로세스를 완료해야 합니다. 또한 관리자 비밀번호를 변경하고 최종 사용자 라이센스 계약(EULA)에 동의해야 합니다.

설정 프로세스에서는 시간 설정, 디바이스 등록 및 라이센싱, 업데이트 예약 등 관리 레벨의 많은 초기 작업을 실행할 수 있습니다. 설정 및 등록 과정에서 선택하는 옵션에 따라 기본 인터페이스, 인라인 세트, 영역, 시스템에서 생성하고 적용하는 정책이 결정됩니다.

이러한 초기 컨피그레이션 및 정책의 목적은 즉시 사용 가능한 환경을 제공하고 옵션을 제한하는 대신 구축을 빠르게 설정할 수 있도록 돕는 것입니다. 디바이스를 초기에 어떻게 구성하는지와 상관없이, 방어 센터를 사용하여 해당 컨피그레이션을 언제든지 변경할 수 있습니다. 예를 들어, 설정 중 탐지 모드 또는 액세스 제어 정책을 선택할 경우 반드시 특정 디바이스, 영역 또는 정책 컨피그레이션을 사용해야 하는 것은 아닙니다.

참고 ASA FirePOWER 디바이스 설정에 대한 자세한 내용은 ASA 설명서를 참조하십시오.

초기 설정 프로세스에서 각 단계에 대한 자세한 내용은 다음 섹션을 참조 하십시오.

- 설정 프로세스 이해, 페이지 5-2에서는 어플라이언스의 모델 및 어플라이언스에 대한 물리적 액세스 권한이 있는지 여부에 따라 달라지는 설정 프로세스에 대해 설명합니다.

참고 아직 설정 프로세스에 대해 잘 모르는 경우 Cisco에서는 이 섹션을 먼저 읽도록 **적극** 권장합니다.

- 스크립트를 사용하여 네트워크 구성, 페이지 5-4에서는 스크립트를 사용하여 관리 네트워크에서 새로운 어플라이언스가 통신할 수 있도록 네트워크 설정을 지정하는 방법에 대해 설명합니다. 이 단계는 키보드 및 모니터를 사용하여 액세스하는 모든 방어 센터에 필요합니다.
- CLI를 사용하여 Series 3 디바이스에서 초기 설정 수행, 페이지 5-5에서는 인터랙티브 CLI(Command Line Interface)를 사용하여 Series 3 디바이스에서 설정 프로세스를 수행하는 방법에 대해 설명합니다.
- 초기 설정 페이지: 디바이스, 페이지 5-8에서는 디바이스의 웹 인터페이스를 사용하여 초기 설정을 완료하는 방법에 대해 설명합니다.
- 초기 설정 페이지: 방어 센터, 페이지 5-11에서는 방어 센터의 웹 인터페이스를 사용하여 초기 설정을 완료하는 방법에 대해 설명합니다.
- 다음 단계, 페이지 5-16에는 FireSIGHT System 구축을 설정할 때 수행할 수 있는 설정 후 작업에 대한 안내가 포함되어 있습니다.

주의 이 장의 절차는 전원을 끄지 않은 상태에서 어플라이언스를 설정하는 방법에 대해 설명합니다. 하지만 어떤 이유로 전원을 꺼야 하는 경우 *FireSIGHT System 사용 설명서*의 디바이스 관리 장에 설명된 절차를 사용하거나 Series 3 디바이스의 CLI에서 `system shutdown` 명령 또는 어플라이언스 셸(전문가 모드라고도 함)에서 `shutdown -h now` 명령을 사용합니다.

설정 프로세스 이해

새로운 FireSIGHT System 어플라이언스를 구축 및 설치한 다음, 본 설명서의 이전 장에 설명된 대로 설정 프로세스를 완료해야 합니다. 설정을 시작하기 전에 다음 조건을 충족할 수 있는지 확인하십시오.

플라이언스 모델

설정하는 어플라이언스를 알아야 합니다. FireSIGHT System *어플라이언스*는 트래픽을 감지하는 관리되는 *디바이스*이거나 관리하는 *방어 센터*입니다. 각 어플라이언스 유형에는 여러 *모델*이 있으며 이러한 모델은 추가적으로 *Series*와 *제품군*으로 그룹화됩니다. 자세한 내용은 FireSIGHT System 어플라이언스, 페이지 1-2을(를) 참고하십시오.

액세스

새로운 어플라이언스를 설정하려면 키보드 및 모니터/KVM(키보드, 비디오, 마우스) 또는 어플라이언스의 관리 인터페이스에 직접 연결되는 이더넷을 사용하여 연결해야 합니다. 초기 설정 후 시리얼 액세스를 위해 어플라이언스를 구성할 수 있습니다. 자세한 내용은 랙에 어플라이언스 설치, 페이지 4-23을(를) 참조하십시오.

참고 어플라이언스에서 대용량 스토리지 디바이스를 부팅 디바이스로 사용하려고 시도할 수 있으므로 초기 설정을 위해 어플라이언스에 액세스하는 데 USB 대용량 스토리지가 있는 KVM 콘솔을 사용하지 **마십시오**.

Information

어플라이언스가 관리 네트워크에서 통신하는 데 필요한 최소한의 정보는 IPv4 또는 IPv6 관리 IP 주소, 넷마스크 또는 접두사 길이, 기본 게이트웨이입니다.

어플라이언스가 구축되는 방식을 알고 있는 경우 설정 프로세스 중에 등록 및 라이센싱을 포함한 여러 개의 초기 관리 수준 작업을 수행하는 것이 좋습니다.

정보 여러 어플라이언스를 구축하는 경우 우선 디바이스를 설정한 다음 이러한 디바이스를 관리하는 방어 센터를 설정합니다. 디바이스의 초기 설정 프로세스에서는 디바이스를 방어 센터에 사전 등록할 수 있으며, 방어 센터 설정 프로세스에서는 사전 등록된 관리되는 디바이스를 추가 및 라이센싱할 수 있습니다.

설정을 완료한 후 방어 센터의 웹 인터페이스를 사용하여 구축에 대한 대부분의 관리 및 분석 작업을 수행합니다. 물리적 관리되는 디바이스에는 기본 관리를 수행하는 데에만 사용할 수 있는 제한된 웹 인터페이스가 있습니다. 자세한 내용은 다음 단계, 페이지 5-16을(를) 참고하십시오.

각 유형의 어플라이언스를 설정하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

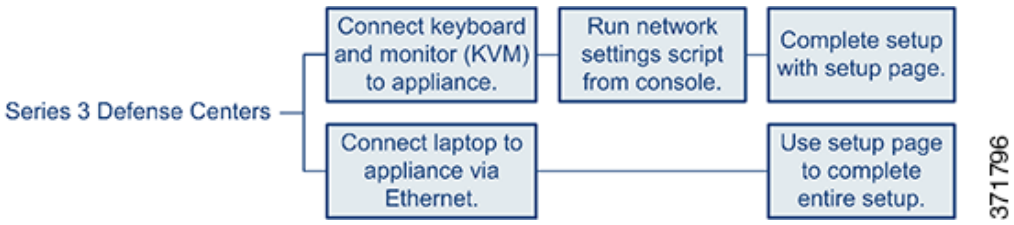
- Series 3 설정 방어 센터, 페이지 5-3
- Series 3 디바이스 설정, 페이지 5-4

정보 어플라이언스를 출고 시 기본 설정으로 복원한 후 어플라이언스를 설정하면서(FireSIGHT System 어플라이언스를 출고 시 기본 설정으로 복원, 페이지 8-1 참조) 어플라이언스의 라이센스 및 네트워크 설정을 삭제하지 않은 경우 관리 네트워크의 컴퓨터를 사용하여 어플라이언스의 웹 인터페이스로 직접 탐색하여 설정을 수행합니다. 초기 설정 페이지: 디바이스, 페이지 5-8 또는 초기 설정 페이지: 방어 센터, 페이지 5-11로 건너뛰십시오.

Series 3 설정 방어 센터

지원되는 방어 센터: Series 3

다음 다이어그램은 Series 3 방어 센터를 설정할 때 지정할 수 있는 선택 사항입니다.



Series 3 방어 센터를 설정하려면 다음을 수행합니다.

액세스: Admin

단계 1 키보드와 모니터를 사용하는 경우 어플라이언스가 관리 네트워크에서 통신할 수 있도록 설정을 구성하는 스크립트를 실행합니다. 스크립트를 사용하여 네트워크 구성, 페이지 5-4을(를) 참조하십시오.

이미지로 다시 설치한 어플라이언스를 설정하면서 복원 프로세스 중 네트워크 설정을 유지한 경우 또는 직접적인 이더넷 연결을 통해 어플라이언스에 액세스하는 경우 다음 단계로 건너뜁니다.

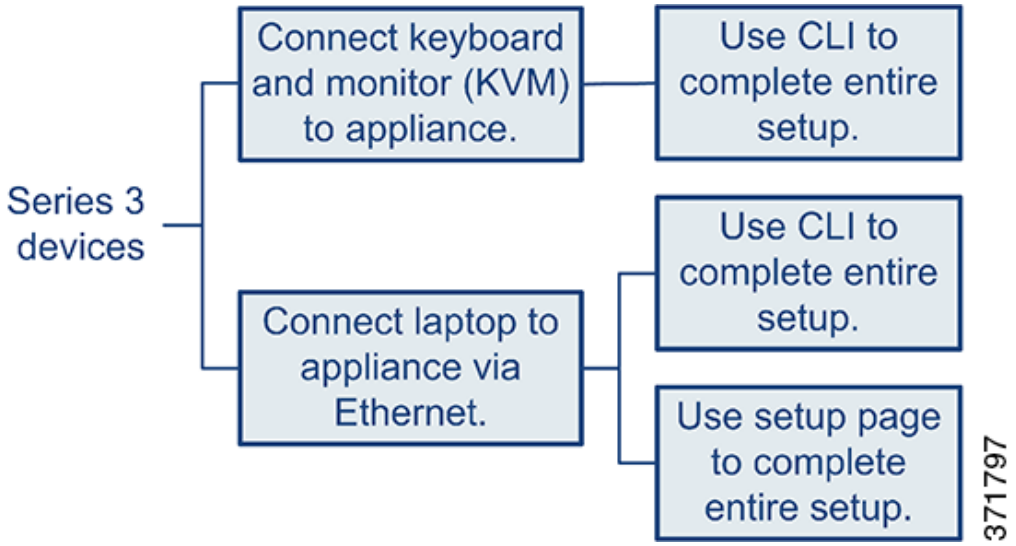
단계 2 관리 네트워크의 컴퓨터에서 어플라이언스의 웹 인터페이스로 이동하여 설정 프로세스를 완료합니다.

- 웹 인터페이스를 사용하여 관리되는 디바이스의 설정을 완료하려면 초기 설정 페이지: 디바이스, 페이지 5-8을(를) 참조하십시오.
- 웹 인터페이스를 사용하여 방어 센터의 설정을 완료하려면 초기 설정 페이지: 방어 센터, 페이지 5-11을(를) 참조하십시오.

Series 3 디바이스 설정

지원되는 디바이스: Series 3

다음 다이어그램은 Series 3 디바이스를 설정할 때 지정할 수 있는 선택 사항입니다.



Series 3 디바이스에 대한 액세스에 따라 설정 방법이 달라집니다. 다음과 같은 옵션이 있습니다.

- 디바이스에 연결된 방식과 상관없이 CLI를 사용하여 설정할 수 있습니다. CLI를 사용하여 Series 3 디바이스에서 초기 설정 수행, 페이지 5-5을(를) 참조하십시오.
- 직접적인 이더넷 연결을 통해 어플라이언스에 액세스하는 경우 로컬 컴퓨터에서 어플라이언스의 웹 인터페이스로 이동할 수 있습니다. 초기 설정 페이지: 디바이스, 페이지 5-8을(를) 참조하십시오.

이미지로 다시 설치한 디바이스를 설정하면서 복원 프로세스의 일부로 네트워크 설정을 유지한 경우 SSH 또는 LOM(Lights-Out Management) 연결을 통해 CLI에 액세스할 수 있습니다. 또한 관리 네트워크의 컴퓨터에서 디바이스의 웹 인터페이스로 이동할 수 있습니다.

스크립트를 사용하여 네트워크 구성

지원되는 디바이스: Series 2

새로운 방어 센터 또는 Series 2 디바이스를 설치하거나 이미지로 다시 설치하는 중 네트워크 설정을 삭제한 경우 어플라이언스가 관리 네트워크에서 통신할 수 있도록 구성해야 합니다. 콘솔에서 스크립트를 실행하여 이 단계를 완료합니다.

FireSIGHT System에서는 IPv4 및 IPv6 관리 환경을 모두 지원하는 이중 스택 구현을 제공합니다. 스크립트에서 IPv4 관리 설정을 구성(또는 비활성화)한 다음 IPv6 관리 설정을 구성하라는 메시지가 차례로 표시됩니다. IPv6 구축의 경우 로컬 라우터에서 설정을 검색할 수 있습니다. IPv4 또는 IPv6 관리 IP 주소, 넷마스크 또는 접두사 길이, 기본 게이트웨이를 입력해야 합니다.

스크립트의 프롬프트를 진행하는 동안 선택형 질문의 경우 `(y/n)`과 같이 선택 사항이 괄호 안에 나열됩니다. 기본값은 `[y]`와 같이 대괄호에 나열됩니다. Enter 키를 눌러 선택을 확인합니다.

스크립트는 어플라이언스의 설정 웹 페이지와 거의 동일한 설정 정보에 대한 메시지를 표시합니다. 자세한 내용은 네트워크 설정, 페이지 5-9(디바이스) 및 네트워크 설정, 페이지 5-13(방어 센터)을(를) 참조하십시오.

스크립트를 사용하여 네트워크 설정을 구성하려면 다음을 수행합니다.

액세스: Admin

단계 1 콘솔에서 어플라이언스에 로그인합니다. 사용자 이름으로 `admin`, 비밀번호로 `Sourcefire`를 사용합니다.

Series 3 또는 가상의 관리되는 디바이스에서는 셸 프롬프트를 표시하려면 `expert`를 입력해야 합니다.

단계 2 admin 프롬프트에서 다음 스크립트를 실행합니다.

```
sudo /usr/local/sf/bin/configure-network
```

단계 3 스크립트의 프롬프트를 따릅니다.

IPv4 및 IPv6 관리 설정을 차례로 구성(또는 비활성화)합니다. 네트워크 설정을 수동으로 지정할 경우 다음 작업을 수행해야 합니다.

- 넷마스크를 포함한 IPv4 주소를 점으로 구분된 10진수로 입력합니다. 예를 들어, 넷마스크로 255.255.0.0을 지정할 수 있습니다.
- IPv6 주소를 콜론으로 구분된 16진수 양식으로 입력합니다. IPv6 접두사의 경우 비트 수를 지정합니다. 예를 들어, 접두사 길이로 112를 입력합니다.

단계 4 설정이 올바른지 확인합니다.

설정을 잘못 입력한 경우 프롬프트에서 `n`을 입력하고 Enter 키를 누릅니다. 그런 다음 올바른 정보를 입력할 수 있습니다. 설정이 구현되면 콘솔에 메시지가 표시될 수 있습니다.

단계 5 어플라이언스에서 로그아웃합니다.

단계 6 다음 단계는 어플라이언스에 따라 다릅니다.

- 웹 인터페이스를 사용하여 관리되는 디바이스의 설정을 완료하려면 초기 설정 페이지: 디바이스, 페이지 5-8을(를) 계속 진행합니다.
- 웹 인터페이스를 사용하여 방어 센터 설정을 완료하려면 초기 설정 페이지: 방어 센터, 페이지 5-11을(를) 계속 진행합니다.

CLI를 사용하여 Series 3 디바이스에서 초기 설정 수행

지원되는 디바이스: Series 3

선택적으로 디바이스의 웹 인터페이스를 사용하는 대신 CLI를 사용하여 Series 3 디바이스를 구성할 수 있습니다. CLI를 사용하여 새로 구성된 디바이스에 처음으로 로그인할 때는 EULA를 읽고 동의해야 합니다. 그런 다음 설정 프롬프트에 따라 관리자 비밀번호를 변경하고 디바이스의 네트워크 설정과 탐지 모드를 구성합니다. 마지막으로, 디바이스를 관리할 방어 센터에 디바이스를 등록합니다.

설정 프롬프트를 따를 경우 `(y/n)`과 같이 선택 사항이 괄호 안에 나열됩니다. 기본값은 `[y]`와 같이 대괄호에 나열됩니다. Enter 키를 눌러 선택을 확인합니다.

CLI는 디바이스의 설정 웹 페이지와 거의 동일한 설정 정보에 대한 메시지를 표시합니다. 이러한 옵션에 대한 자세한 내용은 초기 설정 페이지: 디바이스, 페이지 5-8을(를) 참조하십시오.

CLI를 사용하여 Series 3 디바이스에서 초기 설정을 완료하려면 다음을 수행합니다.

액세스: Admin

단계 1 디바이스에 로그인합니다. 사용자 이름으로 admin, 비밀번호로 Sourcefire를 사용합니다.

- 모니터 및 키보드에 연결된 Series 3 디바이스의 경우 콘솔에서 로그인합니다.
- 이더넷 케이블을 사용하여 컴퓨터를 Series 3 디바이스의 관리 인터페이스에 연결한 경우 인터페이스의 기본 IPv4 주소 192.168.45.45에 SSH를 통해 연결합니다.

EULA를 읽으라는 메시지가 디바이스에 즉시 표시됩니다.

단계 2 EULA를 읽고 그 내용에 동의합니다.

단계 3 admin 계정의 비밀번호를 변경합니다. 이 계정에는 관리자 권한이 있으며 삭제할 수 없습니다.

admin 사용자가 이 비밀번호를 사용하여 디바이스의 웹 인터페이스 및 해당 CLI로 로그인할 수 있습니다. admin 사용자에는 컨피그레이션 CLI 액세스 권한이 있습니다. 어플라이언스의 웹 인터페이스에 대한 사용자 비밀번호를 변경하면 CLI 비밀번호도 변경되며, 그 반대의 경우도 마찬가지입니다.

Cisco에서는 대문자, 소문자, 1개 이상의 숫자가 포함되었으며 8자 이상의 영숫자로 된 강력한 비밀번호를 사용하도록 권장합니다. 사전에 나오는 단어를 사용하지 마십시오. 자세한 내용은 비밀번호 변경, 페이지 5-9을(를) 참고하십시오.

단계 4 디바이스의 네트워크 설정을 구성합니다.

IPv4 및 IPv6 관리 설정을 차례로 구성(또는 비활성화)합니다. 네트워크 설정을 수동으로 지정할 경우 다음 작업을 수행해야 합니다.

- 넷마스크를 포함한 IPv4 주소를 점으로 구분된 10진수로 입력합니다. 예를 들어, 넷마스크로 255.255.0.0을 지정할 수 있습니다.
- IPv6 주소를 콜론으로 구분된 16진수 양식으로 입력합니다. IPv6 접두사의 경우 비트 수를 지정합니다. 예를 들어, 접두사 길이로 112를 입력합니다.

자세한 내용은 네트워크 설정, 페이지 5-9을(를) 참고하십시오. 설정이 구현되면 콘솔에 메시지가 표시될 수 있습니다.

단계 5 LCD 패널을 사용하여 디바이스 네트워크 설정을 변경하도록 허용할지 여부를 선택합니다.

주의 이 옵션을 활성화할 경우 보안 위험에 노출될 수 있습니다. LCD 패널을 사용하여 네트워크 설정을 구성할 경우 인증은 필요하지 않으며 물리적 액세스만 필요합니다. 자세한 내용은 Series 3 디바이스에서 LCD 패널 사용, 페이지 6-1을(를) 참고하십시오.

단계 6 디바이스를 구축한 방식에 따라 탐지 모드를 지정합니다.

자세한 내용은 탐지 모드, 페이지 5-10을(를) 참고하십시오. 설정이 구현되면 콘솔에 메시지가 표시될 수 있습니다. 완료되면 이 디바이스를 방어 센터에 등록하라는 알림이 디바이스에 나타나고 CLI 프롬프트가 표시됩니다.

단계 7 CLI를 사용하여 디바이스를 관리할 방어 센터에 해당 디바이스를 등록하려면 다음 섹션 CLI를 사용하여 Series 3 디바이스를 방어 센터에 등록을 계속 진행하십시오.

방어 센터를 사용하여 디바이스를 관리해야 합니다. 지금 디바이스를 등록하지 않으면 나중에 방어 센터에 추가하기 전에 로그인하고 등록해야 합니다.

단계 8 어플라이언스에서 로그아웃합니다.

CLI를 사용하여 Series 3 디바이스를 방어 센터에 등록

지원되는 디바이스: Series 3

CLI를 사용하여 Series 3을 구성한 경우 Cisco에서는 설정 스크립트 마지막에 CLI를 사용하여 디바이스를 방어 센터에 등록하도록 권장합니다. 디바이스의 CLI에 이미 로그인되어 있으므로, 초기 설정 프로세스 중에 디바이스를 방어 센터에 등록하는 것이 가장 쉬운 방법입니다.

디바이스를 등록하려면 `configure manager add` 명령을 사용합니다. 디바이스를 방어 센터에 등록하려면 고유한 영숫자 등록 키가 항상 필요합니다. 이 키는 최대 37자로 지정하는 간단한 키이며 라이센스 키와 동일하지 않습니다.

대부분의 경우 등록 키와 함께 방어 센터의 호스트 이름 또는 IP 주소를 제공해야 합니다. 예를 들면 다음과 같습니다.

```
configure manager add DC.example.com my_reg_key
```

하지만 디바이스와 방어 센터가 NAT 디바이스로 구분되지 않은 경우 등록 키와 고유한 NAT ID를 입력하고 호스트 이름 대신 `DONTRESOLVE`를 지정합니다. 예를 들면 다음과 같습니다.

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

디바이스를 방어 센터에 등록하려면 다음을 수행합니다.

액세스: 컨피그레이션 CLI

단계 1 컨피그레이션 CLI 액세스 수준이 있는 사용자로 디바이스에 로그인합니다.

- 콘솔에서 초기 설정을 수행하는 경우 필요한 액세스 수준이 있는 `admin` 사용자로 이미 로그인되어 있는 것입니다.
- 그렇지 않을 경우 디바이스의 관리 IP 주소 또는 호스트 이름으로 SSH를 통해 연결합니다.

단계 2 프롬프트에서 다음과 같은 구문의 `configure manager add` 명령을 사용하여 디바이스를 방어 센터에 등록합니다.

```
configure manager add {hostname | IPv4_address | IPv6_address | DONTRESOLVE}
reg_key [nat_id]
```

여기서 각 항목은 다음을 나타냅니다.

- `{hostname | IPv4_address | IPv6_address | DONTRESOLVE}` 는 방어 센터의 완전한 호스트 이름 또는 IP 주소를 지정합니다. 방어 센터의 주소를 직접 지정할 수 없는 경우 `DONTRESOLVE`를 사용합니다.
- *reg_key*는 디바이스를 방어 센터에 등록하는 데 필요한 최대 37자의 고유한 영숫자 등록 키입니다.
- *nat_id*는 방어 센터와 디바이스 간의 등록 프로세스 동안 사용되는 선택적인 영숫자 문자열입니다. 이 문자열은 호스트 이름이 `DONTRESOLVE`로 설정된 경우 필요합니다.

단계 3 어플라이언스에서 로그아웃합니다.

디바이스를 방어 센터에 추가할 준비가 되었습니다.

초기 설정 페이지: 디바이스

모든 관리되는 디바이스의 경우(CLI를 사용하여 구성한 Series 3 디바이스 제외, CLI를 사용하여 Series 3 디바이스에서 초기 설정 수행, 페이지 5-5 참조) 디바이스의 웹 인터페이스에 로그인하고 설정 페이지에서 초기 컨피그레이션 옵션을 지정하여 설정 프로세스를 완료해야 합니다.

관리자 비밀번호를 변경하고, 네트워크 설정을 지정한 다음(아직 지정하지 않은 경우), EULA에 동의해야 합니다. 또한 디바이스를 방어 센터에 사전 등록하고 탐지 모드를 지정할 수 있습니다. 등록 중 선택하는 탐지 모드와 기타 옵션에 따라 시스템에서 생성되는 기본 인터페이스, 인라인 세트 및 영역과 초기에 관리되는 디바이스에 적용되는 정책이 결정됩니다.

웹 인터페이스를 사용하여 물리적 관리되는 디바이스에서 초기 설정을 완료하려면 다음을 수행합니다.

액세스: Admin

단계 1 브라우저에서 `https://mgmt_ip/`로 이동합니다. 여기서, *mgmt_ip*는 디바이스 관리 인터페이스의 IP 주소입니다.

- 컴퓨터에 이더넷 케이블로 연결된 디바이스의 경우 해당 컴퓨터의 브라우저에 기본 관리 인터페이스 IPv4 주소인 `https://192.168.45.45/`를 표시하도록 합니다.
- 네트워크 설정이 이미 구성된 디바이스의 경우 관리 네트워크에서 컴퓨터를 사용하여 디바이스 관리 인터페이스의 IP 주소를 탐색합니다.

로그인 페이지가 나타납니다.

단계 2 사용자 이름으로 `admin`, 비밀번호로 `Sourcefire`를 사용하여 로그인합니다.

설정 페이지가 표시됩니다. 설정 완료에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- 비밀번호 변경, 페이지 5-9
- 네트워크 설정, 페이지 5-9
- Series 3 디바이스 LCD 패널 컨피그레이션, 페이지 5-9
- 원격 관리, 페이지 5-9
- 시간 설정, 페이지 5-10
- 탐지 모드, 페이지 5-10
- 자동 백업, 페이지 5-11
- 최종 사용자 라이센스 계약, 페이지 5-11

단계 3 완료되면 **Apply(적용)**를 클릭합니다.

선택 사항에 따라 디바이스가 구성됩니다. 중간 페이지가 나타나면 관리자 역할이 있는 `admin` 사용자로 웹 인터페이스에 로그인된 것입니다.

단계 4 디바이스에서 로그아웃합니다.

디바이스를 해당 방어 센터에 추가할 준비가 되었습니다.

참고 이더넷 케이블을 사용하여 디바이스에 직접 연결된 경우 컴퓨터 연결을 끊고 디바이스의 관리 인터페이스를 관리 네트워크에 연결합니다. 언제든지 디바이스의 웹 인터페이스에 대한 액세스가 필요한 경우 관리 네트워크에 있는 컴퓨터의 브라우저에서 설정 중 구성한 IP 주소 또는 호스트 이름으로 이동합니다.

비밀번호 변경

admin 계정의 비밀번호를 변경해야 합니다. 이 계정에는 관리자 권한이 있으며 삭제할 수 없습니다.

admin 사용자가 이 비밀번호를 사용하여 디바이스의 웹 인터페이스 및 해당 CLI로 로그인할 수 있습니다. admin 사용자에는 컨피그레이션 CLI 액세스 권한이 있습니다. 어플라이언스의 웹 인터페이스에 대한 사용자 비밀번호를 변경하면 CLI 비밀번호도 변경되며, 그 반대의 경우도 마찬가지입니다.

대문자, 소문자, 1개 이상의 숫자가 포함된 8자 이상의 영숫자로 만든 강력한 비밀번호를 사용하는 것이 좋습니다. 사전에 나오는 단어를 사용하지 마십시오.

네트워크 설정

디바이스의 네트워크 설정을 사용하면 관리 네트워크에서 통신할 수 있습니다. 이미 디바이스의 네트워크 설정을 구성한 경우 페이지의 이 섹션이 미리 채워질 수 있습니다.

FireSIGHT System에서는 IPv4 및 IPv6 관리 환경을 모두 지원하는 이중 스택 구현을 제공합니다. 관리 네트워크 프로토콜(**IPv4**, **IPv6** 또는 **둘 다**)을 지정해야 합니다. 선택 사항에 따라, 설정 페이지에 IPv4 또는 IPv6 관리 IP 주소, 넷마스크 또는 접두사 길이, 기본 게이트웨이를 설정해야 하는 다양한 필드가 표시됩니다.

- IPv4의 경우 주소와 넷마스크를 점으로 구분된 10진수 형식으로 설정해야 합니다(예: 넷마스크 255.255.0.0).
- IPv6 넷마스크의 경우 **Assign the IPv6 address using router autoconfiguration** 확인란을 선택하여 IPv6 네트워크 설정을 자동으로 할당할 수 있습니다. 그렇지 않으면 콜론으로 구분된 16진수 형식의 주소와 접두사의 비트 수를 설정해야 합니다(예: 접두사 길이 112).

또한 최대 3개의 DNS 서버와 디바이스의 호스트 이름 및 도메인을 지정할 수 있습니다.

Series 3 디바이스 LCD 패널 컨피그레이션

지원되는 디바이스: Series 3

Series 3 디바이스를 구성하는 경우 LCD 패널을 사용하여 디바이스의 네트워크 설정을 변경할 수 있도록 허용할지 여부를 선택합니다.

주의 이 옵션을 활성화하면 보안 위험에 노출될 수 있습니다. LCD 패널을 사용하여 네트워크 설정을 구성할 경우 인증은 필요하지 않으며 물리적 액세스만 필요합니다. 자세한 내용은 Series 3 디바이스에서 LCD 패널 사용, 페이지 6-1을(를) 참조하십시오.

원격 관리

방어 센터를 사용하여 Cisco 디바이스를 관리해야 합니다. 이 2단계 프로세스에서는 먼저 디바이스에서 원격 관리를 구성한 다음 디바이스를 방어 센터에 추가합니다. 사용자 편의를 위해 설정 페이지에서 디바이스를 관리할 방어 센터에 디바이스를 사전 등록할 수 있습니다.

Register This Device Now(지금 이 디바이스 등록) 확인란을 활성화된 상태로 둔 다음 **Management Host(관리 호스트)**로 관리하는 방어 센터의 IP 주소 또는 완전한 도메인 이름을 지정합니다. 또한, 나중에 디바이스를 방어 센터에 등록하는 데 사용할 영숫자 **Registration Key(등록 키)**를 입력합니다. 이 키는 최대 37자로 지정하는 간단한 키이며 라이센스 키와 동일하지는 않습니다.

참고 디바이스와 방어 센터가 NAT(Network Address Translation) 디바이스로 구분되지 않은 경우 초기 설정을 완료할 때까지 디바이스 등록을 연기합니다. 자세한 내용은 *FireSIGHT System 사용 설명서*에서 디바이스 관리 장을 참조하십시오.

시간 설정

디바이스의 시간을 수동으로 설정하거나 방어 센터를 포함한 NTP(Network Time Protocol) 서버에서 NTP를 통해 설정할 수 있습니다. Cisco에서는 관리되는 디바이스의 NTP 서버로 방어 센터를 사용하도록 권장합니다.

또한 `admin` 계정의 로컬 웹 인터페이스에 사용되는 시간대를 지정할 수 있습니다. 팝업 창을 사용하여 변경할 현재 시간대를 클릭합니다.

탐지 모드

디바이스에 대해 선택하는 탐지 모드에 따라 시스템이 초기에 디바이스의 인터페이스를 구성하는 방식과 이러한 인터페이스가 인라인 세트 또는 보안 영역에 속하는지가 결정됩니다.

탐지 모드는 나중에 변경할 수 있는 설정이 아니며 시스템이 디바이스의 초기 컨피그레이션을 맞춤 설정하는 데 도움이 되도록 설정 과정에서 선택하는 옵션에 불과합니다. 일반적으로, 디바이스가 구축된 방식을 기준으로 탐지 모드를 선택해야 합니다.

수동

디바이스가 IDS(Intrusion Detection System)로서 수동으로 구축된 경우 이 모드를 선택합니다. 수동 구축에서는 파일 및 악성코드 탐지, 보안 인텔리전스 모니터링, 네트워크 검색을 수행할 수 있습니다.

인라인

디바이스가 침입 방지 시스템으로 인라인으로 구축된 경우 이 모드를 선택합니다. 침입 방지 시스템에서는 일반적으로 *개방* 상태로 장애가 발생하며 일치하지 않는 트래픽을 *허용*합니다.

인라인 구축에서는 네트워크 기반 AMP(Advanced Malware Protection), 파일 제어, 보안 인텔리전스 필터링 및 네트워크 검색도 수행할 수 있습니다.

모든 디바이스에 대해 인라인 모드를 선택할 수 있지만, 다음 인터페이스를 사용하는 인라인 세트에는 바이패스 기능이 없습니다.

- 8000 Series 디바이스의 비 바이패스 NetMod
- 71xx 제품군 디바이스의 SFP 트렌시버

참고 이미지로 다시 설치하면 인라인 구축의 디바이스가 비 바이패스 컨피그레이션으로 재설정되며 바이패스 모드를 다시 구성할 때까지 네트워크 트래픽이 중단됩니다. 자세한 내용은 복원 프로세스 중 트래픽 흐름, 페이지 8-2을(를) 참고하십시오.

액세스 제어

디바이스가 액세스 제어 구축 과정에서 인라인으로 구축된 경우, 즉 애플리케이션, 사용자, URL 제어를 수행하려는 경우 이 모드를 선택합니다. 액세스 제어를 수행하도록 구성된 디바이스는 일반적으로 *닫힌* 상태에서 장애가 발생하며 일치하지 않는 트래픽을 *차단*합니다. 규칙에서는 통과할 트래픽을 명시적으로 지정합니다.

또한 모델에 따라 클러스터링, 엄격한 TCP 적용, 빠른 경로 규칙, 스위칭, 라우팅, DHCP, NAT, VPN 등을 포함하는 디바이스의 특정 하드웨어 기반 기능을 활용하려는 경우에도 이 모드를 선택해야 합니다.

액세스 제어 구축에서는 악성코드 방지, 파일 제어, 보안 인텔리전스 필터링, 네트워크 검색도 수행할 수 있습니다.

네트워크 검색

디바이스가 호스트, 애플리케이션, 사용자 검색만 수행하도록 수동으로 구축된 경우 이 모드를 선택합니다.

다음 표에는 사용자가 선택하는 탐지 모드에 따라 시스템에서 생성되는 인터페이스, 인라인 세트, 영역이 나와 있습니다.

표 5-1 탐지 모드 기반의 초기 컨피그레이션

탐지 모드	보안 영역	인라인 세트	인터페이스
인라인	내부 및 외부	기본 인라인 세트	첫 번째 쌍이 기본 인라인 세트에 추가됨 (하나는 내부, 다른 하나는 외부 영역)
수동	수동	없음	첫 번째 쌍이 수동 영역에 할당됨
액세스 제어	없음	없음	없음
네트워크 검색	수동	없음	첫 번째 쌍이 수동 영역에 할당됨

보안 영역은 실제로 디바이스를 방어 센터에 등록할 때까지 시스템에서 생성하지 않는 방어 센터 수준의 컨피그레이션입니다. 등록 시 방어 센터에 이미 적절한 영역(내부, 외부, 수동)이 있는 경우 등록 프로세스가 목록의 인터페이스를 기존 영역에 추가합니다. 해당 영역이 없을 경우 시스템에서는 영역을 생성하고 인터페이스를 추가합니다. 인터페이스, 인라인 세트, 보안 영역에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

자동 백업

디바이스에서는 장애 발생 시 컨피그레이션 및 이벤트 데이터를 복원할 수 있도록 데이터 보관 메커니즘을 제공합니다. 초기 설정 과정에서 **Apply(적용)**를 수행할 수 있습니다.

이 설정을 활성화하면 디바이스의 컨피그레이션을 매주 백업하는 예약 작업이 생성됩니다.

최종 사용자 라이센스 계약

EULA를 주의하여 읽고 조항을 준수하는 것에 동의할 경우 확인란을 선택합니다. 입력한 모든 정보가 올바른지 확인하고 **Apply**를 클릭합니다. 선택 사항에 따라 디바이스가 구성되며 관리하는 해당 방어 센터에 추가할 수 있습니다.

초기 설정 페이지: 방어 센터

모든 방어 센터에 대해 방어 센터의 웹 인터페이스에 로그인하고 설정 페이지에서 초기 컨피그레이션 옵션을 지정하여 설정 프로세스를 완료해야 합니다. 관리자 비밀번호를 변경하고 아직 수행하지 않은 경우 네트워크 설정을 지정한 후 EULA에 동의해야 합니다.

설정 프로세스에서는 디바이스를 등록 및 라이센싱할 수도 있습니다. 디바이스를 등록하기 전에 디바이스 자체에서 설정 프로세스를 완료하고 방어 센터를 원격 관리자로 추가해야 하며, 그렇지 않을 경우 등록이 실패합니다.

자세한 내용은 관리되는 디바이스 모델별 지원되는 기능, 페이지 1-8 및 FireSIGHT System 라이센싱, 페이지 1-13을(를) 참조하십시오.

웹 인터페이스를 사용하여 방어 센터에서 초기 설정을 완료하려면 다음을 수행합니다.

액세스: Admin

단계 1 브라우저에서 `https://mgmt_ip/`로 이동합니다. 여기서, *mgmt_ip*는 방어 센터 관리 인터페이스의 IP 주소입니다.

- 컴퓨터에 이더넷 케이블로 연결된 방어 센터의 경우 해당 컴퓨터의 브라우저에 기본 관리 인터페이스 IPv4 주소인 `https://192.168.45.45/`가 표시되도록 합니다.
- 네트워크 설정이 이미 구성된 방어 센터의 경우 관리 네트워크에서 컴퓨터를 사용하여 방어 센터의 관리 인터페이스의 IP 주소를 탐색합니다.

로그인 페이지가 나타납니다.

단계 2 사용자 이름으로 `admin`, 비밀번호로 `Sourcefire`를 사용하여 로그인합니다.

설정 페이지가 표시됩니다. 설정 완료에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- 비밀번호 변경, 페이지 5-13
- 네트워크 설정, 페이지 5-13
- 시간 설정, 페이지 5-13
- 반복 규칙 업데이트 가져오기, 페이지 5-13
- 반복 위치 업데이트, 페이지 5-14
- 자동 백업, 페이지 5-14
- 라이센스 설정, 페이지 5-14
- 디바이스 등록, 페이지 5-15
- 최종 사용자 라이센스 계약, 페이지 5-16

단계 3 완료되면 **Apply(적용)**를 클릭합니다.

선택 사항에 따라 방어 센터가 구성됩니다. 중간 페이지가 나타나면 관리자 역할이 있는 `admin` 사용자로 웹 인터페이스에 로그인된 것입니다.

참고 이더넷 케이블을 사용하여 디바이스에 직접 연결된 경우 컴퓨터 연결을 끊고 방어 센터의 관리 인터페이스를 관리 네트워크에 연결합니다. 관리 네트워크의 컴퓨터에 있는 브라우저를 사용하여 방금 구성한 IP 주소 또는 호스트 이름으로 방어 센터에 액세스하고 이 설명서의 나머지 절차를 완료합니다.

단계 4 Task Status(작업 상태) 페이지(**System(시스템) > Monitoring(모니터링) > Task Status(작업 상태)**)를 사용하여 초기 설정이 성공적인지 확인합니다.

페이지가 10초마다 자동으로 새로 고쳐집니다. 초기 디바이스 등록 및 정책 적용 작업에 대해 **Completed(완료)** 상태가 나열될 때까지 페이지를 모니터링합니다. 설정 과정에서 침입 규칙 또는 위치 업데이트를 구성한 경우 해당 작업도 모니터링할 수 있습니다.

방어 센터를 사용할 준비가 되었습니다. 구축 구성에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

단계 5 다음 단계, 페이지 5-16을(를) 계속 진행합니다.

비밀번호 변경

admin 계정의 비밀번호를 변경해야 합니다. 이 계정에는 관리자 권한이 있으며 삭제할 수 없습니다.

대문자, 소문자, 1개 이상의 숫자가 포함된 8자 이상의 영숫자로 만든 강력한 비밀번호를 사용하는 것이 좋습니다. 사전에 나오는 단어를 사용하지 마십시오.

네트워크 설정

방어 센터의 네트워크 설정을 사용하면 관리 네트워크에서 통신할 수 있습니다. 이미 네트워크 설정을 구성한 경우 페이지의 이 섹션이 미리 채워질 수 있습니다.

FireSIGHT System에서는 IPv4 및 IPv6 관리 환경을 모두 지원하는 이중 스택 구현을 제공합니다. 관리 네트워크 프로토콜(**IPv4**, **IPv6** 또는 **둘 다**)을 지정해야 합니다. 선택 사항에 따라, 설정 페이지에 IPv4 또는 IPv6 관리 IP 주소, 넷마스크 또는 접두사 길이, 기본 게이트웨이를 설정해야 하는 다양한 필드가 표시됩니다.

- IPv4의 경우 주소와 넷마스크를 점으로 구분된 10진수 형식으로 설정해야 합니다(예: 넷마스크 255.255.0.0).
- IPv6 넷마스크의 경우 **Assign the IPv6 address using router autoconfiguration** 확인란을 선택하여 IPv6 네트워크 설정을 자동으로 할당할 수 있습니다. 그렇지 않으면 콜론으로 구분된 16진수 형식의 주소와 접두사의 비트 수를 설정해야 합니다(예: 접두사 길이 112).

또한 최대 3개의 DNS 서버와 디바이스의 호스트 이름 및 도메인을 지정할 수 있습니다.

시간 설정

방어 센터 시간을 수동으로 설정하거나 NTP 서버의 NTP(Network Time Protocol)를 통해 설정할 수 있습니다.

또한 admin 계정의 로컬 웹 인터페이스에 사용되는 시간대를 지정할 수 있습니다. 팝업 창을 사용하여 변경할 현재 시간대를 클릭합니다.

반복 규칙 업데이트 가져오기

라이센스: 보호

새로운 취약성이 알려지면 VRT(Vulnerability Research Team)에서 침입 규칙 업데이트를 릴리스합니다. 규칙 업데이트는 업데이트된 새로운 침입 규칙과 프리프로세서 규칙, 기존 규칙의 수정된 상태, 수정된 기본 침입 정책 설정을 제공합니다. 또한 규칙 업데이트는 규칙을 삭제하고 새로운 규칙 범주 및 시스템 변수를 제공할 수 있습니다.

구축 과정에서 침입 탐지 및 방지를 수행하려는 경우 **Enable Recurring Rule Update Imports**를 수행하는 것이 좋습니다.

Import Frequency를 지정하고 규칙이 업데이트될 때마다 침입 **Policy Reapply**를 수행하도록 시스템을 구성할 수 있습니다. 초기 컨피그레이션 프로세스에서 규칙 업데이트를 수행하려면 **Install Now**를 선택합니다.

참고 규칙 업데이트에는 새로운 이진수가 포함될 수 있습니다. 규칙 업데이트를 다운로드 및 설치하는 과정에서 보안 정책을 준수하는지 확인해야 합니다. 또한 규칙 업데이트 규모가 클 수 있으므로 네트워크 이용률이 낮은 시간 동안 규칙을 가져오십시오.

반복 위치 업데이트

지원되는 방어 센터: DC500을 제외한 모든 방어 센터

대부분의 방어 센터를 사용하여 시스템에서 생성한 이벤트와 관련된 라우팅된 IP 주소에 대한 위치 정보를 보고 대시보드 및 Context Explorer(컨텍스트 탐색기)에서 위치 통계를 모니터링할 수 있습니다.

방어 센터의 위치 데이터베이스(GeoDB)에는 IP 주소의 관련 ISP(Internet Service Provider), 연결 유형, 프록시 정보, 정확한 위치 등의 정보가 포함됩니다. 일반 GeoDB 업데이트를 활성화할 경우 시스템에서는 최신 위치 정보를 사용합니다. 구축 과정에서 위치 관련 분석을 수행하려는 경우 **Enable Recurring Weekly Updates**를 수행하는 것이 좋습니다.

GeoDB의 주간 업데이트 빈도를 지정할 수 있습니다. 팝업 창을 사용하여 변경할 현재 시간대를 클릭합니다. 초기 컨피그레이션 프로세스에서 데이터베이스를 다운로드하려면 **Install Now**를 선택합니다.

참고 GeoDB 업데이트는 규모가 클 수 있으며 다운로드 후 설치까지 최대 45분이 소요될 수 있습니다. GeoDB는 네트워크 이용률이 낮은 시간 동안 업데이트해야 합니다.

자동 백업

방어 센터에서는 장애 발생 시 컨피그레이션을 복원할 수 있는 데이터 아카이브 메커니즘을 제공합니다. 초기 설정 과정에서 **Enable Automatic Backups**를 수행할 수 있습니다.

이 설정을 활성화하면 방어 센터의 컨피그레이션을 매주 백업하는 예약 작업을 만들 수 있습니다.

라이센스 설정

다양한 기능의 라이센스를 취득하여 조직에 최적의 FireSIGHT System 구축을 조성할 수 있습니다. 호스트, 애플리케이션, 사용자 검색을 수행하려면 방어 센터의 FireSIGHT 라이센스가 필요합니다. 추가 모델별 라이센스를 사용하면 관리되는 디바이스로 다음과 같이 다양한 기능을 수행할 수 있습니다. 아키텍처 및 리소스 제약으로 인해 일부 라이센스는 모든 관리되는 디바이스에 적용할 수 없습니다. 관리되는 디바이스 모델별 지원되는 기능, 페이지 1-8 및 FireSIGHT System 라이센싱, 페이지 1-13을(를) 참조하십시오.

초기 설정 페이지를 사용하여 조직에서 구입한 라이센스를 추가하는 것이 좋습니다. 지금 라이센스를 추가하지 않을 경우 초기 설정 중에 등록하는 디바이스는 라이센스가 없이 방어 센터에 추가됩니다. 초기 설정 프로세스가 종료된 후 각 디바이스에 개별적으로 라이센스를 부여해야 합니다. 이미지로 다시 설치한 어플라이언스를 설정하면서 복원 프로세스의 일부로 라이센스 설정을 유지한 경우 이 섹션은 미리 채워져 있을 수 있습니다.

라이센스를 아직 받지 못한 경우 `https://keyserver.sourcefire.com/` 링크를 클릭하여 이동한 다음 화면의 지침을 따르십시오. 라이센스 키(초기 설정 페이지에 나열됨) 및 활성화 키(지원 계약과 연결된 연락처로 이메일을 통해 이전에 제공됨)가 필요합니다.

라이센스를 텍스트 상자에 붙여 넣고 **Add/Verify**(추가/검증)를 클릭하여 라이센스를 추가합니다. 유효한 라이센스를 추가하면 페이지가 업데이트되고 추가한 라이센스를 추적할 수 있습니다. 라이센스를 한 번에 하나씩 추가하십시오.

디바이스 등록

방어 센터는 현재 FireSIGHT System에서 지원하는 모든 가상 또는 물리적 디바이스를 관리할 수 있습니다.

참고 디바이스를 방어 센터에 등록하기 전에 **반드시** 디바이스에 원격 관리를 구성해야 합니다.

초기 설정 프로세스 중 대부분의 사전 등록된 디바이스(원격 관리, 페이지 5-9 참조)을(를) 방어 센터에 추가할 수 있습니다. 그러나 디바이스와 방어 센터가 NAT 디바이스에 의해 분리되는 경우 설정 프로세스가 완료된 후에 추가해야 합니다.

참고 기본이 아닌 관리 인터페이스를 사용하여 방어 센터 및 관리되는 디바이스를 연결할 경우, 해당 어플라이언스가 NAT 디바이스로 분리되어 있으면 두 트래픽 채널을 모두 구성하여 동일한 관리 인터페이스를 사용해야 합니다. 자세한 내용은 관리 네트워크에서 구축, 페이지 2-1을(를) 참조하십시오.

관리되는 디바이스를 방어 센터에 등록할 때 등록 시 자동으로 디바이스에 액세스 제어 정책을 적용하려면 **Apply Default Access Control Policies**(기본 액세스 제어 정책 적용) 확인란을 활성화된 상태로 둡니다. 방어 센터에서 각 디바이스에 어떤 정책을 적용하는지는 선택할 수 없으며, 적용 여부만 선택할 수 있습니다. 각 디바이스에 적용되는 정책은 다음 표와 같이 디바이스를 구성할 때 선택한 탐지 모드(탐지 모드, 페이지 5-10 참조)에 따라 달라집니다.

표 5-2 탐지 모드별로 적용되는 기본 액세스 제어 정책

탐지 모드	기본 액세스 제어 정책
인라인	기본 침입 방지
수동	기본 침입 방지
액세스 제어	기본 액세스 제어
네트워크 검색	기본 네트워크 검색

이전에 디바이스를 방어 센터로 관리하면서 디바이스의 초기 인터페이스 컨피그레이션을 변경한 경우 예외가 발생합니다. 이 경우 이 새로운 방어 센터 페이지에서 적용하는 정책은 디바이스의 변경된(현재) 컨피그레이션에 따라 다릅니다. 구성된 인터페이스가 있는 경우 방어 센터는 기본 침입 방지 정책을 적용합니다. 그렇지 않을 경우, 방어 센터는 기본 액세스 제어 정책을 적용합니다.

참고 디바이스가 액세스 제어 정책과 호환되지 않을 경우 정책 적용이 실패합니다. 이러한 문제는 라이센싱 불일치, 모델 제약 조건, 수동 대 인라인 문제, 기타 잘못된 컨피그레이션을 비롯한 여러 가지 이유로 인해 발생할 수 있습니다. 초기 액세스 제어 정책 적용이 실패하면 초기 네트워크 검색 정책 적용도 실패합니다. 오류를 일으킨 문제를 해결한 후에는 액세스 제어 및 네트워크 검색 정책을 디바이스에 수동으로 적용해야 합니다. 액세스 제어 정책 적용의 실패를 일으키는 문제에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

디바이스를 추가하려면 **Hostname** 또는 **IP Address**, 그리고 디바이스를 등록할 때 지정한 **Registration Key**를 입력합니다. 이 키는 사용자가 지정한 최대 37자 길이의 간단한 키이며 라이센스 키와 동일하지 않습니다.

그런 다음 확인란을 사용하여 디바이스에 라이센스된 기능을 추가합니다. 이미 방어 센터에 추가한 라이센스만 선택할 수 있습니다. 라이센스 설정, 페이지 5-14을(를) 참조하십시오.

아키텍처 및 리소스 제한으로 인해, 모든 라이센스가 모든 관리되는 디바이스에서 지원되지는 않습니다. 그러나 설정 페이지에서는 관리되는 디바이스에서 지원되지 않는 라이센스를 활성화하거나 모델별 라이센스가 없는 기능을 활성화할 수 **있습니다**. 그 이유는 방어 센터에서 아직 디바이스 모델을 확인하지 않았기 때문입니다. 시스템에서는 유효하지 않은 라이센스를 활성화할 수 없으며, 유효하지 않은 라이센스를 활성화하려고 시도할 경우 사용 가능한 라이센스 수가 줄어들지 않습니다.

각 라이센스를 각 디바이스 모델에 적용하는 데 사용할 수 있는 방어 센터를 포함한 라이센싱에 대한 자세한 내용은 방어 센터 모델별 지원되는 기능, 페이지 1-7, 관리되는 디바이스 모델별 지원되는 기능, 페이지 1-8 및 FireSIGHT System 라이센싱, 페이지 1-13을(를) 참조하십시오.

라이센스를 활성화한 후 **Add**를 클릭하여 디바이스의 등록 설정을 저장하고, 선택적으로 디바이스를 추가합니다. 잘못된 옵션을 선택했거나 디바이스 이름을 잘못 입력한 경우 **Delete**를 클릭하여 제거합니다. 그런 다음 디바이스를 다시 추가할 수 있습니다.

최종 사용자 라이센스 계약

EULA를 주의하여 읽고 조항을 준수하는 것에 동의할 경우 확인란을 선택합니다. 입력한 모든 정보가 올바른지 확인하고 **Apply(적용)**를 클릭합니다.

선택 사항에 따라 방어 센터가 구성됩니다. 중간 페이지가 나타나면 관리자 역할이 있는 `admin` 사용자로 웹 인터페이스에 로그인된 것입니다. 초기 설정 페이지: 방어 센터, 페이지 5-11의 3단계를 계속 진행하여 방어 센터의 초기 설정을 완료합니다.

다음 단계

Cisco에서는 어플라이언스의 초기 설정 프로세스를 마치고 성공 여부를 확인한 다음 구축을 쉽게 관리할 수 있는 다양한 관리 작업을 완료하도록 권장합니다. 또한 디바이스 등록, 라이센싱과 같이 초기 설정 중 생략한 작업을 완료해야 합니다. 다음 섹션에 설명된 작업과 구축 컨피그레이션을 시작할 수 있는 방법에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

정보 시리얼 또는 LOM/SOL 연결을 사용하여 어플라이언스 콘솔에 액세스하려면 콘솔 출력을 리디렉션해야 합니다. 인라인 바이패스 인터페이스 설치 테스트, 페이지 4-26을(를) 참조하십시오. 특히 LOM을 사용하려는 경우 기능을 활성화하고 한 명 이상의 LOM 사용자를 활성화해야 합니다. LOM 및 LOM 사용자 활성화, 페이지 8-20을(를) 참조하십시오.

개별 사용자 계정

초기 설정을 완료하면 시스템에는 관리자 역할 및 액세스 권한을 가진 `admin` 사용자 한 명만 있게 됩니다. 이 역할의 사용자는 셸 또는 CLI를 포함하여 전체 시스템 메뉴 및 컨피그레이션에 액세스할 수 있습니다. 보안 및 감사 이유로 `admin` 계정(및 관리자 역할)의 사용을 제한하는 것이 좋습니다.

시스템을 사용할 각 사용자에 대해 별도의 계정을 만들 경우, 조직이 각 사용자의 작업과 각 사용자에 의한 변경 사항을 감사할 수 있을 뿐만 아니라 각 사용자와 관련된 사용자 액세스 역할을 제한할 수 있습니다. 이러한 조치는 대부분의 컨피그레이션 및 분석 작업을 수행하는 방어 센터에서 특히 중요합니다. 예를 들어, 분석가는 네트워크 보안을 분석하기 위해 이벤트 데이터에 대한 액세스가 필요할 수 있지만 구축 관리 기능에는 액세스가 필요하지 않을 수 있습니다.

시스템에는 다양한 관리자 및 분석가에게 맞게 설계된 10개의 사전 정의 사용자 역할이 포함되어 있습니다. 또한 특수 액세스 권한의 맞춤형 사용자 역할을 생성할 수도 있습니다.

상태 및 시스템 정책

기본적으로, 모든 어플라이언스에는 초기 시스템 정책이 적용되어 있습니다. 시스템 정책은 메일 릴레이 호스트 기본 설정, 시간 동기화 설정 등 구축의 여러 어플라이언스에서 유사할 수 있는 설정을 관리합니다. 방어 센터 자체와 여기에서 관리하는 모든 디바이스에 동일한 시스템 정책을 적용하는 것이 좋습니다.

기본적으로, 방어 센터에도 상태 정책이 적용되어 있습니다. 상태 정책은 상태 모니터링 기능에 포함되어 있으며 구축된 어플라이언스의 성능을 지속적으로 모니터링하는 기준을 제공합니다. 방어 센터를 사용하여 여기에서 관리하는 모든 디바이스에 상태 정책을 적용하는 것이 좋습니다.

소프트웨어 및 데이터베이스 업데이트

구축을 시작하기 전에 어플라이언스에서 시스템 소프트웨어를 업데이트해야 합니다. 구축된 모든 어플라이언스에서 최신 버전의 FireSIGHT System을 실행하는 것이 좋습니다. 구축 시 최신 버전을 사용하고 있는 경우 최신 침입 규칙 업데이트, VDB, GeoDB도 설치해야 합니다.

주의 FireSIGHT System의 일부를 업데이트하기 전에 업데이트에 포함된 릴리스 노트 또는 권고 문구를 **반드시** 읽어야 합니다. 릴리스 노트에서는 지원되는 플랫폼, 호환성, 전제 조건, 경고, 특정 설치 및 제거 지침과 같은 중요 정보를 제공합니다.

다음 단계

Series 3 디바이스에서 LCD 패널 사용

Series 3 디바이스에서는 시스템의 웹 인터페이스를 사용하지 않고 디바이스 전면의 LCD 패널을 사용하여 디바이스 정보를 보거나 특정 설정을 구성할 수 있습니다.

LCD 패널에는 디스플레이와 4개의 다기능 키가 있으며, 디바이스 상태에 따라 다른 정보를 표시하고 다른 구성을 허용하는 멀티 모드로 작동합니다.

자세한 내용은 다음 섹션을 참조하십시오.

- LCD 패널 구성 요소 이해, 페이지 6-2에서는 LCD 패널의 구성 요소를 식별하고 패널의 주 메뉴를 표시하는 방법을 설명합니다.
- LCD 다기능 키 사용, 페이지 6-3에서는 LCD 패널에서 다기능 키를 사용하는 방법에 대해 설명합니다.
- 유휴 디스플레이 모드, 페이지 6-3에서는 디바이스가 유휴 상태일 때 LCD 패널에 다양한 시스템 정보를 표시하는 방식에 대해 설명합니다.
- 네트워크 구성 모드, 페이지 6-4에서는 LCD 패널을 사용하여 디바이스 관리 인터페이스의 네트워크 구성(IPv4, IPv6 주소, 서브넷 마스크 또는 접두사, 기본 게이트웨이)을 설정하는 방법에 대해 설명합니다.

주의 LCD 패널을 사용한 재구성을 허용할 경우 보안 위험에 노출될 수 있습니다. LCD 패널을 사용하여 구성할 경우 인증은 필요하지 않으며 물리적 액세스만 필요합니다.

- 시스템 상태 모드, 페이지 6-6에서는 링크 상태 전파, 바이패스 상태, 시스템 리소스 등의 모니터링되는 시스템 정보를 보고 LCD 패널 밝기 및 대비를 변경하는 방법에 대해 설명합니다.
- Information(정보) 모드, 페이지 6-8에서는 디바이스의 섀시 일련 번호, IP 주소, 모델, 소프트웨어, 펌웨어 버전과 같은 식별 시스템 정보를 보는 방법에 대해 설명합니다.
- 오류 경고 모드, 페이지 6-9에서는 LCD 패널이 바이패스, 팬 상태 또는 하드웨어 경고 등의 오류 또는 장애 상태를 알리는 방법에 대해 설명합니다.

참고 LCD 패널을 사용하려면 디바이스 전원을 켜야 합니다. 디바이스의 전원을 안전하게 켜거나 끄는 방법에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*의 디바이스 관리 장을 참조하십시오.

LCD 패널 구성 요소 이해

Series 3 디바이스의 전면에 있는 LCD 패널에는 디스플레이와 4개의 다기능 키가 있습니다.

- 디스플레이에는 2개의 텍스트 라인(각각 최대 17자)과 다기능 키 맵이 포함되어 있습니다. 기호를 포함하는 맵은 해당 다기능 키로 수행할 수 있는 작업을 나타냅니다.
- 다기능 키를 사용하면 LCD 패널 모드에 따라 달라지는 기본 구성 작업을 완료하고 시스템 정보를 볼 수 있습니다. 자세한 내용은 LCD 다기능 키 사용, 페이지 6-3을(를) 참고하십시오.

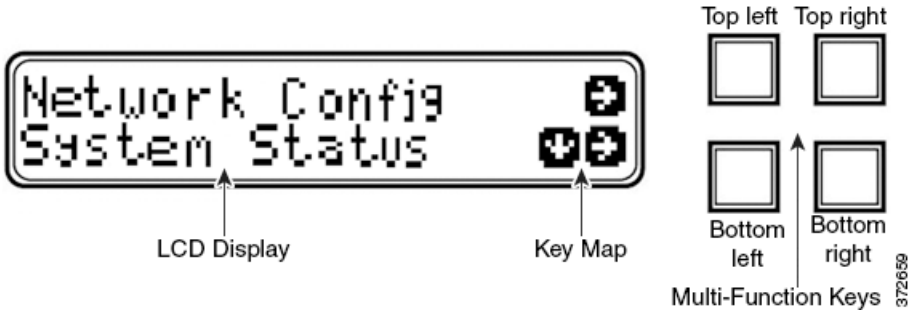
다음 그래픽은 키 맵이 포함되지 않은 패널의 기본 유휴 디스플레이 모드를 보여줍니다.

그림 6-1 LCD 패널, 유휴 디스플레이 모드

유휴 디스플레이 모드에서는 패널에 CPU 사용률 및 사용 가능한 메모리와 섀시 일련 번호가 번갈아 표시됩니다. 아무 키나 누르면 유휴 디스플레이 모드가 중단되고 네트워크 컨피그레이션, 시스템 상태 및 정보 모드에 액세스할 수 있는 LCD 패널의 주 메뉴가 시작됩니다.

다음 그래픽은 4개의 다기능 키(상단 왼쪽, 상단 오른쪽, 하단 왼쪽, 하단 오른쪽)에 해당하는 키 맵이 포함된 주 메뉴입니다.

그림 6-2 LCD 패널, 주 메뉴



주 메뉴에 액세스하려면 다음을 수행합니다.

단계 1 유휴 디스플레이 모드에서 아무 다기능 키나 누릅니다.

주 메뉴가 표시됩니다.

- 디바이스의 네트워크 컨피그레이션을 변경하려면 네트워크 구성 모드, 페이지 6-4을(를) 참조하십시오.
- 모니터링되는 시스템 정보를 보거나 LCD 패널 밝기 및 대비를 조정하려면 시스템 상태 모드, 페이지 6-6을(를) 참조하십시오.
- 식별 시스템 정보를 보려면 Information(정보) 모드, 페이지 6-8을(를) 참조하십시오.

참고 LCD 패널이 유휴 디스플레이 모드로 전환될 때 다기능 키를 누를 경우 패널에 예기치 않은 메뉴가 표시될 수 있습니다.

LCD 다기능 키 사용

4개의 다기능 키를 사용하면 Series 3 디바이스의 LCD 패널에 있는 메뉴와 옵션을 탐색할 수 있습니다. 디스플레이에 키 맵이 표시되면 다기능 키를 사용할 수 있습니다. 맵에서 기호의 위치는 해당 기능을 수행하는 데 사용되는 키의 위치와 기능에 해당합니다. 기호가 표시되지 않을 경우 해당 키는 기능이 없는 것입니다.

정보 기호의 기능 및 해당 키 맵은 LCD 패널 모드에 따라 달라집니다. 예상하는 결과를 얻지 못한 경우 LCD 패널의 모드를 확인하십시오.

다음 표는 다기능 키 기능에 대해 설명합니다.

표 6-1 LCD 패널 다기능 키

기호	설명	기능
↑	위쪽 화살표	현재 메뉴 옵션 목록을 위로 스크롤합니다.
↓	아래쪽 화살표	현재 메뉴 옵션 목록을 아래로 스크롤합니다.
←	왼쪽 화살표	다음 작업 중 하나를 수행합니다. • 아무런 작업을 수행하지 않고 LCD 패널 메뉴를 표시합니다. • 커서를 왼쪽으로 이동합니다. • 편집을 다시 활성화합니다.
→	오른쪽 화살표	다음 작업 중 하나를 수행합니다. • 해당 라인에 표시된 메뉴 옵션을 입력합니다. • 커서를 오른쪽으로 이동합니다. • 계속되는 텍스트를 스크롤합니다.
X	취소	작업을 취소합니다.
+	추가	선택한 자릿수를 1만큼 증가시킵니다.
-	빼기	선택한 자릿수를 1만큼 감소시킵니다.
✓	확인 표시	동작을 승인합니다.

유휴 디스플레이 모드

LCD 패널에서 60초간 아무 작업도 하지 않고(다기능 키를 누르지 않음) 감지된 오류가 없을 경우 유휴 디스플레이 모드로 전환됩니다. 시스템에서 오류를 감지하면 오류가 해결될 때까지 패널이 오류 경고 모드(오류 경고 모드, 페이지 6-9 참조)로 전환됩니다. 네트워크 구성을 편집하거나 진단을 실행할 때는 유휴 디스플레이 모드가 비활성화됩니다.

유휴 디스플레이 모드에서는 패널에 CPU 사용률 및 사용 가능한 메모리와 섀시 일련 번호가 5초 간격으로 번갈아 표시됩니다.

예를 들어, 각 디스플레이는 다음과 같이 표시됩니다.

```
CPU: 50%
FREE MEM: 1024 MB
```

또는

```
Serial Number:
3D99-101089108-BA0Z
```

유휴 디스플레이 모드에서 아무 다기능 키를 누르면 주 메뉴로 전환됩니다. LCD 패널 구성 요소 이해, 페이지 6-2을(를) 참조하십시오.

참고 LCD 패널이 유휴 디스플레이 모드로 전환될 때 다기능 키를 누를 경우 패널에 예기치 않은 메뉴가 표시될 수 있습니다.

네트워크 구성 모드

FireSIGHT System에서는 IPv4 및 IPv6 관리 환경을 모두 지원하는 이중 스택 구현을 제공합니다. 네트워크 구성 모드에서는 LCD 패널을 사용하여 Series 3 디바이스의 관리 인터페이스에 대한 네트워크 설정(IP 주소, 서브넷 마스크 또는 접두사, 기본 게이트웨이)을 구성할 수 있습니다.

LCD 패널을 사용하여 관리되는 디바이스의 IP 주소를 편집하려면 관리하는 방어 센터에 변경 사항이 반영되는지 확인하십시오. 경우에 따라 디바이스 관리 설정을 수동으로 편집해야 할 수도 있습니다. 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

기본적으로 LCD 패널을 사용하여 네트워크 구성을 변경하는 기능은 비활성화되어 있습니다. 초기 설정 프로세스 중 또는 디바이스의 웹 인터페이스를 사용하여 이 기능을 활성화할 수 있습니다. 자세한 내용은 LCD 패널을 사용하여 네트워크 재구성 허용, 페이지 6-6을(를) 참고하십시오.

주의 이 옵션을 활성화할 경우 보안 위험에 노출될 수 있습니다. LCD 패널을 사용하여 네트워크 설정을 구성할 경우 인증은 필요하지 않으며 물리적 액세스만 필요합니다.

네트워크 구성 모드를 사용하여 네트워크 설정을 구성하려면 다음을 수행합니다.

단계 1 유휴 디스플레이 모드에서 아무 다기능 키를 누르면 주 메뉴로 전환됩니다.

주 메뉴가 표시됩니다.

```
Network Config      →
System Status       ↓ →
```

단계 2 맨 위 행의 오른쪽 화살표(à) 키를 눌러 네트워크 구성 모드에 액세스합니다.

LCD 패널에 다음과 같이 표시됩니다.

```
IPv4          ↓ →
IPv6            →
```

단계 3 오른쪽 화살표 키를 눌러 구성하려는 IP 주소를 선택합니다.

- IPv4의 경우 LCD 패널에 다음이 표시될 수 있습니다.

```
IPv4 set to DHCP.   ←
Enable Manual?      →
```

- IPv6의 경우 LCD 패널에 다음이 표시될 수 있습니다.

```
IPv6 Disabled.      ←
Enable Manual?      →
```

단계 4 네트워크를 수동으로 구성하려면 오른쪽 화살표 키를 누릅니다.

- IPv4의 경우 LCD 패널에 IPv4 주소가 표시됩니다. 예를 들면 다음과 같습니다.

```
IPv4 Address:     - +
194.170.001.001   X →
```

- IPv6의 경우 LCD 패널에 빈 IPv6 주소가 표시됩니다. 예를 들면 다음과 같습니다.

```
IPv6 Address:     - +
0000:0000:0000:00 X →
```

패널의 첫 번째 라인에는 IPv4 또는 IPv6 주소 중 어떤 주소를 편집 중인지가 표시됩니다. 두 번째 라인에는 편집 중인 IP 주소가 표시됩니다. 첫 번째 자리에 밑줄 커서가 표시되며, 이는 편집 중인 자리를 나타냅니다. 두 개의 기호는 각 행의 오른쪽에 있는 다기능 키에 해당합니다.

IPv6 주소는 디스플레이에 완전히 표시되지 않습니다. 각 자리를 편집하고 커서를 오른쪽으로 이동하면 IPv6 주소가 오른쪽으로 스크롤됩니다.

단계 5 필요에 따라 커서로 밑줄 표시된 자리를 편집하고 IP 주소의 다음 자리로 이동합니다.

- 자릿수를 편집하려면 맨 위 행에 있는 - 또는 + 키를 눌러 한 자리씩 줄이거나 늘립니다.
- IP 주소에서 다음 자리로 이동하려면 맨 아래 행에 있는 오른쪽 화살표 키를 눌러 커서를 오른쪽 다음 자리로 이동합니다.

커서가 첫 번째 자리에 있으면 LCD 패널에 IP 주소 끝에 취소 및 오른쪽 화살표 기호가 표시됩니다. 커서가 다른 자리에 있으면 LCD 패널에 왼쪽 및 오른쪽 화살표 기호가 표시됩니다.

단계 6 IPv4 또는 IPv6 주소 편집을 완료하면 오른쪽 화살표 키를 다시 눌러 확인 표시(✓) 키를 표시하고 변경 사항을 승인합니다.

오른쪽 화살표 키를 누르기 전 디스플레이의 기능 기호는 다음 샘플과 같습니다.

```
IPv4 Address:     - +
194.170.001.001   X →
```

오른쪽 화살표 키를 누른 다음 디스플레이의 기능 기호는 다음 샘플과 같습니다.

```
IPv4 Address:     X ✓
194.170.001.001   ←
```

단계 7 IP 주소 변경 사항을 승인하려면 확인 표시 키를 누릅니다.

IPv4의 경우 LCD 패널에 다음이 표시됩니다.

```
Subnet Mask:      - +
000.000.000.000   X →
```

IPv6의 경우 LCD 패널에 다음이 표시됩니다.

```
Prefix:           - +
000.000.000.000   X →
```

단계 8 IP 주소를 편집할 때와 동일한 방식으로 서브넷 마스크 또는 접두사를 편집하고 확인 표시 키를 눌러 변경 사항을 승인합니다.

LCD 패널에 다음과 같이 표시됩니다.

```
Default Gateway   - +
000.000.000.000   X →
```

단계 9 IP 주소를 편집할 때와 동일한 방식으로 기본 게이트웨이를 편집하고 확인 표시 키를 눌러 변경 사항을 승인합니다.

LCD 패널에 다음과 같이 표시됩니다.

```
Save?          ✓
               X
```

단계 10 확인 표시 키를 눌러 변경 사항을 저장합니다.

LCD 패널을 사용하여 네트워크 재구성 허용

LCD 패널을 사용하여 네트워크 구성을 변경할 경우 보안 위험에 노출될 수 있으므로 기본적으로 이 기능은 비활성화되어 있습니다. 초기 설정 프로세스 중(Series 3 디바이스 설정, 페이지 5-4 참조) 또는 다음 절차에 설명된 대로 디바이스의 웹 인터페이스를 사용하여 이 기능을 활성화할 수 있습니다.

디바이스의 LCD 패널을 사용한 네트워크 재구성을 허용하려면 다음을 수행합니다.

액세스: Admin

단계 1 디바이스의 초기 설정을 완료한 후 관리자 권한이 있는 계정을 사용하여 디바이스의 웹 인터페이스에 로그인합니다.

단계 2 **System(시스템) > Local(로컬) > Configuration(컨피그레이션)**을 선택합니다.

Information(정보) 페이지가 나타납니다.

단계 3 **Network(네트워크)**를 클릭합니다.

Network Settings(네트워크 설정) 페이지가 나타납니다.

단계 4 LCD 패널 아래에서 **Allow reconfiguration of network configuration(네트워크 컨피그레이션 재구성 허용)** 확인란을 선택합니다. 보안 경고가 표시되면 이 옵션을 활성화할지 확인합니다.

정보 이 페이지의 다른 옵션에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*를 참조하십시오.

단계 5 **Save(저장)**를 클릭합니다.

네트워크 설정이 변경됩니다.

시스템 상태 모드

LCD 패널의 시스템 상태 모드에서는 링크 상태 전파, 바이패스 상태, 시스템 리소스 등의 모니터링되는 시스템 정보를 표시합니다. 또한 시스템 상태 모드에서 LCD 패널의 밝기와 대비를 변경할 수 있습니다.

다음 표에서는 이 모드에서 사용 가능한 정보 및 옵션에 대해 설명합니다.

표 6-2 시스템 상태 모드 옵션

옵션	설명
리소스	CPU 사용률 및 사용 가능한 메모리를 표시합니다. 유휴 디스플레이 모드에서도 이 정보가 표시됩니다.

Link State	현재 사용 중인 인라인 세트 목록과 해당 세트의 링크 상태를 표시합니다. 첫 번째 라인은 인라인 세트를 식별하고 두 번째 라인은 상태(normal(정상) 또는 tripped(트립))를 표시합니다. 예를 들면 다음과 같습니다.
	`eth2-eth3:`
	`normal`

Fail Open(고장 시 열림)	사용 중인 바이패스 인라인 세트 목록과 해당 쌍의 상태(normal(정상) 또는 in bypass(바이패스 중))를 표시합니다.
Fan Status(팬 상태)	디바이스에 있는 팬의 목록과 상태를 표시합니다.
Diagnostics(진단)	고객 지원에서 알려주는 특정 키 순서를 누른 후 액세스할 수 있습니다. ⚠ **주의** 고객 지원의 안내 없이 진단 메뉴에 액세스하지 **마십시오**. 고객 지원의 구체적인 지침을 받지 않고 진단 메뉴에 액세스할 경우 시스템이 손상될 수 있습니다.
LCD Brightness	LCD 디스플레이의 밝기를 조정할 수 있습니다.
LCD Contrast	LCD 디스플레이의 대비를 조정할 수 있습니다.

시스템 상태 모드로 전환하고 모니터링되는 시스템 정보를 보려면 다음을 수행합니다.

단계 1 유휴 디스플레이 모드에서 아무 다기능 키를 누르면 주 메뉴로 전환됩니다.

주 메뉴가 표시됩니다.

```
Network Config          →
System Status           ↓ →
```

단계 2 맨 아래 행에 있는 오른쪽 화살표(→) 키를 눌러 시스템 상태 모드에 액세스합니다.

LCD 패널에 다음과 같이 표시됩니다.

```
Resources               ↓ →
Link State              ↓ →
```

단계 3 아래쪽 화살표(â) 키를 눌러 옵션을 스크롤합니다. 확인하려는 상태 옆에 있는 행의 오른쪽 화살표 키를 누릅니다.

선택한 옵션에 따라, LCD 패널에 표 6-2 페이지 6-7에 나열된 정보가 표시됩니다. LCD 패널 밝기 또는 대비를 변경하려면 다음 절차를 참조하십시오.

LCD 패널 밝기 또는 대비를 조정하려면 다음을 수행합니다.

단계 1 System Status(시스템 상태) 모드에서 LCD 패널에 LCD Brightness(LCD 밝기) 및 LCD Contrast(LCD 대비) 옵션이 표시될 때까지 아래쪽 화살표(â) 키를 누릅니다.

```
LCD Brightness      ↓ →
LCD Contrast        ↓ →
```

단계 2 조정하려는 LCD 디스플레이 기능(밝기 또는 대비) 옆에 있는 행에서 오른쪽 화살표 키를 누릅니다.

LCD 패널에 다음과 같이 표시됩니다.

```
Increase              →
Decrease            ↓ →
```

단계 3 선택한 디스플레이 기능을 높이거나 낮추려면 오른쪽 화살표 키를 누릅니다.

키를 누르면 LCD 디스플레이가 변경됩니다.

단계 4 Exit(종료) 옵션을 표시하려면 아래쪽 화살표를 누릅니다.

```
Decrease            ↓ →
Exit                  →
```

단계 5 설정을 저장하고 주 메뉴로 돌아가려면 Exit(종료) 행에서 오른쪽 화살표 키를 누릅니다.

Information(정보) 모드

LCD 패널의 Information(정보) 모드에서는 디바이스의 섀시 일련 번호, IP 주소, 모델, 소프트웨어 및 펌웨어 버전과 같은 식별 시스템 정보가 표시됩니다. 고객 지원에 지원을 요청할 때 이러한 정보가 필요할 수 있습니다.

다음 표에서는 이 모드에서 사용 가능한 정보에 대해 설명합니다.

표 6-3 정보 모드 옵션

옵션	설명
IP 주소	디바이스 관리 인터페이스의 IP 주소를 표시합니다.
Model(모델)	디바이스의 모델을 표시합니다.
Serial number(일련 번호)	디바이스의 섀시 일련 번호를 표시합니다.
Versions(버전)	디바이스의 시스템 소프트웨어 및 펌웨어 버전을 표시합니다. 다기능 키를 사용하여 다음 정보를 스크롤합니다. • 제품 버전 • NFE 버전 • 마이크로 엔진 버전 • 플래시 버전 • GerChr 버전

정보(Information) 모드로 전환하고 식별 시스템 정보를 보려면 다음을 수행합니다.

단계 1 유휴 디스플레이 모드에서 아무 다기능 키를 누르면 주 메뉴로 전환됩니다.

주 메뉴가 표시됩니다.

```
Network Config          →
System Status           ↓ →
```

단계 2 LCD 패널에 Information(정보) 모드가 표시될 때까지 아래쪽 화살표(â)를 눌러 모드 사이를 스크롤합니다.

```
System Status           ↓ →
Information             ↓ →
```

단계 3 맨 아래 행에 있는 오른쪽 화살표(→) 키를 눌러 정보 모드에 액세스합니다.

단계 4 아래쪽 화살표(â) 키를 눌러 옵션을 스크롤합니다. 확인하려는 정보 옆에 있는 행의 오른쪽 화살표 키를 누릅니다.

선택한 옵션에 따라, LCD 패널에 표 6-3 페이지 6-8에 나열된 정보가 표시됩니다.

오류 경고 모드

하드웨어 오류 또는 장애 상태가 발생하면 유휴 디스플레이 모드가 중단되고 오류 경고 모드로 전환됩니다. 오류 경고 모드에서는 LCD 디스플레이가 깜박이고 다음 표에 나열된 오류 중 하나 이상이 표시됩니다.

표 6-4 LCD 패널 오류 경고

오류	설명
하드웨어 경보	하드웨어 경보에 대한 경고를 표시합니다.
링크 상태 전파	쌍으로 연결된 인터페이스의 링크 상태를 표시합니다.
바이패스	바이패스 모드에서 구성된 인라인 세트의 상태를 표시합니다.
팬 상태	팬이 위험 상태에 도달하는 경우 경보를 표시합니다.

하드웨어 오류 경고가 발생하면 LCD에 다음과 같은 주 하드웨어 경고 메뉴가 표시됩니다.

```
HARDWARE ERROR!         →
Exit                    →
```

다기능 키를 사용하여 오류 경고 목록을 스크롤하거나 오류 경고 모드를 종료합니다. 모든 오류 조건이 해결될 때까지 LCD 디스플레이가 계속 깜박이면서 경고 메시지를 표시합니다.

LCD 패널에는 항상 플랫폼 데몬 오류 메시지가 먼저 표시되고 다음으로 다른 하드웨어 오류 메시지 목록이 표시됩니다. 다음 표에는 Series 3 디바이스 오류 메시지의 기본 정보가 제공됩니다. 여기서, *x*는 경고를 생생한 NFE 가속기 카드(0 또는 1)를 나타냅니다.

표 6-5 하드웨어 경보 오류 메시지

오류 메시지	모니터링되는 상태	설명
NFE_platformd*X*	플랫폼 데몬	플랫폼 데몬이 실패할 경우 경보를 표시합니다.
NFE_temp*X*	온도 상태	가속기 카드의 온도가 허용 가능한 한도를 초과하는 경우 경보를 표시합니다. • WARNING: 80°C/176°F(7000 Series) 또는 97°C/206°F(8000 Series) 초과 시 • CRITICAL: 90°C/194°F(7000 Series) 또는 102°C/215°F(8000 Series) 초과 시
HeartBeat*X*	하트비트	시스템에서 하트비트를 감지할 수 없는 경우 경보를 표시합니다.
frag*X*	nfe_ipfragd (호스트 조각) 데몬	ipfrag 데몬이 실패하는 경우 경보를 표시합니다.
rules*X*	Rulesd (호스트 규칙) 데몬	Rulesd 데몬이 실패하는 경우 경보를 표시합니다.
TCAM*X*	TCAM 데몬	TCAM 데몬이 실패하는 경우 경보를 표시합니다.
NFEMessD*X*	메시지 데몬	메시지 데몬이 실패하는 경우 경보를 표시합니다.
NFEHardware	하드웨어 상태	하나 이상의 가속기 카드가 통신하지 않는 경보를 표시합니다.
NFEcount	감지된 카드	디바이스에서 감지된 가속기 카드의 수가 플랫폼에 있어야 하는 가속기 카드 수와 다를 경우 경보를 표시합니다.
7000 Series만 해당: GerChr_comm 8000 Series만 해당: NMSB_comm	통신	미디어 어셈블리가 없거나 통신하지 않는 경우 경보를 표시합니다.
7000 Series만 해당: gerd 8000 Series만 해당: scmd	scmd 데몬 상태	scmd 데몬이 실패하는 경우 경보를 표시합니다.
7000 Series만 해당: gpsl 8000 Series만 해당: psls	psls 데몬 상태	psls 데몬이 실패하는 경우 경보를 표시합니다.
7000 Series만 해당: gftw 8000 Series만 해당: ftwo	ftwo 데몬 상태	ftwo 데몬이 실패하는 경우 경보를 표시합니다.
NFE_port18 NFE_port19 NFE_port20 NFE_port21	내부 링크 상태	네트워크 모듈 스위치 보드와 가속기 카드 간 링크가 실패하는 경우 경보를 표시합니다. • 7000 Series 모든 제품군: NFE_port18만 해당 • 8000 Series 81xx 제품군: NFE_port18 및 NFE_port19만 해당 82xx 제품군 및 83xx 제품군: NFE_port18, NFE_port19, NFE_port20, NFE_port21

LCD 디스플레이에 하드웨어 경보 오류 메시지를 확인하려면 다음 절차를 사용합니다.

하드웨어 경보 오류 메시지를 보려면 다음을 수행합니다.

단계 1 오류 경보 모드의 HARDWARE ERROR! 라인에서 오른쪽 화살표(→) 키를 눌러 오류 경보 모드를 트리거한 하드웨어 오류를 확인합니다.

LCD 패널에 `NFE platform` 데몬 장애로 시작하여 다음으로 오류 메시지 목록을 표시하는 오류 경보 메시지가 나열됩니다.

```
NFEplatformd X
NFEtemp X                ↓
```

여기서, *x*는 경보를 생성한 가속기 카드(`0` 또는 `1`)를 나타냅니다.

단계 2 추가 오류를 확인하려면 오류 메시지 라인에서 아래쪽 화살표(â) 키를 누릅니다. 추가 오류가 없는 경우 Exit(종료) 행이 나타납니다.

```
Exit                     →
```

단계 3 오류 경보 모드를 종료하려면 오른쪽 화살표(→) 키를 누릅니다.

경보를 트리거한 오류를 해결하기 전에 오류 경보 모드를 종료하면 LCD 패널이 오류 경보 모드로 돌아갑니다. 도움을 받으려면 고객 지원에 문의하십시오.

하드웨어 사양

FireSIGHT System은 조직의 요구 사항을 충족하기 위해 다양한 어플라이언스에 제공됩니다. 랙에 어플라이언스를 설치하는 데 대한 자세한 내용은 랙 및 캐비닛 마운팅 옵션, 페이지 7-1을(를) 참조하십시오.

참고 ASA FirePOWER 디바이스의 하드웨어 사양에 대한 자세한 내용은 ASA 설명서를 참조하십시오.

각 어플라이언스의 하드웨어 사양은 다음 섹션에 설명되어 있습니다.

랙 및 캐비닛 마운팅 옵션

FireSIGHT System 어플라이언스를 랙 및 서버 캐비닛에 마운팅할 수 있습니다. 어플라이언스는 3D7010, 3D7020, 3D7030 및 3D7050을 제외하고 랙 마운팅 키트로 제공됩니다. 랙에 어플라이언스를 마운트하는 방법에 대한 자세한 내용은 랙 마운팅 키트와 함께 제공되는 지침을 참조하십시오.

3D7010, 3D7020, 3D7030 및 3D7050에는 별도로 제공되는 트레이 및 랙 마운팅 키트가 필요합니다. 다른 어플라이언스의 랙 및 캐비닛 마운팅 키트를 별도로 구매할 수 있습니다.

방어 센터

방어 센터에 대한 자세한 내용은 다음 섹션을 참조하십시오.

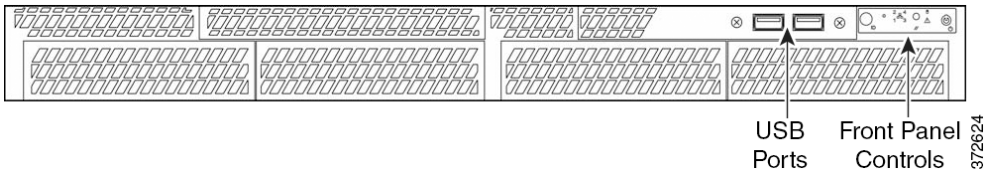
DC750

DC750은 1U 어플라이언스입니다. 어플라이언스에 대한 자세한 내용은 다음 섹션을 참조하십시오.

DC750 섀시 전면 보기

DC750 섀시 전면에는 전면 패널 제어가 포함되어 있습니다.

그림 7-1 DC750



다음 다이어그램은 DC750의 전면 패널 제어 및 LED를 보여줍니다. 하드 디스크 드라이브 및 시스템 상태 아이콘, NIC(1, 2, 3, 4) 활동 상태 번호, 전원 버튼도 LED입니다.

그림 7-2 DC750

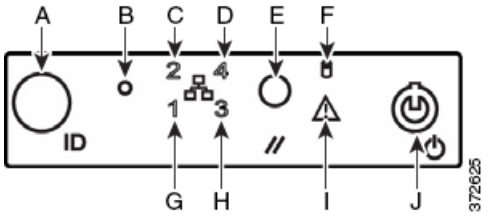


표 7-1 전면 패널 구성 요소

A	ID 버튼 및 ID LED	F	하드 디스크 드라이브 상태 LED
B	마스크 불가능 중단 버튼	G	NIC 1 활동 상태 LED
C	NIC 2 활동 상태 LED	H	NIC 3 활동 상태 LED
D	NIC 4 활동 상태 LED	I	시스템 상태 LED
E	재설정 버튼	J	전원 버튼 및 전원 LED

섀시 전면 패널에는 시스템의 작동 상태를 확인할 수 있는 5개의 LED가 있습니다. 다음 표에서는 전면 패널의 LED에 대해 설명합니다.

표 7-2 DC750 전면 패널 LED

LED	설명
시스템 상태	시스템 상태를 다음과 같이 나타냅니다. • 녹색 표시등은 시스템이 정상 작동 중임을 나타냅니다. • 녹색 표시등이 깜박이는 경우 시스템이 저하된 상태로 작동 중임을 나타냅니다. 자세한 내용은 표 7-3 페이지 7-3을(를) 참고하십시오.
전원	시스템에 전원이 연결되었는지 또는 절전 모드인지를 나타냅니다. • 녹색 표시등은 시스템이 정상 작동 중임을 나타냅니다. • 표시등이 꺼진 경우 시스템 전원이 꺼진 상태를 나타냅니다. • 녹색 표시등이 깜박이는 경우 시스템이 절전 모드임을 나타냅니다. 절전 표시는 대기 시 칩셋에 의해 유지됩니다. BIOS를 통과하지 않고 시스템 전원이 꺼지면 BIOS가 전원을 끌 당시의 상태를 삭제하기 전까지 시스템 전원을 켜면 해당 상태가 복원됩니다. 시스템 전원이 정상적으로 꺼지지 않은 경우에는 장애 또는 컨피그레이션 변경으로 인해 BIOS가 실행되지 않으므로 시스템 상태 표시등이 꺼진 상태에서 전원 표시등이 깜박입니다.
하드 드라이브 활동	하드 드라이브 활동을 나타냅니다. • 녹색 표시등이 깜박이는 경우 고정 디스크 드라이브가 활성 상태임을 나타냅니다. • 표시등이 꺼진 경우 드라이브 활동이 없거나 시스템 전원이 꺼졌거나 절전 모드임을 나타냅니다. 드라이브 활동은 온보드 하드 디스크 컨트롤러에서 결정됩니다. 또한 서버 보드가 헤더를 제공하여 추가 컨트롤러에서 이 표시등에 액세스할 수 있습니다.
NIC 활동	시스템과 네트워크 간의 활동을 나타냅니다. • 녹색 표시등이 깜박이는 경우 활동이 있음을 나타냅니다. • 표시등이 꺼진 경우 활동이 없음을 나타냅니다.

다음 표에서는 시스템 상태 LED가 켜질 수 있는 상태에 대해 설명합니다.

표 7-3 DC750 시스템 상태

상태	설명
위험	다음 이벤트와 관련된 위험하거나 복구 불가능한 임계값 초과 상태입니다. • 온도, 전압 또는 팬의 위험 임계값 초과 • 전원 하위 시스템 장애 • 잘못 설치된 프로세서 또는 프로세서 비호환성으로 인해 시스템 전원을 켤 수 없음 • PCI SERR 및 PERR과 같이 시스템 메모리의 수정 불가능한 ECC 오류 및 치명적/수정 불가능한 버스 오류를 포함한 위험한 이벤트 기록 오류
비위험	비위험 상태는 다음 이벤트와 관련된 임계값이 초과된 상태입니다. • 온도, 전압 또는 팬의 비위험 임계값 초과 • 섀시 침입 • 시스템 BIOS에서 Fault Indication 명령을 설정합니다. BIOS에서는 이 명령을 사용하여 시스템 메모리 또는 CPU 컨피그레이션 변경과 같은 추가적인 비위험 상태를 표시할 수 있습니다.

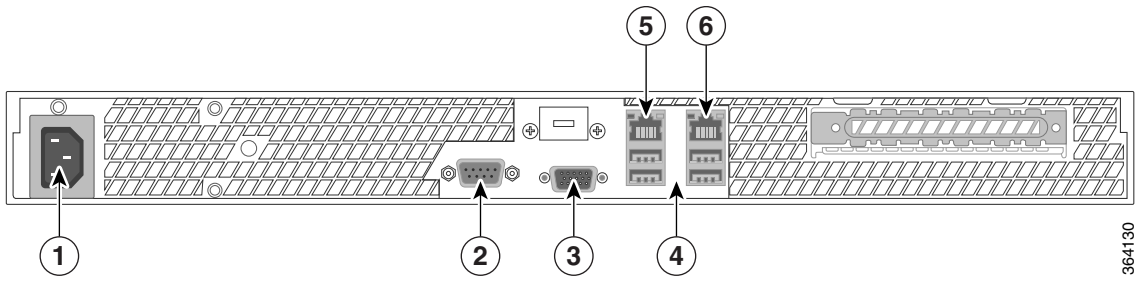
표 7-3 DC750 시스템 상태(계속)

상태	설명
저하됨	저하된 상태는 다음 이벤트와 관련되어 있습니다. • 하나 이상의 프로세서가 FRB(Fault Resilient Boot) 또는 BIOS에 의해 비활성화됨 • BIOS가 시스템 메모리 중 일부를 비활성화하거나 배제함

DC750 섀시 후면 보기

섀시 후면에는 DC750용 전원 공급 장치와 연결 포트가 있습니다.

그림 7-3 DC750



1	전원 공급 장치	**4**	USB 포트
2	시리얼 포트	**5**	기본 관리 인터페이스
3	VGA 포트	**6**	대체 관리 인터페이스

다음 표에서는 어플라이언스 후면에 표시되는 기능에 대해 설명합니다.

표 7-4 DC750 시스템 구성 요소: 후면 보기

기능	설명
전원 공급 장치	AC 전원을 통해 방어 센터에 전원을 공급합니다.
시리얼 포트, VGA 포트 USB 포트	디바이스에 모니터, 키보드 및 마우스를 연결할 수 있습니다.
10/100/1000Mbps 이더넷 관리 인터페이스	OOB(Out of Band) 관리 네트워크 연결에 사용합니다. 관리 인터페이스는 유지 보수 및 컨피그레이션 목적으로**만** 사용되며 서비스 트래픽을 전달하기 위한 용도가 아닙니다.
대체 관리 인터페이스	eStreamer 클라이언트 또는 추가 관리 인터페이스에 대한 대체 인터페이스를 제공합니다.

10/100/1000Mbps 관리 인터페이스는 어플라이언스 후면에 있습니다. 다음 표에서는 관리 인터페이스와 관련된 LED에 대해 설명합니다.

표 7-5 DC750 관리 인터페이스 LED

LED	설명
왼쪽(링크)	링크가 활성 상태인지 여부를 나타냅니다. • 표시등이 켜진 경우 링크가 활성 상태임을 나타냅니다. • 표시등이 꺼진 경우 링크가 없음을 나타냅니다.
오른쪽(활동)	포트의 활동을 나타냅니다. • 표시등이 깜박이는 경우 활동이 있음을 나타냅니다. • 표시등이 꺼진 경우 링크가 없음을 나타냅니다.

DC750 물리적 및 환경 매개변수

다음 표에서는 어플라이언스의 물리적 속성 및 환경 매개변수에 대해 설명합니다.

표 7-6 DC750 물리적 및 환경 매개변수

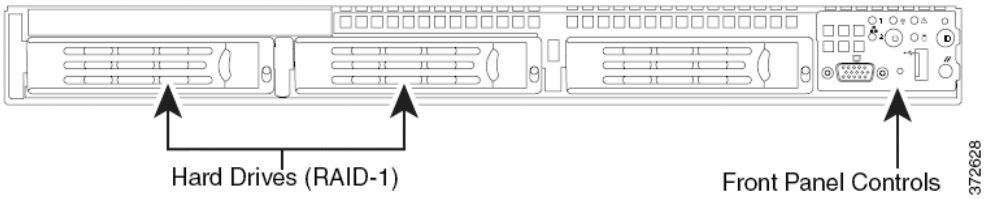
매개변수	DC750
폼 팩터	1U
크기(D x W x H)	21.8인치 x 17.25인치 x 1.67인치(55.37cm x 43.82cm x 4.24cm)
최대 무게	33파운드(15kg)
전원 공급 장치	120VAC의 경우 250W 전원 공급 장치 110볼트, 50/60Hz에서 최대 6.0암페어 220볼트, 50/60Hz에서 최대 3.0암페어
작동 온도	10°C~35°C(50°F~95°F), 최대 변경률은 시간당 10°C(18°F)를 초과하지 않아야 함
비작동 온도	-40°C~+70°C(-40°F~+158°F)
비작동 습도	35°C(95°F)에서 90%, 비응결
음향 노이즈	일반 사무실 주변 온도(23°C +/- 2°C, 73°F +/- 4°F)의 유휴 상태에서 7BA
작동 충격	2G의 반 사인파 충격 시 오류 없음(11ms 동안)
패키지 충격	24인치(60cm)에서 자유 낙하 시 작동 가능, 외부는 손상될 수 있음, 섀시 무게 40~80파운드(18~36kg)
ESD	공중 방전의 경우 +/- 12kV, 접점의 경우 8K
공기 흐름	전면에서 후면
시스템 냉각 요구 사항	시간당 1660BTU

DC1500

DC1500은 1U 어플라이언스입니다. 어플라이언스에 대한 자세한 내용은 다음 섹션을 참조하십시오.

DC1500 섀시 전면 보기

섀시 전면에는 하드 드라이브 및 전면 패널 제어가 포함되어 있습니다.



다음 다이어그램은 전면 패널 제어 및 LED를 보여줍니다.

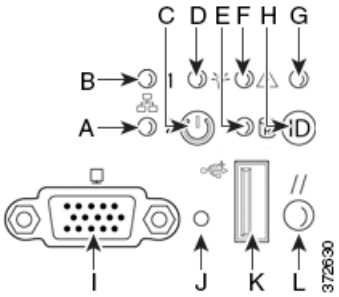


표 7-7 전면 패널 구성 요소

A	NIC 2 활동 LED	G	ID LED
B	NIC 1 활동 LED	H	ID 버튼
C	전원 버튼	I	비디오 커넥터(사용 불가능)
D	전원/절전 LED	J	마스크 불가능 중단 버튼
E	고정 디스크 드라이브 상태	K	USB 2.0 커넥터
F	시스템 상태 LED	L	재설정 버튼

섀시 전면 패널에는 6개의 LED가 있으며 전면 베젤을 장착하거나 장착하지 않은 상태에서 시스템의 운영 상태를 표시할 수 있습니다. 다음 표에서는 전면 패널의 LED에 대해 설명합니다.

표 7-8 DC1500 전면 패널 LED

LED	설명
NIC 1 활동 NIC 2 활동	시스템과 네트워크 간의 활동을 나타냅니다. • 녹색 표시등이 깜박이는 경우 활동이 있음을 나타냅니다. • 표시등이 꺼진 경우 활동이 없음을 나타냅니다.
전원/절전	시스템에 전원이 연결되었는지 또는 절전 모드인지를 나타냅니다. • 녹색 표시등은 시스템이 정상 작동 중임을 나타냅니다. • 녹색 표시등이 깜박이는 경우 시스템이 절전 모드임을 나타냅니다. • 표시등이 꺼진 경우 시스템에 전원이 연결되어 있지 않음을 나타냅니다. 절전 표시는 대기 시 칩셋에 의해 유지됩니다. BIOS를 통과하지 않고 시스템 전원이 꺼지면 BIOS가 전원을 끌 당시의 상태를 삭제하기 전까지 시스템 전원을 켜면 해당 상태가 복원됩니다. 시스템 전원이 정상적으로 꺼지지 않은 경우에는 장애 또는 컨피그레이션 변경으로 인해 BIOS가 실행되지 않으므로 시스템 상태 표시등이 꺼진 상태에서 전원 표시등이 깜박입니다.
하드 드라이브 활동	하드 드라이브 활동을 나타냅니다. • 녹색 표시등이 깜박이는 경우 고정 디스크 드라이브가 활성 상태임을 나타냅니다. • 황색 표시등은 고정 디스크 드라이브에 장애가 발생했음을 나타냅니다. • 표시등이 꺼진 경우 드라이브 활동이 없거나 시스템 전원이 꺼졌거나 절전 모드임을 나타냅니다. 드라이브 활동은 온보드 하드 디스크 컨트롤러에서 결정됩니다. 또한 서버 보드가 헤더를 제공하여 추가 컨트롤러에서 이 표시등에 액세스할 수 있습니다.
시스템 상태	시스템 상태를 다음과 같이 나타냅니다. • 녹색 표시등은 시스템이 정상 작동 중임을 나타냅니다. • 녹색 표시등이 깜박이는 경우 시스템이 저하된 상태로 작동 중임을 나타냅니다. • 황색 표시등은 시스템이 위험하거나 복구 불가능한 상태임을 나타냅니다. • 황색 표시등이 깜박이는 경우 시스템이 위험하지 않은 상태임을 나타냅니다. • 표시등이 꺼진 경우 POST(Power On Self Test)가 진행 중이거나 시스템이 중지된 상태를 나타냅니다. **참고** 황색 상태 표시등이 녹색 상태 표시등보다 우선합니다. 황색 표시등이 켜져 있거나 깜박이는 경우 녹색 표시등이 꺼집니다. 자세한 내용은 표 7-3 페이지 7-3을(를) 참고하십시오.
시스템 ID	고밀도 랙에 설치된 시스템을 다른 유사한 시스템과 식별할 수 있습니다. • 파란색 표시등은 ID 버튼을 눌렀음을 나타내며 파란색 표시등은 어플라이언스 후면에 있습니다. • 표시등이 꺼진 경우 ID 버튼을 누르지 않았음을 나타냅니다.

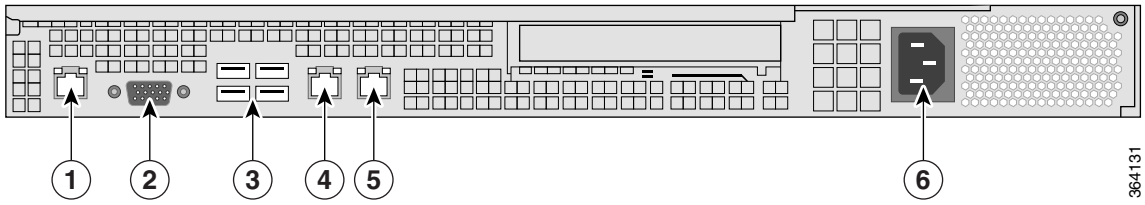
다음 표에서는 시스템 상태 LED가 켜질 수 있는 상태에 대해 설명합니다.

표 7-9 DC1500 시스템 상태

상태	설명
위험	다음 이벤트와 관련된 위험하거나 복구 불가능한 임계값 초과 상태입니다. • 온도, 전압 또는 팬의 위험 임계값 초과 • 전원 하위 시스템 장애 • 잘못 설치된 프로세서 또는 프로세서 비호환성으로 인해 시스템 전원을 켤 수 없음 • PCI SERR 및 PERR과 같이 시스템 메모리의 수정 불가능한 ECC 오류 및 치명적/수정 불가능한 버스 오류를 포함한 위험한 이벤트 기록 오류
비위험	비위험 상태는 다음 이벤트와 관련된 임계값이 초과된 상태입니다. • 온도, 전압 또는 팬의 비위험 임계값 초과 • 섀시 침입 • 시스템 BIOS에서 Fault Indication 명령을 설정합니다. BIOS에서는 이 명령을 사용하여 시스템 메모리 또는 CPU 컨피그레이션 변경과 같은 추가적인 비위험 상태를 표시할 수 있습니다.
저하됨	저하된 상태는 다음 이벤트와 관련되어 있습니다. • 하나 이상의 프로세서가 FRB(Fault Resilient Boot) 또는 BIOS에 의해 비활성화됨 • BIOS가 시스템 메모리 중 일부를 비활성화하거나 배제함

DC1500 섀시 후면 보기

섀시 후면에는 연결 포트와 전원 공급 장치가 있습니다.



1	시리얼 포트	**4**	기본 관리 인터페이스
2	VGA 포트	**5**	대체 관리 인터페이스
3	USB 포트	**6**	전원 공급 장치

다음 표에서는 어플라이언스 후면에 표시되는 기능에 대해 설명합니다.

표 7-10 DC1500 시스템 구성 요소: 후면 보기

기능	설명
전원 공급 장치	AC 전원을 통해 방어 센터에 전원을 공급합니다.
VGA 포트 USB 포트	방어 센터에 모니터, 키보드 및 마우스를 연결할 수 있습니다.

표 7-10 DC1500 시스템 구성 요소: 후면 보기(계속)

기능	설명
10/100/1000Mbps 이더넷 관리 인터페이스	OOB(Out of Band) 관리 네트워크 연결에 사용합니다. 관리 인터페이스는 유지 보수 및 컨피그레이션 목적으로**만** 사용되며 서비스 트래픽을 전달하기 위한 용도가 아닙니다.
대체 관리 인터페이스	eStreamer 클라이언트 또는 추가 관리 인터페이스에 대한 대체 인터페이스를 제공합니다.
RJ45 시리얼 포트	어플라이언스의 모든 관리 서비스에 직접 액세스할 수 있도록 직접적인 워크스테이션-어플라이언스 연결을 설정합니다(RJ45-DB-9 어댑터 사용). RJ45 시리얼 포트는 유지 보수 및 컨피그레이션 목적에**만** 사용되며 서비스 트래픽을 전달하기 위한 용도가 아닙니다. **참고** 전면 및 후면 패널 시리얼 포트를 동시에 사용할 수 없습니다.

10/100/1000Mbps 관리 인터페이스는 어플라이언스 후면에 있습니다. 다음 표에서는 관리 인터페이스와 관련된 LED에 대해 설명합니다.

표 7-11 DC1500 관리 인터페이스 LED

LED	설명
왼쪽(링크)	링크가 활성 상태인지 여부를 나타냅니다. • 표시등이 켜진 경우 링크가 활성 상태임을 나타냅니다. • 표시등이 꺼진 경우 링크가 없음을 나타냅니다.
오른쪽(활동)	포트의 활동을 나타냅니다. • 표시등이 깜박이는 경우 활동이 있음을 나타냅니다. • 표시등이 꺼진 경우 활동이 없음을 나타냅니다.

DC1500 물리적 및 환경 매개변수

다음 표에서는 어플라이언스의 물리적 속성 및 환경 매개변수에 대해 설명합니다.

표 7-12 DC1500 물리적 및 환경 매개변수

매개변수	설명
폼 팩터	1U
크기(D x W x H)	27.2인치.x 16.93인치 x 1.7인치(69.1cm x 43.0cm x 4.3cm)
최대 무게	34파운드(15.4kg)
전원 공급 장치	120VAC의 경우 600 W 전원 공급 장치 110볼트, 50/60Hz에서 최대 9.5암페어 220볼트, 50/60Hz에서 최대 4.75암페어
작동 온도	10°C~35°C(50°F~95°F)
비작동 온도	-40°C~+70°C(-40°F~+158°F)
비작동 습도	28°C(82.4°F)에서 90%, 비응결
음향 노이즈	일반 사무실 주변 온도(23°C +/- 2°C, 73°F +/- 4°F)의 유휴 상태에서 7BA(랙 마운트)
작동 충격	2G의 반 사인파 충격 시 오류 없음(11ms 동안)

표 7-12 DC1500 물리적 및 환경 매개변수(계속)

매개변수	설명
패키지 충격	24인치(60cm)에서 자유 낙하 시 작동 가능, 외부는 손상될 수 있음, 섀시 무게 40~80파운드(18~36kg)
ESD	Intel 환경 테스트 사양당 +/- 15 kV(I/O포트 +/-8KV)
공기 흐름	전면에서 후면
시스템 냉각 요구 사항	시간당 2550BTU

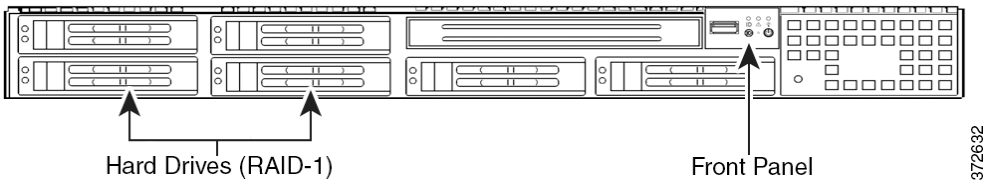
DC3500

DC3500은 1U 어플라이언스입니다. 어플라이언스에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- DC3500 섀시 전면 보기, 페이지 7-10
- DC3500 섀시 후면 보기, 페이지 7-12
- DC3500 물리적 및 환경 매개변수, 페이지 7-14

DC3500 섀시 전면 보기

섀시 전면에는 하드 드라이브와 전면 패널이 포함되어 있습니다.



어플라이언스 전면에는 전면 패널용 제어 및 LED 디스플레이가 있습니다.

다음 다이어그램은 전면 패널 제어 및 LED를 보여줍니다.

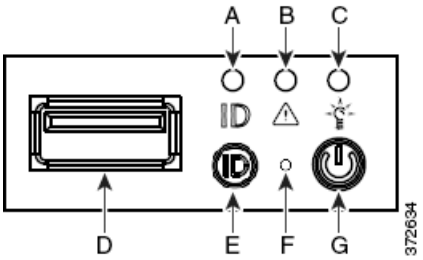


표 7-13 전면 패널 구성 요소

A	ID LED	E	ID 버튼
B	시스템 상태 LED	F	재설정 버튼
C	전원 LED	G	전원 버튼
D	USB 포트		

섀시 전면 패널에는 시스템 작동 상태를 표시하는 3개의 LED가 있습니다. 다음 표에서는 전면 패널의 LED에 대해 설명합니다.

표 7-14 DC3500 전면 패널 LED

LED	설명
전원	시스템에 전원이 연결되었는지 여부를 나타냅니다. • 녹색 표시등은 시스템에 전원이 연결되었음을 나타냅니다. • 표시등이 꺼진 경우 시스템에 전원이 연결되어 있지 않음을 나타냅니다.
시스템 상태	시스템 상태를 다음과 같이 나타냅니다. • 녹색 표시등은 시스템이 정상 작동 중임을 나타냅니다. • 녹색 표시등이 깜박이는 경우 시스템이 저하된 상태로 작동 중임을 나타냅니다. • 황색 표시등이 깜박이는 경우 시스템이 위험하지 않은 상태임을 나타냅니다. • 황색 표시등은 시스템이 위험하거나 복구 불가능한 상태임을 나타냅니다. • 표시등이 꺼진 경우 시스템이 켜지거나 꺼지는 중임을 나타냅니다. **참고** 황색 상태 표시등이 녹색 상태 표시등보다 우선합니다. 황색 표시등이 켜져 있거나 깜박이는 경우 녹색 표시등이 꺼집니다. 자세한 내용은 표 7-15 페이지 7-12을(를) 참조하십시오.
하드 드라이브 활동	하드 드라이브 상태를 다음과 같이 나타냅니다. • 녹색 표시등이 깜박이는 경우 고정 디스크 드라이브가 활성 상태임을 나타냅니다. • 황색 표시등은 고정 디스크 드라이브에 장애가 발생했음을 나타냅니다. • 표시등이 꺼진 경우 드라이브 활동이 없거나 시스템 전원이 꺼진 상태를 나타냅니다.
NIC 활동	네트워크 활동이 있는지 여부를 나타냅니다. • 녹색 표시등은 네트워크 활동이 있음을 나타냅니다. • 표시등이 꺼진 경우 네트워크 활동이 없음을 나타냅니다.
시스템 ID	고밀도 랙에 설치된 시스템을 다른 유사한 시스템과 식별할 수 있습니다. • 파란색 표시등은 ID 버튼을 눌렀음을 나타내며 파란색 표시등은 어플라이언스 후면에 있습니다. • 표시등이 꺼진 경우 ID 버튼을 누르지 않았음을 나타냅니다.

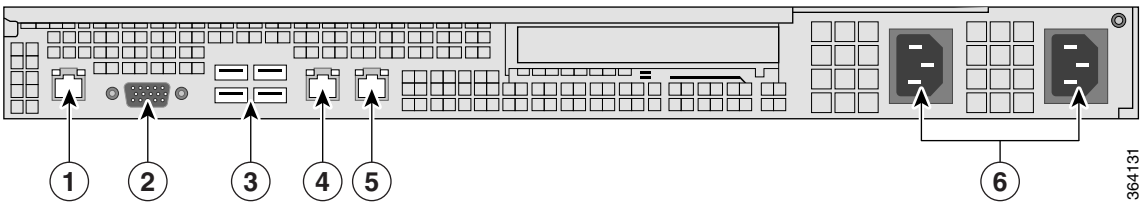
다음 표에서는 시스템 상태 LED가 켜질 수 있는 상태에 대해 설명합니다.

표 7-15 DC3500 시스템 상태

상태	설명
위험	다음 이벤트와 관련된 위험하거나 복구 불가능한 임계값 초과 상태입니다. • 온도, 전압 또는 팬의 위험 임계값 초과 • 전원 하위 시스템 장애 • 잘못 설치된 프로세서 또는 프로세서 비호환성으로 인해 시스템 전원을 켤 수 없음 • PCI SERR 및 PERR과 같이 시스템 메모리의 수정 불가능한 ECC 오류 및 치명적/수정 불가능한 버스 오류를 포함한 위험한 이벤트 기록 오류
비위험	비위험 상태는 다음 이벤트와 관련된 임계값이 초과된 상태입니다. • 온도, 전압 또는 팬의 비위험 임계값 초과 • 섀시 침입 • 시스템 BIOS에서 Fault Indication 명령을 설정합니다. BIOS에서는 이 명령을 사용하여 시스템 메모리 또는 CPU 컨피그레이션 변경과 같은 추가적인 비위험 상태를 표시할 수 있습니다.
저하됨	저하된 상태는 다음 이벤트와 관련되어 있습니다. • 하나 이상의 프로세서가 FRB(Fault Resilient Boot) 또는 BIOS에 의해 비활성화됨 • BIOS가 시스템 메모리 중 일부를 비활성화하거나 배제함 • 전원 공급 장치 중 하나가 연결되지 않았거나 작동하지 않음 **정보** 상태 저하 표시를 확인한 경우 전원 공급 장치가 올바르게 연결되었는지 확인합니다. 어플라이언스 전원을 끄고 두 전원 코드를 분리한 후 다시 연결하여 다시 장착하고 어플라이언스를 다시 시작합니다. ⚠ **주의** 전원을 안전하게 끄려면 *FireSIGHT System 사용 설명서*의 디바이스 관리에 설명된 절차를 사용하거나 방어 센터 셸에서 `shutdown -h now` 명령을 사용합니다.

DC3500 섀시 후면 보기

섀시 후면에는 연결 포트와 전원 공급 장치가 있습니다.



1	시리얼 포트	**4**	기본 관리 인터페이스
2	VGA 포트	**5**	대체 관리 인터페이스
3	USB 포트	**6**	전원 공급 장치

다음 표에서는 어플라이언스 후면에 표시되는 기능에 대해 설명합니다.

표 7-16 DC3500 시스템 구성 요소: 후면 보기

기능	설명
PS/2 마우스 커넥터 PS/2 키보드 커넥터 VGA 포트 USB 포트	RJ45 시리얼 포트를 사용하지 않고 어플라이언스에 모니터, 키보드, 마우스를 연결하여 워크스테이션과 어플라이언스를 직접 연결합니다. 또한 어플라이언스에 기본 제공된 썸 드라이브 사용하여 어플라이언스를 출고 시 상태로 복원하려면 USB 포트를 사용해야 합니다.
RJ45 시리얼 포트	어플라이언스의 모든 관리 서비스에 직접 액세스할 수 있도록 직접적인 워크스테이션-어플라이언스 연결을 설정합니다(RJ45-DB-9 어댑터 사용). RJ45 시리얼 포트는 유지 보수 및 컨피그레이션 목적에**만** 사용되며 서비스 트래픽을 전달하기 위한 용도가 아닙니다. **참고** 전면 및 후면 패널 시리얼 포트를 동시에 사용할 수 없습니다.
10/100/1000Mbps 이더넷 관리 인터페이스	OOB(Out of Band) 관리 네트워크 연결에 사용합니다. 관리 인터페이스는 유지 보수 및 컨피그레이션 목적으로**만** 사용되며 서비스 트래픽을 전달하기 위한 용도가 아닙니다.
대체 관리 인터페이스	eStreamer 클라이언트 또는 추가 관리 인터페이스에 대한 대체 인터페이스를 제공합니다.
예비 전원 공급 장치	AC 전원을 통해 어플라이언스에 전원을 공급합니다.

10/100/1000Mbps 관리 인터페이스는 어플라이언스 후면에 있습니다. 다음 표에서는 관리 인터페이스와 관련된 LED에 대해 설명합니다.

표 7-17 DC3500 관리 인터페이스 LED

LED	설명
왼쪽(활동)	포트의 활동을 나타냅니다. • 표시등이 깜박이는 경우 활동이 있음을 나타냅니다. • 표시등이 꺼진 경우 활동이 없음을 나타냅니다.
오른쪽(링크)	링크가 활성 상태인지 여부를 나타냅니다. • 표시등이 켜진 경우 링크가 활성 상태임을 나타냅니다. • 표시등이 꺼진 경우 링크가 없음을 나타냅니다.

전원 공급 장치 모듈은 어플라이언스 후면에 있습니다. 다음 표는 이중 전원 공급 장치와 관련된 LED에 대해 설명합니다.

표 7-18 DC3500 전원 공급 장치 LED

LED	설명
꺼짐	전원 공급 장치가 연결되어 있지 않습니다.
황색	이 모듈에 전원이 공급되지 않았습니다. 또는 전원 공급 장치에 모듈 장애, 퓨즈 꺼짐, 팬 장애와 같은 위험 이벤트가 발생하여 전원 공급 장치가 종료됩니다.
황색으로 깜박임	전원 공급 장치에 고온, 느린 팬 속도와 같은 경고 이벤트가 발생했지만 전원 공급 장치는 계속 작동합니다.

표 7-18 DC3500 전원 공급 장치 LED(계속)

LED	설명
녹색으로 깜박임	AC 입력이 있고 대기 시 볼트가 감지되며 전원 공급 장치가 꺼져 있습니다.
녹색	전원 공급 장치가 연결되었으며 작동 중입니다.

DC3500 물리적 및 환경 매개변수

다음 표에서는 어플라이언스의 물리적 속성 및 환경 매개변수에 대해 설명합니다.

표 7-19 DC3500 물리적 및 환경 매개변수

매개변수	설명
폼 팩터	1U
크기(D x W x H)	26.2인치 x 16.93인치 x 1.7인치(66.5cm x 43.0cm x 4.3cm)
무게	38파운드(17.2kg)
전원 공급 장치	120VAC의 경우 이중 650W 예비 전원 공급 장치 110볼트, 50/60Hz에서 최대 8.5암페어 220볼트, 50/60Hz에서 최대 4.2암페어
작동 온도	10°C~35°C(50°F~95°F)
비작동 온도	-40°C~70°C(-40°F~158°F)
작동 습도	5%~85%
비작동 습도	35°C(95°F)에서 90%, 비응결
음향 노이즈	일반 사무실 주변 온도(23°C +/- 2°C, 73°F +/- 4°F)의 유휴 상태에서 7BA(랙 마운트)
작동 충격	2G의 반 사인파 충격 시 오류 없음(11ms 동안)
패키지 영향	24인치(60cm)에서 자유 낙하 시 작동 가능, 외부는 손상될 수 있음, 섀시 무게 40~80파운드(18~36kg)
ESD	Intel 환경 테스트 사양당 +/- 15KV(I/O 포트 +/-8KV)
공기 흐름	전면에서 후면
시스템 냉각 요구 사항	시간당 2550BTU
RoHS	RoHS Directive 2002/95/EC 준수

DC2000 및 DC4000

DC2000 및 DC4000은 1U 어플라이언스입니다. 어플라이언스에 대한 자세한 내용은 다음 섹션을 참조하십시오.

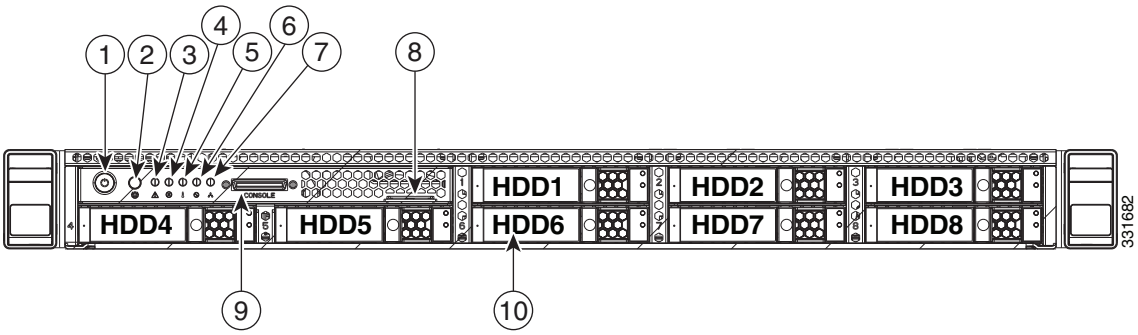
- DC2000 및 DC4000 섀시 전면 보기, 페이지 7-15
- DC2000 및 DC4000 섀시 후면 보기, 페이지 7-17
- DC2000 및 DC4000 물리적 및 환경 매개변수, 페이지 7-19

DC2000 및 DC4000 섀시 전면 보기

섀시 전면에는 스토리지 드라이브, 전면 패널 및 KVM 커넥터가 있습니다. 섀시에는 최대 8개의 SFF(Small Form-Factor) 2.5인치 스토리지 드라이브가 있습니다.

- DC2000 섀시는 4개의 SAS(Serial Attached SCSI)드라이브와 함께 제공됩니다.
- DC4000 섀시는 6개의 SSD(Solid State Drive)와 함께 제공됩니다.

다음 그림은 전면 패널 제어, LED 및 스토리지 드라이브 레이아웃을 포함한 어플라이언스의 전면 패널 기능을 보여줍니다. DC2000 및 DC4000 모두에서 스토리지 드라이브 베이는 맨 위 행에서 시작하여 맨 아래 행까지 왼쪽에서 오른쪽으로 번호가 지정됩니다.



1	전원 버튼/전원 상태 LED	**6**	전원 공급 장치 상태 LED
2	식별 버튼/LED	**7**	네트워크 링크 활동 LED
3	시스템 상태 LED	**8**	풀아웃 자산 태그
4	팬 상태 LED	**9**	KVM 커넥터(USB 2개, VGA 1개, 시리얼 커넥터 1개를 제공하는 KVM 케이블과 함께 사용됨)
5	온도 상태 LED	**10**	운영중 교체 가능한 드라이브(최대 8개의 2.5인치 드라이브)

섀시 전면 패널에는 시스템 작동 상태를 표시하는 7개의 LED가 있습니다. 다음 DC2000 및 DC4000 전면 패널 LED, 상태 정의 표는 전면 패널의 LED에 대해 설명합니다.

표 7-20 DC2000 및 DC4000 전면 패널 LED, 상태 정의

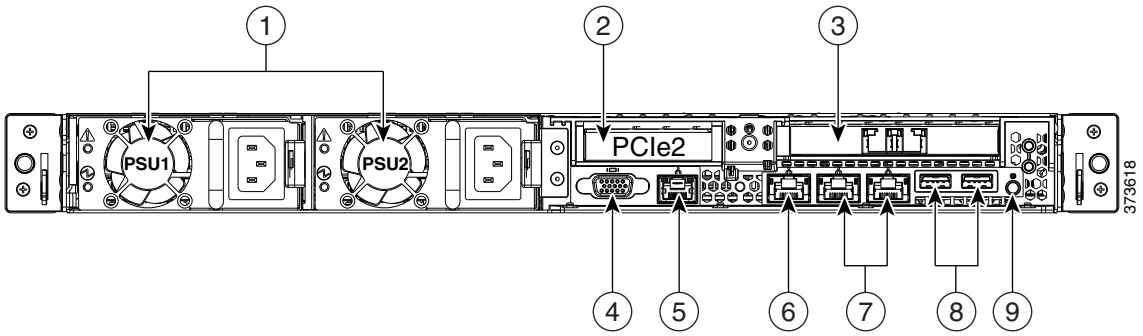
LED 이름	상태
전원 버튼/전원 상태 LED	• 꺼짐—서버에 AC 전원이 연결되지 않았습니다. • 황색—서버가 대기 전원 모드입니다. 전원이 CIMC 및 일부 마더보드 기능에만 공급됩니다. • 녹색—서버가 주 전원 모드입니다. 전원이 모든 서버 구성 요소에 공급됩니다.
식별	• 꺼짐—식별 LED가 사용 중이 아닙니다. • 파란색—식별 LED가 활성화되었습니다.

표 7-20 DC2000 및 DC4000 전면 패널 LED, 상태 정의(계속)

LED 이름	상태
시스템 상태	• 녹색 - 서버가 정상 작동 상태로 실행 중입니다. • 녹색, 깜박임 - 서버에서 시스템 초기화 및 메모리 검사를 수행하고 있습니다. • 황색, 계속 켜져 있음 - 서버가 성능이 저하된 상태로 작동 중입니다. 예를 들면 다음과 같습니다. – 전원 공급 장치 이중화에 문제가 생겼습니다. – CPU가 일치하지 않습니다. – 하나 이상의 CPU에 결함이 있습니다. – 하나 이상의 DIMM에 결함이 있습니다. – RAID 컨피그레이션에서 하나 이상의 드라이브가 작동하지 않습니다. • 황색, 깜박임 - 서버가 심각한 장애 상태입니다. 예를 들면 다음과 같습니다. – 부팅이 실패했습니다. – 치명적인 CPU 및/또는 버스 오류가 감지되었습니다. – 서버가 과열 상태입니다.
팬 상태	• 녹색—모든 팬 모듈이 정상적으로 작동하고 있습니다. • 황색, 계속 켜져 있음—팬 모듈 하나가 작동하지 않습니다. • 황색, 깜박임—중대한 결함. 둘 이상의 팬 모듈이 작동하지 않습니다.
온도 상태	• 녹색—서버가 정상 온도에서 작동하는 중입니다. • 황색, 계속 켜져 있음—하나 이상의 온도 센서가 경고 임계값을 초과했습니다. • 황색, 깜박임—하나 이상의 온도 센서가 중대 임계값을 초과했습니다.
전원 공급 장치 상태	• 녹색—모든 전원 공급 장치가 정상적으로 작동하고 있습니다. • 황색, 계속 켜져 있음—하나 이상의 전원 공급 장치가 성능이 저하된 상태로 작동 중입니다. • 황색, 깜박임—하나 이상의 전원 공급 장치에 중대한 결함이 있습니다.
네트워크 링크 활동	• 꺼짐—이더넷 링크가 유휴 상태입니다. • 녹색—하나 이상의 이더넷 LOM 포트가 링크 활성 상태이지만 활동이 없습니다. • 녹색, 깜박임—하나 이상의 이더넷 LOM 포트가 링크 활성 상태이며 활동이 있습니다.
하드 드라이브 결함	• 꺼짐—하드 드라이브가 정상적으로 작동하고 있습니다. • 황색 - 하드 드라이브에 장애가 발생했습니다. • 황색, 깜박임—디바이스가 재구축 중입니다.
하드 드라이브 활동	• 꺼짐—하드 드라이브 슬레드에 하드 드라이브가 없습니다(액세스 없음, 결함 없음). • 녹색—하드 드라이브가 준비된 상태입니다. • 녹색, 깜박임—하드 드라이브에서 데이터를 읽거나 쓰는 중입니다.

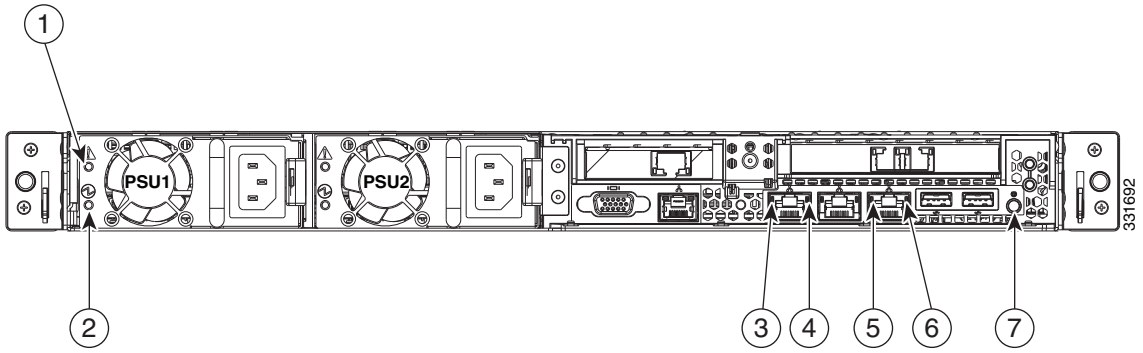
DC2000 및 DC4000 섀시 후면 보기

섀시 후면에는 연결 포트와 전원 공급 장치가 있습니다. 어플라이언스는 1개의 1Gb 이더넷 기본 관리 인터페이스, 2개의 1Gb Base-T 이더넷 포트, 1개의 RS-232 시리얼 포트(RJ-45 커넥터), 1개의 15핀 VGA 커넥터 및 2개의 USB 2.0 커넥터를 제공합니다. 다음 다이어그램은 어플라이언스의 후면을 보여줍니다.



1	전원 공급 장치(2개)	**6**	1Gb 이더넷 관리 인터페이스
2	라이저의 저급 프로필 PCIe 슬롯 2 (절반 높이, 절반 길이, x8 레인)	**7**	이중 1Gb 이더넷 포트(LAN1 및 LAN2), 기본 관리 인터페이스는 왼쪽에 있음
3	이중 10Gb 이더넷 포트	**8**	USB 포트
4	VGA 비디오 커넥터	**9**	후면 식별 버튼/LED
5	시리얼 포트(RJ-45 커넥터)		–

다음 다이어그램은 어플라이언스의 후면에 있는 연결 포트와 전원 공급 장치 및 시스템 식별 버튼과 관련된 LED를 보여줍니다.



1	전원 공급 장치 결함 LED	**5**	1Gb 이더넷 링크 속도 LED
2	전원 공급 장치 상태 LED	**6**	1GB 이더넷 링크 상태 LED
3	1Gb 이더넷 기본 관리 인터페이스 링크 상태 LED	**7**	후면 식별 버튼/LED
4	1Gb 이더넷 기본 관리 인터페이스 링크 속도 LED		–

DC2000 및 DC4000 후면 패널 LED, 상태 정의 표는 기본 관리 인터페이스와 어플라이언스의 후면에 있는 다른 연결 포트, 전원 공급 장치 및 시스템 식별 버튼과 관련된 섀시 후면에 있는 LED에 대해 설명합니다.

표 7-21 DC2000 및 DC4000 후면 패널 LED, 상태 정의

LED 이름	상태
전원 공급 장치 결함	• 꺼짐—전원 공급 장치가 정상적으로 작동하고 있습니다. • 황색, 깜박임—이벤트 경고 임계값에 도달했지만 전원 공급 장치가 계속 작동하고 있습니다. • 황색, 계속 켜져 있음—중대한 결함 임계값에 도달하여 전원 공급 장치가 종료되었습니다(예: 팬 작동 중단, 과열 상태).
전원 공급 장치 상태	AC 전원 공급 장치: • 꺼짐—전원 공급 장치에 AC 전원이 연결되지 않았습니다. • 녹색, 깜박임—AC 전원은 정상이며, DC 출력이 활성화되지 않았습니다. • 녹색, 계속 켜져 있음—AC 전원이 정상이고 DC 출력도 정상입니다. DC 전원 공급 장치: • 꺼짐 - 전원 공급 장치에 DC 전원이 연결되지 않았습니다. • 녹색, 깜박임 - DC 전원은 정상이며, DC 출력이 활성화되지 않았습니다. • 녹색, 계속 켜져 있음 - DC 전원이 정상이고 DC 출력도 정상입니다.
1Gb 이더넷 기본 관리 인터페이스 링크 속도	• 꺼짐 - 링크 속도가 10Mbps입니다. • 황색 - 링크 속도가 100Mbps입니다. • 녹색 - 링크 속도가 1Gbps입니다.
1Gb 이더넷 기본 관리 인터페이스 링크 상태	• 꺼짐—링크가 없습니다. • 녹색—링크가 활성 상태입니다. • 녹색, 깜박임—활성 링크에 트래픽이 있습니다.
1Gb 이더넷 링크 속도	• 꺼짐 - 링크 속도가 10Mbps입니다. • 황색 - 링크 속도가 100Mbps입니다. • 녹색 - 링크 속도가 1Gbps입니다.
1Gb 이더넷 링크 상태	• 꺼짐—링크가 없습니다. • 녹색—링크가 활성 상태입니다. • 녹색, 깜박임—활성 링크에 트래픽이 있습니다.
식별	• 꺼짐—식별 LED가 사용 중이 아닙니다. • 파란색—식별 LED가 활성화되었습니다.

DC2000 및 DC4000 물리적 및 환경 매개변수

다음 표에서는 어플라이언스의 물리적 속성 및 환경 매개변수에 대해 설명합니다.

표 7-22 DC2000 및 DC4000 물리적 및 환경 매개변수

매개변수	설명
폼 팩터	1U
크기(D x W x H)	28.5인치 x 16.9 인치 x 1.7인치(72.4cm x 42.9cm x 4.3cm)
무게	35.6파운드(16.1kg) 최대(8개의 SSD, 2개의 CPU, 16개의 DIMM, 2개의 전원 공급 장치) 22파운드(10kg) 기본(0개의 SSD, 0개의 CPU, 0개의 DIMM, 1개의 전원 공급 장치)
전원 공급 장치	이중 650W 예비 전원 공급 장치 AC 입력 전압 90~264VAC 자동 범위 조정 100~120VAC 공칭 200~240VAC 공칭 AC 입력 주파수: 47~63Hz(단상, 50~60 Hz 공칭) 최대 AC 입력 전원: 100볼트에서 최대 7.6암페어 208볼트에서 최대 3.65암페어 최대 AC 돌입 전류: 11A 최대 출력 전원: 650W 전원 공급 장치 출력 전압: 주 전력: 12VDC 대기 전력: 12VDC
작동 온도	5°C~40°C(41°F~104°F) 해발 고도 305m마다 최대 온도가 1°C(33.8° F)씩 감소합니다.
비작동 온도	-40°C~65°C(-40°F~149°F)
습도(RH) 비작동, 비응결	10%~90%
작동 고도	0~10,000피트(0~3,000m)
비작동 고도	0~40,000피트(0~12,192m)
사운드 출력 수준 A레벨, ISO7779 LwAd(Bels) 기준 23°C(73°F) 작동 시	5.4
음압 수준 A레벨, ISO7779 LpAm(dBA) 기준 23°C(73°F) 작동 시	37
공기 흐름	전면에서 후면

7000 Series 디바이스

모든 7000 Series 디바이스에는 어플라이언스 전면에 LCD 패널이 있습니다. 여기서 어플라이언스를 보고 구성(활성화된 경우)할 수 있습니다.

디바이스에 대한 자세한 내용은 다음 섹션을 참조하십시오.

3D7010, 3D7020, 3D7030 및 3D7050

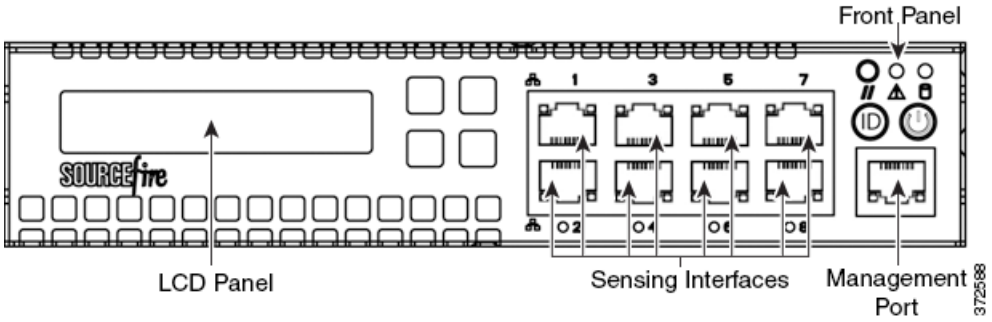
70xx 제품군이라고도 하는 3D7010, 3D7020, 3D7030 및 3D7050 디바이스는 절반 너비의 랙 트레이인 1U 어플라이언스이며 각각 구성 가능한 바이패스 기능이 있는 구리 인터페이스 8개와 함께 제공됩니다. 70xx 제품군 어플라이언스의 안전 고려 사항은 *FirePOWER 및 FireSIGHT 어플라이언스 규정준수 및 안전 정보* 문서를 참조하십시오.

자세한 내용은 다음 섹션을 참조하십시오.

70xx 제품군 전면 보기

섀시 전면에는 LCD 패널, 센싱 인터페이스, 전면 패널 및 관리 인터페이스가 있습니다.

그림 7-4 70xx 제품군(섀시: CHRY-1U-AC; NEME-1U-AC) 전면 보기



다음 표에서는 어플라이언스 전면에 있는 기능에 대해 설명합니다.

표 7-23 70xx 제품군 시스템 구성 요소: 전면 보기

기능	설명
LCD 패널	디바이스를 구성하고 오류 메시지를 표시하며 시스템 상태를 보는 여러 모드에서 작동합니다. 자세한 내용은 Series 3 디바이스에서 LCD 패널 사용, 페이지 6-1을(를) 참고하십시오.
센싱 인터페이스	네트워크에 연결되는 센싱 인터페이스를 포함합니다. 자세한 내용은 센싱 인터페이스, 페이지 7-22 을(를) 참조하십시오.

표 7-23 70xx 제품군 시스템 구성 요소: 전면 보기(계속)

기능	설명
10/100/1000 이더넷 관리 인터페이스	OOB(Out of Band) 관리 네트워크 연결에 사용합니다. 관리 인터페이스는 유지 보수 및 컨피그레이션 목적으로**만** 사용되며 서비스 트래픽을 전달하기 위한 용도가 아닙니다.
전면 패널	시스템의 작동 상태와 전원 버튼과 같은 다양한 제어를 표시하는 LED가 있습니다. 자세한 내용은 표 7-333D7110 및 3D7120 전면 패널 구성 요소, 페이지 7-26을(를) 참고하십시오.

그림 7-5 70xx 제품군 전면 패널

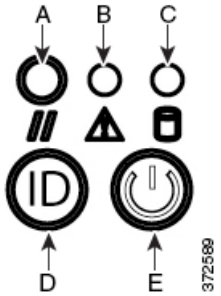


표 7-24 전면 패널 구성 요소

A	재설정 버튼	D	시스템 ID 버튼
B	시스템 상태 LED	E	전원 버튼 및 LED
C	하드 드라이브 활동 LED		

섀시 전면 패널에는 시스템 작동 상태를 표시하는 LED가 있습니다. 다음 표에서는 전면 패널의 LED에 대해 설명합니다.

표 7-25 70xx 제품군 전면 패널 LED

LED	설명
재설정 버튼	전원 공급 장치에서 연결을 끊지 않고도 어플라이언스를 재부팅할 수 있습니다.
시스템 상태	시스템 상태를 다음과 같이 나타냅니다. • 녹색 표시등은 시스템 전원이 켜져 있고 정상적으로 작동 중이거나 전원이 꺼져 있고 AC 전원에 연결된 상태를 나타냅니다. • 황색 표시등은 시스템 장애를 나타냅니다. 자세한 내용은 표 7-26 페이지 7-22을(를) 참조하십시오.
하드 드라이브 활동	하드 드라이브 상태를 다음과 같이 나타냅니다. • 녹색 표시등이 깜박이는 경우 고정 디스크 드라이브가 활성 상태임을 나타냅니다. • 표시등이 꺼진 경우 드라이브 활동이 없거나 시스템 전원이 꺼져 있음을 나타냅니다.
시스템 ID	이 ID 버튼을 누르면 파란색으로 표시되며 섀시 후면에서도 파란색 LED를 볼 수 있습니다.
전원 버튼 및 LED	어플라이언스에 전원이 연결되었는지 여부를 나타냅니다. • 녹색 표시등은 어플라이언스에 전원이 연결되었고 시스템이 켜져 있음을 나타냅니다. • 표시등이 꺼진 경우 시스템이 종료되었거나 전원이 연결되어 있지 않음을 나타냅니다.

다음 표에서는 시스템 상태 LED가 켜질 수 있는 상태에 대해 설명합니다.

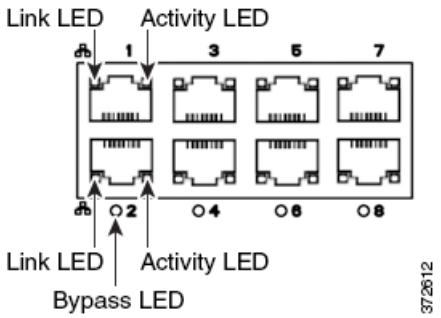
표 7-26 70xx 제품군 시스템 상태

상태	설명
위험	다음 이벤트와 관련된 위험하거나 복구 불가능한 임계값 초과 상태입니다. • 온도, 전압 또는 팬의 위험 임계값 초과 • 전원 하위 시스템 장애 • 잘못 설치된 프로세서 또는 프로세서 비호환성으로 인해 시스템 전원을 켤 수 없음 • PCI SERR 및 PERR과 같이 시스템 메모리의 수정 불가능한 ECC 오류 및 치명적/수정 불가능한 버스 오류를 포함한 위험한 이벤트 기록 오류
비위험	비위험 상태는 다음 이벤트와 관련된 임계값이 초과된 상태입니다. • 온도, 전압 또는 팬의 비위험 임계값 초과 • 시스템 BIOS에서 Fault Indication 명령을 설정합니다. BIOS에서는 이 명령을 사용하여 시스템 메모리 또는 CPU 컨피그레이션 변경과 같은 추가적인 비위험 상태를 표시할 수 있습니다.
저하됨	저하된 상태는 다음 이벤트와 관련되어 있습니다. • 하나 이상의 프로세서가 FRB(Fault Resilient Boot) 또는 BIOS에 의해 비활성화됨 • BIOS가 시스템 메모리 중 일부를 비활성화하거나 배제함 • 전원 공급 장치 중 하나가 연결되지 않았거나 작동하지 않음

센싱 인터페이스

70xx 제품군 어플라이언스는 각각에 구성 가능한 바이패스 기능이 있는 8개의 구리 인터페이스와 함께 제공됩니다.

그림 7-6 8포트 1000BASE-T 구리 인터페이스



다음 표에서 구리 인터페이스의 활동 및 링크 LED를 확인할 수 있습니다.

표 7-27 70xx 제품군 구리 링크/활동 LED

상태	설명
두 LED가 모두 꺼짐	인터페이스에 링크가 없습니다.
황색 링크	인터페이스의 트래픽 속도가 10Mb 또는 100Mb입니다.

표 7-27 70xx 제품군 구리 링크/활동 LED(계속)

상태	설명
녹색 링크	인터페이스의 트래픽 속도가 1Gb입니다.
활동이 녹색으로 깜박임	인터페이스에 링크가 있으며 트래픽이 이동 중입니다.

다음 표에서 구리 인터페이스의 바이패스 LED를 확인할 수 있습니다.

표 7-28 70xx 제품군 구리 바이패스 LED

상태	설명
꺼짐	인터페이스 쌍이 바이패스 모드가 아니거나 전원이 없습니다.
녹색으로 켜져 있음	인터페이스 쌍이 바이패스 모드로 전환할 준비가 되었습니다.
황색으로 켜져 있음	인터페이스 쌍이 의도적으로 바이패스 모드로 배치되었거나 단계적으로 바이패스 모드로 전환되었으며 트래픽을 검사하지 않습니다.
황색으로 깜박임	인터페이스 쌍이 예기치 않게 바이패스 모드로 전환되었습니다. 즉, 열기에 실패했습니다.

10/100/1000 관리 인터페이스는 어플라이언스 전면에 있습니다. 다음 표에서는 관리 인터페이스와 관련된 LED에 대해 설명합니다.

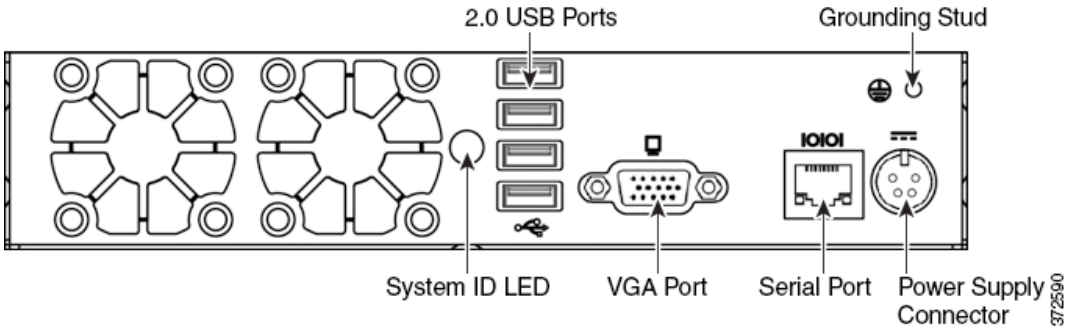
표 7-29 70xx 제품군 관리 인터페이스 LED

LED	설명	
왼쪽(링크)	7010/20/30	링크가 활성 상태인지 여부를 나타냅니다. 표시등이 켜진 경우 링크가 활성 상태임을 나타냅니다. 표시등이 꺼진 경우 링크가 없는 상태입니다.
	7050	10Mbps 링크의 경우 링크 표시등이 밝게 표시되지 않습니다. 링크 상태는 오른쪽(활동) LED와 공유됩니다.
오른쪽(활동)	7010/20/30	포트의 활동을 나타냅니다. 표시등이 깜박이는 경우 활동이 있는 상태입니다. 표시등이 꺼져 있는 경우 활동이 없는 상태입니다.
	7050	10Mbps 링크의 경우 표시등이 켜져 있으면 링크와 활동이 있는 상태입니다. 표시등이 꺼져 있으면 링크 또는 활동이 없는 상태입니다.

70xx 제품군 후면 보기

섀시 후면에는 시스템 ID LED, 연결 포트, 접지 스터드 및 전원 공급 장치 커넥터가 있습니다.

그림 7-7 70xx 제품군(섀시: CHRY-1U-AC) 후면 보기



다음 표에서는 어플라이언스 후면에 표시되는 기능에 대해 설명합니다.

표 7-30 70xx 제품군 시스템 구성 요소: 후면 보기

기능	설명
시스템 ID LED	고밀도 랙에 설치된 시스템을 다른 유사한 시스템과 식별할 수 있습니다. 파란색 LED는 ID 버튼을 눌렀음을 나타냅니다.
2.0 USB 포트 VGA 포트 시리얼 포트	디바이스에 모니터와 키보드를 연결하여 워크스테이션과 어플라이언스를 직접 연결할 수 있습니다.
접지 스터드	어플라이언스를 공통의 본딩 네트워크에 연결할 수 있습니다. 자세한 내용은 FirePOWER 디바이스의 전력 요구 사항, 페이지 A-1을(를) 참조하십시오.
12V 전원 공급 장치 커넥터	AC 전원을 통해 디바이스에 전원을 연결할 수 있습니다.

70xx 제품군 물리적 및 환경 매개변수

다음 표에서는 어플라이언스의 물리적 속성 및 환경 매개변수에 대해 설명합니다.

표 7-31 70xx 제품군 물리적 및 환경 매개변수

매개변수	설명
폼 팩터	1U, 절반 랙 너비
크기(D x W x H)	단일 섀시: 12.49인치 x 7.89인치 x 1.66인치(31.74cm x 20.04cm x 4.21cm) 2개 섀시 트레이: 25.05 인치 x 17.24인치 x 1.73인치(63.62cm x 43.8cm x 4.44cm)
섀시 무게 최대 설치	섀시: 7파운드(3.17kg) 트레이의 단일 섀시 및 전원 공급 장치: 17.7 파운드(8.03kg) 단일 트레이의 이중 섀시 및 전원 공급 장치: 24.7 파운드(11.2kg)
구리 1000BASE-T	쌍으로 연결된 컨피그레이션의 기가비트 구리 이더넷 바이패스 가능 인터페이스 케이블 및 거리: 50m에서 Cat5E

표 7-31 70xx 제품군 물리적 및 환경 매개변수(계속)

매개변수	설명	
전원 공급 장치	200W AC 전원 공급 장치 전압: 100VAC~240VAC 공칭 범위(90VAC~264VAC 최대 범위) 전류: 전체 범위에서 최대 2A 주파수 범위: 공칭 50/60Hz(47Hz~최대 63Hz)	
작동 온도	7010/20/30	0°C~40°C(32°F~104°F)
	7050	-5°C~40°C(23°F~104°F)
비작동 온도	7010/20/30	-20°C~70°C(-4°F~158°F)
	7050	-10°C~60°C(14°F~140°F)
작동 습도	7010/20/30	5%~95%, 비응결 이러한 한도를 초과할 경우 작동을 보장할 수 없으며 권장하지 않습니다.
	7050	5%~85%, 비응결 이러한 한도를 초과할 경우 작동을 보장할 수 없으며 권장하지 않습니다.
비작동 습도	7010/20/30	0%~95%, 비응결
	7050	0%~85%, 비응결
	장치를 최대값 미만의 비응결 상대 습도에서 보관하십시오. 기기를 실제로 운용하기 최소 48시간 전에 최대 작동 습도 미만의 습도에서 적응하도록 합니다.	
고도	0피트(해수면)~5905피트(0~1800m)	
냉각 요구 사항	시간당 682BTU 어플라이언스를 요구되는 작동 온도 범위 내로 유지할 수 있도록 충분한 냉각을 제공해야 합니다. 그렇지 않을 경우 어플라이언스에 오작동 또는 손상이 발생할 수 있습니다.	
음향 노이즈	유휴 상태에서 53dBA 전체 프로세서 부하에서 62dBA	
작동 충격	5G의 반 사인파 충격 시 오류 없음(11ms 동안)	
공기 흐름	분당 20ft^3(0.57 m^3) 어플라이언스를 통과하는 공기 흐름이 전면과 측면으로 진입하여 후면으로 배출됩니다.	

3D7110 및 3D7120

71xx 제품군에 속하는 3D7110 및 3D7120 디바이스 1U 어플라이언스이며 각각 구성 가능한 바이패스 기능이 있는 8개의 구리 또는 8개의 파이버 인터페이스와 함께 제공됩니다. 71xx 제품군 어플라이언스의 안전 고려 사항은 *FirePOWER 및 FireSIGHT 어플라이언스 규정준수 및 안전 정보* 문서를 참조하십시오.

자세한 내용은 다음 섹션을 참조하십시오.

- 3D7110 및 3D7120 섀시 전면 보기, 페이지 7-26
- 3D7110 및 3D7120 섀시 후면 보기, 페이지 7-30
- 3D7110 및 3D7120 물리적 및 환경 매개변수, 페이지 7-31

3D7110 및 3D7120 섀시 전면 보기

섀시 전면에는 LCD 패널, USB 포트, 전면 패널, 구리 또는 파이버 센싱 인터페이스가 있습니다.

그림 7-8 구리 인터페이스 포함 3D7110 및 3D7120(섀시: GERY-1U-8-C-AC)

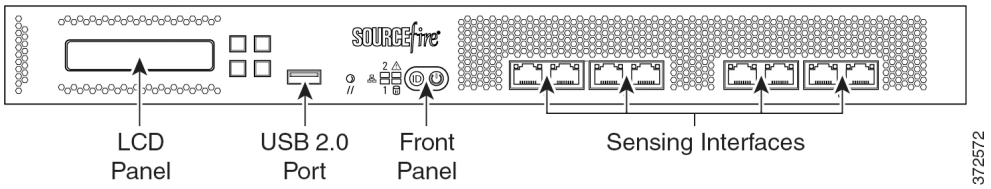
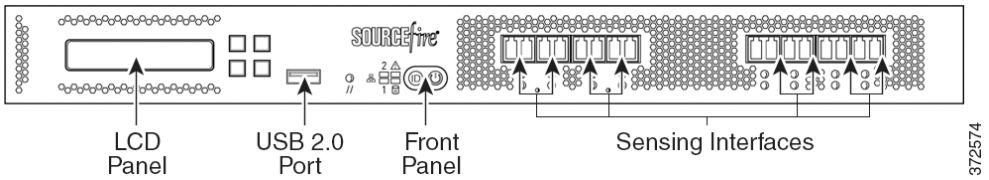


그림 7-9 파이버 인터페이스 포함 3D7110 및 3D7120(섀시: GERY-1U-8-FM-AC)



다음 표에서는 어플라이언스 전면에 있는 기능에 대해 설명합니다.

표 7-32 3D7110 및 3D7120 시스템 구성 요소: 전면 보기

기능	설명
LCD 패널	디바이스를 구성하고 오류 메시지를 표시하며 시스템 상태를 보는 여러 모드에서 작동합니다. 자세한 내용은 Series 3 디바이스에서 LCD 패널 사용, 페이지 6-1을(를) 참고하십시오.
전면 패널 USB 2.0 포트	디바이스에 키보드를 연결할 수 있습니다.
전면 패널	시스템의 작동 상태와 전원 버튼과 같은 다양한 제어를 표시하는 LED가 있습니다. 자세한 내용은 그림 7-103D7110 및 3D7120 전면 패널, 페이지 7-26을(를) 참고하십시오.
센싱 인터페이스	네트워크에 연결되는 센싱 인터페이스를 포함합니다. 자세한 내용은 3D7110 및 3D7120 센싱 인터페이스, 페이지 7-28을(를) 참고하십시오.

그림 7-10 3D7110 및 3D7120 전면 패널

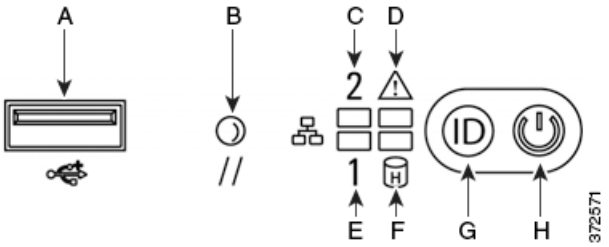


표 7-33 3D7110 및 3D7120 전면 패널 구성 요소

A	USB 2.0 커넥터	E	NIC1 활동 LED
B	재설정 버튼	F	하드 드라이브 활동 LED

표 7-33 3D7110 및 3D7120 전면 패널 구성 요소(계속)

C	NIC2 활동 LED	G	ID 버튼
D	시스템 상태 LED	H	전원 버튼 및 LED

섀시 전면 패널에는 시스템 작동 상태를 표시하는 LED가 있습니다. 다음 표에서는 전면 패널의 LED에 대해 설명합니다.

표 7-34 3D7110 및 3D7120 전면 패널 LED

LED	설명
NIC 활동(1 및 2)	네트워크 활동이 있는지 여부를 나타냅니다. • 녹색 표시등은 네트워크 활동이 있음을 나타냅니다. • 표시등이 꺼진 경우 네트워크 활동이 없음을 나타냅니다.
시스템 상태	시스템 상태를 다음과 같이 나타냅니다. • 표시등이 꺼진 경우 시스템이 정상 작동 중이거나 전원이 꺼져 있음을 나타냅니다. • 빨간색 표시등은 시스템 오류를 나타냅니다. 자세한 내용은 표 7-353D7110 및 3D7120 시스템 상태, 페이지 7-28을(를) 참조하십시오.
재설정 버튼	전원 공급 장치에서 연결을 끊지 않고도 어플라이언스를 재부팅할 수 있습니다.
하드 드라이브 활동	하드 드라이브 상태를 다음과 같이 나타냅니다. • 녹색 표시등이 깜박이는 경우 고정 디스크 드라이브가 활성 상태임을 나타냅니다. • 황색 표시등은 고정 디스크 드라이브에 장애가 발생했음을 나타냅니다. • 표시등이 꺼진 경우 드라이브 활동이 없거나 시스템 전원이 꺼져 있음을 나타냅니다.
시스템 ID	고밀도 랙에 설치된 시스템을 다른 유사한 시스템과 식별할 수 있습니다. • 파란색 표시등은 ID 버튼을 눌렀음을 나타내며 파란색 표시등은 어플라이언스 후면에 있습니다. • 표시등이 꺼진 경우 ID 버튼을 누르지 않았음을 나타냅니다.
전원 버튼 및 LED	어플라이언스에 전원이 연결되었는지 여부를 나타냅니다. • 녹색 표시등은 어플라이언스에 전원이 연결되었고 시스템이 켜져 있음을 나타냅니다. • 녹색 표시등이 깜박이는 경우 어플라이언스에 전원이 연결되었으며 종료되었음을 나타냅니다. • 표시등이 꺼진 경우 시스템에 전원이 연결되어 있지 않음을 나타냅니다.

다음 표에서는 시스템 상태 LED가 켜질 수 있는 상태에 대해 설명합니다.

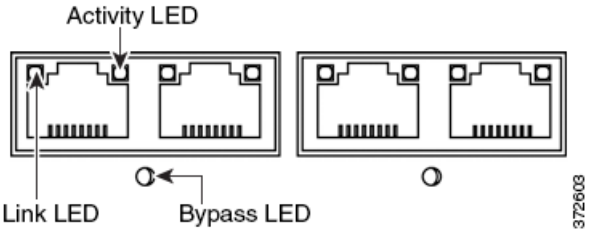
표 7-35 3D7110 및 3D7120 시스템 상태

상태	설명
위험	다음 이벤트와 관련된 위험하거나 복구 불가능한 임계값 초과 상태입니다. • 온도, 전압 또는 팬의 위험 임계값 초과 • 전원 하위 시스템 장애 • 잘못 설치된 프로세서 또는 프로세서 비호환성으로 인해 시스템 전원을 켤 수 없음 • PCI SERR 및 PERR과 같이 시스템 메모리의 수정 불가능한 ECC 오류 및 치명적/수정 불가능한 버스 오류를 포함한 위험한 이벤트 기록 오류
비위험	비위험 상태는 다음 이벤트와 관련된 임계값이 초과된 상태입니다. • 온도, 전압 또는 팬의 비위험 임계값 초과 • 섀시 침입 • 시스템 BIOS에서 Fault Indication 명령을 설정합니다. BIOS에서는 이 명령을 사용하여 시스템 메모리 또는 CPU 컨피그레이션 변경과 같은 추가적인 비위험 상태를 표시할 수 있습니다.
저하됨	저하된 상태는 다음 이벤트와 관련되어 있습니다. • 하나 이상의 프로세서가 FRB(Fault Resilient Boot) 또는 BIOS에 의해 비활성화됨 • BIOS가 시스템 메모리 중 일부를 비활성화하거나 배제함 • 전원 공급 장치 중 하나가 연결되지 않았거나 작동하지 않음 **정보** 상태 저하 표시를 확인한 경우 전원 공급 장치가 올바르게 연결되었는지 확인합니다. 디바이스 전원을 끄고 두 전원 코드를 분리한 후 다시 연결하여 다시 장착하고 디바이스를 다시 시작합니다. ⚠ **주의** 전원을 안전하게 끄려면 *FireSIGHT System 사용 설명서*의 디바이스 관리에 설명된 절차를 사용하거나 CLI에서 `system shutdown` 명령을 사용합니다.

3D7110 및 3D7120 센싱 인터페이스

3D7110 및 3D7120 디바이스는 각각에 구성 가능한 바이패스 기능이 있는 8포트 구리 또는 8포트 파이버 인터페이스와 함께 제공됩니다.

그림 7-11 8포트 1000BASE-T 구리 인터페이스



다음 표에서 구리 인터페이스의 활동 및 링크 LED를 확인할 수 있습니다.

표 7-36 3D7110 및 3D7120 구리 링크/활동 LED

상태	설명
두 LED가 모두 꺼짐	인터페이스에 링크가 없습니다.
황색 링크	인터페이스의 트래픽 속도가 10Mb 또는 100Mb입니다.
녹색 링크	인터페이스의 트래픽 속도가 1Gb입니다.
활동이 녹색으로 깜박임	인터페이스에 링크가 있으며 트래픽이 이동 중입니다.

다음 표에서 구리 인터페이스의 바이패스 LED를 확인할 수 있습니다.

표 7-37 3D7110 및 3D7120 구리 바이패스 LED

상태	설명
꺼짐	인터페이스 쌍이 바이패스 모드가 아니거나 전원이 없습니다.
녹색으로 켜져 있음	인터페이스 쌍이 바이패스 모드로 전환할 준비가 되었습니다.
황색으로 켜져 있음	인터페이스 쌍이 바이패스 모드로 전환되었으며 트래픽을 검사하지 않습니다.
황색으로 깜박임	인터페이스 쌍이 바이패스 모드입니다. 즉, Failed Open입니다.

그림 7-12 8포트 1000BASE-SX 바이패스 구성 가능 파이버 인터페이스

다음 표에서 파이버 인터페이스의 링크 및 활동 LED를 확인할 수 있습니다.

표 7-38 3D7110 및 3D7120 파이버 링크/활동 LED

상태	설명
위(활동)	인라인 인터페이스: 인터페이스에 활동이 있는 경우 표시등이 켜집니다. 꺼진 경우 활동이 없는 상태입니다. 수동 인터페이스: 표시등이 작동하지 않습니다.
아래(링크)	인라인 인터페이스 또는 수동 인터페이스: 인터페이스에 링크가 있는 경우 표시등이 켜집니다. 꺼진 경우 링크가 없는 상태입니다.

다음 표에서 파이버 인터페이스의 활동 및 링크 LED를 확인할 수 있습니다.

표 7-39 3D7110 및 3D7120 파이버 바이패스 LED

상태	설명
꺼짐	인터페이스 쌍이 바이패스 모드가 아니거나 전원이 없습니다.
녹색으로 켜져 있음	인터페이스 쌍이 바이패스 모드로 전환할 준비가 되었습니다.

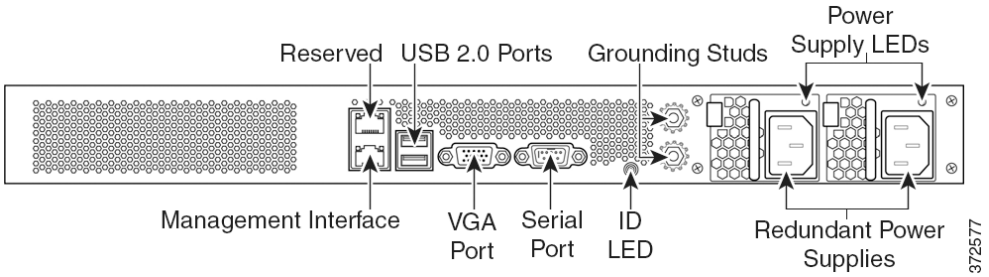
표 7-39 3D7110 및 3D7120 파이버 바이패스 LED(계속)

상태	설명
황색으로 켜져 있음	인터페이스 쌍이 바이패스 모드로 전환되었으며 트래픽을 검사하지 않습니다.
황색으로 깜박임	인터페이스 쌍이 바이패스 모드입니다. 즉, Failed Open입니다.

3D7110 및 3D7120 섀시 후면 보기

섀시 후면에 관리 인터페이스, 연결 포트, 접지 스터드, 전원 공급 장치가 있습니다.

그림 7-13 3D7110 및 3D7120(섀시: GERY-1U-8-C-AC or GERY-1U-8-FM-AC) 후면 보기



다음 표에서는 어플라이언스 후면에 표시되는 기능에 대해 설명합니다.

표 7-40 3D7110 및 3D7120 시스템 구성 요소: 후면 보기

기능	설명
VGA 포트 USB 포트	디바이스에 모니터, 키보드, 마우스를 연결하여 워크스테이션과 어플라이언스를 직접 연결할 수 있습니다.
10/100/1000 이더넷 관리 인터페이스	OOB(Out of Band) 관리 네트워크 연결에 사용합니다. 관리 인터페이스는 유지 보수 및 컨피그레이션 목적으로**만** 사용되며 서비스 트래픽을 전달하기 위한 용도가 아닙니다.
시스템 ID LED	고밀도 랙에 설치된 시스템을 다른 유사한 시스템과 식별할 수 있습니다. 파란색 표시등은 ID 버튼을 눌렀음을 나타냅니다.
접지 스터드	어플라이언스를 공통의 본딩 네트워크에 연결할 수 있습니다. 자세한 내용은 FirePOWER 디바이스의 전력 요구 사항, 페이지 A-1을(를) 참조하십시오.
예비 전원 공급 장치	AC 전원을 통해 디바이스에 전원을 공급합니다. 섀시 후면을 보면 왼쪽에 전원 공급 장치 #1이 있고 오른쪽에 전원 공급 장치 #2가 있습니다.
전원 공급 장치 LED	전원 공급 장치 상태를 나타냅니다. 표 7-423D7110 및 3D7120 전원 공급 장치 LED, 페이지 7-31을(를) 참조하십시오.

10/100/1000 관리 인터페이스는 어플라이언스 후면에 있습니다. 다음 표에서는 관리 인터페이스와 관련된 LED에 대해 설명합니다.

표 7-41 3D7110 및 3D7120 관리 인터페이스 LED

LED	설명
왼쪽(활동)	포트의 활동을 나타냅니다. • 표시등이 깜박이는 경우 활동이 있음을 나타냅니다. • 표시등이 꺼진 경우 활동이 없음을 나타냅니다.
오른쪽(링크)	링크가 활성 상태인지 여부를 나타냅니다. • 표시등이 켜진 경우 링크가 활성 상태임을 나타냅니다. • 표시등이 꺼진 경우 링크가 없음을 나타냅니다.

전원 공급 장치 모듈은 어플라이언스 후면에 있습니다. 다음 표에서는 전원 공급 장치와 연결된 LED에 대해 설명합니다.

표 7-42 3D7110 및 3D7120 전원 공급 장치 LED

LED	설명
꺼짐	전원 코드가 연결되어 있지 않습니다.
빨간색	이 모듈에 전원이 공급되지 않았습니다. 또는 전원 공급 장치에 모듈 장애, 퓨즈 꺼짐, 팬 장애와 같은 위험 이벤트가 발생하여 전원 공급 장치가 종료됩니다.
빨간색으로 깜박임	전원 공급 장치에 고온, 느린 팬 속도와 같은 경고 이벤트가 발생했지만 전원 공급 장치는 계속 작동합니다.
녹색으로 깜박임	AC 입력이 있고 대기 시 볼트가 감지되며 전원 공급 장치가 꺼져 있습니다.
녹색	전원 공급 장치가 연결되었으며 작동 중입니다.

3D7110 및 3D7120 물리적 및 환경 매개변수

다음 표에서는 어플라이언스의 물리적 속성 및 환경 매개변수에 대해 설명합니다.

표 7-43 3D7110 및 3D7120 물리적 및 환경 매개변수

매개변수	설명
폼 팩터	1U
크기(D x W x H)	21.6인치 x 19.0인치 x 1.73인치(54.9cm x 48.3cm x 4.4cm)
무게 최대 설치	27.5파운드(12.5 kg)
구리 1000BASE-T	쌍으로 연결된 컨피그레이션의 기가비트 구리 이더넷 바이패스 가능 인터페이스 케이블 및 거리: 50m에서 Cat5E
파이버 1000BASE-SX	LC 커넥터를 사용하는 파이버 바이패스 지원 인터페이스 케이블 및 거리: SX는 550m(표준)에서 멀티 모드 파이버(850nm)

표 7-43 3D7110 및 3D7120 물리적 및 환경 매개변수(계속)

매개변수	설명
전원 공급 장치	450W 이중 예비(1+1) AC 전원 공급 장치 전압: 100VAC~240VAC 공칭 범위(85VAC~264VAC 최대 범위) 전류: 공급 장치당 90VAC~132VAC에서 최대 3A 공급 장치당 187VAC~264VAC에서 최대 1.5A 주파수 범위: 47Hz~63Hz
작동 온도	5ºC~40ºC(41ºF~104ºF)
비작동 온도	-20ºC~70ºC(-29ºF~158ºF)
작동 습도	5%~85%, 비응결
비작동 습도	25ºC~35ºC(77ºF~95ºF) 온도에서 최대 28ºC(82ºF) 습구 이용 시 5%~90%, 비응결 기기를 95% 미만의 비응결 상대 습도에서 보관하십시오. 기기를 실제로 운용하기 최소 48시간 전에 최대 작동 습도 미만의 습도에서 적응하도록 합니다.
고도	0피트(해수면)~5905피트(0~1800m)
냉각 요구 사항	시간당 900BTU 어플라이언스를 요구되는 작동 온도 범위 내로 유지할 수 있도록 충분한 냉각을 제공해야 합니다. 그렇지 않을 경우 어플라이언스에 오작동 또는 손상이 발생할 수 있습니다.
음향 노이즈	전체 프로세서 부하, 정상 팬 작동 시 64dBA GR63-CORE 4.6 음향 노이즈 충족
작동 충격	Bellecore GR63-CORE 표준과 호환
공기 흐름	분당 140 ft^3(3.9 m^3) 공기 흐름이 전면으로 진입해서 후면으로 배출되어 어플라이언스를 통과하며 측면 통풍은 없습니다.

3D7115, 3D7125 및 AMP7150

71xx 제품군에 속하는 3D7115, 3D7125 및 AMP7150 디바이스는 구성 가능한 바이패스 기능이 있는 4포트 구리 인터페이스와 바이패스 기능이 없고 운영 중 교체 가능한 SFP(Small Form-Factor Pluggable) 포트 8개와 함께 제공됩니다. 호환성을 보장하기 위해 Cisco SFP 트렌시버만 사용하십시오. *FirePOWER 및 FireSIGHT 어플라이언스 규정준수 및 안전 정보*

참고 FirePOWER AMP7150에는 3D7115 및 3D7125와 동일한 폼 팩터가 여러 개 포함되어 있지만 FireSIGHT System의 네트워크 기반 AMP(Advanced Malware Protection) 기능을 활용하도록 최적화되었습니다.

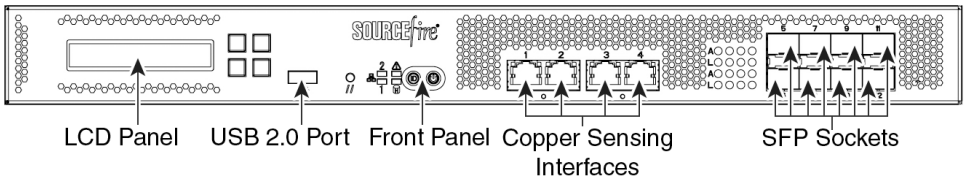
자세한 내용은 다음 섹션을 참조하십시오.

- 3D7115, 3D7125 및 AMP7150 섀시 전면 보기, 페이지 7-33
- 3D7115, 3D7125 및 AMP7150 섀시 후면 보기, 페이지 7-37
- 3D7115, 3D7125, AMP7150 물리적 및 환경 매개변수, 페이지 7-39

3D7115, 3D7125 및 AMP7150 섀시 전면 보기

섀시 전면에는 LCD 패널, USB 포트, 전면 패널, 구리 센싱 인터페이스 및 SFP 소켓이 있습니다.

그림 7-14 3D7115, 3D7125 및 AMP7150(섀시: GERY-1U-8-4C8S-AC) 전면 보기



다음 표에서는 어플라이언스 전면에 있는 기능에 대해 설명합니다.

표 7-44 3D7115, 3D7125 및 AMP7150 시스템 구성 요소: 전면 보기

기능	설명
LCD 패널	디바이스를 구성하고 오류 메시지를 표시하며 시스템 상태를 보는 여러 모드에서 작동합니다. 자세한 내용은 Series 3 디바이스에서 LCD 패널 사용, 페이지 6-1을(를) 참고하십시오.
전면 패널 USB 2.0 포트	디바이스에 키보드를 연결할 수 있습니다.
전면 패널	시스템의 작동 상태와 전원 버튼과 같은 다양한 제어를 표시하는 LED가 있습니다. 자세한 내용은 그림 7-153D7115, 3D7125 및 AMP7150 전면 패널, 페이지 7-33을(를) 참고하십시오.
센싱 인터페이스	네트워크에 연결되는 센싱 인터페이스를 포함합니다. 자세한 내용은 3D7115, 3D7125 및 AMP7150 센싱 인터페이스, 페이지 7-35을(를) 참고하십시오.

그림 7-15 3D7115, 3D7125 및 AMP7150 전면 패널

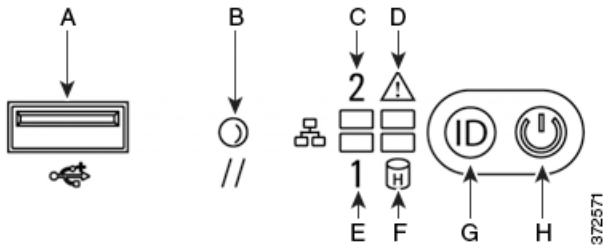


표 7-45 3D7115, 3D7125 및 AMP7150 전면 패널 구성 요소

A	USB 2.0 커넥터	E	NIC1 활동 LED
B	재설정 버튼	F	하드 드라이브 활동 LED
C	NIC2 활동 LED	G	ID 버튼
D	시스템 상태 LED	H	전원 버튼 및 LED

섀시 전면 패널에는 시스템 작동 상태를 표시하는 LED가 있습니다. 다음 표에서는 전면 패널의 LED에 대해 설명합니다.

표 7-46 3D7115, 3D7125 및 AMP7150 전면 패널 LED

LED	설명
NIC 활동(1 및 2)	네트워크 활동이 있는지 여부를 나타냅니다. • 녹색 표시등은 네트워크 활동이 있음을 나타냅니다. • 표시등이 꺼진 경우 네트워크 활동이 없음을 나타냅니다.
시스템 상태	시스템 상태를 다음과 같이 나타냅니다. • 표시등이 꺼진 경우 시스템이 정상 작동 중이거나 전원이 꺼져 있음을 나타냅니다. • 빨간색 표시등은 시스템 오류를 나타냅니다. 자세한 내용은 표 7-473D7115, 3D7125 및 AMP7150 시스템 상태, 페이지 7-34을(를) 참조하십시오.
재설정 버튼	전원 공급 장치에서 연결을 끊지 않고도 어플라이언스를 재부팅할 수 있습니다.
하드 드라이브 활동	하드 드라이브 상태를 다음과 같이 나타냅니다. • 녹색 표시등이 깜박이는 경우 고정 디스크 드라이브가 활성 상태임을 나타냅니다. • 황색 표시등은 고정 디스크 드라이브에 장애가 발생했음을 나타냅니다. • 표시등이 꺼진 경우 드라이브 활동이 없거나 시스템 전원이 꺼져 있음을 나타냅니다.
시스템 ID	고밀도 랙에 설치된 시스템을 다른 유사한 시스템과 식별할 수 있습니다. • 파란색 표시등은 ID 버튼을 눌렀음을 나타내며 파란색 표시등은 어플라이언스 후면에 있습니다. • 표시등이 꺼진 경우 ID 버튼을 누르지 않았음을 나타냅니다.
전원 버튼 및 LED	어플라이언스에 전원이 연결되었는지 여부를 나타냅니다. • 녹색 표시등은 어플라이언스에 전원이 연결되었고 시스템이 켜져 있음을 나타냅니다. • 녹색 표시등이 깜박이는 경우 어플라이언스에 전원이 연결되었으며 종료되었음을 나타냅니다. • 표시등이 꺼진 경우 시스템에 전원이 연결되어 있지 않음을 나타냅니다.

다음 표에서는 시스템 상태 LED가 켜질 수 있는 상태에 대해 설명합니다.

표 7-47 3D7115, 3D7125 및 AMP7150 시스템 상태

Condition	설명
Critical	다음 이벤트와 관련된 위험하거나 복구 불가능한 임계값 초과 상태입니다. • 온도, 전압 또는 팬의 위험 임계값 초과 • 전원 하위 시스템 장애 • 잘못 설치된 프로세서 또는 프로세서 비호환성으로 인해 시스템 전원을 켤 수 없음 • PCI SERR 및 PERR과 같이 시스템 메모리의 수정 불가능한 ECC 오류 및 치명적/수정 불가능한 버스 오류를 포함한 위험한 이벤트 기록 오류

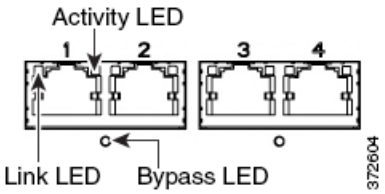
표 7-47 3D7115, 3D7125 및 AMP7150 시스템 상태(계속)

Condition	설명
비위험	비위험 상태는 다음 이벤트와 관련된 임계값이 초과된 상태입니다. • 온도, 전압 또는 팬의 비위험 임계값 초과 • 섀시 침입 • 시스템 BIOS에서 Fault Indication 명령을 설정합니다. BIOS에서는 이 명령을 사용하여 시스템 메모리 또는 CPU 컨피그레이션 변경과 같은 추가적인 비위험 상태를 표시할 수 있습니다.
저하됨	저하된 상태는 다음 이벤트와 관련되어 있습니다. • 하나 이상의 프로세서가 FRB(Fault Resilient Boot) 또는 BIOS에 의해 비활성화됨 • BIOS가 시스템 메모리 중 일부를 비활성화하거나 배제함 • 전원 공급 장치 중 하나가 연결되지 않았거나 작동하지 않음 **정보** 상태 저하 표시를 확인한 경우 전원 공급 장치가 올바르게 연결되었는지 확인합니다. 디바이스 전원을 끄고 두 전원 코드를 분리한 후 다시 연결하여 다시 장착하고 디바이스를 다시 시작합니다. ⚠ **주의** 전원을 안전하게 끄려면 *FireSIGHT System 사용 설명서*의 디바이스 관리에 설명된 절차를 사용하거나 CLI에서 `system shutdown` 명령을 사용합니다.

3D7115, 3D7125 및 AMP7150 센싱 인터페이스

3D7115, 3D7125 및 AMP7150 디바이스는 구성 가능한 바이패스 기능이 있는 4포트 구리 인터페이스와 바이패스 기능이 없고 운영 중 교체 가능한 SFP(Small Form-Factor Pluggable) 포트 8개와 함께 제공됩니다.

그림 7-16 4개의 1000BASE-T 구리 인터페이스



다음 표에서 구리 인터페이스의 링크 및 활동 LED를 확인할 수 있습니다.

표 7-48 3D7115, 3D7125 및 AMP7150 구리 링크/활동 LED

상태	설명
두 LED가 모두 꺼짐	인터페이스에 링크가 없습니다.
황색 링크	인터페이스의 트래픽 속도가 10Mb 또는 100Mb입니다.
녹색 링크	인터페이스의 트래픽 속도가 1Gb입니다.
활동이 녹색으로 깜박임	인터페이스에 링크가 있으며 트래픽이 이동 중입니다.

다음 표에서 구리 인터페이스의 바이패스 LED를 확인할 수 있습니다.

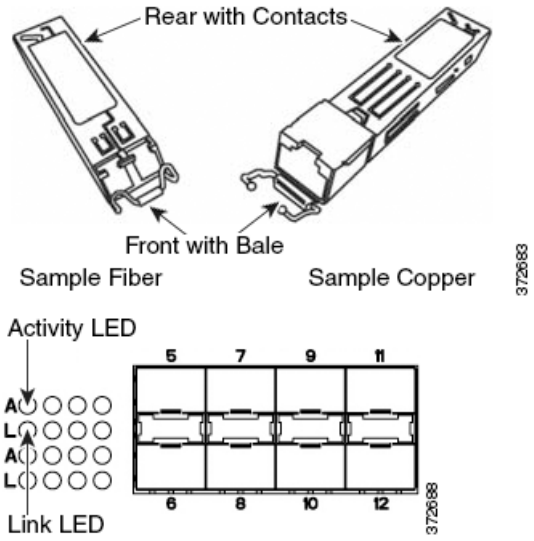
표 7-49 3D7115, 3D7125 및 AMP7150 구리 바이패스 LED

상태	설명
꺼짐	인터페이스 쌍이 바이패스 모드가 아니거나 전원이 없습니다.
녹색으로 켜져 있음	인터페이스 쌍이 바이패스 모드로 전환할 준비가 되었습니다.
황색으로 켜져 있음	인터페이스 쌍이 바이패스 모드로 전환되었으며 트래픽을 검사하지 않습니다.
황색으로 깜박임	인터페이스 쌍이 바이패스 모드입니다. 즉, Failed Open입니다.

SFP 인터페이스

1G 구리, 1G 단거리 파이버 또는 1G 장거리 파이버로 제공되며 운영 중 교체 가능한 Cisco SFP 트렌시버를 최대 8개까지 설치할 수 있습니다. SFP 트렌시버에는 바이패스 기능이 없으며 침입 방지 구축에 사용할 수 없습니다. 자세한 내용은 3D71x5 및 AMP7150 디바이스에서 SFP 트렌시버 사용, 페이지 B-1을(를) 참조하십시오.

그림 7-17 샘플 SFP 트렌시버



다음 표에서 파이버 LED를 확인할 수 있습니다.

표 7-50 3D7115, 3D7125 및 AMP7150 SFP 소켓 활동/링크 LED

상태	설명
위(활동)	인라인 인터페이스: 인터페이스에 활동이 있는 경우 표시등이 켜집니다. 꺼진 경우 활동이 없는 상태입니다. 수동 인터페이스: 표시등이 작동하지 않습니다.
아래(링크)	인라인 인터페이스 또는 수동 인터페이스: 인터페이스에 링크가 있는 경우 표시등이 켜집니다. 꺼진 경우 링크가 없는 상태입니다.

다음 표에서 SFP 옵티컬 트렌시버의 사양을 확인할 수 있습니다.

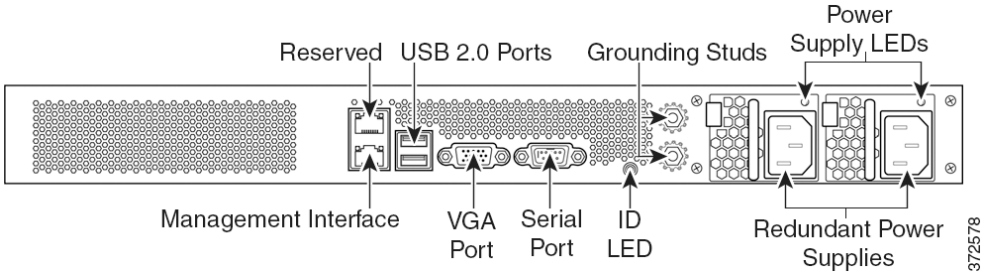
표 7-51 3D7115, 3D7125 및 AMP7150 SFP 옵티컬 매개변수

매개변수	1000BASE-SX	1000BASE-LX
옵티컬 커넥터	LC 이중	LC 이중
비트 속도	1000Mbps	1000Mbps
보드율/인코딩/허용 범위	1250Mbps 8b/10b 인코딩	1250Mbps 8b/10b 인코딩
옵티컬 인터페이스	멀티 모드	단일 모드만 해당
작동 거리	62.5μm/125μm 파이버에서 656피트(200m) 50μm/125μm 파이버에서 1640피트(500m)	9μm/125μm 파이버에서 6피트~6.2마일(2m~10km)
송신기 파장	770~860nm (일반 850nm)	1270~1355nm (일반 1310nm)
최대 평균 시동 전력	0dBm	-3dBm
최소 평균 시동 전력	-9.5dBm	-11.5dBm
수신기의 최대 평균 전력	0dBm	-3dBm
수신기 감도	-17dBm	-19dBm

3D7115, 3D7125 및 AMP7150 섀시 후면 보기

섀시 후면에 관리 인터페이스, 연결 포트, 접지 스터드, 전원 공급 장치가 있습니다.

그림 7-18 3D7115, 3D7125 및 AMP7150(섀시: GERY-1U-8-4C8S-AC) 후면 보기



다음 표에서는 어플라이언스 후면에 표시되는 기능에 대해 설명합니다.

표 7-52 3D7115, 3D7125 및 AMP7150 시스템 구성 요소: 후면 보기

기능	설명
VGA 포트 USB 포트	디바이스에 모니터, 키보드, 마우스를 연결하여 워크스테이션과 어플라이언스를 직접 연결할 수 있습니다.
10/100/1000 이더넷 관리 인터페이스	OOB(Out of Band) 관리 네트워크 연결에 사용합니다. 관리 인터페이스는 유지 보수 및 컨피그레이션 목적으로**만** 사용되며 서비스 트래픽을 전달하기 위한 용도가 아닙니다.
시스템 ID LED	고밀도 랙에 설치된 시스템을 다른 유사한 시스템과 식별할 수 있습니다. 파란색 표시등은 ID 버튼을 눌렀음을 나타냅니다.

표 7-52 3D7115, 3D7125 및 AMP7150 시스템 구성 요소: 후면 보기(계속)

기능	설명
접지 스터드	어플라이언스를 공통의 본딩 네트워크에 연결할 수 있습니다. 자세한 내용은 FirePOWER 디바이스의 전력 요구 사항, 페이지 A-1을(를) 참조하십시오.
예비 전원 공급 장치	AC 전원을 통해 디바이스에 전원을 공급합니다. 섀시 후면을 보면 왼쪽에 전원 공급 장치 #1이 있고 오른쪽에 전원 공급 장치 #2가 있습니다.
전원 공급 장치 LED	전원 공급 장치 상태를 나타냅니다. 표 7-543D7115, 3D7125 및 AMP7150 전원 공급 장치 LED, 페이지 7-38을(를) 참조하십시오.

10/100/1000 관리 인터페이스는 어플라이언스 후면에 있습니다. 다음 표에서는 관리 인터페이스와 관련된 LED에 대해 설명합니다.

표 7-53 3D7115, 3D7125 및 AMP7150 관리 인터페이스 LED

LED	설명
왼쪽(활동)	포트의 활동을 나타냅니다. • 표시등이 깜박이는 경우 활동이 있음을 나타냅니다. • 표시등이 꺼진 경우 활동이 없음을 나타냅니다.
오른쪽(링크)	링크가 활성 상태인지 여부를 나타냅니다. • 표시등이 켜진 경우 링크가 활성 상태임을 나타냅니다. • 표시등이 꺼진 경우 링크가 없음을 나타냅니다.

전원 공급 장치 모듈은 어플라이언스 후면에 있습니다. 다음 표에서는 전원 공급 장치와 연결된 LED에 대해 설명합니다.

표 7-54 3D7115, 3D7125 및 AMP7150 전원 공급 장치 LED

LED	설명
꺼짐	전원 코드가 연결되어 있지 않습니다.
빨간색	이 모듈에 전원이 공급되지 않았습니다. 또는 전원 공급 장치에 모듈 장애, 퓨즈 꺼짐, 팬 장애와 같은 위험 이벤트가 발생하여 전원 공급 장치가 종료됩니다.
빨간색으로 깜박임	전원 공급 장치에 고온, 느린 팬 속도와 같은 경고 이벤트가 발생했지만 전원 공급 장치는 계속 작동합니다.
녹색으로 깜박임	AC 입력이 있고 대기 시 볼트가 감지되며 전원 공급 장치가 꺼져 있습니다.
녹색	전원 공급 장치가 연결되었으며 작동 중입니다.

3D7115, 3D7125, AMP7150 물리적 및 환경 매개변수

다음 표에서는 어플라이언스의 물리적 속성 및 환경 매개변수에 대해 설명합니다.

표 7-55 3D7115, 3D7125, AMP7150 물리적 및 환경 매개변수

매개변수	설명
폼 팩터	1U
크기(D x W x H)	21.6인치 x 19.0인치 x 1.73인치(54.9cm x 48.3cm x 4.4cm)
무게 최대 설치	29.0 파운드(13.2 kg)
구리 1000BASE-T	쌍으로 연결된 컨피그레이션의 기가비트 구리 이더넷 바이패스 가능 인터페이스 케이블 및 거리: 50m에서 Cat5E
구리 1000BASE-T SFP	쌍으로 연결된 컨피그레이션의 기가비트 구리 이더넷 바이패스 불가능 인터페이스 케이블 및 거리: 50m에서 Cat5E
파이버 1000BASE-SX SFP	LC 커넥터를 사용하는 파이버 바이패스 비지원 인터페이스 케이블 및 거리: SX는 550m(표준)에서 멀티 모드 파이버(850nm) 62.5μm/125μm 파이버에서 656피트(200m) 50μm/125μm 파이버에서 1640피트(500m)
파이버 1000BASE-LX SFP	LC 커넥터를 사용하는 파이버 바이패스 비지원 인터페이스 케이블 및 거리: LX는 9μm/125μm 파이버(표준)의 경우 10km에서 단일 모드 파이버(1310m)
전원 공급 장치	450W 이중 예비(1+1) AC 전원 공급 장치 전압: 100VAC~240VAC 공칭 범위(85VAC~264VAC 최대 범위) 전류: 공급 장치당 90VAC~132VAC에서 최대 3A 공급 장치당 187VAC~264VAC에서 최대 1.5A 주파수 범위: 47Hz~63Hz
작동 온도	5ºC~40ºC(41ºF~104ºF)
비작동 온도	-20ºC~70ºC(-29ºF~158ºF)
작동 습도	5%~85%, 비응결
비작동 습도	25ºC~35ºC(77ºF~95ºF) 온도에서 최대 28ºC(82ºF) 습구 이용 시 5%~90%, 비응결 기기를 95% 미만의 비응결 상대 습도에서 보관하십시오. 기기를 실제로 운용하기 최소 48시간 전에 최대 작동 습도 미만의 습도에서 적응하도록 합니다.
고도	0피트(해수면)~5905피트(0~1800m)
냉각 요구 사항	시간당 900BTU 어플라이언스를 요구되는 작동 온도 범위 내로 유지할 수 있도록 충분한 냉각을 제공해야 합니다. 그렇지 않을 경우 어플라이언스에 오작동 또는 손상이 발생할 수 있습니다.
음향 노이즈	전체 프로세서 부하, 정상 팬 작동 시 64dBA GR63-CORE 4.6 음향 노이즈 충족
작동 충격	Bellecore GR63-CORE 표준과 호환
공기 흐름	분당 140 ft^3(3.9 m^3) 공기 흐름이 전면으로 진입해서 후면으로 배출되어 어플라이언스를 통과하며 측면 통풍은 없습니다.

8000 Series 디바이스

8000 Series 디바이스는 구리 또는 파이버 센싱 인터페이스가 포함된 네트워크 모듈(NetMod)을 사용합니다. 디바이스를 완전히 조립된 상태로 출고하거나 사용자가 모듈을 설치할 수 있습니다. FireSIGHT System을 설치하기 전에 디바이스를 조립하십시오. 모듈과 함께 제공된 조립 지침을 참조하십시오.

일부 8000 Series 디바이스를 스태킹하여 시스템 기능을 증가시킬 수 있습니다. 각 스태킹 키트에 대해 NetMod를 스태킹 모듈로 교체하고 8000 Series 스태킹 케이블을 사용하여 디바이스를 서로 연결합니다. 자세한 내용은 스태킹 컨피그레이션에서 디바이스 사용, 페이지 4-16을(를) 참조하십시오.

8000 Series 디바이스는 다양한 섀시에서 제공됩니다.

- 81xx 제품군이라고도 하는 3D8120, 3D8130, 3D8140, AMP8150은 1U 섀시이며 최대 3개의 모듈을 포함할 수 있습니다. 3D8140에서만 스태킹 키트를 추가하여 총 2U 컨피그레이션이 가능합니다.
- AMP8050은 1U 섀시이며 최대 3개의 모듈을 포함할 수 있습니다.
- 82xx 제품군에 속하는 3D8250은 2U 섀시이며 최대 7개의 모듈을 포함할 수 있습니다. 최대 3개의 스태킹 키트를 추가하여 총 8U 컨피그레이션이 가능합니다.
- 82xx 제품군에 속하는 3D8260은 2개의 2U 섀시가 포함된 4U 컨피그레이션입니다. 기본 섀시에는 하나의 스태킹 모듈과 최대 6개의 센싱 모듈이 포함되어 있습니다. 보조 섀시에는 하나의 스태킹 모듈이 포함되어 있습니다. 최대 2개의 스태킹 키트를 추가하여 총 8U 컨피그레이션이 가능합니다.
- 82xx 제품군에 속하는 3D8270은 3개의 2U 섀시가 포함된 6U 컨피그레이션입니다. 기본 섀시에는 2개의 스태킹 모듈과 최대 5개의 센싱 모듈이 포함되어 있습니다. 각 보조 섀시에는 하나의 스태킹 모듈이 포함되어 있습니다. 하나의 스태킹 키트를 추가하여 총 8U 컨피그레이션이 가능합니다.
- 82xx 제품군에 속하는 3D8290은 4개의 2U 섀시가 포함된 8U 컨피그레이션입니다. 기본 섀시에는 3개의 스태킹 모듈과 최대 4개의 센싱 모듈이 포함되어 있습니다. 각 보조 섀시에는 하나의 스태킹 모듈이 포함되어 있습니다. 이 모델은 완전히 구성되어 있으며 스태킹 키트를 추가할 수 없습니다.
- 83xx 제품군에 속하는 3D8350 및 AMP8350은 2U 섀시이며 최대 7개의 모듈을 장착할 수 있습니다. 최대 3개의 스태킹 키트를 추가하여 총 8U 컨피그레이션이 가능합니다.
- 83xx 제품군에 속하는 3D8360 및 AMP8360은 2개의 2U 섀시가 포함된 4U 컨피그레이션입니다. 기본 섀시에는 하나의 스태킹 모듈과 최대 6개의 센싱 모듈이 포함되어 있습니다. 보조 섀시에는 하나의 스태킹 모듈이 포함되어 있습니다. 최대 2개의 스태킹 키트를 추가하여 총 8U 컨피그레이션이 가능합니다.
- 83xx 제품군에 속하는 3D8370 및 AMP8370은 3개의 2U 섀시가 포함된 6U 컨피그레이션입니다. 기본 섀시에는 2개의 스태킹 모듈과 최대 5개의 센싱 모듈이 포함되어 있습니다. 각 보조 섀시에는 하나의 스태킹 모듈이 포함되어 있습니다. 하나의 스태킹 키트를 추가하여 총 8U 컨피그레이션이 가능합니다.
- 83xx 제품군에 속하는 3D8390 및 AMP8390은 4개의 2U 섀시가 포함된 8U 컨피그레이션입니다. 기본 섀시에는 3개의 스태킹 모듈과 최대 4개의 센싱 모듈이 포함되어 있습니다. 각 보조 섀시에는 하나의 스태킹 모듈이 포함되어 있습니다. 이 모델은 완전히 구성되어 있으며 스태킹 키트를 추가할 수 없습니다.

참고 FirePOWER AMP8150에는 3D8150과 동일한 폼 팩터가 있으며, AMP8350과 3D8350, AMP83560과 3D8360, AMP8370과 3D8370, AMP8390과 3D8390의 경우에도 마찬가지로 각각 동일한 폼 팩터가 있습니다. AMP 모델은 FireSIGHT 시스템의 네트워크 기반 AMP(Advanced Malware Protection) 기능을 활용하도록 최적화되었습니다.

자세한 내용은 다음 섹션을 참조하십시오.

- 8000 Series 섀시 전면 보기, 페이지 7-41
- 8000 Series 섀시 후면 보기, 페이지 7-44
- 8000 Series 물리적 및 환경 매개변수, 페이지 7-47
- 8000 Series 모듈, 페이지 7-50

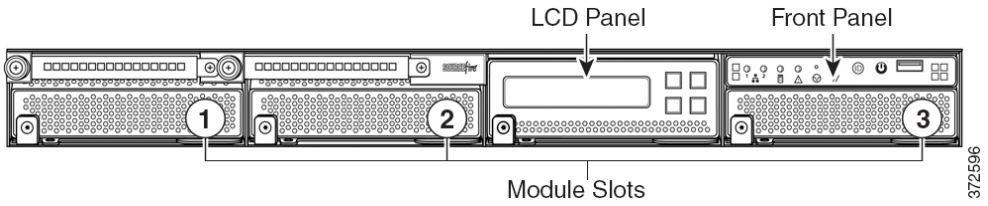
8000 Series 섀시 전면 보기

8000 Series 섀시는 AMP8050 및 81xx 제품군, 82xx 제품군 또는 83xx 제품군에 장착할 수 있습니다. AMP8050, 81xx 제품군, 82xx 제품군 및 83xx 제품군 어플라이언스에 대한 안전 고려 사항은 *FirePOWER 및 FireSIGHT 어플라이언스 규정준수 및 안전 정보* 문서를 참조하십시오.

AMP8050 및 81xx 제품군 섀시 전면 보기

섀시 전면에는 LCD 패널, 전면 패널 및 3개의 모듈 슬롯이 있습니다.

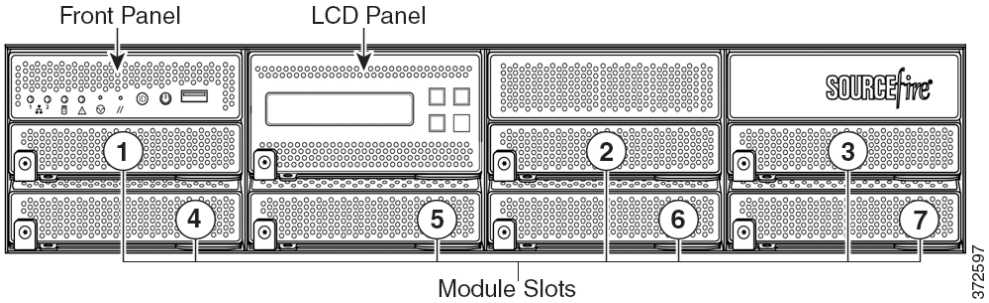
그림 7-19 AMP8050 및 81xx 제품군(섀시: CHAS-1U-AC/DC) 전면 보기



82xx 제품군 및 83xx 제품군 섀시 전면 보기

섀시 전면에는 LCD 패널, 전면 패널 및 7개의 모듈 슬롯이 있습니다.

그림 7-20 82xx 제품군(섀시: CHAS-2U-AC/DC) 및 83xx 제품군(PG35-2U-AC/DC) 전면 보기



다음 표에서는 어플라이언스 전면에 있는 기능에 대해 설명합니다.

표 7-56 8000 Series 시스템 구성 요소: 전면 보기

기능	설명
모듈 슬롯	모듈을 포함합니다. 사용 가능한 모듈에 대한 자세한 내용은 8000 Series 모듈, 페이지 7-50을(를) 참조하십시오.
LCD 패널	디바이스를 구성하고 오류 메시지를 표시하며 시스템 상태를 보는 여러 모드에서 작동합니다. 자세한 내용은 Series 3 디바이스에서 LCD 패널 사용, 페이지 6-1을(를) 참고하십시오.
전면 패널 제어	시스템의 작동 상태와 전원 버튼과 같은 다양한 제어를 표시하는 LED가 있습니다. 자세한 내용은 그림 7-2282xx 제품군 및 83xx 제품군 전면 패널, 페이지 7-42을(를) 참고하십시오.
전면 패널 USB 포트	USB 2.0 포트를 사용하여 디바이스에 키보드를 연결할 수 있습니다.

자세한 내용은 다음 섹션을 참조하십시오.

- 8000 Series 전면 패널, 페이지 7-42
- 8000 Series 새시 후면 보기, 페이지 7-44

8000 Series 전면 패널

81xx 제품군, 82xx 제품군 및 83xx 제품군의 전면 패널에는 동일한 구성 요소가 있습니다.

그림 7-21 81xx 제품군 전면 패널

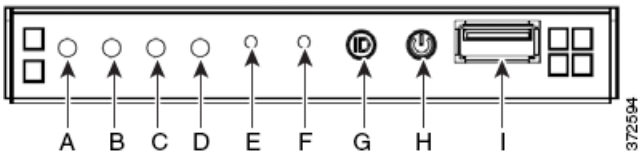


그림 7-22 82xx 제품군 및 83xx 제품군 전면 패널

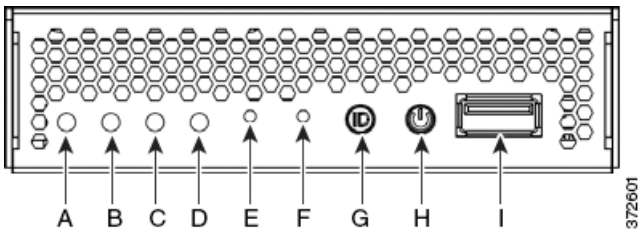


표 7-57 8000 Series 전면 패널 구성 요소

A	NIC 활동 LED	F	재설정 버튼
B	예약됨	G	ID 버튼
C	하드 드라이브 활동 LED	H	전원 버튼 및 LED
D	시스템 상태 LED	I	USB 2.0 커넥터
E	마스크 불가능 중단 버튼		

섀시 전면 패널에는 시스템 작동 상태를 표시하는 LED가 있습니다. 다음 표는 전면 패널의 LED에 대해 설명합니다.

표 7-58 8000 Series 전면 패널 LED

LED	설명
NIC 활동	네트워크 활동이 있는지 여부를 나타냅니다. • 녹색 표시등은 네트워크 활동이 있음을 나타냅니다. • 표시등이 꺼진 경우 네트워크 활동이 없는 상태입니다.
하드 드라이브 활동	하드 드라이브 상태를 다음과 같이 나타냅니다. • 녹색 표시등이 깜박이는 경우 고정 디스크 드라이브가 활성 상태임을 나타냅니다. • 황색은 고정 디스크 드라이브에 장애가 있음을 나타냅니다. • 표시등이 꺼진 경우 드라이브 활동이 없거나 시스템 전원이 꺼져 있음을 나타냅니다.
시스템 상태	시스템 상태를 다음과 같이 나타냅니다. • 녹색은 시스템이 정상 작동 중임을 나타냅니다. • 녹색 표시등이 깜박이는 경우 시스템이 저하된 상태로 작동 중임을 나타냅니다. • 황색 표시등이 깜박이는 경우 시스템이 위험하지 않은 상태임을 나타냅니다. • 황색 표시등은 시스템이 위험하거나 복구 불가능한 상태이거나 시스템이 시동 중임을 나타냅니다. • 표시등이 꺼진 경우 시스템이 켜지거나 꺼지는 중임을 나타냅니다. **참고** 황색 상태 표시등이 녹색 상태 표시등보다 우선합니다. 황색 표시등이 켜져 있거나 깜박이는 경우 녹색 표시등이 꺼집니다. 자세한 내용은 표 7-59 페이지 7-43을(를) 참조하십시오.
시스템 ID	고밀도 랙에 설치된 시스템을 다른 유사한 시스템과 식별할 수 있습니다. • 파란색 표시등은 ID 버튼을 눌렀음을 나타내며 파란색 표시등은 어플라이언스 후면에 있습니다. • 표시등이 꺼진 경우 ID 버튼을 누르지 않았음을 나타냅니다.
전원 버튼 및 LED	시스템에 전원이 연결되었는지 여부를 나타냅니다. • 녹색은 시스템에 전원이 연결되었음을 나타냅니다. • 표시등이 꺼진 경우 시스템에 전원이 연결되어 있지 않음을 나타냅니다.

다음 표에서는 시스템 상태 LED가 켜질 수 있는 상태에 대해 설명합니다.

표 7-59 8000 Series 시스템 상태

상태	설명
위험	다음 이벤트와 관련된 위험하거나 복구 불가능한 임계값 초과 상태입니다. • 온도, 전압 또는 팬의 위험 임계값 초과 • 전원 하위 시스템 장애 • 잘못 설치된 프로세서 또는 프로세서 비호환성으로 인해 시스템 전원을 켤 수 없음 • PCI SERR 및 PERR과 같이 시스템 메모리의 수정 불가능한 ECC 오류 및 치명적/수정 불가능한 버스 오류를 포함한 위험한 이벤트 기록 오류

표 7-59 8000 Series 시스템 상태(계속)

상태	설명
비위험	비위험 상태는 다음 이벤트와 관련된 임계값이 초과된 상태입니다. • 온도, 전압 또는 팬의 비위험 임계값 초과 • 섀시 침입 • 시스템 BIOS에서 Fault Indication 명령을 설정합니다. BIOS에서는 이 명령을 사용하여 시스템 메모리 또는 CPU 컨피그레이션 변경과 같은 추가적인 비위험 상태를 표시할 수 있습니다.
저하됨	저하된 상태는 다음 이벤트와 관련되어 있습니다. • 하나 이상의 프로세서가 FRB(Fault Resilient Boot) 또는 BIOS에 의해 비활성화됨 • BIOS가 시스템 메모리 중 일부를 비활성화하거나 배제함 • 전원 공급 장치 중 하나가 연결되지 않았거나 작동하지 않음 **정보** 상태 저하 표시를 확인한 경우 전원 공급 장치가 올바르게 연결되었는지 확인합니다. 디바이스 전원을 끄고 두 전원 코드를 분리한 후 다시 연결하여 다시 장착하고 디바이스를 다시 시작합니다. ⚠ **주의** 전원을 안전하게 끄려면 *FireSIGHT System 사용 설명서*의 디바이스 관리에 설명된 절차를 사용하거나 CLI에서 `system shutdown` 명령을 사용합니다.

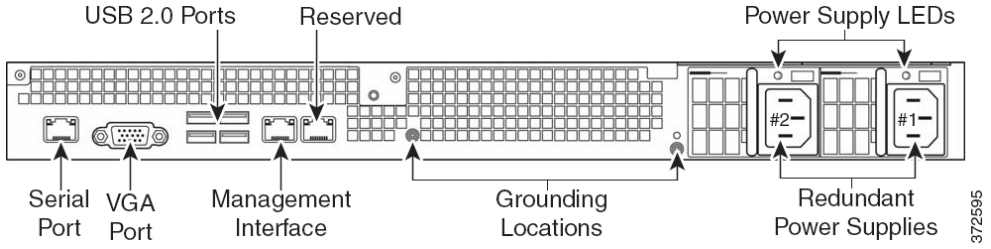
8000 Series 섀시 후면 보기

8000 Series 섀시는 81xx 제품군, 82xx 제품군 또는 83xx 제품군에 장착할 수 있습니다.

AMP8050 및 81xx 제품군 섀시 후면 보기

섀시 후면에는 연결 포트, 관리 인터페이스 및 전원 공급 장치가 있습니다.

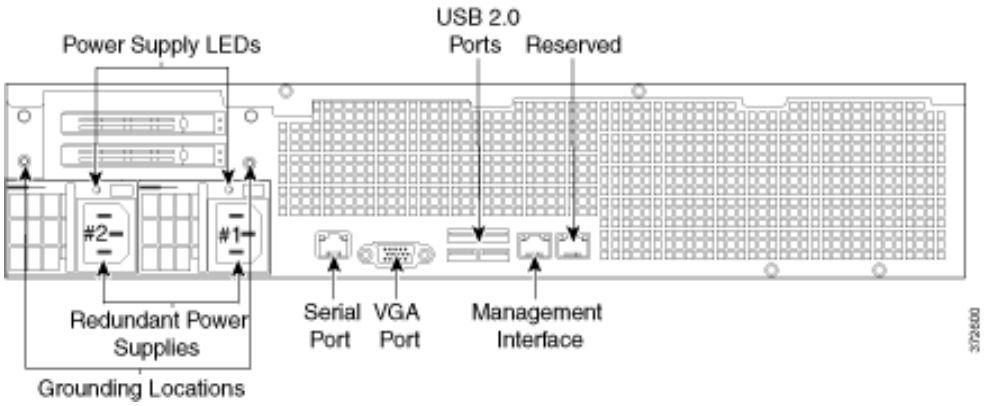
그림 7-23 AMP8050 및 81xx 제품군(섀시: CHAS-1U-AC/DC) 후면 보기



82xx 제품군 섀시 후면 보기

섀시 후면 보기에는 전원 공급 장치, 연결 포트 및 관리 인터페이스가 있습니다.

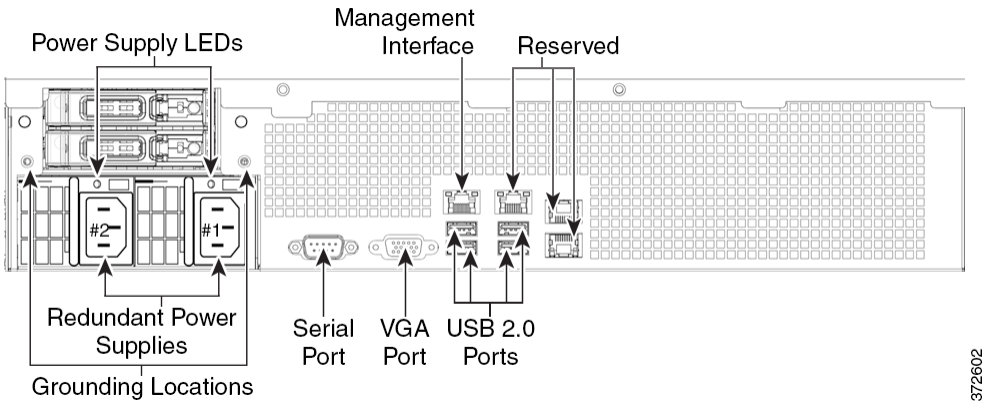
그림 7-24 82xx 제품군(섀시: CHAS-2U-AC/DC) 후면 보기



83xx 제품군 섀시 후면 보기

섀시 후면 보기에는 전원 공급 장치, 연결 포트 및 관리 인터페이스가 있습니다.

그림 7-25 83xx 제품군(섀시: PG35-2U-AC/DC) 후면 보기



다음 표에서는 어플라이언스 후면에 표시되는 기능에 대해 설명합니다.

표 7-60 8000 Series 시스템 구성 요소: 후면 보기

기능	설명
VGA 포트 USB 2.0 포트	시리얼 포트를 사용하는 대신에 모니터, 키보드, 마우스를 디바이스에 연결하여 워크스테이션과 어플라이언스를 직접 연결할 수 있습니다.
RJ45 시리얼 포트 (81xx 제품군 및 82xx 제품군)	디바이스스의 모든 관리 서비스에 직접 액세스할 수 있도록 직접적인 워크스테이션-어플라이언스 연결을 설정합니다(RJ45-DB-9 어댑터 사용). RJ45 시리얼 포트는 유지 보수 및 컨피그레이션 목적에**만** 사용되며 서비스 트래픽을 전달하기 위한 용도가 아닙니다.

표 7-60 8000 Series 시스템 구성 요소: 후면 보기(계속)

기능	설명
RS232 시리얼 포트 (83xx 제품군)	워크스테이션과 어플라이언스를 직접 연결하여 디바이스의 모든 관리 서비스에 직접 액세스할 수 있습니다. RJ232 시리얼 포트는 유지 보수 및 컨피그레이션 목적에**만** 사용되고 서비스 트래픽을 전달하기 위한 용도가 아닙니다.
10/100/1000 이더넷 관리 인터페이스	OOB(Out of Band) 관리 네트워크 연결에 사용합니다. 관리 인터페이스는 유지 보수 및 컨피그레이션 목적으로**만** 사용되며 서비스 트래픽을 전달하기 위한 용도가 아닙니다.
예비 전원 공급 장치	AC 전원을 통해 디바이스에 전원을 공급합니다. 섀시 후면을 보면 오른쪽에 전원 공급 장치 #1이 있고 왼쪽에 전원 공급 장치 #2가 있습니다.
접지 위치	어플라이언스를 공통의 본딩 네트워크에 연결할 수 있습니다. 자세한 내용은 FirePOWER 디바이스의 전력 요구 사항, 페이지 A-1을(를) 참조하십시오.

10/100/1000 관리 인터페이스는 어플라이언스 후면에 있습니다. 다음 표에서는 관리 인터페이스와 관련된 LED에 대해 설명합니다.

표 7-61 8000 Series 관리 인터페이스 LED

LED	설명
왼쪽(활동)	포트의 활동을 나타냅니다. • 표시등이 깜박이는 경우 활동이 있음을 나타냅니다. • 표시등이 꺼진 경우 활동이 없음을 나타냅니다.
오른쪽(링크)	링크가 활성 상태인지 여부를 나타냅니다. • 표시등이 켜진 경우 링크가 활성 상태임을 나타냅니다. • 표시등이 꺼진 경우 링크가 없음을 나타냅니다.

전원 공급 장치 모듈은 어플라이언스 후면에 있습니다. 다음 표에서는 관리 인터페이스와 관련된 LED에 대해 설명합니다.

표 7-62 8000 Series 전원 공급 장치 LED

LED	설명
꺼짐	전원 공급 장치가 연결되어 있지 않습니다.
황색	이 모듈에 전원이 공급되지 않았습니다. 또는 전원 공급 장치에 모듈 장애, 퓨즈 꺼짐, 팬 장애와 같은 위험 이벤트가 발생하여 전원 공급 장치가 종료됩니다.
황색으로 깜박임	전원 공급 장치에 고온, 느린 팬 속도와 같은 경고 이벤트가 발생했지만 전원 공급 장치는 계속 작동합니다.
녹색으로 깜박임	AC 입력이 있고 대기 시 볼트가 감지되며 전원 공급 장치가 꺼져 있습니다.
녹색	전원 공급 장치가 연결되었으며 작동 중입니다.

8000 Series 물리적 및 환경 매개변수

다음 표에서는 AMP8050 및 81xx 제품군 디바이스의 물리적 속성 및 환경 매개변수에 대해 설명합니다.

표 7-63 AMP8050 및 81xx 제품군 물리적 및 환경 매개변수

매개변수	설명
폼 팩터	1U
크기 (D x W x H)	28.7인치 x 17.2인치 x 1.73인치(72.8cm x 43.3cm x 4.4cm)
무게 최대 설치	43.5 파운드(19.8kg)
구리 1000BASE-T 바이패스 구성 가능 NetMod	쌍으로 연결된 컨피그레이션의 쿼드 포트 기가비트 구리 이더넷 바이패스 구성 가능 인터페이스 케이블 및 거리: 50m에서 Cat5E
파이버 10GBASE 바이패스 구성 가능 MMSR 또는 SMLR NetMod	LC 커넥터를 사용하는 듀얼 포트 파이버 바이패스 구성 가능 인터페이스 케이블 및 거리: LR은 5000m에서 단일 모드(사용 가능) SR은 550m에서 멀티 모드 파이버(850mm)(표준)
파이버 1000BASE-SX 바이패스 구성 가능 NetMod	LC 커넥터를 사용하는 쿼드 포트 파이버 바이패스 구성 가능 인터페이스 1000BASE-SX 케이블 및 거리: SX는 550m(표준)에서 멀티 모드 파이버(850nm)
구리 1000BASE-T 비 바이패스 NetMod	쌍으로 연결된 컨피그레이션의 쿼드 포트 기가비트 구리 이더넷 비 바이패스 인터페이스 케이블 및 거리: 50m에서 Cat5E
파이버 10GBASE 비 바이패스 MMSR 또는 SMLR NetMod	LC 커넥터를 사용하는 쿼드 포트 파이버 비 바이패스 인터페이스 케이블 및 거리: LR은 5000m에서 단일 모드(사용 가능) SR은 550m에서 멀티 모드 파이버(850mm)(표준)
파이버 1000BASE-SX 비 바이패스 NetMod	LC 커넥터를 사용하는 쿼드 포트 파이버 비 바이패스 인터페이스 1000BASE-SX 케이블 및 거리: SX는 550m(표준)에서 멀티 모드 파이버(850nm)
전원 공급 장치	AC 또는 DC용으로 설계된 이중 650 W 예비 전원 공급 장치 AC 전압: 100VAC~240VAC 공칭 범위(85VAC~264VAC 최대 범위) AC 전류: 공급 장치당 전체 범위에서 최대 5.2A 공급 장치당 187VAC~264VAC에서 최대 2.6A AC 주파수 범위: 47Hz~63Hz DC 전압: RTN 기준 공칭 -48VDC -40VDC~최대 -72VDC DC 전류: 공급 장치당 최대 11A
작동 온도	10°C~35°C(50°F~95°F)
비작동 온도	-20°C~70°C(-29°F~158°F)
작동 습도	5%~85%, 비응결
비작동 습도	25°C~35°C(77°F~95°F) 온도에서 최대 28ºC(82ºF)의 습구 이용 시 5%~90%, 비응결
고도	0피트(해수면)~6000피트(0~1800m)

표 7-63 AMP8050 및 81xx 제품군 물리적 및 환경 매개변수(계속)

매개변수	설명
냉각 요구 사항	시간당 1725BTU 어플라이언스를 요구되는 작동 온도 범위 내로 유지할 수 있도록 충분한 냉각을 제공해야 합니다. 그렇지 않을 경우 어플라이언스에 오작동 또는 손상이 발생할 수 있습니다.
음향 노이즈	최대 공칭 작동 노이즈는 87.6dB LWAd(고온)입니다. 일반 공칭 작동 노이즈는 80dB LWAd입니다.
작동 충격	2G의 반 사인파 충격 시 오류 없음(11ms 동안)
공기 흐름	분당 160 ft^3(4.5 m^3) 전면 또는 후면을 막거나 충분한 공간이 없는 캐비닛에 기기를 장착하는 등 공기 흐름을 제한할 경우 주변 온도가 작동 범위인 경우에도 기기가 과열될 수 있습니다. 어플라이언스를 통과하는 공기 흐름이 전면으로 진입하여 후면으로 배출됩니다. 전면 및 후면에 권장되는 최소 공간은 20cm(7.9인치)입니다. 이 최소값은 어플라이언스 앞에 저온 공기를 공급하는 경우에만 적용될 수 있습니다.

다음 표에서는 82xx 제품군 및 83xx 제품군 디바이스의 물리적 속성 및 환경 매개변수에 대해 설명합니다.

표 7-64 82xx 제품군 및 83xx 제품군 물리적 및 환경 매개변수

매개변수	설명	
폼 팩터	2U	
크기(D x W x H)	29.0인치 x 17.2인치 x 3.48인치(73.5cm x 43.3cm x 88.2cm)	
최대 설치 무게	82xx 제품군:	58파운드(25.3kg)
	83xx 제품군:	67파운드(30.5kg)
구리 1000BASE-T 바이패스 구성 가능 NetMod	쌍으로 연결된 컨피그레이션의 쿼드 포트 기가비트 구리 이더넷 바이패스 구성 가능 인터페이스 케이블 및 거리: 50m에서 Cat5E	
파이버 10GBASE MMSR 또는 SMLR 바이패스 구성 가능 NetMod	LC 커넥터를 사용하는 듀얼 포트 파이버 바이패스 구성 가능 인터페이스 케이블 및 거리: LR은 5000m에서 단일 모드(사용 가능) SR은 550m에서 멀티 모드 파이버(850mm)(표준)	
파이버 1000BASE-SX 바이패스 구성 가능 NetMod	LC 커넥터가 있는 쿼드 포트 파이버 바이패스 구성 가능 인터페이스 1000BASE-SX 케이블 및 거리: SX는 550m(표준)에서 멀티 모드 파이버(850nm)	
파이버 40GBASE-SR4 바이패스 구성 가능 NetMod	OTP/MTP 커넥터를 사용하는 듀얼 포트 파이버 바이패스 구성 가능 인터페이스 케이블 및 거리: OM3: 850nm 멀티 모드에서 100m OM4: 850nm 멀티 모드에서 150m	
구리 1000BASE-T 비 바이패스 NetMod	쌍으로 연결된 컨피그레이션의 쿼드 포트 기가비트 구리 이더넷 비 바이패스 인터페이스 케이블 및 거리: 50m에서 Cat5E	

표 7-64 82xx 제품군 및 83xx 제품군 물리적 및 환경 매개변수(계속)

매개변수	설명	
파이버 10GBASE 비 바이패스 MMSR 또는 SMLR NetMod	LC 커넥터를 사용하는 쿼드 포트 파이버 비 바이패스 인터페이스 케이블 및 거리: LR은 5000m에서 단일 모드(사용 가능) SR은 550m에서 멀티 모드 파이버(850mm)(표준)	
파이버 1000BASE-SX 비 바이패스 NetMod	LC 커넥터를 사용하는 쿼드 포트 파이버 비 바이패스 인터페이스 1000BASE-SX 케이블 및 거리: SX는 550m에서 멀티 모드 파이버(850mm)(표준)	
전원 공급 장치	82xx 제품군:	AC 또는 DC용으로 설계된 이중 750 W 예비 전원 공급 장치 AC 전압: 100VAC~240VAC 공칭 범위(85VAC~264VAC최대 범위) AC 전류: 공급 장치당 전체 범위에서 최대 8A 공급 장치당 187VAC~264VAC에서 최대 4A AC 주파수 범위: 47Hz~63Hz DC 전압: RTN 기준 공칭 -48VDC -40VDC~최대 -72VDC DC 전류: 공급 장치당 최대 18A
	83xx 제품군:	AC 또는 DC용으로 설계된 이중 1000 W 예비 전원 공급 장치 AC 전압: 100VAC~240VAC 공칭 범위(85VAC~264VAC최대 범위) AC 전류: 공급 장치당 전체 범위에서 최대 11A 공급 장치당 187VAC~264VAC에서 최대 5.5A AC 주파수 범위: 47Hz~63Hz DC 전압: RTN 기준 공칭 -48VDC -40VDC~최대 -72VDC DC 전류: 공급 장치당 최대 25A
작동 온도	82xx 제품군:	10°C~35°C(50°F~95°F)
	83xx 제품군:	5°C~40°C(41°F~104°F)
비작동 온도	-20°C~70°C(-29°F~158°F)	
작동 습도	5%~85%, 비응결	
비작동 습도	25°C~35°C(77°F~95°) 온도에서 최대 28°C(82°F)의 습구 이용 시 5%~90%, 비응결	
고도	0피트(해수면)~6000피트(0~1800m)	
냉각 요구 사항	시간당 최대 2900BTU 어플라이언스를 요구되는 작동 온도 범위 내로 유지할 수 있도록 충분한 냉각을 제공해야 합니다. 그렇지 않을 경우 어플라이언스에 오작동 또는 손상이 발생할 수 있습니다.	
음향 노이즈	최대 공칭 작동 노이즈는 81.6dB LWAd(고온)입니다. 일반 공칭 작동 노이즈는 81.4dB LWAd입니다.	

표 7-64 82xx 제품군 및 83xx 제품군 물리적 및 환경 매개변수(계속)

매개변수	설명
작동 충격	2G의 반 사인파 충격 시 오류 없음(11ms 동안)
공기 흐름	전면에서 후면으로, 분당 210피트^3(6m^3) 전면 또는 후면을 막거나 충분한 공간이 없는 캐비닛에 기기를 장착하는 등 공기 흐름을 제한할 경우 주변 온도가 작동 범위인 경우에도 기기가 과열될 수 있습니다. 어플라이언스를 통과하는 공기 흐름이 전면으로 진입하여 후면으로 배출됩니다. 전면 및 후면에 권장되는 최소 공간은 20cm(7.9인치)입니다. 이 최소값은 어플라이언스 앞에 저온 공기를 공급하는 경우에만 적용될 수 있습니다.

8000 Series 모듈

8000 Series 어플라이언스의 센싱 인터페이스는 구리 또는 파이버 인터페이스로 제공될 수 있습니다.

주의 모듈은 운영 중 교체할 수 **없습니다**. 자세한 내용은 8000 Series 모듈 삽입 및 제거, 페이지 C-1을(를) 참조하십시오.

다음 모듈에는 바이패스 기능을 구성할 수 있는 센싱 인터페이스가 포함되어 있습니다.

- 구성 가능한 바이패스 기능이 포함된 쿼드 포트 1000BASE-T 구리 인터페이스. 쿼드 포트 1000BASE-T 구리 바이패스 구성 가능 NetMod, 페이지 7-51을 참조하십시오.
- 구성 가능한 바이패스 기능이 포함된 쿼드 포트 1000BASE-SX 파이버 인터페이스. 자세한 내용은 쿼드 포트 1000BASE-SX 파이버 바이패스 구성 가능 NetMod, 페이지 7-52을(를) 참조하십시오.
- 구성 가능한 바이패스 기능이 포함된 듀얼 포트 10GBASE(MMSR 또는 SMLR) 파이버 인터페이스. 자세한 내용은 듀얼 포트 10GBASE(MMSR 또는 SMLR) 파이버 바이패스 구성 가능 NetMod, 페이지 7-53을(를) 참조하십시오.
- 구성 가능한 바이패스 기능이 포함된 듀얼 포트 40GBASE-SR4 파이버 인터페이스(2U 디바이스만 해당). 자세한 내용은 듀얼 포트 40GBASE-SR4 파이버 바이패스 구성 가능 NetMod, 페이지 7-55을(를) 참조하십시오.

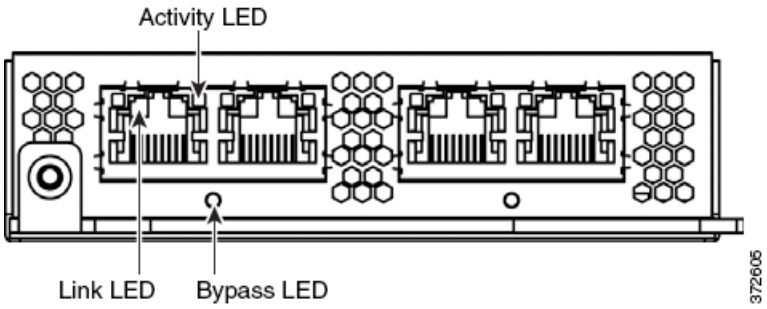
다음 모듈에는 비 바이패스 센싱 인터페이스가 포함되어 있습니다.

- 바이패스 기능이 없는 쿼드 포트 1000BASE-T 구리 인터페이스. 자세한 내용은 쿼드 포트 1000BASE-T 구리 비 바이패스 NetMod, 페이지 7-56을(를) 참조하십시오.
- 바이패스 기능이 없는 쿼드 포트 1000BASE-SX 파이버 인터페이스. 자세한 내용은 쿼드 포트 1000BASE-SX 파이버 비 바이패스 NetMod, 페이지 7-57을(를) 참조하십시오.
- 바이패스 기능이 없는 쿼드 포트 10GBASE(MMSR 또는 SMLR) 파이버 인터페이스. 자세한 내용은 쿼드 포트 10GBASE(MMSR 또는 SMLR) 파이버 비- 바이패스 NetMod, 페이지 7-58을(를) 참조하십시오.

또한 스태킹 모듈로 2개의 3D8140, 최대 4개의 3D8250 또는 최대 4개의 3D8350 디바이스를 연결하여 처리 능력을 결합하고 처리량을 높일수 있습니다. 자세한 내용은 스태킹 모듈, 페이지 7-59을(를) 참조하십시오.

쿼드 포트 1000BASE-T 구리 바이패스 구성 가능 NetMod

쿼드 포트 1000BASE-T 구리 바이패스 구성 가능 NetMod에는 4개의 카퍼(copper) 포트 및 링크, 활동, 바이패스 LED가 있습니다.



다음 표에서 구리 인터페이스의 링크 및 활동 LED를 확인할 수 있습니다.

표 7-65 구리 링크/활동 LED

상태	설명
두 LED가 모두 꺼짐	인터페이스가 링크가 없으며 바이패스 모드가 아닙니다.
황색 링크	인터페이스의 트래픽 속도가 10Mb 또는 100Mb입니다.
녹색 링크	인터페이스의 트래픽 속도가 1Gb입니다.
활동이 녹색으로 깜박임	인터페이스에 링크가 있으며 트래픽이 이동 중입니다.

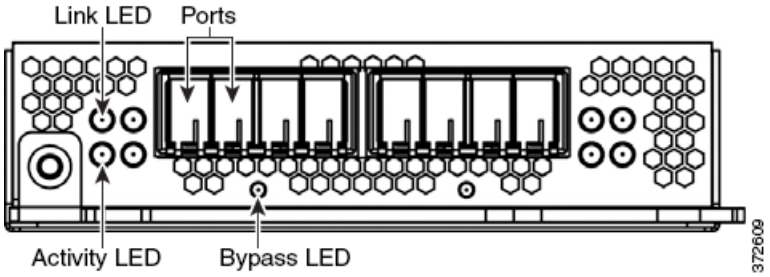
다음 표에서 구리 인터페이스의 바이패스 LED를 확인할 수 있습니다.

표 7-66 구리 바이패스 LED

상태	설명
꺼짐	인터페이스가 링크가 없으며 바이패스 모드가 아닙니다.
녹색으로 켜져 있음	인터페이스에 링크가 있으며 트래픽이 이동 중입니다.
황색으로 켜져 있음	인터페이스가 고의적으로 차단되었습니다.
황색으로 깜박임	인터페이스가 바이패스 모드입니다. 즉, Failed Open입니다.

쿼드 포트 1000BASE-SX 파이버 바이패스 구성 가능 NetMod

쿼드 포트 1000BASE-SX 파이버 바이패스 구성 가능 NetMod에는 4개의 파이버 포트와 링크, 활동 및 바이패스 LED가 있습니다.



다음 표에서 파이버 인터페이스의 링크 및 활동 LED를 확인할 수 있습니다.

표 7-67 파이버 링크/활동 LED

상태	설명
위	인라인 또는 수동 인터페이스: • 표시증이 깜박이는 경우 인터페이스에 활동이 있음을 나타냅니다. • 표시등이 꺼진 경우 활동이 없음을 나타냅니다.
아래	인라인 인터페이스: • 표시등이 켜진 경우 인터페이스에 활동이 있음을 나타냅니다. • 표시등이 꺼진 경우 활동이 없음을 나타냅니다. 수동 인터페이스: 표시등이 항상 켜져 있습니다.

다음 표에서 파이버 인터페이스의 바이패스 LED를 확인할 수 있습니다.

표 7-68 파이버 인터페이스 LED

상태	설명
꺼짐	인터페이스가 링크가 없으며 바이패스 모드가 아닙니다.
녹색으로 켜져 있음	인터페이스에 링크가 있으며 트래픽이 이동 중입니다.
황색으로 켜져 있음	인터페이스가 고의적으로 차단되었습니다.
황색으로 깜박임	인터페이스가 바이패스 모드입니다. 즉, Failed Open입니다.

다음 표에서 파이버 인터페이스의 옵티컬 사양을 확인할 수 있습니다.

표 7-69 1000BASE-SX NetMod 옵티컬 매개변수

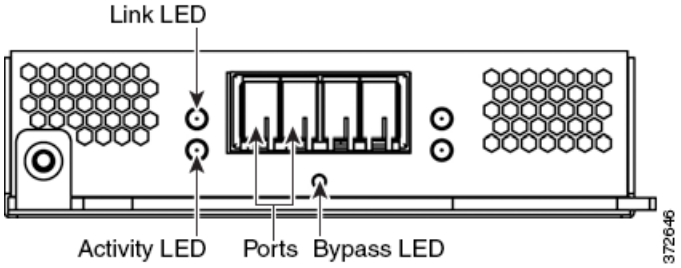
매개변수	1000BASE-SX
옵티컬 커넥터	LC 이중
비트 속도	1000Mbps
보드율/인코딩/허용 범위	1250Mbps 8b/10b 인코딩

표 7-69 1000BASE-SX NetMod 옵티컬 매개변수(계속)

매개변수	1000BASE-SX
옵티컬 인터페이스	멀티 모드
작동 거리	62.5μm/125μm 파이버에서 656피트(200m) 50μm/125μm 파이버에서 1640피트(500m)
송신기 파장	770~860nm(850nm 일반)
최대 평균 시동 전력	0dBm
최소 평균 시동 전력	-9.5dBm
수신기의 최대 평균 전력	0dBm
수신기 감도	-17dBm

듀얼 포트 10GBASE(MMSR 또는 SMLR) 파이버 바이패스 구성 가능 NetMod

듀얼 포트 10GBASE(MMSR 또는 SMLR) 파이버 바이패스 구성 가능 NetMod에는 2개의 파이버 포트와 링크, 활동 및 바이패스 LED가 있습니다.



다음 표에서 파이버 인터페이스의 링크 및 활동 LED를 확인할 수 있습니다.

표 7-70 파이버 링크/활동 LED

상태	설명
위	인라인 또는 수동 인터페이스: • 표시증이 깜박이는 경우 인터페이스에 활동이 있음을 나타냅니다. • 표시등이 꺼진 경우 활동이 없음을 나타냅니다.
아래	인라인 인터페이스: • 표시등이 켜진 경우 인터페이스에 활동이 있음을 나타냅니다. • 표시등이 꺼진 경우 활동이 없음을 나타냅니다. 수동 인터페이스: 표시등이 항상 켜져 있습니다.

다음 표에서 파이버 인터페이스의 바이패스 LED를 확인할 수 있습니다.

표 7-71 파이버 인터페이스 LED

상태	설명
꺼짐	인터페이스가 링크가 없으며 바이패스 모드가 아닙니다.
녹색으로 켜져 있음	인터페이스에 링크가 있으며 트래픽이 이동 중입니다.
황색으로 켜져 있음	인터페이스가 고의적으로 차단되었습니다.
황색으로 깜박임	인터페이스가 바이패스 모드입니다. 즉, Failed Open입니다.

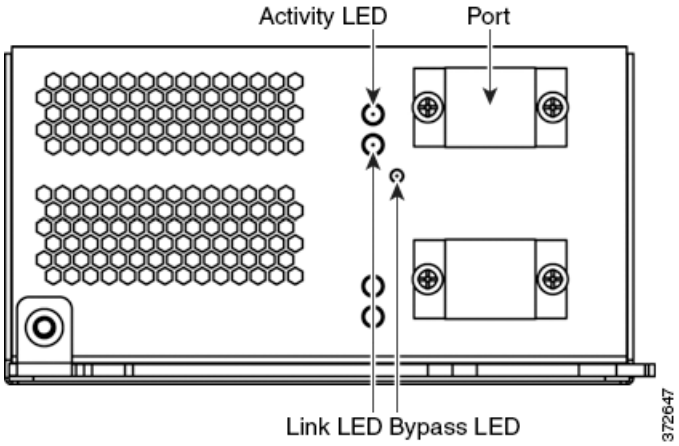
다음 표에서 파이버 인터페이스의 옵티컬 매개변수를 확인할 수 있습니다.

표 7-72 10GBASE MMSR 및 SMLR NetMod 옵티컬 매개변수

매개변수	10GBASE MMSR	10GBASE SMLR
옵티컬 커넥터	LC 이중	LC 이중
비트 속도	10.000Gbps	10.000Gbps
보드율/인코딩/허용 범위	10.3125Gbps 64/66b 인코딩 +/- 100 ppm	10.3125Gbps 64/166b 인코딩 +/- 100 ppm
옵티컬 인터페이스	멀티 모드	단일 모드만 해당
작동 거리	840~860nm (일반 850nm) 62.5μm/125μm 파이버에서 85피트(26m)~108피트(33m)(각각 모달 BW 160~200) 50μm/125μm 파이버에서 216피트(66m)~269피트(82m)(각각 모달 BW 400~500) 980피트(300 m)까지의 거리는 고품질(OM3) 파이버에서 사용 가능합니다. 최소 거리(전체): 6피트(2m)	1270~1355nm (일반 1310nm) 9μm/125μm 파이버에서 6피트~6.2마일(2m~10km)
송신기 파장	840~860nm (일반 850nm)	1270~1355nm (일반 1310nm)
최대 평균 시동 전력	-1dBm	-0.5dBm
최소 평균 시동 전력	-7.3dBm	-8.2dBm
수신기의 최대 평균 전력	-1dBm	-0.5dBm
수신기 감도	-9.9dBm	-14.4dBm

듀얼 포트 40GBASE-SR4 파이버 바이패스 구성 가능 NetMod

듀얼 포트 40GBASE-SR4 파이버 바이패스 구성 가능 NetMod에는 2개의 파이버 포트와 링크, 활동 및 바이패스 LED가 있습니다.



40G NetMod는 3D8270, 3D8290, 3D8360, 3D8370, 3D8390 또는 40G 지원 3D8250, 3D8260, 3D8350에서만 사용할 수 있습니다. 40G를 지원하지 않는 디바이스에 40G 인터페이스를 생성하려고 시도하면 관리 방어 센터 웹 인터페이스의 40G 인터페이스 화면이 빨간색으로 표시됩니다. 40G를 지원하는 3D8250의 경우 LCD 패널에 "3D 8250-40G"가 표시되고 40G를 지원하는 3D8350의 경우에는 LCD 패널에 "3D 8350-40G"가 표시됩니다. 배치 정보는 8000 Series 모듈, 페이지 4-11을(를) 참조하십시오.

다음 표에서 파이버 인터페이스의 링크 및 활동 LED를 확인할 수 있습니다.

표 7-73 파이버 링크/활동 LED

상태	설명
위(활동)	인터페이스에 활동이 있는 경우 표시등이 깜박입니다. 꺼진 경우 활동이 없는 상태입니다.
아래(링크)	인터페이스에 링크가 있는 경우 표시등이 켜집니다. 꺼진 경우 링크가 없는 상태입니다.

다음 표에서 파이버 인터페이스의 바이패스 LED를 확인할 수 있습니다.

표 7-74 파이버 바이패스 LED

상태	설명
꺼짐	인터페이스 쌍에 링크가 없고 바이패스 모드가 아니거나 전원이 없습니다.
녹색으로 켜져 있음	인터페이스 쌍에 링크가 있으며 트래픽이 이동 중입니다.
황색으로 켜져 있음	인터페이스가 고의적으로 차단되었습니다.
황색으로 깜박임	인터페이스가 바이패스 모드입니다. 즉, Failed Open입니다.

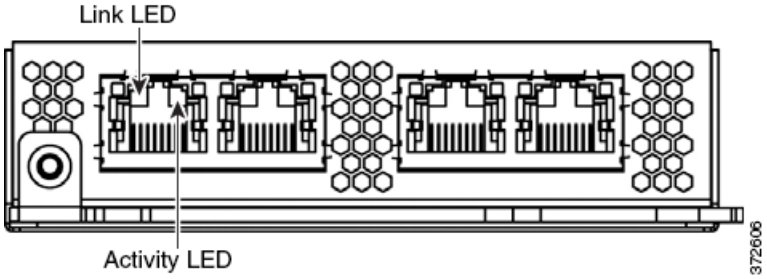
다음 표에서 파이버 인터페이스의 옵티컬 매개변수를 확인할 수 있습니다.

표 7-75 40GBASE-SR4 NetMod 옵티컬 매개변수

매개변수	40GBASE-SR4
옵티컬 커넥터	OTP/MTP 단일 행의 12개 파이버 위치. 바깥쪽 8개 파이버만 사용됩니다.
비트 속도	40.000Gbps
보드율/인코딩/허용 범위	10.3125Gbps 64/66b 인코딩 +/- 100 ppm
옵티컬 인터페이스	멀티 모드
작동 거리	50μm/125μm 파이버(OM3)에서 320피트(100m) 최소 거리: 2피트(0.5m) 40G 옵틱이 MPO 커넥터를 이용하여 8개 파이버 케이블로 전송됩니다.
송신기 파장	840~860nm(850nm 일반)
최대 평균 시동 전력	2.4dBm
최소 평균 시동 전력	-7.8dBm
수신기의 최대 평균 전력	2.4dBm
수신기 감도	-9.5dBm

쿼드 포트 1000BASE-T 구리 비 바이패스 NetMod

쿼드 포트 1000BASE-T 구리 비 바이패스 NetMod에는 4개의 카퍼(copper) 포트와 링크 및 활동 LED가 있습니다.



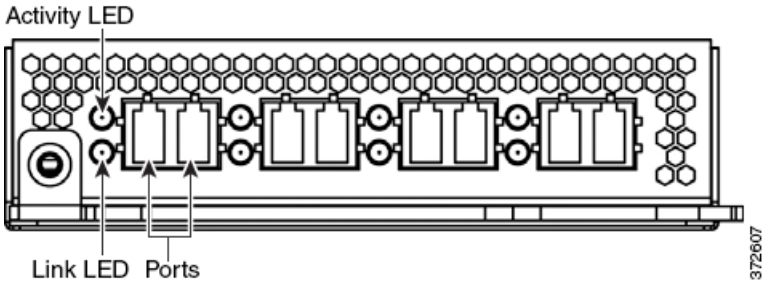
다음 표에서 구리 LED를 확인할 수 있습니다.

표 7-76 비- 바이패스 구리 링크/활동 LED

상태	설명
두 LED가 모두 꺼짐	인터페이스에 링크가 없습니다.
황색 링크	인터페이스의 트래픽 속도가 10Mb 또는 100Mb입니다.
녹색 링크	인터페이스의 트래픽 속도가 1Gb입니다.
활동이 녹색으로 깜박임	인터페이스에 링크가 있으며 트래픽이 이동 중입니다.

쿼드 포트 1000BASE-SX 파이버 비 바이패스 NetMod

쿼드 포트 1000BASE-SX 파이버 비 바이패스 NetMod에는 4개의 파이버 포트와 링크 및 활동 LED가 있습니다.



다음 표에서 파이버 인터페이스의 링크 및 활동 LED를 확인할 수 있습니다.

표 7-77 비 바이패스 파이버 링크/활동 LED

상태	설명
위 (활동)	인라인 인터페이스 또는 수동 인터페이스: 인터페이스에 활동이 있는 경우 표시등이 깜박입니다. 꺼진 경우 활동이 없는 상태입니다.
아래 (링크)	인라인 인터페이스: 인터페이스에 링크가 있는 경우 표시등이 켜집니다. 꺼진 경우 링크가 없는 상태입니다. 수동 인터페이스: 표시등이 항상 켜져 있습니다.

다음 표에서 파이버 인터페이스의 옵티컬 매개변수를 확인할 수 있습니다.

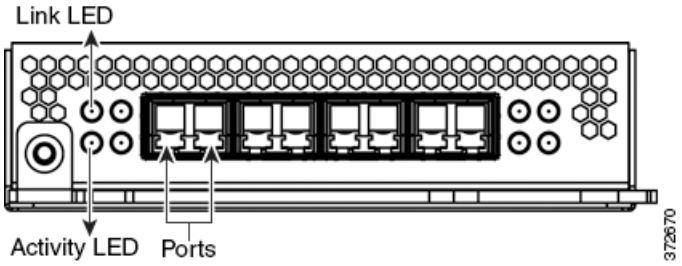
표 7-78 1000BASE-SX NetMod 옵티컬 매개변수

매개변수	1000BASE-SX
옵티컬 커넥터	LC 이중
비트 속도	1000Mbps
보드율/인코딩/허용 범위	1250Mbps 8b/10b 인코딩
옵티컬 인터페이스	멀티 모드
작동 거리	62.5μm/125μm 파이버에서 656피트(200m) 50μm/125μm 파이버에서 1640피트(500m)
송신기 파장	770~860nm(850nm 일반)
최대 평균 시동 전력	0dBm
최소 평균 시동 전력	-9.5dBm
수신기의 최대 평균 전력	0dBm
수신기 감도	-17dBm

쿼드 포트 10GBASE(MMSR 또는 SMLR) 파이버 비- 바이패스 NetMod

쿼드 포트 10GBASE(MMSR 또는 SMLR) 파이버 비 바이패스 NetMod에는 4개의 파이버 포트와 링크 및 활동 LED가 있습니다.

주의 쿼드 포트 10GBASE 비 바이패스 NetMod에는 비착탈식 SFP가 포함되어 있습니다. SFP를 제거하려고 시도하면 모듈이 손상될 수 있습니다.



다음 표에서 파이버 인터페이스의 링크 및 활동 LED를 확인할 수 있습니다.

표 7-79 파이버 링크/활동 LED

상태	설명
위	인라인 인터페이스 또는 수동 인터페이스: 인터페이스에 활동이 있는 경우 표시등이 깜박입니다. 꺼진 경우 활동이 없는 상태입니다.
아래	인라인 인터페이스: 인터페이스에 링크가 있는 경우 표시등이 켜집니다. 꺼진 경우 링크가 없는 상태입니다. 수동 인터페이스: 표시등이 항상 켜져 있습니다.

다음 표에서 파이버 인터페이스의 옵티컬 매개변수를 확인할 수 있습니다.

표 7-80 10GBASE MMSR 및 SMLR NetMod 옵티컬 매개변수

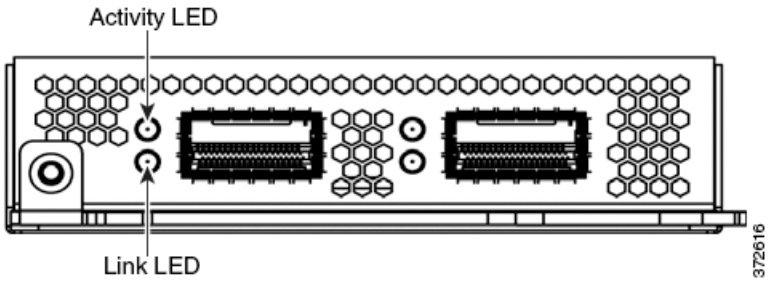
매개변수	10GBASE MMSR	10GBASE SMLR
옵티컬 커넥터	LC 이중	LC 이중
비트 속도	10.000Gbps	10.000Gbps
보드율/ 인코딩/허용 한도	10.3125Gbps 64/66b 인코딩 +/- 100 ppm	10.3125Gbps 64/66b 인코딩 +/- 100 ppm
옵티컬 인터페이스	멀티 모드	단일 모드만 해당

표 7-80 10GBASE MMSR 및 SMLR NetMod 옵티컬 매개변수(계속)

매개변수	10GBASE MMSR	10GBASE SMLR
작동 거리	840~860nm (일반 850nm) 62.5μm/125μm 파이버에서 85피트(26m)~108피트(33m)(각각 모달 BW 160~200) 50μm/125μm 파이버에서 216피트(66m)~269피트(82m)(각각 모달 BW 400~500) 980피트(300 m)까지의 거리는 고품질(OM3) 파이버에서 사용 가능합니다. 최소 거리(전체): 6피트(2m)	1270~1355nm (일반 1310nm) 9μm/125μm 파이버에서 6피트~6.2마일(2m~10km)
송신기 파장	840~860nm (일반 850nm)	1270~1355nm (일반 1310nm)
최대 평균 시동 전력	-1dBm	-0.5dBm
최소 평균 시동 전력	-7.3dBm	-8.2dBm
수신기의 최대 평균 전력	-1dBm	-0.5dBm
수신기 감도	-9.9dBm	-14.4dBm

스태킹 모듈

스태킹 모듈에는 8000 Series 스태킹 케이블과 활동 및 링크 LED용 연결 포트 2개가 있습니다.



다음 표에서 스태킹 LED를 확인할 수 있습니다. 스태킹 모듈은 3D8140, 3D8250, 3D8350으로 제공되며 3D8260/3D8270/3D8290 및 3D8360/3D8370/3D8390에 포함되어 있습니다.

표 7-81 스태킹 LED

상태	설명
위	인터페이스의 활동을 나타냅니다. • 표시등이 깜박이는 경우 인터페이스에 활동이 있음을 나타냅니다. • 표시등이 꺼진 경우 활동이 없음을 나타냅니다.
아래	인터페이스에 링크가 있는지 여부를 나타냅니다. • 표시등이 켜진 경우 인터페이스에 링크가 있음을 나타냅니다. • 표시등이 꺼진 경우 링크가 없음을 나타냅니다.

FireSIGHT System 어플라이언스를 출고 시 기본 설정으로 복원

Cisco에서는 지원 사이트에 방어 센터 및 관리되는 디바이스를 원래 출고 시 설정으로 복원하거나 이미지로 다시 설치하기 위한 ISO 이미지를 제공합니다.

참고 ASA FirePOWER 디바이스 복원 또는 이미지로 다시 설치에 대한 자세한 내용은 ASA 설명서를 참조하십시오.

자세한 내용은 다음 섹션을 참조하십시오.

시작하기 전에

어플라이언스를 출고 시 기본 설정으로 복원하기 전에 먼저 복원 프로세스 중 시스템의 예상 동작을 숙지하고 있어야 합니다.

컨피그레이션 및 이벤트 백업 지침

Cisco에서는 복원 프로세스를 시작하기 전에 어플라이언스에 있는 백업 파일을 삭제하거나 이동한 다음 현재 이벤트 및 컨피그레이션 데이터를 외부 위치로 백업하도록 권장합니다.

어플라이언스를 출고 시 기본 설정으로 복원하면 어플라이언스의 거의 **모든** 컨피그레이션과 이벤트 데이터가 손실됩니다. 복원 유틸리티에서 어플라이언스의 라이센스, 네트워크, 콘솔 및 LOM(Lights-Out Management) 설정을 유지할 수 있지만 복원 프로세스가 완료된 후 다른 모든 설정 작업을 수행해야 합니다.

복원 프로세스 중 트래픽 흐름

Cisco에서는 네트워크의 트래픽 흐름이 중단되지 않도록 유지 보수 창에 있는 동안이나 중단이 구축에 최소한의 영향을 미치는 시점에 어플라이언스를 복원하도록 권장합니다.

인라인 방식으로 구축된 관리되는 디바이스를 복원하면 디바이스가 비 바이패스(Fail Closed) 컨피그레이션으로 재설정되어 네트워크의 트래픽이 중단됩니다. 디바이스에 바이패스 지원 인라인 세트를 구성할 때까지 트래픽이 차단됩니다.

디바이스 컨피그레이션을 편집하여 바이패스를 구성하는 방법에 대한 자세한 내용은 *FireSIGHT System 사용 설명서*의 디바이스 관리 장을 참조하십시오.

복원 프로세스 이해

FireSIGHT System *어플라이언스*는 트래픽을 감지하는 관리되는 *디바이스*이거나 관리하는 *방어 센터*입니다. 각 어플라이언스 유형에는 여러 *모델*이 있으며 이러한 모델은 추가적으로 *Series*와 *제품군*으로 그룹화됩니다. 자세한 내용은 FireSIGHT System 어플라이언스, 페이지 1-2을(를) 참조하십시오.

어플라이언스를 복원하기 위한 정확한 단계는 어플라이언스 모델 및 어플라이언스에 대한 물리적 액세스가 있는지 여부에 따라 달라지지만, 일반 프로세스는 동일합니다.

참고 유지 보수 기간 중에만 어플라이언스를 이미지로 다시 설치하십시오. 이미지로 다시 설치할 경우 바이패스 모드의 어플라이언스가 비 바이패스 컨피그레이션으로 재설정되고 바이패스 모드를 재구성할 때까지 네트워크의 트래픽이 중단됩니다. 자세한 내용은 복원 프로세스 중 트래픽 흐름, 페이지 8-2을(를) 참고하십시오.

FireSIGHT System 어플라이언스를 복원하려면 다음을 수행합니다.

액세스: Admin

단계 1 복원하려는 어플라이언스(디바이스 또는 방어 센터) 모델을 결정합니다.

단계 2 지원 사이트에서 올바른 복원 ISO 이미지를 확보합니다.

단계 3 이미지를 적절한 스토리지 미디어로 복사합니다.

단계 4 어플라이언스에 연결합니다.

단계 5 어플라이언스를 재부팅하고 복원 유틸리티를 호출합니다.

단계 6 ISO 이미지를 설치합니다.

사용자 편의를 위해 대부분의 어플라이언스에서 복원 프로세스의 일부로 시스템 소프트웨어 및 침입 규칙 업데이트를 설치할 수 있습니다.

다음 표에 다양한 FireSIGHT System 어플라이언스 모델을 복원하는 방법이 요약되어 있습니다.

표 8-1 어플라이언스 모델별 지원되는 복원 방법

모델	복원 방법	물리적 액세스 필요 여부	복원 중 업데이트 여부
DC1000 DC3000	ISO 이미지가 사전 로드된 Cisco에서 제공하는 CD-ROM을 사용하거나 자신의 CD를 생성합니다.	CD를 로드하려면 필요	아니요
DC500 모든 Series 2 디바이스(3D9900 제외)	Cisco에서 제공하는 외부 USB 드라이브에서 부팅하고 인터랙티브 메뉴를 사용하여 ISO 이미지를 다운로드하고 어플라이언스에 설치합니다.	USB 드라이브를 삽입하려면 필요	예
3D9900 Series 3 어플라이언스	어플라이언스의 내부 플래시 드라이브에서 부팅하고 인터랙티브 메뉴를 사용하여 ISO 이미지를 다운로드하고 어플라이언스에 설치합니다.	아니요, 원격 KVM 스위치(모두) 또는 LOM(Series 3)을 사용하여 원격으로 복원	예

웹 인터페이스를 사용하여 어플라이언스를 복원할 수 **없습니다**. 어플라이언스를 복원하려면 다음 중 한 가지 방법으로 연결해야 합니다.

키보드 및 모니터/KVM

USB 키보드와 VGA 모니터를 FireSIGHT System 어플라이언스에 연결할 수 있으며, 이는 KVM(키보드, 비디오, 마우스) 스위치에 연결된 랙 마운트 어플라이언스에 유용합니다. 원격 액세스가 가능한 KVM이 있는 경우 물리적 액세스 없이 Series 3 어플라이언스 및 3D9900을 복원할 수 있습니다.

시리얼 연결/노트북 컴퓨터

롤오버 시리얼 케이블(NULL 모뎀 케이블 또는 Cisco 콘솔 케이블이라고도 함)을 사용하여 3D2100/2500/3500/4500 디바이스를 제외한 모든 FireSIGHT System 어플라이언스에 컴퓨터를 연결할 수 있습니다. 시리얼 포트를 찾으려면 어플라이언스 하드웨어 사양을 참조하십시오. 어플라이언스와 상호 작용하려면 HyperTerminal이나 XModem 등의 터미널 에뮬레이션 소프트웨어를 사용합니다. 어플라이언스별 시리얼 포트 커넥터 표를 포함한 자세한 내용은 시리얼 연결/노트북 컴퓨터, 페이지 4-24을(를) 참조하십시오.

SOL(Serial over LAN)을 사용한 LOM(Lights-Out Management)

SOL(Serial over LAN) 연결을 통해 LOM(Lights-Out Management)을 사용하여 Series 3 어플라이언스에 대해 제한적 동작을 수행할 수 있습니다. LOM 지원 어플라이언스를 출고 시 기본값으로 복원해야 하고 어플라이언스에 대한 물리적 액세스가 없는 경우 LOM을 사용하여 복원 프로세스를 수행할 수 있습니다. LOM을 사용하여 어플라이언스에 연결한 다음 물리적 시리얼 연결을 사용하는 것처럼 복원 유틸리티에 명령을 실행합니다. 기본(`eth0`) 관리 인터페이스에서만 LOM(Lights-Out Management)을 사용할 수 있습니다. 자세한 내용은 LOM(Lights-Out Management) 설정, 페이지 8-18을(를) 참고하십시오.

복원 ISO 및 업데이트 파일 가져오기

Cisco에서는 어플라이언스를 원래 출고 시 기본 설정으로 복원하는 ISO 이미지를 제공합니다. 어플라이언스를 복원하기 전에 지원 사이트에서 올바른 ISO 이미지를 가져오십시오.

어플라이언스를 복원하는 데 사용해야 하는 ISO 이미지는 Cisco에서 해당 어플라이언스 모델에 대한 지원을 소개한 시기에 따라 다릅니다. ISO 이미지가 새로운 어플라이언스 모델을 지원하는 부 버전으로 릴리스되지 않은 이상 ISO 이미지는 일반적으로 시스템 소프트웨어의 주 버전과 관련되어 있습니다(예: 5.3 또는 5.4). Cisco에서는 호환되지 않는 시스템 버전을 설치하지 않도록 항상 어플라이언스에 사용 가능한 최신 ISO 이미지를 사용하도록 권장합니다.

대부분의 어플라이언스는 사용자가 복원 유틸리티를 실행할 수 있도록 외부 USB 또는 내부 플래시 드라이브를 사용하여 어플라이언스를 부팅합니다. 그러나 DC1000 및 DC3000 방어 센터에는 복원 ISO CD가 필요합니다. DC1000 또는 DC3000이 있는 경우 어플라이언스를 구매할 때 Cisco에서 ISO 이미지가 탑재된 CD-ROM을 제공했습니다. 어플라이언스를 다른 버전으로 복원하려는 경우 적절한 ISO 이미지를 다운로드하고 새로운 복원 ISO(데이터 아님) CD를 생성하여 어플라이언스를 복원하는 데 사용할 수 있습니다.

또한 Cisco에서는 항상 어플라이언스에서 지원하는 최신 버전의 시스템 소프트웨어를 실행하도록 권장합니다. 어플라이언스를 지원되는 최신 주 버전으로 복원한 다음 시스템 소프트웨어, 침입 규칙 및 VDB(Vulnerability Database)를 업데이트해야 합니다. 자세한 내용은 적용하려는 업데이트의 릴리스 정보와 *FireSIGHT System 사용 설명서*의 시스템 소프트웨어 업데이트 장을 참조하십시오.

사용자 편의를 위해 대부분의 어플라이언스에서 복원 프로세스의 일부로 시스템 소프트웨어 및 침입 규칙 업데이트를 설치할 수 있습니다. 예를 들어, 디바이스를 버전 5.4로 복원하고 해당 프로세스의 일부로 디바이스를 버전 5.4.0.1로 업데이트할 수도 있습니다. 방어 센터에만 규칙 업데이트가 필요합니다.

CD를 사용하여 DC1000 및 DC3000 방어 센터를 복원하므로 복원 프로세스의 일부로 이러한 어플라이언스에 업데이트를 설치할 수 없습니다. 대신, 나중에 어플라이언스를 업데이트하십시오.

복원 ISO 및 기타 업데이트 파일을 가져오려면 다음을 수행합니다.

액세스: 모두

단계 1 지원 계정의 사용자 이름과 비밀번호를 사용하여 지원 사이트(https://support.sourcefire.com/)에 로그인합니다.

단계 2 **Downloads**를 클릭하고 표시되는 페이지에서 **3D System** 탭을 선택한 다음 설치하려는 시스템 소프트웨어의 주 버전을 클릭합니다.

예를 들어, 버전 5.4 또는 버전 5.4.1 ISO 이미지를 다운로드하라면 **Downloads(다운로드) > 3D System(3D 시스템) > 5.4**를 클릭합니다.

단계 3 다운로드하려는 이미지(ISO 이미지)를 찾습니다.

페이지의 해당 섹션을 보려면 페이지의 왼쪽에 있는 링크 중 하나를 클릭합니다. 예를 들어, **5.4.1 Images(5.4.1 이미지)**를 클릭하면 FireSIGHT System 버전 5.4.1에 대한 이미지 및 릴리스 정보를 볼 수 있습니다.

단계 4 다운로드하려는 ISO 이미지를 클릭합니다.

파일 다운로드가 시작됩니다.

단계 5 선택적으로 시스템 소프트웨어 및 침입 규칙 업데이트를 다운로드합니다.

- 시스템 소프트웨어 업데이트는 지원 사이트에서 ISO 이미지와 동일한 페이지에 있습니다. 페이지의 해당 섹션을 보려면 페이지의 왼쪽에 있는 링크 중 하나를 클릭합니다. 예를 들어, **5.4.1**을 클릭하면 FireSIGHT System 버전 5.4.1에 대한 업데이트와 릴리스 정보를 볼 수 있습니다.

- 규칙 업데이트를 다운로드하려면 **Downloads(다운로드) > Rules & VDB(규칙 및 VDB) > Rules(규칙)**를 선택합니다. 최신 규칙 업데이트가 페이지 상단에 있습니다.

DC1000 또는 DC3000을 복원하는 경우 복원 프로세스가 완료된 후 업데이트를 설치해야 합니다.

단계 6 어플라이언스를 복원하는 방법

- USB 또는 내부 플래시 드라이브로 복원하는 대부분의 어플라이언스의 경우에는 어플라이언스가 관리 네트워크에서 액세스할 수 있는 HTTP(웹) 서버, FTP 서버 또는 SCP 지원 호스트로 파일을 복사합니다.
- DC1000 및 DC3000의 경우 ISO 이미지를 사용하여 복원 CD를 생성합니다.

주의 ISO 또는 업데이트 파일을 이메일로 전송하지 **마십시오**. 파일이 손상될 수 있습니다. 또한 파일 이름을 변경하지 **마십시오**. 복원 유틸리티의 이름은 지원 사이트에 표기된 이름과 동일해야 합니다.

복원 프로세스 시작

지원되는 디바이스: 모두

지원되는 방어 센터: DC1000, DC3000을 제외한 모든 방어 센터

DC1000 및 DC3000 방어 센터를 제외한 모든 어플라이언스에서는 어플라이언스 모델에 따라 외부 USB 또는 내부 플래시 드라이브에서 어플라이언스를 부팅하여 복원 프로세스를 시작합니다. 표 8-1 페이지 8-3을(를) 참조하십시오.

어플라이언스에 대한 적절한 액세스 수준 및 연결과 올바른 ISO 이미지가 있는지 확인하고 다음 중 한 가지 절차에 따라 어플라이언스를 복원합니다.

- KVM 또는 물리적 시리얼 포트를 사용하여 복원 유틸리티 시작, 페이지 8-6에서는 LOM을 지원하지 않는 어플라이언스 또는 LOM 액세스가 없는 어플라이언스에 대해 복원 프로세스를 시작하는 방법을 설명합니다. 이 방법을 사용하여 DC1000 또는 DC3000 방어 센터를 제외한 모든 어플라이언스를 복원할 수 있습니다.
- LOM(Lights-Out Management)을 사용하여 복원 유틸리티 시작, 페이지 8-7에서는 LOM을 사용하여 SOL 연결을 통해 Series 3 어플라이언스의 복원 프로세스를 시작하는 방법을 설명합니다.
- CD를 사용하여 DC1000 또는 DC3000 복원, 페이지 8-17에서는 CD를 사용하여 DC1000 또는 DC3000 방어 센터를 복원하는 방법을 설명합니다.

주의 이 장의 절차는 전원을 *끄*지 않은 상태에서 어플라이언스를 복원하는 방법에 대해 설명합니다. 하지만 어떤 이유로 전원을 *꺼*야 하는 경우 *FireSIGHT System 사용 설명서*의 디바이스 관리 장에 설명된 절차를 사용하거나 Series 3 디바이스의 CLI에서 `system shutdown` 명령 또는 어플라이언스 셸(전문가 모드라고도 함)에서 `shutdown -h now` 명령을 사용합니다.

KVM 또는 물리적 시리얼 포트를 사용하여 복원 유틸리티 시작

지원되는 디바이스: 모두

지원되는 방어 센터: DC1000, DC3000을 제외한 모든 방어 센터

DC1000 및 DC3000 방어 센터를 제외한 모든 어플라이언스의 경우, Cisco에서는 어플라이언스 모델에 따라 외부 USB 또는 내부 플래시 드라이브에 복원 유틸리티를 제공합니다. 표 8-1 페이지 8-3을(를) 참조하십시오.

참고 어플라이언스에서 대용량 스토리지 디바이스를 부팅 디바이스로 사용하려고 시도할 수 있으므로 초기 설정을 위해 어플라이언스에 액세스하는 데 USB 대용량 스토리지가 있는 KVM 콘솔을 사용하지 **마십시오**.

Series 3 어플라이언스를 출고 시 기본 설정으로 복원해야 하고 어플라이언스에 대한 물리적 액세스가 없는 경우 LOM을 사용하여 복원 프로세스를 수행할 수 있습니다. LOM(Lights-Out Management)을 사용하여 복원 유틸리티 시작, 페이지 8-7을(를) 참조하십시오.

복원 유틸리티를 시작하려면 다음을 수행합니다.

액세스: Admin

단계 1 USB 드라이브를 사용하여 3D9900을 제외한 Series 2 디바이스 또는 DC500을 복원하는 경우 어플라이언스에서 사용 가능한 USB 포트에 USB 드라이브를 삽입합니다.

그렇지 않으면 다음 단계로 건너뜁니다.

단계 2 키보드/모니터 또는 시리얼 연결을 사용하여 관리자 권한이 있는 계정으로 어플라이언스에 로그인합니다. 비밀번호는 어플라이언스의 웹 인터페이스 비밀번호와 동일합니다.

어플라이언스에 대한 프롬프트가 나타납니다.

단계 3 어플라이언스를 재부팅합니다.

- 방어 센터 또는 Series 2 관리되는 디바이스에서는 `sudo reboot`를 입력합니다.
- Series 3 관리되는 디바이스에서는 `system reboot`를 입력합니다.

어플라이언스가 재부팅됩니다. DC500 방어 센터 또는 3D500/1000/2000 디바이스에서는 스플래시 화면이 표시됩니다.

단계 4 재부팅 상태를 다음과 같이 모니터링합니다.

- 시스템에서 데이터베이스 점검을 수행하는 경우 다음과 같은 메시지가 표시될 수 있습니다.
  `The system is not operational yet. Checking and repairing database are in progress. This may take a long time to finish.`(시스템이 아직 작동하지 않습니다. 데이터베이스 점검 및 복구를 진행 중입니다. 이 작업을 완료하는 데 오랜 시간이 걸릴 수 있습니다.)
- 스플래시 화면이 표시되면 DC500 방어 센터 또는 3D500/1000/2000 디바이스에서 Ctrl + U를 천천히 반복적으로 누릅니다.
- 키보드 및 모니터 연결을 사용하는 다른 어플라이언스의 경우 빨간색 LILO 부팅 메뉴가 표시됩니다. 어플라이언스가 현재 설치된 시스템 버전에서 부팅되지 않도록 화살표 중 하나를 빠르게 누릅니다.
- 시리얼 연결을 사용하는 다른 어플라이언스의 경우 BIOS 부팅 옵션이 표시될 때 (어플라이언스가 현재 설치된 시스템 버전에서 부팅되지 않도록) Tab을 천천히 반복적으로 누릅니다. LILO 부팅 프롬프트가 표시됩니다.

```
LILO 22.8 boot:
3D-5.4 System_Restore
```

단계 5 시스템을 복원할 것임을 나타냅니다.

- DC500 방어 센터 또는 3D500/1000/2000 디바이스에서는 Enter를 누릅니다.
- 키보드 및 모니터 연결을 사용하는 다른 모든 어플라이언스의 경우 화살표 키를 사용하여 `System_Restore`를 선택하고 Enter를 누릅니다.
- 시리얼 연결을 사용하는 다른 어플라이언스의 경우 프롬프트에서 `System_Restore`를 입력합니다.

다음과 같은 선택 사항 다음에 `boot` 프롬프트가 나타납니다.

```
0. Load with standard console
1. Load with serial console
```

단계 6 유틸리티의 인터랙티브 메뉴를 복원하는 디스플레이 모드를 선택합니다.

- 키보드 및 모니터 연결의 경우 `0`을 입력하고 Enter를 누릅니다.
- 시리얼 연결의 경우 `1`을 입력하고 Enter를 누릅니다.

디스플레이 모드를 선택하지 않을 경우 30초 후 복원 유틸리티가 기본 설정인 표준 콘솔로 돌아갑니다.

처음으로 어플라이언스를 이 주 버전으로 복원하는 경우가 아닌 이상 유틸리티는 마지막으로 사용한 복원 컨피그레이션을 자동으로 로드합니다. 계속하려면 일련의 페이지에서 설정을 확인합니다.

복원 유틸리티 저작권 정보가 표시됩니다.

단계 7 Enter를 눌러 저작권 정보를 확인한 후 인터랙티브 메뉴를 사용하여 어플라이언스 복원, 페이지 8-8을(를) 계속 진행합니다.

LOM(Lights-Out Management)을 사용하여 복원 유틸리티 시작

지원되는 디바이스: Series 3

지원되는 방어 센터: Series 3

Series 3 어플라이언스를 출고 시 기본 설정으로 복원해야 하고 어플라이언스에 대한 물리적 액세스가 없는 경우 LOM을 사용하여 복원 프로세스를 수행할 수 있습니다. LOM을 사용하여 초기 설정을 구성하려면 초기 설정 중 **반드시** 네트워크 설정을 유지해야 합니다. 기본(`eth0`) 관리 인터페이스에서만 LOM을 사용할 수 있습니다.

참고 LOM을 사용하여 어플라이언스를 복원하기 전에 해당 기능을 활성화해야 합니다. LOM(Lights-Out Management) 설정, 페이지 8-18을(를) 참조하십시오.

LOM을 사용하여 복원 유틸리티를 시작하려면 다음을 수행합니다.

액세스: Admin

단계 1 컴퓨터의 명령 프롬프트에서 IPMI 명령을 입력하여 SOL 세션을 시작합니다.

- IPMItool의 경우 다음을 입력합니다.

```
sudo ipmitool -I lanplus -H IP_address -U username sol activate
```

- ipmiutil의 경우 다음을 입력합니다.

```
sudo ipmiutil sol -a -V4 -J3 -N IP_address -U username -P password
```

여기서 *IP_address*는 어플라이언스의 관리 인터페이스의 IP 주소이고, *username*은 권한이 있는 LOM 계정의 사용자 이름이며, *password*는 해당 계정의 비밀번호입니다. IPMItool에서 `sol activate` 명령을 입력한 다음 비밀번호를 입력하라는 메시지를 표시합니다.

Series 3 또는 가상의 관리되는 디바이스를 사용하는 경우 `expert`를 입력하여 셸 프롬프트를 표시합니다.

단계 2 어플라이언스를 루트 사용자로 재부팅합니다.

- 방어 센터의 경우 `sudo reboot`를 입력합니다.
- Series 3 디바이스의 경우 `system reboot`를 입력합니다.

어플라이언스가 재부팅됩니다.

단계 3 리부팅 상태를 모니터링합니다.

시스템에서 데이터베이스 점검을 수행하는 경우 다음과 같은 메시지가 표시될 수 있습니다. `The system is not operational yet. Checking and repairing database are in progress. This may take a long time to finish.`(시스템이 아직 작동하지 않습니다. 데이터베이스 점검 및 복구를 진행 중입니다. 이 작업을 완료하는 데 오랜 시간이 걸릴 수 있습니다.)

BIOS 부팅 옵션이 표시되면 LILO 부팅 프롬프트가 나타날 때까지 어플라이언스가 현재 설치된 시스템 버전에서 부팅되지 않도록 Tab을 천천히 반복적으로 누릅니다.

```
LILO 22.8 boot:
3D-5.4 System_Restore
```

단계 4 `boot` 프롬프트에서 `System_Restore`를 입력하여 복원 유틸리티를 시작합니다.

다음과 같은 선택 사항 다음에 `boot` 프롬프트가 나타납니다.

```
0. Load with standard console
1. Load with serial console
```

단계 5 `1`을 입력하고 Enter를 눌러 어플라이언스의 시리얼 연결을 통해 인터랙티브 복원 메뉴를 로드합니다.

참고 디스플레이 모드를 선택하지 않을 경우 30초 후 복원 유틸리티가 기본 설정인 표준 콘솔로 돌아갑니다.

처음으로 어플라이언스를 이 주 버전으로 복원하는 경우가 아닌 이상 유틸리티는 마지막으로 사용한 복원 컨피그레이션을 자동으로 로드합니다. 계속하려면 일련의 페이지에서 설정을 확인합니다.

복원 유틸리티 저작권 정보가 표시됩니다.

단계 6 Enter를 눌러 저작권 정보를 확인한 후 인터랙티브 메뉴를 사용하여 어플라이언스 복원, 페이지 8-8을(를) 계속 진행합니다.

인터랙티브 메뉴를 사용하여 어플라이언스 복원

지원되는 디바이스: 모두

지원되는 방어 센터: DC1000/3000을 제외한 모든 방어 센터

대부분의 FireSIGHT System 어플라이언스 복원 유틸리티는 인터랙티브 메뉴를 사용하여 복원 과정을 안내합니다.

정보 CD를 사용하여 DC1000 또는 DC3000을 복원하는 경우 CD를 사용하여 DC1000 또는 DC3000 복원, 페이지 8-17.로 건너뛰십시오.

참고 유지 보수 기간 중에만 어플라이언스를 이미지로 다시 설치하십시오. 이미지로 다시 설치할 경우 바이패스 모드의 어플라이언스가 비 바이패스 컨피그레이션으로 재설정되고 바이패스 모드를 재구성할 때까지 네트워크의 트래픽이 중단됩니다. 자세한 내용은 복원 프로세스 중 트래픽 흐름, 페이지 8-2을(를) 참고하십시오.

다음 표에 나열된 옵션이 메뉴에 표시됩니다.

표 8-2 복원 메뉴 옵션

옵션	설명	자세한 내용은 다음을 참조하십시오.
1 IP Configuration(IP 컨피그레이션)	어플라이언스가 ISO 및 업데이트 파일이 저장되어 있는 서버와 통신할 수 있도록 복원하려는 어플라이언스의 관리 인터페이스에 대한 네트워크 정보를 지정합니다.	어플라이언스의 관리 인터페이스 식별, 페이지 8-10
2 Choose the transport protocol(전송 프로토콜 선택)	어플라이언스 및 어플라이언스가 파일을 다운로드하는 데 필요한 자격 증명을 복원하는 데 사용할 ISO 이미지의 위치를 지정합니다.	ISO 이미지 위치 및 전송 모드 지정, 페이지 8-11
3 Select Patches/Rule Updates(패치/규칙 업데이트 선택)	어플라이언스가 ISO 이미지의 기본 버전으로 복원된 이후 적용할 시스템 소프트웨어 및 침입 규칙 업데이트를 지정합니다.	복원 중 시스템 소프트웨어 및 침입 규칙 업데이트, 페이지 8-12
4 Download and Mount ISO(ISO 다운로드 및 마운트)	적절한 ISO 이미지와 시스템 소프트웨어 또는 침입 규칙 업데이트를 다운로드합니다. ISO 이미지를 마운트합니다.	ISO 및 업데이트 파일 다운로드 및 이미지 마운트, 페이지 8-13
5 Run the Install(설치 실행)	복원 프로세스를 호출합니다.	복원 프로세스 호출, 페이지 8-13
6 Save Configuration(컨피그레이션 저장) 7 Load Configuration(컨피그레이션 로드)	나중에 사용할 수 있도록 복원 컨피그레이션 집합을 저장하거나 저장된 집합을 로드합니다.	복원 컨피그레이션 저장 및 로드, 페이지 8-16
8 Wipe Contents of Disk(디스크 콘텐츠 삭제)	하드 드라이브 콘텐츠에 더 이상 액세스할 수 없도록 안전하게 삭제합니다.	하드 드라이브 삭제, 페이지 D-1

화살표 키를 사용하여 메뉴를 탐색합니다. 메뉴 옵션을 선택하려면 위쪽 및 아래쪽 화살표를 사용합니다. 오른쪽 및 왼쪽 화살표 키를 사용하여 페이지 하단에 있는 **OK(확인)** 및 **Cancel(취소)** 버튼 사이를 전환합니다.

메뉴에 두 가지 종류의 옵션이 표시됩니다.

- 번호로 표시된 옵션을 선택하려면 위쪽 및 아래쪽 화살표를 사용하여 올바른 옵션을 강조 표시한 다음 페이지 하단의 **OK(확인)** 버튼이 강조 표시되어 있는 상태에서 Enter를 누릅니다.
- 선택형(라디오 버튼) 옵션을 선택하려면 위쪽 및 아래쪽 화살표를 사용하여 올바른 옵션을 강조 표시한 다음 페이지 하단의 스페이스바를 눌러 해당 옵션에 x를 표시합니다. 선택 사항을 승인하려면 **OK(확인)** 버튼이 강조 표시되어 있는 상태에서 Enter를 누릅니다.

대부분의 경우에는 **1**, **2**, **4**, **5**의 순서로 메뉴 옵션을 완료합니다. 선택적으로 복원 프로세스 중에 메뉴 옵션 **3**을 사용하여 시스템 소프트웨어 및 침입 규칙 업데이트를 설치합니다.

현재 어플라이언스에 설치되어 있는 버전과 다른 주 버전으로 복원하는 경우는 2단계 복원 프로세스가 필요합니다. 첫 번째 단계에서는 운영 체제를 업데이트하고 두 번째 단계에서는 새 버전의 시스템 소프트웨어를 설치합니다.

두 번째 단계이거나 사용하려는 복원 컨피그레이션을 복원 유틸리티에서 자동으로 로드한 경우 메뉴 옵션 **4**: ISO 및 업데이트 파일 다운로드 및 이미지 마운트, 페이지 8-13에서 시작할 수 있습니다. 그러나 Cisco에서는 계속하기 전에 복원 컨피그레이션에서 설정을 거듭 확인하도록 권장합니다.

정보 이전에 저장된 컨피그레이션을 사용하려면 메뉴 옵션 **6**: 복원 컨피그레이션 저장 및 로드, 페이지 8-16에서 시작합니다. 컨피그레이션을 로드한 이후 메뉴 옵션 **4**: ISO 및 업데이트 파일 다운로드 및 이미지 마운트, 페이지 8-13으로 건너뜁니다.

인터랙티브 메뉴를 사용하여 어플라이언스를 복원하려면 다음 단계를 사용합니다.

단계 1 **1 IP Configuration(IP 컨피그레이션)** - 어플라이언스의 관리 인터페이스 식별, 페이지 8-10 참조

단계 2 **2 Choose the transport protocol(전송 프로토콜 선택)** - ISO 이미지 위치 및 전송 모드 지정, 페이지 8-11 참조

단계 3 **3 Select Patches/Rule Updates(패치/규칙 업데이트 선택)**(선택 사항) - 복원 중 시스템 소프트웨어 및 침입 규칙 업데이트, 페이지 8-12 참조

단계 4 **4 Download and Mount ISO(ISO 다운로드 및 마운트)** - ISO 및 업데이트 파일 다운로드 및 이미지 마운트, 페이지 8-13 참조

단계 5 **5 Run the Install(설치 실행)** - 복원 프로세스 호출, 페이지 8-13 참조

어플라이언스의 관리 인터페이스 식별

지원되는 디바이스: 모두

지원되는 방어 센터: DC1000/3000을 제외한 모든 방어 센터

복원 유틸리티를 실행하는 첫 번째 단계는 ISO 및 업데이트 파일을 복사한 서버와 어플라이언스가 통신할 수 있도록 복원하려는 어플라이언스에서 관리 인터페이스를 식별하는 것입니다. LOM을 사용하는 경우 어플라이언스의 관리 IP 주소가 LOM IP 주소가 **아님**을 기억하십시오.

어플라이언스의 관리 인터페이스를 식별하려면 다음을 수행합니다.

액세스: Admin

단계 1 주 메뉴에서 **1 IP Configuration(IP 컨피그레이션)**을 선택합니다.

Pick Device(디바이스 선택) 페이지가 나타납니다.

단계 2 어플라이언스의 관리 인터페이스(일반적으로 **eth0**)를 선택합니다.

IP Configuration(IP 컨피그레이션) 페이지가 나타납니다.

단계 3 관리 네트워크에 사용하는 프로토콜로 **IPv4** 또는 **IPv6**를 선택합니다.

관리 인터페이스에 IP 주소를 할당하기 위한 옵션이 나타납니다.

단계 4 관리 인터페이스에 IP 주소를 할당하는 방법으로 **Static(정적)** 또는 **DHCP**를 선택합니다.

- **Static(정적)**을 선택하는 경우 일련의 페이지가 표시되고 관리 인터페이스의 IP 주소, 네트워크 마스크 또는 접두사 길이 및 기본 게이트웨이를 입력하라는 메시지가 나타납니다.
- **DHCP**를 선택하는 경우 어플라이언스에서 관리 인터페이스의 IP 주소, 네트워크 마스크 또는 접두사 길이 및 기본 게이트웨이를 자동으로 감지한 다음 IP 주소를 표시합니다.

단계 5 메시지가 표시되면 설정을 확인합니다.

메시지가 표시되면 어플라이언스의 관리 인터페이스에 할당된 IP 주소를 확인합니다. 주 메뉴가 다시 표시됩니다.

단계 6 다음 섹션, ISO 이미지 위치 및 전송 모드 지정을 계속 진행합니다.

ISO 이미지 위치 및 전송 모드 지정

지원되는 디바이스: 모두

지원되는 방어 센터: DC1000/3000을 제외한 모든 방어 센터

복원 프로세스에서 필요한 파일을 다운로드하는 데 사용할 관리 IP 주소를 구성한 다음 어플라이언스를 복원하는 데 사용할 ISO 이미지를 식별해야 합니다. 즉, 지원 사이트에서 다운로드하여(복원 ISO 및 업데이트 파일 가져오기, 페이지 8-4 참조) 웹 서버, FTP 서버 또는 SCP 지원 호스트에 저장한 ISO 이미지입니다.

인터랙티브 메뉴는 다음 표에 나열된 대로 다운로드를 완료하는 데 필요한 정보를 입력하라는 메시지를 표시합니다.

표 8-3 복원 파일을 다운로드하는 데 필요한 정보

사용할 위치	입력해야 하는 정보
HTTP	• 웹 서버의 IP 주소 • ISO 이미지 디렉토리의 전체 경로(예: `/downloads/ISOs/`)
FTP	• FTP 서버의 IP 주소 • 사용하려는 자격 증명을 소유한 사용자의 홈 디렉토리의 상대적 경로로 나타낸 ISO 이미지 디렉토리의 경로(예: `mydownloads/ISOs/`) • FTP 서버에 대해 권한이 있는 사용자 이름 및 비밀번호
SCP	• SCP 서버의 IP 주소 • SCP 서버에 대해 권한이 있는 사용자 이름 • ISO 이미지 디렉토리의 전체 경로 • 앞에서 입력한 사용자 이름의 비밀번호 비밀번호를 입력하기 전에 어플라이언스에서 SCP 서버를 신뢰할 수 있는 호스트 목록에 추가하라는 메시지를 표시할 수 있습니다. 계속하려면 동의해야 합니다.

복원 유틸리티가 ISO 이미지 디렉토리에서 업데이트 파일도 찾습니다.

복원 파일의 위치 및 전송 방법을 지정하려면 다음을 수행합니다.

액세스: Admin

단계 1 주 메뉴에서 **2 Choose the transport protocol(전송 프로토콜 선택)**을 선택합니다.

단계 2 표시되는 페이지에서 **HTTP**, **FTP** 또는 **SCP**를 선택합니다.

단계 3 표 8-3 페이지 8-11의 설명에 따라 복원 유틸리티에서 표시하는 일련의 페이지를 사용하여 선택한 프로토콜에 필요한 정보를 제공합니다.

정보가 올바른 경우 어플라이언스가 서버에 연결하고 사용자가 지정한 위치에 Cisco ISO 이미지 목록을 표시합니다.

단계 4 사용할 ISO 이미지를 선택합니다.

단계 5 메시지가 표시되면 설정을 확인합니다.

주 메뉴가 다시 표시됩니다.

단계 6 복원 프로세스 중 시스템 소프트웨어 또는 침입 규칙 업데이트를 설치하시겠습니까?

- 설치하려는 경우 다음 섹션, 복원 중 시스템 소프트웨어 및 침입 규칙 업데이트을(를) 계속 진행합니다.
- 설치하지 않으려면 ISO 및 업데이트 파일 다운로드 및 이미지 마운트, 페이지 8-13을(를) 계속 진행합니다. 복원 프로세스가 완료된 다음 시스템의 웹 인터페이스를 사용하여 업데이트를 수동으로 설치할 수 있습니다.

복원 중 시스템 소프트웨어 및 침입 규칙 업데이트

지원되는 디바이스: 모두

지원되는 방어 센터: DC1000/3000을 제외한 모든 방어 센터

선택적으로 어플라이언스가 ISO 이미지의 기본 버전으로 복원된 후 복원 유틸리티를 사용하여 시스템 소프트웨어와 침입 규칙을 업데이트할 수 있습니다. 방어 센터에만 규칙 업데이트가 필요합니다.

복원 유틸리티는 하나의 시스템 소프트웨어 업데이트와 하나의 규칙 업데이트만 사용할 수 있습니다. 하지만 시스템 업데이트는 마지막 주 버전으로 다시 누적됩니다. 규칙 업데이트도 누적됩니다. Cisco에서는 어플라이언스에 사용 가능한 최신 업데이트를 가져오는 것을 권장합니다. 복원 ISO 및 업데이트 파일 가져오기, 페이지 8-4을(를) 참조하십시오.

복원 프로세스 중 어플라이언스를 업데이트하지 않도록 선택하는 경우 시스템 웹 인터페이스를 사용하여 나중에 업데이트할 수 있습니다. 자세한 내용은 설치하려는 업데이트의 릴리스 정보와 *FireSIGHT System 사용 설명서*의 시스템 소프트웨어 업데이트 장을 참조하십시오.

복원 프로세스의 일부로 업데이트를 설치하려면 다음을 수행합니다.

액세스: Admin

단계 1 주 메뉴에서 **3 Select Patches/Rule Updates(패치/규칙 업데이트 선택)**를 선택합니다.

복원 유틸리티는 이전 절차에서 지정한 프로토콜과 위치를 사용하여(ISO 이미지 위치 및 전송 모드 지정, 페이지 8-11 참조) 해당 위치에 있는 시스템 소프트웨어 업데이트 파일 목록을 검색 및 표시합니다. SCP를 사용하는 경우 해당 메시지가 표시되면 비밀번호를 입력하여 업데이트 파일 목록을 표시합니다.

단계 2 사용하려는 시스템 소프트웨어 업데이트(있는 경우)를 선택합니다.

업데이트를 선택하지 않아도 됩니다. 계속하려면 업데이트를 선택하지 않고 Enter를 누릅니다. 적절한 위치에 시스템 소프트웨어 업데이트가 없는 경우 시스템에서 계속하려면 Enter를 누르라는 메시지를 표시합니다.

복원 유틸리티가 규칙 업데이트 파일 목록을 검색 및 표시합니다. SCP를 사용하는 경우 해당 메시지가 표시되면 비밀번호를 입력하여 목록을 표시합니다.

단계 3 사용하려는 규칙 업데이트(있는 경우)를 선택합니다.

업데이트를 선택하지 않아도 됩니다. 계속하려면 업데이트를 선택하지 않고 Enter를 누릅니다. 적절한 위치에 규칙 업데이트가 없는 경우 계속하려면 Enter를 누르라는 메시지가 표시됩니다.

선택 사항이 저장되고 주 메뉴가 다시 나타납니다.

단계 4 다음 섹션, ISO 및 업데이트 파일 다운로드 및 이미지 마운트을(를) 계속 진행합니다.

ISO 및 업데이트 파일 다운로드 및 이미지 마운트

지원되는 디바이스: 모두

지원되는 방어 센터: DC1000, DC3000을 제외한 모든 방어 센터

복원 프로세스를 호출하기 전 마지막 단계는 필요한 파일을 다운로드하고 ISO 이미지를 마운트하는 것입니다.

정보 이 단계를 시작하기 전에 나중에 사용할 수 있도록 복원 컨피그레이션을 저장할 수 있습니다. 자세한 내용은 복원 컨피그레이션 저장 및 로드, 페이지 8-16을(를) 참고하십시오.

ISO 이미지를 다운로드하여 마운트하려면 다음을 수행합니다.

액세스: Admin

단계 1 주 메뉴에서 **4 Download and Mount ISO(ISO 다운로드 및 마운트)**를 선택합니다.

단계 2 메시지가 표시되면 선택 사항을 확인합니다. SCP 서버에서 다운로드하는 경우 메시지가 표시되면 비밀번호를 입력합니다.

적절한 파일을 다운로드하여 마운트합니다. 주 메뉴가 다시 표시됩니다.

단계 3 다음 섹션, 복원 프로세스 호출을(를) 계속 진행합니다.

복원 프로세스 호출

지원되는 디바이스: 모두

지원되는 방어 센터: DC1000, DC3000을 제외한 모든 방어 센터

ISO 이미지를 다운로드하여 마운트한 후 복원 프로세스를 호출할 수 있습니다. 현재 어플라이언스에 설치되어 있는 버전과 다른 주 버전으로 복원하는 경우는 2단계 복원 프로세스가 필요합니다. 첫 번째 단계에서는 운영 체제를 업데이트하고 두 번째 단계에서는 새 버전의 시스템 소프트웨어를 설치합니다.

2단계 중 첫 번째 단계(주 버전만 변경)

어플라이언스를 다른 주 버전으로 복원하는 경우 복원 유틸리티는 첫 번째 단계로 어플라이언스의 운영 체제를 업데이트하고, 필요에 따라 유틸리티 자체를 복원합니다.

참고 어플라이언스를 동일한 주 버전으로 복원하는 중이거나 프로세스의 두 번째 단계를 실행하는 경우 다음 절차, 두 번째 또는 유일한 단계, 페이지 8-15로 건너뛰십시오.

2단계 복원 프로세스 중 첫 번째 단계를 수행하려면 다음과 같이 합니다.

액세스: Admin

단계 1 주 메뉴에서 **5 Run the Install(설치 실행)**을 선택합니다.

단계 2 메시지가 (두 번) 표시되면 어플라이언스를 재부팅할 것임을 확인합니다.

참고 외부 USB 드라이브를 사용하여 복원하는 어플라이언스의 경우 드라이브에 다른 시스템 버전과 관련된 복원 유틸리티가 있으면 드라이브에서 유틸리티를 업데이트해야 계속할 수 있습니다. 메시지가 표시되면 `yes(예)`를 입력하고 유틸리티를 업데이트합니다(그리고 저장된 모든 복원 컨피그레이션 삭제). 그런 다음 업데이트된 드라이브에서 재부팅할 것임을 확인합니다. USB 드라이브를 업데이트하지 않을 경우 어플라이언스가 재부팅됩니다. 이 드라이브를 사용하여 어플라이언스를 복원할 수 없습니다.

단계 3 재부팅을 모니터링하고 복원 프로세스를 다시 호출합니다.

- 시스템에서 데이터베이스 점검을 수행하는 경우 다음과 같은 메시지가 표시될 수 있습니다.
  `The system is not operational yet. Checking and repairing database are in progress. This may take a long time to finish.(시스템이 아직 작동하지 않습니다. 데이터베이스 점검 및 복구를 진행 중입니다. 이 작업을 완료하는 데 오랜 시간이 걸릴 수 있습니다.)`
- 키보드 및 모니터 연결의 경우 빨간색 LILO 부팅 메뉴가 나타납니다. 어플라이언스가 현재 설치된 시스템 버전에서 부팅되지 않도록 화살표 중 하나를 빠르게 누릅니다.
- 시리얼 또는 SOL/LOM 연결에서 BIOS 부팅 옵션이 표시되면 LILO 부팅 프롬프트가 나타날 때까지 Tab을 천천히 반복적으로 누릅니다.

```
LILO 22.8 boot:
3D-5.4 System_Restore
```

단계 4 시스템을 복원할 것임을 나타냅니다.

- 키보드 및 모니터 연결의 경우 화살표 키를 사용하여 `System_Restore`를 선택하고 Enter를 누릅니다.
- 시리얼 또는 SOL/LOM 연결의 경우 프롬프트에서 `System_Restore`를 입력하고 Enter를 누릅니다.

두 경우 모두에 다음 선택 항목 다음에 `boot` 프롬프트가 나타납니다.

```
0. Load with standard console
1. Load with serial console
```

단계 5 유틸리티의 인터랙티브 메뉴를 복원하는 디스플레이 모드를 선택합니다.

- 키보드 및 모니터 연결의 경우 `0`을 입력하고 Enter를 누릅니다.
- 시리얼 또는 SOL/LOM 연결의 경우 `1`을 입력하고 Enter를 누릅니다.

디스플레이 모드를 선택하지 않을 경우 30초 후 복원 유틸리티가 기본 설정인 표준 콘솔로 돌아갑니다.

처음으로 어플라이언스를 이 주 버전으로 복원하는 경우가 아닌 이상 유틸리티는 마지막으로 사용한 복원 컨피그레이션을 자동으로 로드합니다. 계속하려면 일련의 페이지에서 설정을 확인합니다.

복원 유틸리티 저작권 정보가 표시됩니다.

단계 6 Enter를 눌러 저작권 정보를 확인한 후 인터랙티브 메뉴를 사용하여 어플라이언스 복원, 페이지 8-8을(를) 시작하여 프로세스의 2단계를 시작합니다.

두 번째 또는 유일한 단계

복원 프로세스의 두 번째 단계 또는 유일한 단계를 수행하려면 다음 절차를 사용합니다.

복원 프로세스의 두 번째 단계 또는 유일한 단계를 수행하려면 다음과 같이 합니다.

액세스: Admin

단계 1 주 메뉴에서 **5 Run the Install(설치 실행)**을 선택합니다.

단계 2 어플라이언스를 복원할 것임을 확인하고 다음 단계를 계속 진행합니다.

단계 3 어플라이언스의 라이센스 및 네트워크 설정을 삭제할 것인지 여부를 선택합니다. 이러한 설정을 삭제하면 디스플레이(콘솔) 설정이 재설정되고 Series 3 어플라이언스의 경우 LOM이 재설정됩니다.

대부분의 경우는 초기 설정 프로세스가 짧아질 수 있으므로 이러한 설정을 삭제하지 않습니다. 복원을 실행하고 초기 설정을 마친 다음 설정을 변경할 경우 지금 설정을 재설정하는 경우보다 시간이 더 적게 소요됩니다. 자세한 내용은 다음 단계, 페이지 8-18을(를) 참고하십시오.

주의 LOM 연결을 사용하여 어플라이언스를 복원하는 경우 네트워크 설정을 삭제하지 **마십시오**. 어플라이언스를 재부팅한 다음 LOM을 통해 다시 연결할 수 없습니다.

단계 4 USB 드라이브를 사용하여 어플라이언스를 복원하는 경우 복원 유틸리티에서 어플라이언스를 복원할 것인지 마지막으로 확인하는 메시지를 표시하면 드라이브를 제거합니다.

단계 5 어플라이언스를 복원할 것임을 마지막으로 확인합니다.

복원 프로세스의 최종 단계가 시작됩니다. 이 단계가 완료되고 재부팅 메시지가 표시되면 어플라이언스를 재부팅할 것임을 확인합니다.

주의 복원 프로세스가 완료될 때까지 여유 있게 기다립니다. 내부 플래시 드라이브가 장착된 어플라이언스에서 유틸리티가 먼저 플래시 드라이브를 업데이트하면 이 플래시 드라이브를 사용하여 다른 복원 작업을 수행합니다. 플래시 업데이트 중 종료할 경우(예: Ctrl + C 누름) 복구 불가능한 오류가 발생할 수 있습니다. 복원이 너무 오래 걸린다는 생각이 들거나 이 프로세스에 다른 문제가 발생하는 경우 종료하지 **마십시오**. 대신, 고객 지원에 문의하십시오.

참고 이미지로 다시 설치할 경우 바이패스 모드의 어플라이언스가 비 바이패스 컨피그레이션으로 재설정되고 바이패스 모드를 재구성할 때까지 네트워크의 트래픽이 중단됩니다. 자세한 내용은 복원 프로세스 중 트래픽 흐름, 페이지 8-2을(를) 참고하십시오.

단계 6 다음 단계, 페이지 8-18을(를) 계속 진행합니다.

복원 컨피그레이션 저장 및 로드

지원되는 디바이스: 모두

지원되는 방어 센터: DC1000, DC3000을 제외한 모든 방어 센터

대부분의 어플라이언스에서 어플라이언스를 다시 복원해야 할 경우 복원 유틸리티를 사용하여 사용할 복원 컨피그레이션을 저장할 수 있습니다. 복원 유틸리티가 마지막으로 사용된 컨피그레이션을 자동으로 저장하지만, 다음과 같은 여러 컨피그레이션을 저장할 수 있습니다.

- 어플라이언스의 관리 인터페이스에 대한 네트워크 정보, 어플라이언스의 관리 인터페이스 식별, 페이지 8-10 참조
- 복원 ISO 이미지의 위치 및 어플라이언스에서 파일을 다운로드하는 데 필요한 전송 프로토콜 및 자격 증명, ISO 이미지 위치 및 전송 모드 지정, 페이지 8-11 참조
- 어플라이언스가 ISO 이미지의 기본 버전으로 복원된 후 적용하려는 시스템 소프트웨어 및 침입 규칙 업데이트(있는 경우), 복원 중 시스템 소프트웨어 및 침입 규칙 업데이트, 페이지 8-12 참조

SCP 비밀번호는 저장되지 않습니다. 컨피그레이션에 유틸리티가 ISO 및 기타 파일을 어플라이언스로 전송하는 데 반드시 SCP를 사용하도록 지정된 경우 서버를 재인증해야 복원 프로세스를 완료할 수 있습니다.

위에 나열된 정보를 입력한 후 ISO 이미지를 다운로드 및 마운트하기 전까지가 복원 컨피그레이션을 저장하기에 가장 적합합니다. 복원 USB 드라이브가 시스템의 다른 주 버전과 호환되도록 업데이트하는 경우 저장된 복원 컨피그레이션은 손실됩니다.

복원 컨피그레이션을 저장하려면 다음을 수행합니다.

액세스: Admin

단계 1 복원 유틸리티의 주 메뉴에서 **6 Save Configuration(컨피그레이션 저장)**을 선택합니다.

유틸리티에서 저장하고 있는 컨피그레이션의 설정을 표시합니다.

단계 2 메시지가 표시되면 컨피그레이션을 저장할 것임을 확인합니다.

단계 3 메시지가 표시되면 컨피그레이션의 이름을 입력합니다.

컨피그레이션이 저장되고 주 메뉴가 다시 나타납니다.

단계 4 방금 저장한 컨피그레이션을 사용하여 어플라이언스를 복원하려는 경우 ISO 및 업데이트 파일 다운로드 및 이미지 마운트, 페이지 8-13을(를) 계속 진행합니다.

저장된 복원 컨피그레이션을 로드하려면 다음을 수행합니다.

액세스: Admin

단계 1 주 메뉴에서 **7 Load Configuration(컨피그레이션 로드)**을 선택합니다.

유틸리티에서 저장된 복원 컨피그레이션 목록을 표시합니다. 첫 번째 옵션인 **default_config**는 어플라이언스를 복원하는 데 마지막으로 사용한 컨피그레이션입니다. 다른 옵션은 사용자가 저장한 복원 컨피그레이션입니다.

단계 2 사용하려는 컨피그레이션을 선택합니다.

유틸리티에 로드 중인 컨피그레이션의 설정이 표시됩니다.

단계 3 메시지가 표시되면 컨피그레이션을 로드할 것임을 확인합니다.

컨피그레이션이 로드됩니다. 메시지가 표시되면 어플라이언스의 관리 인터페이스에 할당된 IP 주소를 확인합니다. 주 메뉴가 다시 표시됩니다.

단계 4 방금 로드한 컨피그레이션을 사용하여 어플라이언스를 복원하려면 ISO 및 업데이트 파일 다운로드 및 이미지 마운트, 페이지 8-13을(를) 계속 진행합니다.

CD를 사용하여 DC1000 또는 DC3000 복원

지원되는 디바이스: 없음

지원되는 방어 센터: DC1000, DC3000

CD-ROM 드라이브가 있는 DC1000 및 DC3000 방어 센터의 경우 어플라이언스를 구매할 때 Cisco에서 제공한 복원 CD가 있습니다. 어플라이언스를 다른 버전으로 복원하려는 경우 적절한 ISO 이미지를 다운로드하고 새로운 ISO(데이터 아님) 복원 CD를 생성하여 시스템을 복원하는 데 사용할 수 있습니다. 복원 ISO 및 업데이트 파일 가져오기, 페이지 8-4을(를) 참조하십시오.

CD를 사용하여 이러한 방어 센터를 복원하므로 복원 프로세스 중 해당 어플라이언스에 업데이트를 설치할 수 없습니다. 대신, 나중에 어플라이언스를 업데이트하십시오.

CD를 사용하여 DC1000 또는 DC3000을 복원하려면 다음을 수행합니다.

액세스: Admin

단계 1 복원 CD를 방어 센터의 CD 트레이에 놓습니다.

어플라이언스가 꺼져 있는 경우 전원을 켜서 트레이를 엽니다.

단계 2 키보드/모니터 또는 시리얼 연결을 사용하여 관리자 권한의 계정으로 방어 센터에 로그인합니다. 비밀번호는 방어 센터 웹 인터페이스 비밀번호와 동일합니다.

방어 센터에 대한 프롬프트가 나타납니다.

단계 3 프롬프트에서 루트 사용자로 `sudo reboot`를 입력하여 방어 센터를 재부팅합니다.

방어 센터가 CD에서 부팅됩니다. 이 작업에는 몇 분이 소요될 수 있습니다.

단계 4 메시지가 표시되면 방어 센터를 복원할 것임을 확인합니다.

단계 5 어플라이언스의 라이센스 및 네트워크 설정을 삭제할 것인지 여부를 선택합니다. 이러한 설정을 삭제하면 디스플레이(콘솔) 설정도 재설정됩니다.

대부분의 경우는 초기 설정 프로세스가 짧아질 수 있으므로 이러한 설정을 삭제하지 않습니다. 복원을 실행하고 초기 설정을 마친 다음 설정을 변경할 경우 지금 설정을 재설정하는 경우보다 시간이 더 적게 소요됩니다. 자세한 내용은 다음 단계, 페이지 8-18을(를) 참고하십시오.

단계 6 어플라이언스를 복원할 것임을 마지막으로 확인합니다.

복원 프로세스가 시작되고 화면에 진행률이 표시됩니다.

주의 복원 프로세스가 완료될 때까지 여유 있게 기다립니다. 흔하진 않지만, 종료할 경우(예: Ctrl + C를 누르거나 어플라이언스 전원 끄기) 복구 불가능한 오류가 발생할 수 있습니다. 복원이 너무 오래 걸린다는 생각이 들거나 이 프로세스에 다른 문제가 발생하는 경우 종료하지 **마십시오**. 대신, 고객 지원에 문의하십시오.

단계 7 메시지가 표시되면 Enter를 눌러 계속합니다.

방어 센터에서 CD가 배출됩니다. CD를 꺼내고 트레이를 닫습니다.

단계 8 메시지가 다시 표시되면 Enter를 눌러 복원이 완료되었고 어플라이언스를 재부팅할 것임을 확인합니다.

어플라이언스가 재부팅됩니다.

단계 9 다음 단계를 계속 진행합니다.

다음 단계

어플라이언스를 출고 시 기본 설정으로 복원할 경우 인라인 방식으로 구축된 디바이스의 바이패스 컨피그레이션을 포함하여 어플라이언스에 있는 거의 **모든** 컨피그레이션과 이벤트 데이터가 손실됩니다. 자세한 내용은 복원 프로세스 중 트래픽 흐름, 페이지 8-2을(를) 참고하십시오.

어플라이언스를 복원한 이후 초기 설정 프로세스를 완료해야 합니다.

- 어플라이언스의 라이센스 및 네트워크 설정을 삭제하지 않은 경우 관리 네트워크의 컴퓨터를 사용하여 어플라이언스의 웹 인터페이스를 직접 탐색하여 설정을 수행할 수 있습니다. 자세한 내용은 초기 설정 페이지: 디바이스, 페이지 5-8 및 초기 설정 페이지: 방어 센터, 페이지 5-11을(를) 참조하십시오.
- 라이센스 및 네트워크 설정을 삭제한 경우 어플라이언스가 관리 네트워크에서 통신할 수 있도록 하는 컨피그레이션부터 시작하여 새로운 어플라이언스인 것처럼 구성해야 합니다. FireSIGHT System 어플라이언스 설정, 페이지 5-1을(를) 참조하십시오.

라이센스와 네트워크 설정을 삭제할 경우 디스플레이(콘솔) 설정이 삭제되고, Series 3 어플라이언스의 경우 LOM 설정이 삭제됩니다. 초기 설정 프로세스를 완료한 후 다음을 수행합니다.

- 시리얼 또는 SOL/LOM 연결을 사용하여 어플라이언스의 콘솔에 액세스하려면 콘솔 출력을 리디렉션해야 합니다. 인라인 바이패스 인터페이스 설치 테스트, 페이지 4-26을(를) 참조하십시오.
- LOM을 사용하려는 경우 기능을 다시 활성화하고 한 명 이상의 LOM 사용자를 활성화해야 합니다. LOM 및 LOM 사용자 활성화, 페이지 8-20을(를) 참조하십시오.

LOM(Lights-Out Management) 설정

지원되는 디바이스: Series 3

지원되는 방어 센터: Series 3

Series 3 어플라이언스를 출고 시 기본 설정으로 복원하려는 경우 어플라이언스에 대한 물리적 액세스가 없으면 LOM(Lights-Out Management)을 사용하여 복원 프로세스를 수행할 수 있습니다. LOM을 사용하여 Series 2 어플라이언스를 복원할 수 **없습니다**. Series 3 어플라이언스만 LOM을 지원합니다. 기본(`eth0`) 관리 인터페이스에서만 LOM(Lights-Out Management)을 사용할 수 있습니다.

참고 Series 3 어플라이언스의 베이스보드 관리 컨트롤러(BMC)는 10/100Mbps로 제한됩니다. 디바이스의 전원이 꺼져 있으면 BMC는 활성 상태로 유지되고 10/100Mbps의 이더넷 링크만 설정할 수 있습니다. 따라서 LOM을 사용하여 디바이스 전원을 원격으로 제어하는 경우 10/100Mbps로 자동 협상될 수 있는 네트워크 디바이스에 연결됩니다. 연결된 네트워크 디바이스를 1000Mbps로 정적으로 구성하면 센서 전원이 꺼지거나 중단된 경우 LOM 연결이 손실됩니다.

LOM 기능을 사용하면 SOL(Serial over LAN) 연결을 통해 Series 3 방어 센터 또는 관리되는 디바이스에 대해 제한된 작업을 수행할 수 있습니다. LOM의 경우 OOB(Out of Band) 관리 연결에서 명령행 인터페이스를 사용하여 섀시 일련 번호 보기, 팬 속도 및 온도 등의 상태 모니터링과 같은 작업을 수행할 수 있습니다.

LOM 명령의 구문은 사용 중인 유틸리티에 따라 다르지만 LOM 명령에는 일반적으로 다음 표에 나열된 요소가 포함되어 있습니다.

표 8-4 LOM 명령 구문

IPMItool(Linux/Mac)	ipmiutil(Windows)	설명
`ipmitool`	`ipmiutil`	IPMI 유틸리티를 호출합니다.
해당 없음	`-V4`	ipmiutil에서만 LOM 세션의 관리자 권한을 활성화합니다.
`-I lanplus`	`-J3`	LOM 세션의 암호화를 활성화합니다.
`-H` *`IP_address`*	`-N` *`IP_address`*	어플라이언스에서 관리 인터페이스의 IP 주소를 지정합니다.
`-U` *`username`*	`-U` *`username`*	권한이 있는 LOM 계정의 사용자 이름을 지정합니다.
해당 없음(로그인 시 프롬프트됨)	-P *`password`*	ipmiutil에서만 권한이 있는 LOM 계정의 비밀번호를 지정합니다.
`command`	*`command`*	어플라이언스에 실행하려는 명령. 명령을 실행하는 위치는 유틸리티에 따라 다릅니다. • IPMItool의 경우 명령을 마지막에 입력합니다. • ipmiutil의 경우 명령을 가장 먼저 입력합니다.

따라서 IPMItool의 경우 다음과 같이 입력합니다.

```
ipmitool -I lanplus -H IP_address -U username command
```

또는 ipmiutil의 경우 다음과 같이 입력합니다.

```
ipmiutil command -V4 -J3 -N IP_address -U username -P password
```

`chassis power off` 및 `chassis power cycle` 명령은 70xx 제품군 어플라이언스에서 유효하지 않습니다. FireSIGHT System에서 지원되는 전체 LOM 명령 목록은 *FireSIGHT System 사용 설명서*의 어플라이언스 설정 구성 장을 참조하십시오.

참고 SOL을 사용하여 7000 Series 디바이스에 연결하기 전에 디바이스의 관리 인터페이스에 연결된 모든 서드파티 스위칭 장비에서 STP(Spanning Tree Protocol)를 비활성화해야 합니다.

참고 일부 전원 주기 시나리오에서는 관리 인터페이스를 통해 네트워크에 연결된 3D7050의 베이스보드 관리 컨트롤러(BMC)가 DHCP 서버에서 할당한 IP 주소를 유실할 수 있습니다. 이러한 이유로 Cisco에서는 3D7050 BMC를 고정 IP 주소로 구성하도록 권장합니다. 또는 네트워크 케이블을 분리한 후 다시 연결하거나 디바이스의 전원을 제거한 후 복원하여 강제로 링크를 다시 협상할 수 있습니다.

LOM을 사용하여 어플라이언스를 복원하기 전에 복원을 수행할 사용자와 어플라이언스 둘 다에 대해 LOM을 활성화해야 합니다. 그런 다음 서드파티 IPMI(Intelligent Platform Management Interface) 유틸리티를 사용하여 어플라이언스에 액세스합니다. 또한 어플라이언스의 콘솔 출력을 시리얼 포트로 리디렉션해야 합니다.

자세한 내용은 다음 섹션을 참조하십시오.

- LOM 및 LOM 사용자 활성화, 페이지 8-20
- IPMI 유틸리티 설치, 페이지 8-21

LOM 및 LOM 사용자 활성화

지원되는 디바이스: Series 3

지원되는 방어 센터: Series 3

LOM을 사용하여 어플라이언스를 복원하려면 먼저 해당 기능을 활성화하고 구성해야 합니다. 또한 기능을 사용할 사용자에게 LOM 권한을 명시적으로 부여해야 합니다.

각 어플라이언스의 로컬 웹 인터페이스를 사용하여 어플라이언스별로 LOM 및 LOM 사용자를 구성합니다. 즉, 방어 센터를 사용하여 관리되는 디바이스에서 LOM을 구성할 수 없습니다. 마찬가지로, 사용자는 어플라이언스별로 독립적으로 관리되므로 방어 센터에서 LOM 지원 사용자를 생성할 경우 해당 기능이 관리되는 디바이스의 사용자로 전달되지 않습니다.

또한 LOM 사용자에는 다음과 같은 제한이 있습니다.

- 사용자에게 관리자 역할을 할당해야 합니다.
- 사용자 이름은 최대 16자의 영숫자로 지정할 수 있습니다. LOM 사용자는 16자보다 긴 사용자 이름과 하이픈을 사용할 수 없습니다.
- 비밀번호는 최대 20자의 영숫자로 지정할 수 있습니다. LOM 사용자는 20자보다 긴 비밀번호를 사용할 수 없습니다. 사용자의 LOM 비밀번호는 해당 사용자의 시스템 비밀번호와 동일합니다.
- Series 3 방어 센터 및 8000 Series 디바이스에는 최대 13명의 LOM 사용자가 있을 수 있습니다. 7000 Series 디바이스는 최대 8명의 LOM 사용자를 지원합니다.

정보 다음 작업에 대한 자세한 지침은 *FireSIGHT System 사용 설명서*에서 어플라이언스 설정 구성 장을 참조하십시오.

LOM을 활성화하려면 다음을 수행합니다.

액세스: Admin

단계 1 **System(시스템 선택) > Local(로컬) > Configuration(컨피그레이션)**을 선택한 다음 **Console Configuration(콘솔 컨피그레이션)**을 클릭합니다.

단계 2 다음 단계는 어플라이언스 모델에 따라 다릅니다.

- 방어 센터 및 8000 Series 디바이스에서 LOM을 활성화하려면 LOM IP 주소, 넷마스크, 기본 게이트웨이를 지정하기 전에 **Physical Serial Port(물리적 시리얼 포트)**를 사용하여 원격 접속을 활성화해야 합니다(또는 DHCP를 사용하여 이러한 값을 자동으로 할당).
- 7000 Series 디바이스에서 **Lights Out Management**를 선택하여 LOM 설정을 구성합니다. 7000 Series 디바이스는 LOM과 물리적 시리얼 액세스를 동시에 지원하지 않습니다.

참고 LOM IP 주소는 어플라이언스의 관리 인터페이스 IP 주소와 달라야 합니다.

FireSIGHT System 사용자의 LOM 기능을 활성화하려면 다음을 수행합니다.

액세스: Admin

단계 1 **System(시스템) > Local(로컬) > User Management(사용자 관리)**를 선택한 다음 기존 사용자를 편집하여 LOM 권한을 추가하거나 어플라이언스에 대한 LOM 액세스에 사용할 새 사용자를 만듭니다.

단계 2 관리자 역할이 아직 활성화되지 않은 경우 User Configuration(사용자 컨피그레이션) 페이지에서 **Administrator(관리자)** 역할을 활성화합니다.

단계 3 **Allow Lights-Out Management Access(LOM 액세스 허용)** 확인란을 활성화하고 변경 사항을 저장합니다.

IPMI 유틸리티 설치

컴퓨터에서 서드파티 IPMI 유틸리티를 사용하여 어플라이언스에 대한 SOL 연결을 생성합니다.

컴퓨터에서 Linux 또는 Mac OS를 실행하는 경우 IPMItool을 사용합니다. 대부분의 Linux 배포에서는 IPMItool이 기본적으로 탑재되어 있지만 Mac에서는 IPMItool을 설치해야 합니다. 먼저 Mac에 Apple의 xCode 개발자 툴 패키지가 설치되어 있는지 확인합니다. 또한 명령행 개발을 위한 선택적 구성 요소가 설치되었는지 확인합니다(새 버전의 경우 "UNIX 개발" 및 "시스템 툴", 이전 버전의 경우 "명령행 지원"). 마지막으로 MacPorts와 IPMItool을 설치합니다. 자세한 내용은 선호하는 검색 엔진을 사용하거나 다음 사이트를 참조하십시오.

```
https://developer.apple.com/technologies/tools/
http://www.macports.org/
```

Windows 환경의 경우 직접 컴파일해야 하는 ipmiutil을 사용합니다. 컴파일러에 액세스할 수 없는 경우 ipmiutil 자체를 사용하여 컴파일할 수 있습니다. 자세한 내용은 선호하는 검색 엔진을 사용하거나 다음 사이트를 참조하십시오.

```
http://ipmiutil.sourceforge.net/
```

FirePOWER 디바이스의 전력 요구 사항

다음 섹션에서는 FirePOWER 디바이스의 전원 요구 사항과 관련 정보에 대해 설명합니다.

참고 ASA FirePOWER 디바이스의 전원 요구 사항은 ASA 설명서를 참조하십시오.

경고 및 주의 사항

이 설명서에는 경고 및 주의 사항이 포함되어 있습니다. 경고는 안전과 관련되어 있습니다. 다음 경고를 따르지 않으면 부상 또는 장비 손상이 발생할 수 있습니다. 주의 사항은 올바른 작동을 위한 요구 사항입니다. 주의 사항을 준수하지 않으면 올바르게 작동하지 않을 수 있습니다.

주의 장비 또는 부속품의 빌딩 내 포트는 건물 내 연결, 노출된 배선 또는 케이블링에만 적합합니다. 장비 또는 부속품의 건물 내 포트는 OSP(Outside the Plant) 또는 해당 배선에 연결하는 인터페이스에 금속을 이용하여 연결하지 **않아야** 합니다. 이러한 인터페이스는 건물 내 인터페이스에만 사용하도록 설계되었으며(GR1089-CORE 4호에 설명된 Type 2 또는 Type 4 포트) 노출된 OSP 케이블링과 격리되어야 합니다. 기본 보호기를 추가하더라도 금속을 이용한 이러한 인터페이스의 OSP 배선 연결이 충분히 보호되지 않습니다.

정전기 관리

주의 어플라이언스 포장을 풀고 설치 또는 이동하기 전에 접지된 손목끈 및 ESD 작업 표면과 같은 정전기 관리 절차가 마련되어 있어야 합니다. 과도한 정전기는 어플라이언스를 손상시키거나 의도하지 않은 작동을 유발할 수 있습니다.

70xx 제품군 어플라이언스

이 섹션에서는 다음과 같은 Cisco 디바이스의 전원 요구 사항에 대해 설명합니다.

- 3D7010, 3D7020, 3D7030(CHRY-1U-AC)
- 3D7050(NEME-1U-AC)

이러한 Cisco 디바이스는 National Electric Code가 적용되는 네트워크 통신 설비 및 위치에서 자격을 갖춘 담당자가 설치해야 합니다. 각 디바이스는 AC 어플라이언스로만 사용할 수 있습니다.

Cisco에서는 반품이 필요할 경우에 대비하여 포장재를 보관해 두도록 권장합니다.

자세한 내용은 다음 섹션을 참조하십시오.

- 회로 설치, 전압, 전류, 주파수 범위 및 전원 코드에 대한 자세한 내용은 설치, A-2페이지를 참조하십시오.
- 본딩 위치, 권장되는 터미널 및 접지 배선 요구 사항은 접지 요구 사항, A-3페이지를 참조하십시오.

설치

FireSIGHT System 어플라이언스는 NFPA 70 NEC(National Electric Code) 핸드북의 250조 및 현지 전기 관련 규정 요구 사항에 따라 설치해야 합니다.

어플라이언스는 단일 전원 공급 장치를 사용합니다. FireSIGHT System이 설치될 네트워크 장비의 입력 부분에 외장 서지 보호 디바이스를 사용해야 합니다.

회로는 어플라이언스의 최대 정격에 맞아야 합니다.

전압

전원 공급 장치는 100VAC~240VAC 공칭 범위(90VAC~264VAC 최대 범위)에서 작동합니다. 이 범위를 초과하는 전압을 사용할 경우 어플라이언스가 손상될 수 있습니다.

전류

레이블에 표기된 정격 전류는 전체 범위에서 최대 2A입니다. 화재 위험을 줄이려면 적절한 배선 및 차단기를 사용해야 합니다.

주파수 범위

AC 전원 공급 장치의 주파수 범위는 47Hz~63Hz입니다. 이 범위 밖의 주파수에서는 어플라이언스가 작동하지 않거나 올바르게 작동하지 않을 수 있습니다.

전원 코드

전원 공급 장치는 IEC C14 커넥터를 사용하여 전원을 연결하며 IEC C13 커넥터를 지원합니다. UL 인식 전원 코드를 사용해야 합니다. 최소 배선 게이지는 16AWG입니다. 어플라이언스에 기본 제공되는 코드는 NEMA 515P 플러그가 포함된 16AWG, UL 인식 코드입니다. 다른 전원 코드에 대한 자세한 내용은 공장에 문의하십시오.

참고 전원 공급 장치의 코드를 절단하지 **마십시오**.

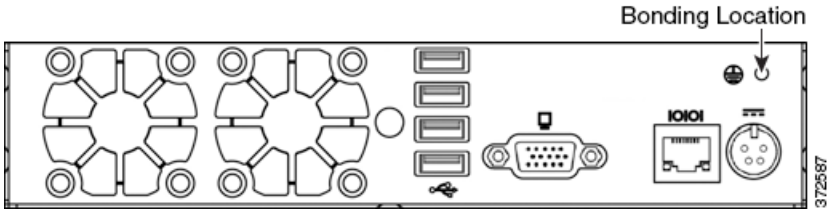
접지 요구 사항

어플라이언스를 공통 본딩 네트워크에 접지해야 합니다.

본딩 위치

접지 본딩 위치는 섀시의 후면에 있습니다. M4 스터드가 제공됩니다. 링 터미널을 연결할 수 있는 외부 톱니형 와셔가 제공됩니다. 각 스터드에서 표준 접지 기호를 사용할 수 있습니다.

다음 그림은 섀시의 본딩 위치를 나타냅니다.



권장되는 터미널

접지 연결에는 UL 승인 터미널을 사용해야 합니다. #6(M3.5) 스터드용 클리어런스 홀이 포함된 링 터미널을 사용할 수 있습니다. 16AWG 전선의 경우 AMP/Tyco 36151이 권장됩니다. 이는 #6 스터드용 홀이 포함된 UL 승인 링 터미널입니다.

접지 배선 요구 사항

접지 배선은 단일 장애 발생 시 회로의 전류를 처리하는 데 충분한 규격이어야 합니다. 접지 배선의 크기는 회로를 보호하는 데 사용되는 차단기의 전류와 동일해야 합니다. 전류, A-2페이지를 참조하십시오.

베어 전도체는 크림프 연결 전 산화방지제로 코팅해야 합니다. 구리 케이블만 접지 용도로 사용할 수 있습니다.

71xx 제품군 어플라이언스

이 섹션에서는 다음과 같은 Cisco 디바이스의 전원 요구 사항에 대해 설명합니다.

- 3D7110 및 3D7120(GERY-1U-8-AC)
- 3D7115 및 3D7125(GERY-1U-4C8S-AC)

이러한 Cisco 디바이스는 National Electric Code가 적용되는 네트워크 통신 설비 및 위치에서 자격을 갖춘 담당자가 설치해야 합니다. 각 디바이스는 AC 어플라이언스로만 사용할 수 있습니다.

Cisco에서는 반품이 필요할 경우에 대비하여 포장재를 보관해 두도록 권장합니다.

자세한 내용은 다음 섹션을 참조하십시오.

- 회로 설치, 전압, 전류, 주파수 범위 및 전원 코드 정보는 설치, A-4페이지를 참조하십시오.
- 본딩 위치, 권장되는 터미널 및 접지 배선 요구 사항은 접지 요구 사항, A-5페이지를 참조하십시오.

설치

FireSIGHT System은 NFPA 70 NEC(National Electric Code) 핸드북의 250조 및 현지 전기 관련 규정 요구 사항에 따라 설치해야 합니다.

예비 전원을 생성하려면 별도의 회로가 필요합니다. 입력 라인 전원 결함으로 인한 전력 상태 문제 또는 전력 손실을 방지하려면 무정전 또는 배터리 백업 전원을 사용합니다.

각 전원 공급 장치에 전체 어플라이언스를 실행할 수 있는 충분한 전력을 공급합니다. 각 공급 장치의 정격 전압 및 전류는 어플라이언스 레이블에 표기되어 있습니다.

FireSIGHT System이 설치될 네트워크 장비의 입력 부분에 외장 서지 보호 디바이스를 사용합니다.

별도의 회로 설치

별도의 회로가 사용되는 경우 각 회로는 어플라이언스의 최대 정격에 맞아야 합니다. 이 컨피그레이션을 통해 회로 장애 및 전원 공급 장치 장애에 대비할 수 있습니다.

예: 각 공급 장치가 다른 220V 회로에 연결됩니다. 각 회로는 레이블에 명시된 대로 5A를 공급할 수 있어야 합니다.

동일한 회로 설치

동일한 회로를 사용하여 두 공급 장치 모두에 전원을 공급하는 경우 한 공급 장치의 정격 전력이 전체 박스에 적용됩니다. 이 컨피그레이션은 전원 공급 장치 장애만 보호합니다.

예: 두 공급 장치가 동일한 220V 회로에 연결됩니다. 이 회로의 최대 전류는 레이블에 명시된 대로 5A입니다.

전압

전원 공급 장치는 100VAC~240VAC 공칭 범위(85VAC~264VAC 최대 범위) 전압에서 작동합니다. 이 범위를 초과하는 전압을 사용할 경우 어플라이언스가 손상될 수 있습니다.

전류

각 공급 장치의 레이블에 표기된 정격 전류는 전체 범위에서 공급 장치당 최대 10A, 187VAC~264VAC의 경우 공급 장치당 최대 5A입니다. 화재 위험을 줄이려면 적절한 배선 및 차단기를 사용해야 합니다.

주파수 범위

AC 전원 공급 장치의 주파수 범위는 47Hz~63Hz입니다. 이 범위 밖의 주파수에서는 어플라이언스가 작동하지 않거나 올바르게 작동하지 않을 수 있습니다.

전원 코드

전원 공급 장치는 IEC C14 커넥터로 전원을 연결하며 IEC C13 커넥터를 사용할 수 있습니다. UL 인식 전원 코드를 사용해야 합니다. 최소 배선 게이지는 16AWG입니다. 어플라이언스에 기본 제공되는 코드는 NEMA 515P 플러그가 포함된 16AWG, UL 인식 코드입니다. 다른 전원 코드에 대한 자세한 내용은 공장에 문의하십시오.

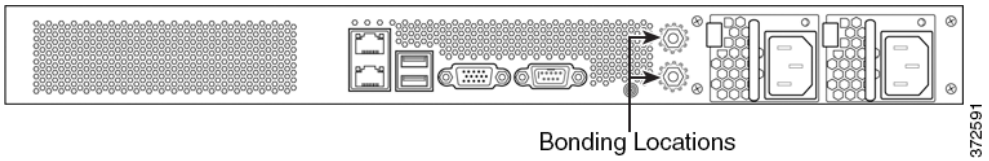
접지 요구 사항

FireSIGHT System을 공통 본딩 네트워크에 접지해야 합니다.

본딩 위치

접지 본딩 위치는 섀시의 후면에 있습니다. M4 스터드가 제공됩니다. 링 터미널을 연결할 수 있는 외부 톱니형 와셔가 제공됩니다. 각 스터드에서 표준 접지 기호를 사용할 수 있습니다.

다음 그림은 섀시의 본딩 위치를 나타냅니다.



권장되는 터미널

접지 연결에는 UL 승인 터미널을 사용해야 합니다. 4mm 또는 #8 스터드용 클리어런스 홀이 포함된 링 터미널을 사용할 수 있습니다. 10~12AWG 전선의 경우 Tyco 34853이 권장됩니다. 이는 #8 스터드용 홀이 포함된 UL 승인 링 터미널입니다.

접지 배선 요구 사항

접지 배선은 단일 장애 발생 시 회로의 전류를 처리하는 데 충분한 규격이어야 합니다. 접지 배선의 크기는 회로를 보호하는 데 사용되는 차단기의 전류와 동일해야 합니다. 전류, A-4페이지를 참조하십시오.

베어 전도체는 크림프 연결 전 산화방지제로 코팅해야 합니다. 구리 케이블만 접지 용도로 사용할 수 있습니다.

81xx 제품군 어플라이언스

이 섹션에서는 다음과 같은 Cisco 디바이스의 전원 요구 사항에 대해 설명합니다.

- 3D8120, 3D8130 및 3D8140(CHAS-1U-AC, CHAS-1U-DC 또는 CHAS-1U-AC/DC)

이러한 Cisco 디바이스는 National Electric Code가 적용되는 네트워크 통신 설비 및 위치에서 자격을 갖춘 담당자가 설치해야 합니다.

Cisco에서는 반품이 필요할 경우에 대비하여 포장재를 보관해 두도록 권장합니다.

자세한 내용은 다음 섹션을 참조하십시오.

- 회로 설치, 전압, 전류, 주파수 범위 및 전원 코드 정보는 AC 설치, A-6페이지를 참조하십시오.
- 회로 설치, 전압, 전류, 접지 기준, 터미널, 차단기 요구 사항 및 최소 배선 규격은 DC 설치, A-7페이지를 참조하십시오.
- 본딩 위치, 권장되는 터미널, 접지 배선 요구 사항 및 DC 공급 장치는 접지 요구 사항, A-8페이지를 참조하십시오.

AC 설치

FireSIGHT System은 NFPA 70 NEC(National Electric Code) 핸드북의 250조 및 현지 전기 관련 규정 요구 사항에 따라 설치해야 합니다.

주의 DC 전원을 AC 공급 장치에 연결하지 **마십시오**.

예비 전원을 생성하려면 별도의 회로가 필요합니다. 입력 라인 전원 결함으로 인한 전력 상태 문제 또는 전력 손실을 방지하려면 무정전 또는 배터리 백업 전원을 사용합니다.

각 전원 공급 장치에 전체 어플라이언스를 실행할 수 있는 충분한 전력을 공급합니다. 각 공급 장치의 정격 전압 및 전류는 어플라이언스 레이블에 표기되어 있습니다.

FireSIGHT System이 설치될 네트워크 장비의 입력 부분에 외장 서지 보호 디바이스를 사용합니다.

별도의 회로 설치

별도의 회로가 사용되는 경우 각 회로는 어플라이언스의 최대 정격에 맞아야 합니다. 이 컨피그레이션을 통해 회로 장애 및 전원 공급 장치 장애에 대비할 수 있습니다.

예: 각 공급 장치가 다른 220V 회로에 연결됩니다. 각 회로는 레이블에 명시된 대로 5A를 공급할 수 있어야 합니다.

동일한 회로 설치

동일한 회로를 사용하여 두 공급 장치 모두에 전원을 공급하는 경우 한 공급 장치의 정격 전력이 전체 박스에 적용됩니다. 이 컨피그레이션은 전원 공급 장치 장애만 보호합니다.

예: 두 공급 장치가 동일한 220V 회로에 연결됩니다. 이 회로의 최대 전류는 레이블에 명시된 대로 5A입니다.

AC 전압

전원 공급 장치는 100VAC~240VAC 공칭 범위(85VAC~264VAC 최대 범위) 전압에서 작동합니다. 이 범위를 초과하는 전압을 사용할 경우 어플라이언스가 손상될 수 있습니다.

AC 전류

각 공급 장치의 레이블에 표기된 정격 전류는 전체 범위에서 공급 장치당 최대 5.2A, 187VAC~264VAC의 경우 공급 장치당 최대 2.6A입니다. 화재 위험을 줄이려면 적절한 배선 및 차단기를 사용해야 합니다.

주파수 범위

AC 전원 공급 장치의 주파수 범위는 47Hz~63Hz입니다. 이 범위 밖의 주파수에서는 어플라이언스가 작동하지 않거나 올바르게 작동하지 않을 수 있습니다.

전원 코드

전원 공급 장치는 IEC C14 커넥터로 전원을 연결하며 IEC C13 커넥터를 사용할 수 있습니다. UL 인식 전원 코드를 사용해야 합니다. 최소 배선 게이지는 16AWG입니다. 어플라이언스에 기본 제공되는 코드는 NEMA 515P 플러그가 포함된 16AWG, UL 인식 코드입니다. 다른 전원 코드에 대한 자세한 내용은 공장에 문의하십시오.

DC 설치

예비 전원을 생성하려면 별도의 회로가 필요합니다. 입력 라인 전원 결함으로 인한 전력 상태 문제 또는 전력 손실을 방지하려면 무정전 또는 배터리 백업 전원을 사용합니다.

⚠

주의 AC 전력을 DC 공급 장치에 연결하지 **마십시오**.

각 전원 공급 장치에 전체 어플라이언스를 실행할 수 있는 충분한 전력을 공급합니다. 각 공급 장치의 정격 전압 및 전류는 어플라이언스 레이블에 표기되어 있습니다.

FireSIGHT System이 설치될 네트워크 장비의 입력 부분에 외장 서지 보호 디바이스를 사용합니다.

별도의 회로 설치

별도의 회로가 사용되는 경우 각 회로는 어플라이언스의 최대 정격에 맞아야 합니다. 이 컨피그레이션을 통해 회로 장애 및 전원 공급 장치 장애에 대비할 수 있습니다.

예: 각 공급 장치가 다른 -48VDC 회로에 연결됩니다. 각 회로는 레이블에 명시된 대로 20A를 공급할 수 있어야 합니다.

동일한 회로 설치

동일한 회로를 사용하여 두 공급 장치 모두에 전원을 공급하는 경우 한 공급 장치의 정격 전력이 전체 박스에 적용됩니다. 이 컨피그레이션은 전원 공급 장치 장애만 보호합니다.

예: 두 공급 장치가 동일한 -48VDC 회로에 연결됩니다. 이 회로의 최대 전류는 레이블에 명시된 대로 20A입니다.

⚠

주의 이러한 최적화를 사용하려면 전원 코드가 각 공급 장치의 최대 정격에 맞아야 합니다.

DC 전압

전원 공급 장치는 다음과 같은 전압에서 작동합니다.

- RTN 기준 공칭 -48VDC
- -40VDC~최대 -72VDC

이 범위를 초과하는 전압을 사용할 경우 어플라이언스가 손상될 수 있습니다.

DC 전류

공급 장치당 최대 11A

접지 기준

DC 전원 공급 장치는 접기 기준에서 완전히 격리되어 있습니다.

권장되는 터미널

나사 터미널을 통해 DC 공급 장치에 전원을 연결합니다. UL 승인 터미널이어야 합니다. 터미널에는 M4 또는 #8 나사를 지원하는 홀이 있어야 합니다. 터미널의 최대 너비는 8.1mm(0.320인치)입니다. 10~12게이지 전선의 대표 스페이드 터미널은 Tyco 325197입니다.

차단기 요구 사항

정격 전압에서 정격 전류를 전달하는 데 충분한 차단기를 제공해야 합니다. 자동 차단기는 다음 요구 사항을 충족해야 합니다.

- UL 인식
- CSA 승인(권장)
- VDE 승인(권장)
- 최대 부하(20A) 지원
- 설치 전압(전원 공급 장치의 요구 사항에 따라 -40V~-72VDC) 지원
- DC 용도

권장하는 차단기는 Airpax IELK1-1-72-20.0-01-V입니다. 사용되는 터미널 옵션은 설치에 따라 다릅니다. 이 차단기는 단일 폴이며 80V DC 정격의 20A 차단기입니다. *지연이 긴* 제품으로 나열되어 있습니다. 이 차단기에 대한 정보는 http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf에서 확인할 수 있습니다.

최소 배선 규격 요구 사항

레이스웨이당 3개 전선(1개 회로)이 포함된 전원 피드에는 12AWG 전선을 사용할 수 있습니다. 레이스웨이당 회로가 2개 이상인 전력 피드에는 10AWG 전선을 사용해야 합니다. 예비 전원 공급 장치에 대한 2개의 개별 피드는 2개 회로이며 10AWG 전선을 사용해야 합니다.

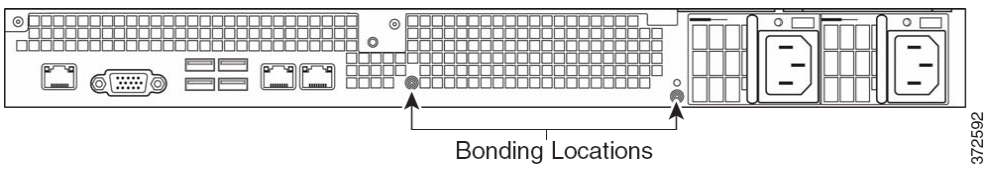
접지 요구 사항

FireSIGHT System을 공통 본딩 네트워크에 접지해야 합니다.

본딩 위치

접지 본딩 위치는 섀시의 후면에 있습니다. M4 스터드가 제공됩니다. 링 터미널을 연결할 수 있는 외부 톱니형 와셔가 제공됩니다. 각 스터드에서 표준 접지 기호를 사용할 수 있습니다.

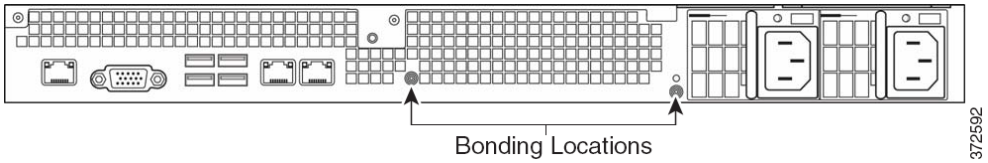
다음 그림은 1U 섀시의 본딩 위치를 나타냅니다.



권장되는 터미널

접지 연결에는 UL 승인 터미널을 사용해야 합니다. 4mm 또는 #8 스터드용 클리어런스 홀이 포함된 링 터미널을 사용할 수 있습니다. 10~12AWG 전선의 경우 Tyco 34853이 권장됩니다. 이는 #8 스터드용 홀이 포함된 UL 승인 링 터미널입니다.

접지 배선 요구 사항



접지 배선은 단일 장애 발생 시 회로의 전류를 처리하는 데 충분한 규격이어야 합니다. 접지 배선의 크기는 회로를 보호하는 데 사용되는 차단기의 전류와 동일해야 합니다. AC 회로에 대한 자세한 내용은 AC 전류, A-6페이지를 참조하십시오. DC 회로에 대한 자세한 내용은 DC 전류, A-7페이지를 참조하십시오.

베어 전도체는 크림프 연결 전 산화방지제로 코팅해야 합니다. 구리 케이블만 접지 용도로 사용할 수 있습니다.

DC 공급 장치

DC 전원 공급 장치에는 각 공급 장치당 추가 접지 연결이 있습니다. 따라서 전원, 리턴, 접지에 운영 중 교체 가능한 공급 장치를 연결하여 안전하게 삽입할 수 있습니다. 이 접지 러그를 반드시 연결해야 합니다.

외부 톱니형 와셔 나사가 포함된 M4 나사입니다.

접지 배선의 규격은 회로의 차단기와 일치해야 합니다.

82xx 제품군 어플라이언스

이 섹션에서는 다음과 같은 Cisco 디바이스의 전원 요구 사항에 대해 설명합니다.

- 3D8250, 3D8260, 3D8270 및 3D8290(CHAS-2U-AC, CHAS-2U-DC 또는 CHAS-2U-AC/DC)

이러한 Cisco 디바이스는 National Electric Code가 적용되는 네트워크 통신 설비 및 위치에서 자격을 갖춘 담당자가 설치해야 합니다.

Cisco에서는 반품이 필요할 경우에 대비하여 포장재를 보관해 두도록 권장합니다.

자세한 내용은 다음 섹션을 참조하십시오.

- 회로 설치, 전압, 전류, 주파수 범위 및 전원 코드 정보는 AC 설치, A-10페이지를 참조하십시오.
- 회로 설치, 전압, 전류, 접지 기준, 터미널, 차단기 요구 사항 및 최소 배선 규격은 DC 설치, A-11페이지를 참조하십시오.
- 본딩 위치, 권장되는 터미널, 접지 배선 요구 사항 및 DC 공급 장치는 접지 요구 사항, A-12페이지를 참조하십시오.

AC 설치

FireSIGHT System은 NFPA 70 NEC(National Electric Code) 핸드북의 250조 및 현지 전기 관련 규정 요구 사항에 따라 설치해야 합니다.

주의 DC 전원을 AC 공급 장치에 연결하지 **마십시오**.

예비 전원을 생성하려면 별도의 회로가 필요합니다. 입력 라인 전원 결함으로 인한 전력 상태 문제 또는 전력 손실을 방지하려면 무정전 또는 배터리 백업 전원을 사용합니다.

각 전원 공급 장치에 전체 어플라이언스를 실행할 수 있는 충분한 전력을 공급합니다. 각 공급 장치의 정격 전압 및 전류는 어플라이언스 레이블에 표기되어 있습니다.

FireSIGHT System이 설치될 네트워크 장비의 입력 부분에 외장 서지 보호 디바이스를 사용합니다.

별도의 회로 설치

별도의 회로가 사용되는 경우 각 회로는 어플라이언스의 최대 정격에 맞아야 합니다. 이 컨피그레이션을 통해 회로 장애 및 전원 공급 장치 장애에 대비할 수 있습니다.

예: 각 공급 장치가 다른 220V 회로에 연결됩니다. 각 회로는 레이블에 명시된 대로 5A를 공급할 수 있어야 합니다.

동일한 회로 설치

동일한 회로를 사용하여 두 공급 장치 모두에 전원을 공급하는 경우 한 공급 장치의 정격 전력이 전체 박스에 적용됩니다. 이 컨피그레이션은 전원 공급 장치 장애만 보호합니다.

예: 두 공급 장치가 동일한 220V 회로에 연결됩니다. 이 회로의 최대 전류는 레이블에 명시된 대로 5A입니다.

AC 전압

전원 공급 장치는 100VAC~240VAC 공칭 범위(85VAC~264VAC 최대 범위) 전압에서 작동합니다. 이 범위를 초과하는 전압을 사용할 경우 어플라이언스가 손상될 수 있습니다.

AC 전류

각 공급 장치의 레이블에 표기된 정격 전류는 전체 범위에서 공급 장치당 최대 8A,
187VAC~264VAC의 경우 공급 장치당 최대 4A입니다. 화재 위험을 줄이려면 적절한 배선 및 차단기를 사용해야 합니다.

주파수 범위

AC 전원 공급 장치의 주파수 범위는 47Hz~63Hz입니다. 이 범위 밖의 주파수에서는 어플라이언스가 작동하지 않거나 올바르게 작동하지 않을 수 있습니다.

전원 코드

전원 공급 장치는 IEC C14 커넥터로 전원을 연결하며 IEC C13 커넥터를 사용할 수 있습니다. UL 인식 전원 코드를 사용해야 합니다. 최소 배선 게이지는 16AWG입니다. 어플라이언스에 기본 제공되는 코드는 NEMA 515P 플러그가 포함된 16AWG, UL 인식 코드입니다. 다른 전원 코드에 대한 자세한 내용은 공장에 문의하십시오.

DC 설치

예비 전원을 생성하려면 별도의 회로가 필요합니다. 입력 라인 전원 결함으로 인한 전력 상태 문제 또는 전력 손실을 방지하려면 무정전 또는 배터리 백업 전원을 사용합니다.

⚠
주의 AC 전력을 DC 공급 장치에 연결하지 **마십시오**.

각 전원 공급 장치에 전체 어플라이언스를 실행할 수 있는 충분한 전력을 공급합니다. 각 공급 장치의 정격 전압 및 전류는 어플라이언스 레이블에 표기되어 있습니다.

FireSIGHT System이 설치될 네트워크 장비의 입력 부분에 외장 서지 보호 디바이스를 사용합니다.

별도의 회로 설치

별도의 회로가 사용되는 경우 각 회로는 어플라이언스의 최대 정격에 맞아야 합니다. 이 컨피그레이션을 통해 회로 장애 및 전원 공급 장치 장애에 대비할 수 있습니다.

예: 각 공급 장치가 다른 -48VDC 회로에 연결됩니다. 각 회로는 레이블에 명시된 대로 20A를 공급할 수 있어야 합니다.

동일한 회로 설치

동일한 회로를 사용하여 두 공급 장치 모두에 전원을 공급하는 경우 한 공급 장치의 정격 전력이 전체 박스에 적용됩니다. 이 컨피그레이션은 전원 공급 장치 장애만 보호합니다.

예: 두 공급 장치가 동일한 -48VDC 회로에 연결됩니다. 이 회로의 최대 전류는 레이블에 명시된 대로 20A입니다.

⚠
주의 이러한 최적화를 사용하려면 전원 코드가 각 공급 장치의 최대 정격에 맞아야 합니다.

DC 전압

전원 공급 장치는 다음과 같은 전압에서 작동합니다.

- RTN 기준 공칭 -48VDC
- -40VDC~최대 -72VDC

이 범위를 초과하는 전압을 사용할 경우 어플라이언스가 손상될 수 있습니다.

DC 전류

공급 장치당 최대 18A

접지 기준

DC 전원 공급 장치는 접기 기준에서 완전히 격리되어 있습니다.

권장되는 터미널

나사 터미널을 통해 DC 공급 장치에 전원을 연결합니다. UL 승인 터미널이어야 합니다. 터미널에는 M4 또는 #8 나사를 지원하는 홀이 있어야 합니다. 터미널의 최대 너비는 8.1mm(0.320인치)입니다. 10~12게이지 전선의 대표 스페이드 터미널은 Tyco 325197입니다.

차단기 요구 사항

정격 전압에서 정격 전류를 전달하는 데 충분한 차단기를 제공해야 합니다. 자동 차단기는 다음 요구 사항을 충족해야 합니다.

- UL 인식
- CSA 승인(권장)
- VDE 승인(권장)
- 최대 부하(20A) 지원
- 설치 전압(전원 공급 장치의 요구 사항에 따라 -40V~-72VDC) 지원
- DC 용도

권장하는 차단기는 Airpax IELK1-1-72-20.0-01-V입니다. 사용되는 터미널 옵션은 설치에 따라 다릅니다. 이 차단기는 단일 폴이며 80V DC 정격의 20A 차단기입니다. *지연이 긴* 제품으로 나열되어 있습니다. 이 차단기에 대한 정보는 http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf에서 확인할 수 있습니다.

최소 배선 규격 요구 사항

레이스웨이당 3개 전선(1개 회로)이 포함된 전원 피드에는 12AWG 전선을 사용할 수 있습니다. 레이스웨이당 회로가 2개 이상인 전력 피드에는 10AWG 전선을 사용해야 합니다. 예비 전원 공급 장치에 대한 2개의 개별 피드는 2개 회로이며 10AWG 전선을 사용해야 합니다.

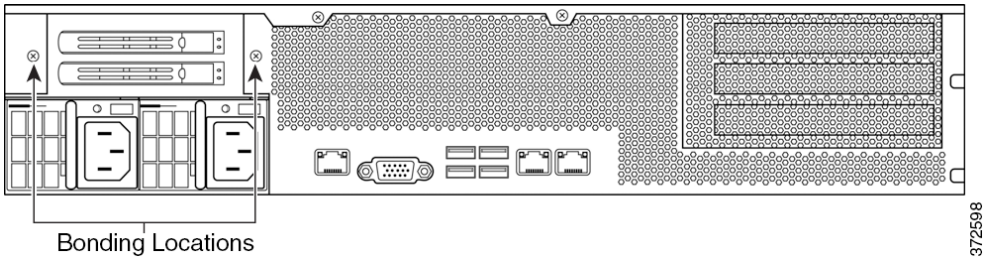
접지 요구 사항

FireSIGHT System을 공통 본딩 네트워크에 접지해야 합니다.

본딩 위치

접지 본딩 위치는 섀시의 후면에 있습니다. M4 스터드가 제공됩니다. 링 터미널을 연결할 수 있는 외부 톱니형 와셔가 제공됩니다. 각 스터드에서 표준 접지 기호를 사용할 수 있습니다.

다음 그림은 2U 섀시의 본딩 위치를 나타냅니다.



권장되는 터미널

접지 연결에는 UL 승인 터미널을 사용해야 합니다. 4mm 또는 #8 스터드용 클리어런스 홀이 포함된 링 터미널을 사용할 수 있습니다. 10~12AWG 전선의 경우 Tyco 34853이 권장됩니다. 이는 #8 스터드용 홀이 포함된 UL 승인 링 터미널입니다.

접지 배선 요구 사항

접지 배선은 단일 장애 발생 시 회로의 전류를 처리하는 데 충분한 규격이어야 합니다. 접지 배선의 크기는 회로를 보호하는 데 사용되는 차단기의 전류와 동일해야 합니다. AC 회로에 대한 자세한 내용은 AC 전류, A-6페이지를 참조하십시오. DC 회로에 대한 자세한 내용은 DC 전류, A-7페이지를 참조하십시오.

베어 전도체는 크림프 연결 전 산화방지제로 코팅해야 합니다. 구리 케이블만 접지 용도로 사용할 수 있습니다.

DC 공급 장치

DC 전원 공급 장치에는 각 공급 장치당 추가 접지 연결이 있습니다. 따라서 전원, 리턴, 접지에 운영 중 교체 가능한 공급 장치를 연결하여 안전하게 삽입할 수 있습니다. 이 접지 러그를 반드시 연결해야 합니다.

외부 톱니형 와셔 나사가 포함된 M4 나사입니다.

접지 배선의 규격은 회로의 차단기와 일치해야 합니다.

83xx 제품군 어플라이언스

이 섹션에서는 다음과 같은 Cisco 디바이스의 전원 요구 사항에 대해 설명합니다.

- 3D8350, 3D8360, 3D8370 및 3D8390(PG35-2U-AC/DC)

이러한 Cisco 디바이스는 National Electric Code가 적용되는 네트워크 통신 설비 및 위치에서 자격을 갖춘 담당자가 설치해야 합니다.

Cisco에서는 반품이 필요할 경우에 대비하여 포장재를 보관해 두도록 권장합니다.

자세한 내용은 다음 섹션을 참조하십시오.

- 회로 설치, 전압, 전류, 주파수 범위 및 전원 코드 정보는 AC 설치, A-14페이지를 참조하십시오.
- 회로 설치, 전압, 전류, 접지 기준, 터미널, 차단기 요구 사항 및 최소 배선 규격은 DC 설치, A-15페이지를 참조하십시오.
- 본딩 위치, 권장되는 터미널, 접지 배선 요구 사항 및 DC 공급 장치는 접지 요구 사항, A-16페이지를 참조하십시오.

AC 설치

FireSIGHT System은 NFPA 70 NEC(National Electric Code) 핸드북의 250조 및 현지 전기 관련 규정 요구 사항에 따라 설치해야 합니다.

주의 DC 전원을 AC 공급 장치에 연결하지 **마십시오**.

예비 전원을 생성하려면 별도의 회로가 필요합니다. 입력 라인 전원 결함으로 인한 전력 상태 문제 또는 전력 손실을 방지하려면 무정전 또는 배터리 백업 전원을 사용합니다.

각 전원 공급 장치에 전체 어플라이언스를 실행할 수 있는 충분한 전력을 공급합니다. 각 공급 장치의 정격 전압 및 전류는 어플라이언스 레이블에 표기되어 있습니다.

FireSIGHT System이 설치될 네트워크 장비의 입력 부분에 외장 서지 보호 디바이스를 사용합니다.

별도의 회로 설치

별도의 회로가 사용되는 경우 각 회로는 어플라이언스의 최대 정격에 맞아야 합니다. 이 컨피그레이션을 통해 회로 장애 및 전원 공급 장치 장애에 대비할 수 있습니다.

예: 각 공급 장치가 다른 220V 회로에 연결됩니다. 각 회로는 레이블에 명시된 대로 10A를 공급할 수 있어야 합니다.

동일한 회로 설치

동일한 회로를 사용하여 두 공급 장치 모두에 전원을 공급하는 경우 한 공급 장치의 정격 전력이 전체 박스에 적용됩니다. 이 컨피그레이션은 전원 공급 장치 장애만 보호합니다.

예: 두 공급 장치가 동일한 220V 회로에 연결됩니다. 이 회로의 최대 전류는 레이블에 명시된 대로 10A입니다.

AC 전압

전원 공급 장치는 100VAC~240VAC 공칭 범위(85VAC~264VAC 최대 범위) 전압에서 작동합니다. 이 범위를 초과하는 전압을 사용할 경우 어플라이언스가 손상될 수 있습니다.

AC 전류

각 공급 장치의 레이블에 표기된 정격 전류는 전체 범위에서 공급 장치당 최대 11A, 187VAC~264VAC의 경우 공급 장치당 최대 5.5A입니다. 화재 위험을 줄이려면 적절한 배선 및 차단기를 사용해야 합니다.

주파수 범위

AC 전원 공급 장치의 주파수 범위는 47Hz~63Hz입니다. 이 범위 밖의 주파수에서는 어플라이언스가 작동하지 않거나 올바르게 작동하지 않을 수 있습니다.

전원 코드

전원 공급 장치는 IEC C14 커넥터로 전원을 연결하며 IEC C13 커넥터를 사용할 수 있습니다. UL 인식 전원 코드를 사용해야 합니다. 최소 배선 게이지는 16AWG입니다. 어플라이언스에 기본 제공되는 코드는 NEMA 515P 플러그가 포함된 16AWG, UL 인식 코드입니다. 다른 전원 코드에 대한 자세한 내용은 공장에 문의하십시오.

DC 설치

예비 전원을 생성하려면 별도의 회로가 필요합니다. 입력 라인 전원 결함으로 인한 전력 상태 문제 또는 전력 손실을 방지하려면 무정전 또는 배터리 백업 전원을 사용합니다.

⚠

주의 AC 전력을 DC 공급 장치에 연결하지 **마십시오**.

각 전원 공급 장치에 전체 어플라이언스를 실행할 수 있는 충분한 전력을 공급합니다. 각 공급 장치의 정격 전압 및 전류는 어플라이언스 레이블에 표기되어 있습니다.

FireSIGHT System이 설치될 네트워크 장비의 입력 부분에 외장 서지 보호 디바이스를 사용합니다.

별도의 회로 설치

별도의 회로가 사용되는 경우 각 회로는 어플라이언스의 최대 정격에 맞아야 합니다. 이 컨피그레이션을 통해 회로 장애 및 전원 공급 장치 장애에 대비할 수 있습니다.

예: 각 공급 장치가 다른 -48VDC 회로에 연결됩니다. 각 회로는 레이블에 명시된 대로 25A를 공급할 수 있어야 합니다.

동일한 회로 설치

동일한 회로를 사용하여 두 공급 장치 모두에 전원을 공급하는 경우 한 공급 장치의 정격 전력이 전체 박스에 적용됩니다. 이 컨피그레이션은 전원 공급 장치 장애만 보호합니다.

예: 두 공급 장치가 동일한 -48VDC 회로에 연결됩니다. 이 회로의 최대 전류는 레이블에 명시된 대로 25A입니다.

⚠

주의 이러한 최적화를 사용하려면 전원 코드가 각 공급 장치의 최대 정격에 맞아야 합니다.

DC 전압

전원 공급 장치는 다음과 같은 전압에서 작동합니다.

- RTN 기준 공칭 -48VDC
- -40VDC~최대 -72VDC

이 범위를 초과하는 전압을 사용할 경우 어플라이언스가 손상될 수 있습니다.

DC 전류

공급 장치당 최대 25A

접지 기준

DC 전원 공급 장치는 접기 기준에서 완전히 격리되어 있습니다.

권장되는 터미널

나사 터미널을 통해 DC 공급 장치에 전원을 연결합니다. UL 승인 터미널이어야 합니다. 터미널에는 M4 또는 #8 나사를 지원하는 홀이 있어야 합니다. 터미널의 최대 너비는 8.1mm(0.320인치)입니다. 10~12게이지 전선의 대표 스페이드 터미널은 Tyco 325197입니다.

차단기 요구 사항

정격 전압에서 정격 전류를 전달하는 데 충분한 차단기를 제공해야 합니다. 자동 차단기는 다음 요구 사항을 충족해야 합니다.

- UL 인식
- CSA 승인(권장)
- VDE 승인(권장)
- 최대 부하(20A) 지원
- 설치 전압(전원 공급 장치의 요구 사항에 따라 -40V~-72VDC) 지원
- DC 용도

권장하는 차단기는 Airpax IELK1-1-72-20.0-01-V입니다. 사용되는 터미널 옵션은 설치에 따라 다릅니다. 이 차단기는 단일 폴이며 80V DC 정격의 20A 차단기입니다. *지연이 긴* 제품으로 나열되어 있습니다. 이 차단기에 대한 정보는 http://www.airpax.net/site/utilities/eliterature/pdfs/ial.pdf에서 확인할 수 있습니다.

최소 배선 규격 요구 사항

레이스웨이당 3개 전선(1개 회로)이 포함된 전원 피드에는 12AWG 전선을 사용할 수 있습니다. 레이스웨이당 회로가 2개 이상인 전력 피드에는 10AWG 전선을 사용해야 합니다. 예비 전원 공급 장치에 대한 2개의 개별 피드는 2개 회로이며 10AWG 전선을 사용해야 합니다.

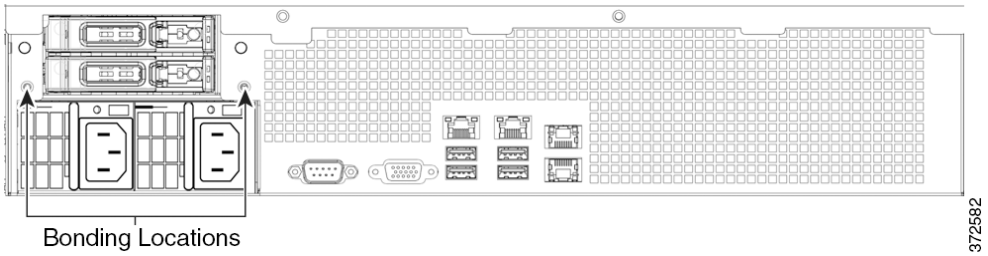
접지 요구 사항

FireSIGHT System을 공통 본딩 네트워크에 접지해야 합니다.

본딩 위치

접지 본딩 위치는 새시의 후면에 있습니다. M4 스터드가 제공됩니다. 링 터미널을 연결할 수 있는 외부 톱니형 와셔가 제공됩니다. 각 스터드에서 표준 접지 기호를 사용할 수 있습니다.

다음 그림은 83xx 제품군 2U 새시의 본딩 위치를 나타냅니다.



권장되는 터미널

접지 연결에는 UL 승인 터미널을 사용해야 합니다. 4mm 또는 #8 스터드용 클리어런스 홀이 포함된 링 터미널을 사용할 수 있습니다. 10~12AWG 전선의 경우 Tyco 34853이 권장됩니다. 이는 #8 스터드용 홀이 포함된 UL 승인 링 터미널입니다.

접지 배선 요구 사항

접지 배선은 단일 장애 발생 시 회로의 전류를 처리하는 데 충분한 규격이어야 합니다. 접지 배선의 크기는 회로를 보호하는 데 사용되는 차단기의 전류와 동일해야 합니다. AC 회로에 대한 자세한 내용은 AC 전류, A-14페이지를 참조하십시오. DC 회로에 대한 자세한 내용은 DC 전류, A-15페이지를 참조하십시오.

베어 전도체는 크림프 연결 전 산화방지제로 코팅해야 합니다. 구리 케이블만 접지 용도로 사용할 수 있습니다.

DC 공급 장치

DC 전원 공급 장치에는 각 공급 장치당 추가 접지 연결이 있습니다. 따라서 전원, 리턴, 접지에 운영 중 교체 가능한 공급 장치를 연결하여 안전하게 삽입할 수 있습니다. 이 접지 러그를 반드시 연결해야 합니다.

외부 톱니형 와셔 나사가 포함된 M4 나사입니다.

접지 배선의 규격은 회로의 차단기와 일치해야 합니다.

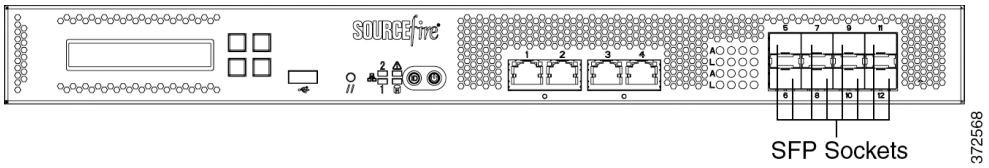
3D71x5 및 AMP7150 디바이스에서 SFP 트렌시버 사용

다음 섹션은 3D7115 및 3D7125(총칭하여 3D71x5), AMP7150에서의 SFP(Small Form-Factor Pluggable) 소켓 및 트렌시버 사용에 대한 자세한 정보를 제공합니다.

3D71x5 및 AMP7150 SFP 소켓 및 트렌시버

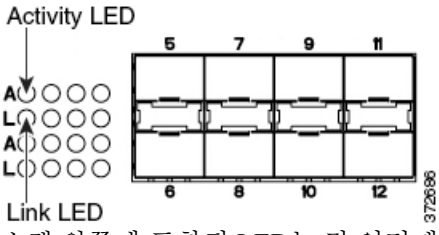
3D71x5 및 AMP7150 어플라이언스에는 8개의 SFP(Small Form-Factor Pluggable) 소켓이 포함되어 있으며 최대 8개의 SFP 트렌시버를 장착할 수 있습니다.

그림 B-1 3D71x5 및 AMP7150 전면 보기



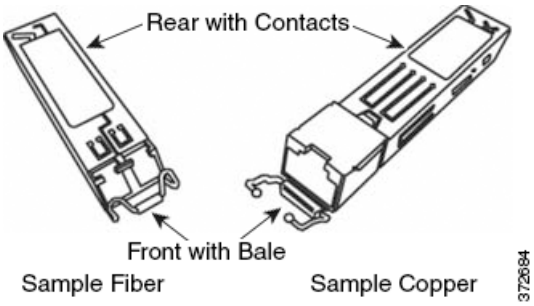
3D71x5 및 AMP7150 SFP 소켓

8개의 SFP 소켓은 5번부터 12번까지 세로 방향으로 배치되어 있으며 탭이 가운데를 향하도록 구성되어 있습니다(상단 행이 위를 향하고 하단 행이 아래를 향함).



소켓 왼쪽에 포함된 LED는 각 인터페이스의 활동 및 링크에 대한 정보를 표시합니다. 자세한 내용은 표 7-503D7115, 3D7125 및 AMP7150 SFP 소켓 활동/링크 LED, 7-36페이지을(를) 참조하십시오.

샘플 SFP 트렌시버



3D71x5 및 AMP7150은 세 가지 형식의 임의 조합으로 최대 8개의 SFP 트렌시버를 지원할 수 있습니다.

- SFP-C-1: 구리 트렌시버
- SFP-F-1-SR: 단거리 파이버 트렌시버
- SFP-F-1-LR: 장거리 파이버 트렌시버

3D71x5 및 AMP 7150에서는 Cisco SFP 트렌시버만 사용하십시오. Cisco 제품이 아닌 SFP 트렌시버는 소켓에 걸릴 수 있으며 트렌시버, 섀시 또는 둘 다를 영구적으로 손상시킬 수 있습니다.

디바이스가 작동하는 동안 트렌시버를 삽입 또는 제거할 수 있습니다. 컨피그레이션 변경 사항을 보려면 Defense Center에서 사용자 인터페이스를 새로 고칩니다.

SFP 트렌시버에는 바이패스 기능이 없습니다. 디바이스에 장애 또는 정전이 발생할 경우 디바이스가 모든 트래픽을 중단하도록 지정하려는 수동 구축 또는 인라인 구축에서 이러한 트렌시버를 사용합니다(예: 가상 스위치, 가상 라우터, 일부 액세스 제어 정책).

수동 구축의 경우 최대 8개 소켓에서 트렌시버를 임의로 결합하여 최대 8개의 네트워크 세그먼트를 모니터링할 수 있습니다. 인라인 구축의 경우 세로 방향으로 순차적인 소켓(5 및 6, 7 및 8, 9 및 10, 11 및 12)에서 임의로 결합된 트렌시버(구리, 파이버 또는 혼합)를 사용하여 최대 4개의 네트워크 세그먼트를 모니터링할 수 있습니다.

디바이스를 관리하는 Defense Center를 사용하여 트렌시버에 포트를 구성합니다.

SFP 트렌시버 삽입

트렌시버를 삽입할 때에는 적절한 정전기 방지(ESD) 절차를 따르십시오. 후면의 접점에 손을 대지 않도록 하고 접점과 포트에 먼지나 흙이 묻지 않도록 하십시오.

주의 SFP 트렌시버를 소켓에 억지로 넣을 경우 트렌시버가 걸리고 트렌시버, 섀시 또는 둘 다 영구적으로 손상될 수 있습니다.

SFP 트렌시버를 삽입하려면 다음을 수행합니다.

단계 1 후면의 접점에 손을 대지 않도록 주의하면서 손가락으로 베일의 측면을 잡고 트렌시버 후면을 섀시의 소켓에 밀어 넣습니다. 상단 행의 소켓은 위를 향하고 하단 행의 소켓은 아래를 향해 있습니다.

단계 2 베일을 트렌시버로 살짝 밀어 베일을 닫아 잠그면 트렌시버가 제자리에 고정됩니다.

단계 3 트렌시버에서 포트를 구성하려면 FireSIGHT System 어플라이언스 설치, 4-1페이지의 절차를 따르십시오.

트렌시버를 현재 작동 중인 디바이스에 삽입할 경우 Defense Center에서 사용자 인터페이스를 새로 고쳐 변경 사항을 확인해야 합니다.

SFP 트렌시버 제거

트렌시버를 제거할 때에는 적절한 정전기 방지(ESD) 절차를 따르십시오. 후면의 접점에 손을 대지 않도록 하고 접점과 포트에 먼지나 흙이 묻지 않도록 하십시오.

SFP 트렌시버를 제거하려면 다음을 수행합니다.

단계 1 디바이스에서 제거하려는 트렌시버의 모든 케이블을 분리합니다.

단계 2 손가락을 이용하여 섀시에서 트렌시버의 베일을 가볍게 잡아당겨 연결 상태를 해제합니다.

상단 행에 있는 트렌시버의 경우 아래로 당깁니다. 하단 행에 있는 트렌시버는 위로 들어 올립니다.

단계 3 트렌시버 후면의 접점에 손이 닿지 않도록 주의하면서 손가락으로 베일 측면을 잡고 베일을 손잡이로 사용하여 섀시에서 트렌시버를 가볍게 잡아당깁니다.

8000 Series 모듈 삽입 및 제거

8000 Series 어플라이언스는 구축 시 모듈을 유연하게 구성할 수 있습니다. 이 섹션의 단계를 사용하여 다음을 수행할 수 있습니다.

- 새 모듈을 어플라이언스에 삽입
- 어플라이언스에 사전 설치된 모듈 제거 또는 교체

다음 섹션에서는 8000 Series 모듈을 삽입, 제거 또는 교체하는 방법에 대해 설명합니다.

8000 Series 어플라이언스의 모듈 슬롯

8000 Series 어플라이언스는 다음과 같은 슬롯에 모듈을 사용할 수 있습니다.

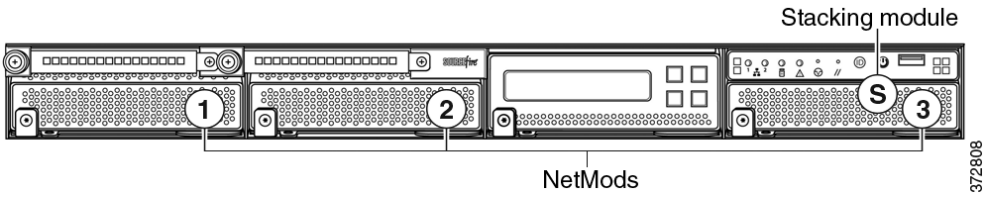
모듈을 어플라이언스에 삽입한 후 다음 섹션에서 모듈 사용에 대한 자세한 내용을 참조합니다.

- 센싱 인터페이스 구성에 대한 자세한 내용은 센싱 인터페이스 식별, 4-5페이지을(를) 참조하십시오.
- 스태킹 모듈 사용에 대한 자세한 내용은 스태킹 컨피그레이션에서 디바이스 사용, 4-16페이지을(를) 참조하십시오.

81xx 제품군

81xx 제품군 어플라이언스는 다음과 같은 슬롯에 모듈을 사용할 수 있습니다.

그림 C-1 81xx 제품군 기본 디바이스



스태킹 컨피그레이션 고려 사항

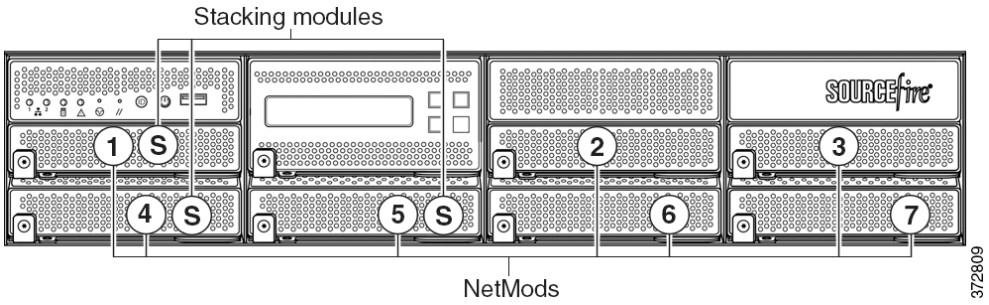
스태킹된 디바이스에 대해 다음과 같이 모듈을 구성합니다.

- 기본 디바이스에만 NetMod를 설치합니다.
- 기본 디바이스와 보조 디바이스에 스태킹 모듈을 하나씩 설치합니다.
- 모든 디바이스를 단일 디바이스로 등록하고 스태킹한 후 스태킹된 보조 디바이스에 대한 관리 인터페이스를 제거하거나 비활성화지 마십시오.

82xx 제품군 및 83xx 제품군

82xx 제품군 및 83xx 제품군 어플라이언스는 다음 슬롯에 모듈을 사용할 수 있습니다.

그림 C-2 82xx 제품군 및 83xx 제품군 기본 디바이스

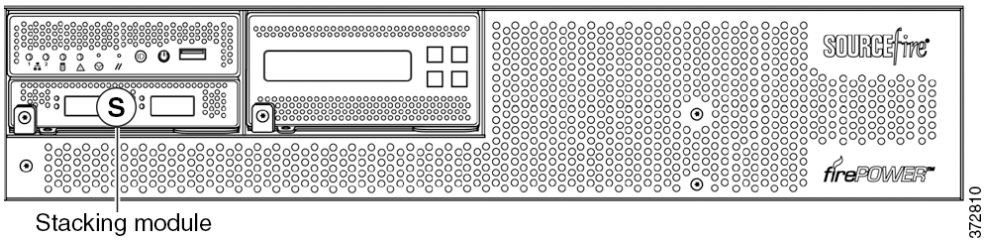


스태킹 컨피그레이션 고려 사항

스태킹된 디바이스에 대해 다음과 같이 모듈을 구성합니다.

- 기본 디바이스에만 NetMod를 설치합니다.
- 각 스태킹된 보조 디바이스에 대한 기본 디바이스에 스태킹 모듈 하나를 설치하고 보조 디바이스마다 스태킹 모듈 하나를 설치합니다.
- 모든 디바이스를 단일 디바이스로 등록하고 스태킹한 후 스태킹된 보조 디바이스에 대한 관리 인터페이스를 제거하거나 비활성화지 마십시오.

그림 C-3 82xx 제품군 및 83xx 제품군 보조 디바이스



포함된 항목

모듈 어셈블리 키트에는 T8 Torx 드라이버 하나와 다음 모듈이 하나 이상 포함되어 있습니다.

- 쿼드 포트 1000BASE-T 구리 바이패스 구성 가능 NetMod. 자세한 내용은 쿼드 포트 1000BASE-T 구리 바이패스 구성 가능 NetMod, 7-51페이지을(를) 참고하십시오.
- 쿼드 포트 1000BASE-SX 파이버 바이패스 구성 가능 NetMod. 자세한 내용은 쿼드 포트 1000BASE-SX 파이버 바이패스 구성 가능 NetMod, 7-52페이지을(를) 참고하십시오.
- 듀얼 포트 10GBASE(MMSR 또는 SMLR) 파이버 바이패스 구성 가능 NetMod. 자세한 내용은 듀얼 포트 10GBASE(MMSR 또는 SMLR) 파이버 바이패스 구성 가능 NetMod, 7-53페이지을(를) 참고하십시오.
- 듀얼 포트 40GBASE-SR4 파이버 바이패스 구성 가능 NetMod. 자세한 내용은 듀얼 포트 40GBASE-SR4 파이버 바이패스 구성 가능 NetMod, 7-55페이지을(를) 참고하십시오.

참고 이 듀얼 슬롯 NetMod는 40G 용량의 3D8250 또는 3D8350에서만 사용하십시오. 어플라이언스를 업그레이드해야 하는 경우 *Cisco 8000 Series 디바이스 40G 용량 업그레이드 가이드*를 참조하십시오.

- 쿼드 포트 1000BASE-T 구리 비 바이패스 NetMod. 자세한 내용은 쿼드 포트 1000BASE-T 구리 비 바이패스 NetMod, 7-56페이지을(를) 참고하십시오.
- 쿼드 포트 1000BASE-SX 파이버 비 바이패스 NetMod. 자세한 내용은 쿼드 포트 1000BASE-SX 파이버 비 바이패스 NetMod, 7-57페이지을(를) 참고하십시오.
- 쿼드 포트 10GBASE(MMSR 또는 SMLR) 파이버 비 바이패스 NetMod. 자세한 내용은 쿼드 포트 10GBASE(MMSR 또는 SMLR) 파이버 비- 바이패스 NetMod, 7-58페이지을(를) 참고하십시오.

주의 쿼드 포트 10GBASE 파이버 비 바이패스 NetMod에는 제거 불가능한 SFP(Small Form Factor Pluggable) 트렌시버가 포함되어 있습니다. SFP 제거를 시도할 경우 모듈이 손상될 수 있습니다.

- 스태킹 모듈. 자세한 내용은 스태킹 모듈, 7-59페이지을(를) 참고하십시오.

NetMod를 어플라이언스의 호환되지 않는 슬롯에 설치하거나 NetMod가 시스템과 다른 부분에서 호환되지 않는 경우 NetMod 구성을 시도하면 관리하는 Defense Center 디바이스의 웹 인터페이스에 오류 또는 경고 메시지가 나타납니다. 도움을 받으려면 고객 지원에 문의하십시오.

참고 NetMod를 교체하면 완벽하게 구성된 대한민국 인증(KCC 마크) 어플라이언스의 컨피그레이션이 변경될 수 있습니다. 자세한 내용은 어플라이언스의 원래 컨피그레이션 설명서 및 *FirePOWER 및 FireSIGHT 어플라이언스 규정준수 및 안전 정보* 설명서를 참조하십시오.

모듈 부품 식별

모든 모듈에는 모듈의 센싱 인터페이스, 속도 또는 크기와 상관없이 동일한 부품이 포함되어 있습니다.

그림 C-4 샘플 모듈 또는 슬롯 덮개(열린 모습)

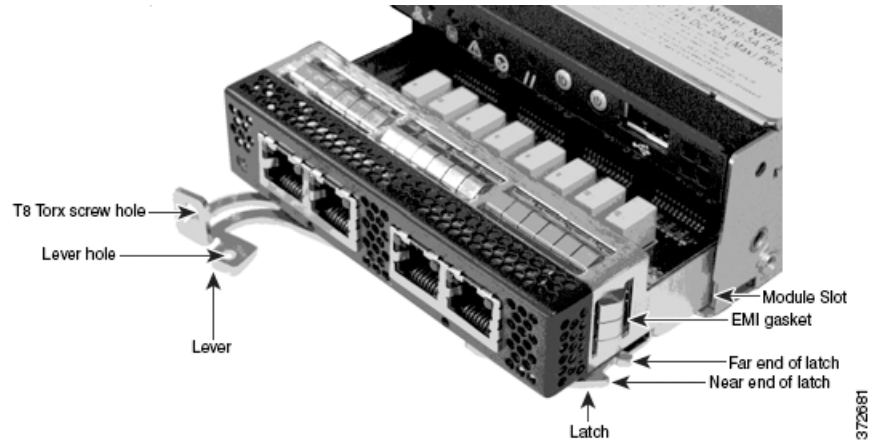
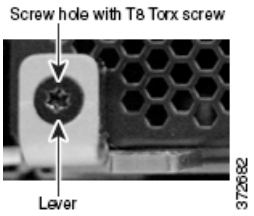


그림 C-5 샘플 모듈 레버(나사로 구멍을 닫은 모습)



시작하기 전에

다음 지침에 따라 모듈을 삽입 또는 제거할 준비를 합니다.

- 모든 어플라이언스와 모듈 부품을 식별합니다.
- NetMod를 설치할 슬롯을 식별합니다.

정보 NetMod를 사용 가능한 호환 슬롯에 삽입할 수 있습니다.

- 스태킹 모듈에 적합한 슬롯을 식별합니다. 스태킹 컨피그레이션에서 디바이스 사용, 4-16페이지을(를) 참조하십시오.
- 3D8140: 슬롯 3
- 3D8250, 3D8260 및 3D8350, 3D8360 기본 슬롯: 슬롯 5
- 3D8270 및 3D8370 기본 슬롯: 슬롯 5 및 1
- 3D8290 및 3D8390 기본 슬롯: 슬롯 5, 1, 4
- 3D82xx 및 3D83xx 보조: 슬롯 S
- EMI 가스켓이 제자리에 있는지 확인합니다.
- 어플라이언스에서 모든 전원 코드를 분리합니다.

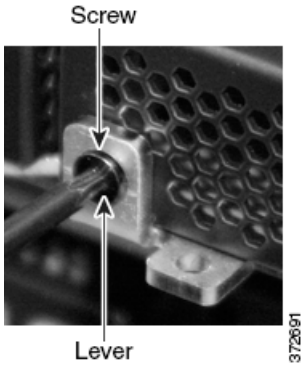
주의 운영 중 모듈을 교체할 수 **없습니다**. 모듈을 삽입 또는 제거하기 전에 전원을 끄고 어플라이언스에서 두 전원 코드를 **모두** 분리해야 합니다.

모듈 또는 슬롯 덮개 제거

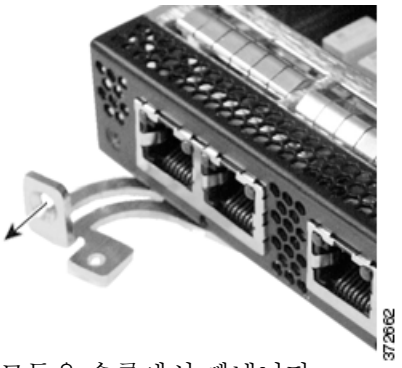
모듈을 취급할 때는 손목끈을 사용하거나 ESD 작업 표면을 사용하는 등 적절한 정전기 방지(ESD) 절차를 준수해야 합니다. 사용하지 않는 모듈은 손상되지 않도록 ESD 가방 또는 상자에 보관합니다.

모듈 또는 슬롯 덮개를 제거하려면 다음을 수행합니다.

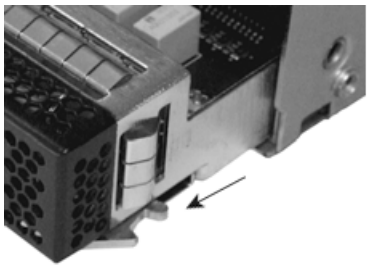
단계 1 포함된 드라이버를 사용하여 모듈 레버에서 T8 Torx 나사를 제거하여 보관합니다.



단계 2 모듈에서 레버를 잡아당겨 래치를 해제합니다.



단계 3 모듈을 슬롯에서 빼냅니다.

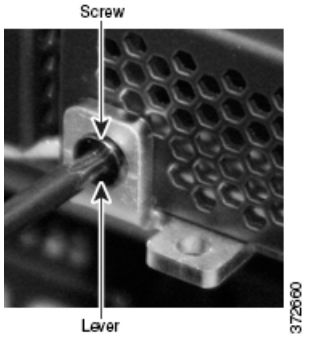


모듈 또는 슬롯 덮개 삽입

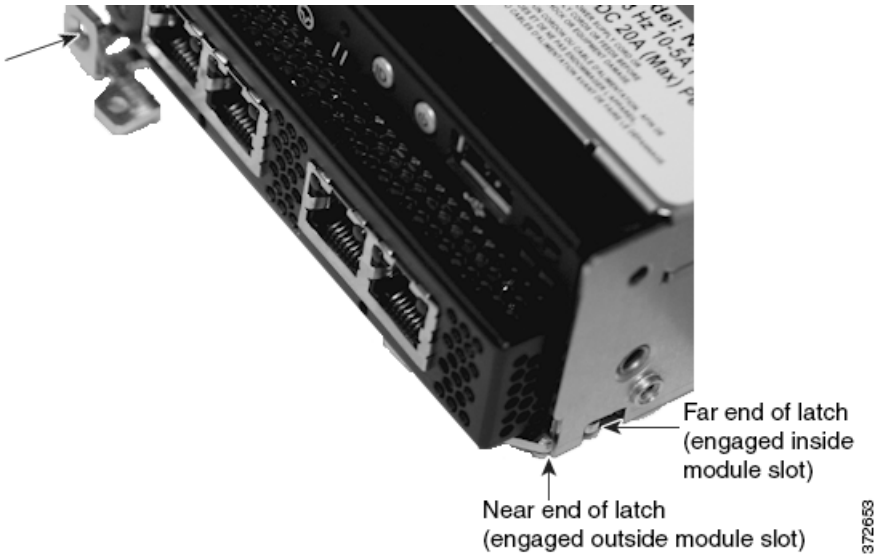
새로운 모듈을 장착할 슬롯을 준비하려면 기존 모듈 또는 슬롯 덮개를 제거합니다. 자세한 내용은 모듈 또는 슬롯 덮개 제거, C-5페이지을(를) 참조하십시오.

모듈 또는 슬롯 덮개를 삽입하려면 다음을 수행합니다.

단계 1 포함된 드라이버를 사용하여 모듈 레버에서 T8 Torx 나사를 제거하여 보관합니다.

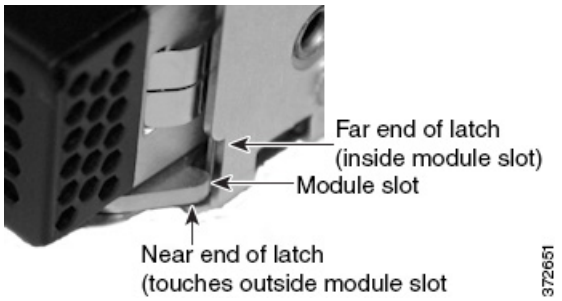


단계 2 모듈에서 레버를 잡아당겨 래치를 엽니다. 사용자와 가까운 쪽의 래치 끝부분이 보입니다. 반대편의 래치 끝부분은 모듈 내부에 있습니다.

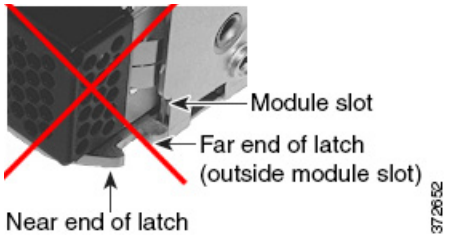


단계 3 반대편의 래치 끝부분이 슬롯 안에 들어가고 가까운 쪽이 모듈 슬롯 외부와 닿을 때까지 모듈을 슬롯 안에 삽입합니다.

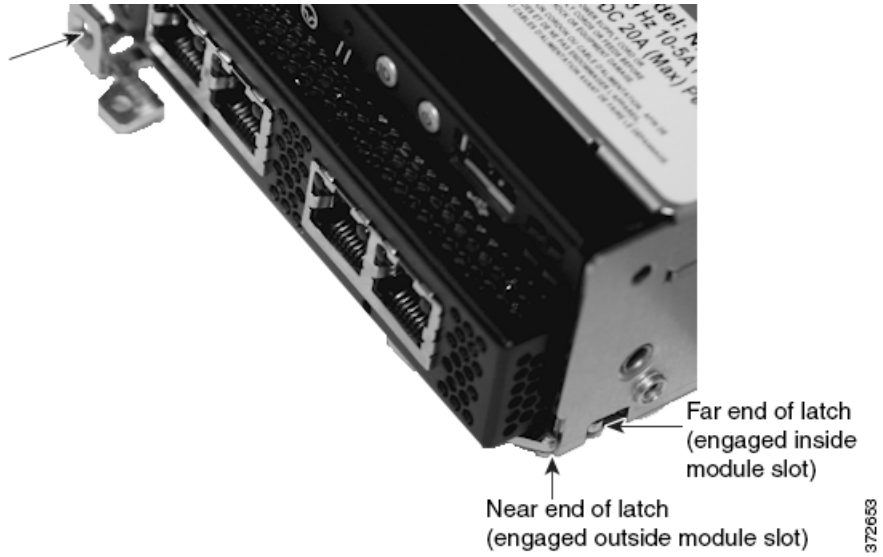
올바른 모듈 배열



잘못된 모듈 배열

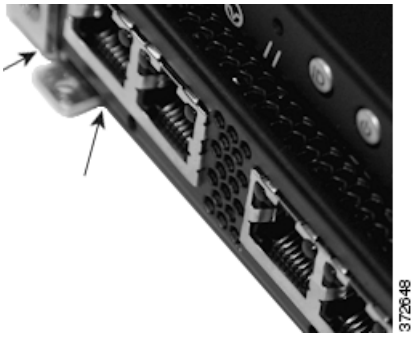


단계 4 레버를 모듈 쪽으로 눌러 래치를 끼우고 모듈을 슬롯에 넣습니다.

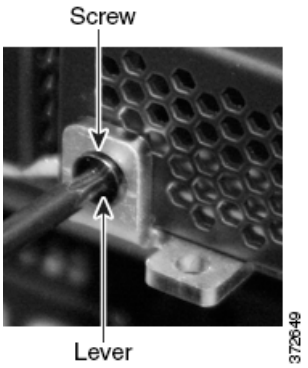


주의 과도한 힘을 가하지 **마십시오**. 래치가 끼워지지 않을 경우 모듈을 뺐다가 다시 맞춘 후 다시 시도하십시오.

단계 5 나사 구멍을 꽉 누르고 레버를 모듈 쪽으로 끝까지 밀어서 래치를 고정합니다. 레버가 모듈 끝까지 장착되고 모듈은 섀시와 수평이 됩니다.



단계 6 보관해 둔 T8 Torx 나사를 레버에 삽입하고 조입니다.



하드 드라이브 삭제

대부분의 Defense Center 및 관리되는 디바이스의 하드 드라이브 콘텐츠에 액세스할 수 없도록 안전하게 삭제할 수 있습니다. 예를 들어, 민감한 데이터가 포함된 어플라이언스에서 결함이 발생하여 반품해야 할 경우 이 기능을 사용하여 데이터를 덮어쓸 수 있습니다.

하드 드라이브 콘텐츠 삭제

지원되는 디바이스: 모두

지원되는 방어 센터: DC1000, DC3000을 제외한 모든 방어 센터

이러한 디스크 삭제 모드는 다음과 같은 군사 표준을 준수합니다.

표준

DoD 삭제 순서는 주소 지정 가능한 모든 위치를 문자, 해당 문자의 보수, 랜덤 문자로 차례로 덮어쓴 다음 확인해야 하는 착탈식 및 비착탈식 하드 디스크 삭제에 관한 DoD 5220.22-M 절차를 준수합니다. 추가 제약 사항은 DoD 설명서를 참조하십시오.

주의 하드 드라이브를 삭제하면 어플라이언스의 **모든** 데이터가 손실되고 해당 어플라이언스를 작동할 수 없습니다.

인터랙티브 메뉴를 사용하여 어플라이언스 복원, 8-8페이지에 설명된 인터랙티브 메뉴의 옵션을 사용하여 하드 드라이브를 삭제합니다.

하드 드라이브를 삭제하려면 다음을 수행합니다.

???: Admin

단계 1 어플라이언스에 액세스하는 방법에 따라 다음 섹션 중 하나에 있는 지침을 사용하여 복원 유틸리티의 인터랙티브 메뉴를 표시합니다.

- KVM 또는 물리적 시리얼 포트를 사용하여 복원 유틸리티 시작, 8-6페이지
- LOM(Lights-Out Management)을 사용하여 복원 유틸리티 시작, 8-7페이지

참고 DC1000 및 DC3000은 이 기능을 지원하지 **않습니다**.

단계 2 주 메뉴에서 **8 Wipe Contents of Disk(디스크 콘텐츠 삭제)**를 선택합니다.

단계 3 확인 메시지가 표시되면 하드 드라이브를 삭제할 것임을 확인합니다.

하드 드라이브가 삭제됩니다. 삭제 프로세스를 완료하는 데 몇 시간이 걸릴 수 있으며, 드라이브가 클수록 더 오래 걸립니다.

FireSIGHT System 어플라이언스 사전 구성

대상 위치(스테이징 위치와 다른 위치)에 구축할 어플라이언스(Defense Center 또는 디바이스)를 *스테이징* 위치(여러 어플라이언스를 사전 구성 또는 스테이징할 중앙 위치)에서 사전 구성할 수 있습니다.

어플라이언스를 사전 구성하고 대상 위치에 구축하려면 다음 단계를 수행합니다.

- 스테이징 위치에 있는 디바이스에 시스템을 설치합니다.
- 선택적으로 디바이스를 Defense Center에 등록합니다.
- 선택적으로 관리하는 Defense Center의 업데이트를 디바이스로 푸시합니다.
- 선택적으로 Defense Center에서 디바이스의 등록을 취소합니다.
- 어플라이언스를 종료하고 대상 위치로 배송합니다.
- 대상 위치에 어플라이언스를 구축합니다.

자세한 내용은 다음 섹션을 참조하십시오.

- 시작하기 전에, E-1페이지
- 시스템 설치, E-3페이지
- 디바이스 등록, E-3페이지
- 어플라이언스 배송 준비, E-4페이지
- 어플라이언스 사전 구성 트러블슈팅, E-6페이지

정보 모든 포장재를 보관해두고 어플라이언스를 재포장할 때 모든 참조 자료와 전원 코드를 함께 포장하시기 바랍니다.

시작하기 전에

어플라이언스를 사전 구성하기 전에 스테이징 위치 및 대상 위치에 대한 네트워크 설정, 라이센스, 기타 관련 정보를 수집합니다.

정보 스테이징 위치와 대상 위치에서 이 정보를 관리하기 위해 스프레드시트를 만드는 것이 도움이 될 수 있습니다.

초기 설정 중 어플라이언스를 네트워크에 연결하고 시스템을 설치하는 데 필요한 정보를 사용하여 어플라이언스를 구성합니다. 선택적으로 디바이스를 Defense Center에 연결하고 Defense Center의 모든 업데이트를 디바이스로 푸시할 수 있습니다. 또한 초기 설정에는 필요하지 않지만 사전 구성할 경우 유용한 다른 기능을 활성화할 수 있습니다. 자세한 내용은 다음 섹션을 참조하십시오.

- 필수 사전 구성 정보, E-2페이지
- 선택적 사전 구성 정보, E-2페이지
- 시간 관리 사전 구성, E-3페이지

필수 사전 구성 정보

어플라이언스를 사전 구성하려면 최소한 다음과 같은 정보가 필요합니다.

- 새 비밀번호(초기 설정 시 비밀번호 변경 필요)
- 어플라이언스의 호스트 이름
- 어플라이언스의 도메인 이름
- 어플라이언스의 IP 관리 주소
- 대상 위치의 어플라이언스 네트워크 마스크
- 대상 위치의 어플라이언스 기본 게이트웨이
- 스테이징 위치(또는 액세스 가능한 경우 대상 위치)의 DNS 서버 IP 주소
- 스테이징 위치(또는 액세스 가능한 경우 대상 위치)의 NTP 서버 IP 주소
- 대상 위치의 탐지 모드

선택적 사전 구성 정보

다음과 같은 몇 가지 기본 컨피그레이션을 변경할 수 있습니다.

- LCD 패널에 액세스하여 디바이스를 구성할 수 있도록 허용(Series 3 관리되는 디바이스만 해당)
- 어플라이언스의 시간을 수동으로 설정하도록 선택하는 경우 시간대 설정
- 자동 백업을 위해 원격 스토리지 위치를 설정
- 디바이스에서 LOM(Lights-Out Management)을 활성화하기 위해 Series 3 디바이스에 LOM IP 주소 설정

참고 일부 전원 주기 시나리오에서는 관리 인터페이스를 통해 네트워크에 연결된 3D7050의 베이스보드 관리 컨트롤러(BMC)가 DHCP 서버에서 할당한 IP 주소를 유실할 수 있습니다. 이러한 이유로 Cisco에서는 3D7050 BMC를 고정 IP 주소로 구성하도록 권장합니다. 또는 네트워크 케이블을 분리한 후 다시 연결하거나 디바이스의 전원을 제거한 후 복원하여 강제로 링크를 다시 협상할 수 있습니다.

디바이스를 Defense Center에 등록하려면 다음과 같은 정보가 필요합니다.

- 관리되는 디바이스의 이름 또는 IP 주소
- 관리 호스트(Defense Center)의 이름
- 등록 키(개인적으로 만든 최대 37자의 고유한 영숫자 키)

시간 관리 사전 구성

다음과 같은 고려 사항에 주의하십시오.

- Cisco에서는 물리적 NTP 서버와 시간을 동기화하도록 권장합니다. 관리되는 디바이스를 가상 Defense Center와 동기화하지 마십시오. 가상 어플라이언스의 성능 최적화는 실제 시각에 영향을 미칠 수 있습니다.
- 스테이징 위치의 네트워크가 대상 위치의 DNS 및 NTP 서버에 액세스할 수 있는 경우 대상 위치의 DNS 및 NTP 서버에 대한 IP 주소를 사용합니다. 그렇지 않을 경우 스테이징 위치 정보를 사용하고 대상 위치에서 재설정합니다.
- 어플라이언스의 시간을 NTP를 사용하지 않고 수동으로 설정할 경우 대상 구축의 시간대를 사용합니다. 시간 설정, 5-10페이지을(를) 참조하십시오.

시스템 설치

FireSIGHT System 어플라이언스 설치, 4-1페이지 및 FireSIGHT System 어플라이언스 설정, 5-1페이지에 설명된 설치 절차를 사용합니다. 시스템을 사전 구성할 경우 다음에 주의하십시오.

- Series 3 디바이스에서 LCD 패널을 사용하여 디바이스의 네트워크 설정에 액세스할 수 있도록 허용할 경우 디바이스에 물리적으로 액세스하여 무단으로 변경할 수 있는 보안 위험에 노출됩니다. Series 3 디바이스 LCD 패널 컨피그레이션, 5-9페이지을(를) 참조하십시오.
- 대상 구축에서 Defense Center의 호스트 이름 또는 IP 주소를 사용하여 디바이스를 사전 등록합니다. 나중에 등록을 완료하는 데 사용하도록 등록 키를 기록해 두십시오. 원격 관리, 5-9페이지을(를) 참조하십시오.
- 기본 탐지 모드를 변경할 경우 대상 구축의 해당 담당자에게 반드시 알려야 합니다. 탐지 모드와 다르게 인터페이스를 구성하면 시스템에서 인터페이스를 잘못 할당할 수 있습니다. 탐지 모드, 5-10페이지을(를) 참조하십시오.
- 디바이스에 대한 NAT(Network Address Translation)를 구성해야 할 경우 디바이스에서 CLI를 사용하거나(Series 3 디바이스만 해당) 관리하는 Defense Center에서 웹 인터페이스를 사용하여 디바이스를 등록할 때 디바이스의 NAT ID를 입력합니다. *FireSIGHT System 사용 설명서*의 CLI를 사용하여 Series 3 디바이스를 방어 센터에 등록, 5-7페이지 및 NAT 환경에서 작업을 참조하십시오.
- 초기 설정 중에 라이센스를 추가합니다. 이때 라이센스를 추가하지 않을 경우 초기 설정 중 등록하는 디바이스는 라이센스 없이 Defense Center에 추가됩니다. 초기 설정 프로세스가 종료된 후 각 디바이스에 개별적으로 라이센스를 부여해야 합니다. 라이센스 설정, 5-14페이지을(를) 참조하십시오.

디바이스 등록

Defense Center에서 디바이스의 소프트웨어 버전과 동일하거나 그 이상인 소프트웨어 버전을 실행하는 경우 디바이스를 Defense Center에 등록하여 관리되는 디바이스로 정책과 업데이트를 푸시할 수 있습니다.

참고 Defense Center 및 해당 관리되는 디바이스를 다른 대상 위치에 구축하는 경우 어플라이언스를 종료하기 전에 Defense Center에서 디바이스를 삭제해야 합니다. Defense Center에서 디바이스 삭제, E-4페이지을(를) 참조하십시오.

디바이스를 Defense Center에 등록하려면 다음을 수행합니다.

단계 1 디바이스에서 대상 구축에 있는 Defense Center의 호스트 이름 또는 IP 주소를 사용하여 원격 관리를 구성합니다. 나중에 등록을 완료하는 데 사용하도록 등록 키를 기록해 두십시오. 원격 관리, 5-9 페이지을(를) 참조하십시오.

참고 디바이스를 Defense Center에 등록하기 전에 반드시 디바이스에 원격 관리를 구성해야 합니다.

단계 2 Defense Center에서 원격 관리 컨피그레이션의 등록 정보를 사용하여 디바이스를 등록합니다. 디바이스 등록, 5-15페이지을(를) 참조하십시오.

어플라이언스 배송 준비

어플라이언스 배송을 준비하려면 어플라이언스를 안전하게 종료한 다음 포장해야 합니다.

- Defense Center 및 관리되는 디바이스가 대상 위치와 동일한 컨피그레이션에서 사용되지 않는 경우 Defense Center에서 디바이스를 삭제한 다음 어플라이언스를 종료하고 다시 포장합니다. Defense Center에서 디바이스 삭제, E-4페이지을(를) 참조하십시오.
- 어플라이언스를 안전하게 종료하려면 어플라이언스 종료, E-5페이지을(를) 참조하십시오.
- 어플라이언스를 안전하게 배송하도록 준비되었는지 확인하려면 배송 고려 사항, E-6페이지을(를) 참조하십시오.

Defense Center에서 디바이스 삭제

Defense Center 및 해당 관리되는 디바이스를 동일한 대상 위치에 구축하지 않을 경우 Defense Center에서 디바이스를 삭제해야 합니다. 그러면 디바이스를 대상 위치에서 다른 Defense Center에 등록할 때 디바이스가 원래 Defense Center의 UUID를 검색하지 않습니다.

Defense Center에서 디바이스를 삭제하려면 다음을 수행합니다.

단계 1 Defense Center에서 **Devices(디바이스) > Device Management(디바이스 관리)**를 선택합니다.

Device Management(디바이스 관리) 페이지가 표시됩니다.

단계 2 삭제하려는 디바이스 옆에 있는 삭제 아이콘( )을 클릭합니다.

메시지가 표시되면 디바이스를 삭제할 것임을 확인합니다. 디바이스와 Defense Center 간 통신이 중단되고 Device Management(디바이스 관리) 페이지에서 디바이스가 삭제됩니다. 디바이스에 NTP를 통해 Defense Center에서 시간을 수신하도록 하는 시스템 정책이 있는 경우 해당 디바이스는 로컬 시간 관리로 되돌아갑니다.

Defense Center에서 디바이스를 삭제한 다음 Defense Center에서 해당 디바이스가 원격으로 관리되지 않는지 확인합니다.

디바이스가 Defense Center에서 관리되지 않는지 확인하려면 다음을 수행합니다.

단계 1 관리되는 디바이스에서 웹 인터페이스 또는 CLI를 사용할 수 있습니다.

- 관리되는 디바이스의 웹 인터페이스에서 **System(시스템) > Local(로컬) > Registration(등록) > Remote Management(원격 관리)**로 이동한 다음 Remote Management(원격 관리) 화면의 호스트 목록이 비어 있는지 확인합니다.
- 관리되는 디바이스의 CLI에서 `show manager` 명령을 실행하고 호스트가 표시되지 않는지 확인합니다.

Defense Center에서 라이센스 삭제

어떤 이유로 라이센스를 삭제해야 하는 경우 다음 절차를 사용하십시오. Cisco에서는 각 Defense Center의 고유한 라이센스 키를 기준으로 라이센스를 생성하므로 한 Defense Center에서 라이센스를 삭제한 다음 다른 Defense Center에서 다시 사용할 수 없습니다. 자세한 내용은 *FireSIGHT System 사용 설명서*에서 FireSIGHT System 라이센싱을 참조하십시오.

라이센스를 삭제하려면 다음을 수행합니다.

단계 1 **Systems(시스템) > Licenses(라이센스)**를 선택합니다.

License(라이센스) 페이지가 나타납니다.

단계 2 삭제하려는 라이센스 옆에 있는 삭제 아이콘( )을 클릭합니다.

라이센스를 삭제하면 해당 라이센스를 사용하는 모든 디바이스에서 라이센스가 부여된 기능이 제거됩니다. 예를 들어, 보호 라이센스가 유효하고 관리되는 디바이스 100대에 대해 활성화된 경우 라이센스를 삭제하면 전체 디바이스 100대에서 보호 기능이 제거됩니다.

단계 3 라이센스를 삭제할 것임을 확인합니다.

라이센스가 삭제됩니다.

어플라이언스 종료

전원 공급 장치를 분리하기 전에 다음 절차에 따라 어플라이언스를 안전하게 종료합니다.

Defense Center를 종료하려면 다음을 수행합니다.

단계 1 Defense Center에서 명령행에 다음을 입력합니다.

```
sudo shutdown -h now
```

Defense Center가 안전하게 종료됩니다.

관리되는 디바이스를 종료하려면 다음을 수행합니다.

단계 1 디바이스에서 명령행에 다음을 입력합니다.

```
system shutdown
```

디바이스가 안전하게 종료됩니다.

배송 고려 사항

어플라이언스를 대상 위치로 배송할 수 있도록 준비하려면 어플라이언스를 안전하게 종료한 다음 포장해야 합니다. 다음과 같은 고려 사항에 주의하십시오.

- 원래 포장재를 사용하여 어플라이언스를 다시 포장합니다.
- 어플라이언스와 함께 모든 참조 자료와 전원 코드를 포함합니다.
- 잘못된 취급 또는 과도한 압력으로 인해 NetMod와 SFP가 손상되지 않도록 보호합니다.
- 대상 위치에 새로운 비밀번호와 탐지 모드를 포함한 모든 설정 및 컨피그레이션 정보를 제공합니다.

어플라이언스 사전 구성 트러블슈팅

어플라이언스가 대상 구축에 맞게 사전 구성된 경우 추가 컨피그레이션 없이 어플라이언스를 설치 및 구축할 수 있습니다.

어플라이언스에 로그인하는 데 문제가 있는 경우 사전 구성에 오류가 발생했을 수 있습니다. 다음과 같은 트러블슈팅 절차를 시도해 보십시오.

- 모든 전원 및 통신 케이블이 어플라이언스에 올바르게 연결되어 있는지 확인합니다.
- 어플라이언스의 최신 비밀번호가 있는지 확인합니다. 스테이징 위치의 초기 설정에서 비밀번호를 변경하라는 메시지를 표시합니다. 스테이징 위치에서 새 비밀번호에 대해 제공하는 컨피그레이션 정보를 참조하십시오.
- 네트워크 설정이 올바른지 확인합니다. 참조: 초기 설정 페이지: 디바이스, 5-8페이지 및 초기 설정 페이지: 방어 센터, 5-11페이지
- 올바른 통신 포트가 제대로 작동하는지 확인합니다. 방화벽 포트 관리에 대한 자세한 내용은 방화벽 설명서를 참조하십시오. 필요한 개방 포트는 통신 포트 요구 사항, 1-19페이지을(를) 참조하십시오.
- 구축에서 NAT(Network Address Translation) 어플라이언스를 사용하는 경우 NAT가 올바르게 구성되었는지 확인합니다. *FireSIGHT System 사용자 설명서*의 NAT 환경에서 작업을 참조하십시오.

계속해서 문제가 발생하는 경우 IT 부서에 문의하십시오.

7000 Series

Series 3 FirePOWER 관리되는 디바이스의 그룹. 이 시리즈의 디바이스에는 70xx 제품군(3D7010, 3D7020, 3D7030, 3D7050 모델) 및 71xx 제품군(3D7110, 3D7115, 3D7120, 3D7125, AMP7150 모델)이 있습니다.

8000 Series

Series 3 FirePOWER 관리되는 디바이스의 그룹. 이 시리즈의 디바이스에는 81xx 제품군(3D8120, 3D8130, 3D8140, AMP8150 모델), 82xx 제품군(3D8250, 3D8260, 3D8270, 3D8290 모델) 및 83xx 제품군(3D8350, 3D8360, 3D8370, 3D8390 모델)이 있습니다. 8000 Series 디바이스는 일반적으로 7000 Series 디바이스보다 강력합니다.

AMP(Advanced Malware Protection)

약자로 AMP로 표기하며, FireSIGHT System의 네트워크 기반 악성코드 탐지 및 악성코드 클라우드 조회기능입니다. 이 기능을 FireAMP, Cisco의 엔드포인트 기반 AMP 툴(FireAMP 서브스크립션 필요)과 비교하십시오.

ASA FirePOWER

Cisco ASA with FirePOWER Services의 간단한 이름입니다.

Cisco ASA with FirePOWER Services

Cisco ASA(Adaptive Security Appliance) 관리되는 디바이스 그룹. 이 시리즈의 디바이스에는 ASA5506-X, ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X, ASA5585-X-SSP-10, ASA5585-X-SSP-20, ASA5585-X-SSP-40 및 ASA5585-X-SSP-60 모델이 있습니다.

Cisco VRT

Cisco의 Vulnerability Research Team.

Cisco 인텔리전스 피드

Cisco VRT에서 평판이 나쁜 것으로 판단하고 정기적으로 업데이트되는 IP 주소 목록의 컬렉션. 피드의 각 목록은 특정 범주, 즉, 오픈 릴레이, 알려진 공격, 가짜 IP 주소(bogon) 등을 나타냅니다. 액세스 제어 정책에서는 보안 인텔리전스를 사용하여 임의의 범주 모든 범주를 블랙리스트에 추가할 수 있습니다. 인텔리전스 피드는 정기적으로 업데이트되므로 이 피드를 사용하면 시스템에서 최신 정보를 사용하여 네트워크 트래픽을 필터링할 수 있습니다.

Cisco 클라우드

*클라우드 서비스*라고도 하며, 방어 센터에서 악성코드, 보안 인텔리전스, URL 필터링 데이터 등의 최신 관련 정보를 얻을 수 있고 Cisco에서 호스팅하는 외부 서버. 악성코드 클라우드 조회도 참조하십시오.

CLI

명령행 인터페이스을 참조하십시오.

Context Explorer

침입, 연결, 파일, 위치정보, 악성코드 및 검색 정책을 사용하여 모니터링되는 네트워크에 대한 자세한 인터랙티브 그래픽 정보를 표시하는 페이지. 개별 섹션은 선명한 선, 막대, 파이, 도넛 그래프 형식과 자세한 목록으로 정보를 표시합니다. 쉽게 사용자 정의 필터를 만들고 적용하여 정밀 분석을 수행할 수 있으며 그래프 영역을 클릭하거나 커서를 올려놓으면 데이터 섹션을 자세히 검토할 수 있습니다. 매우 간편하게 사용자 정의할 수 있고 분류되며 실시간으로 업데이트되는 대시보드와 비교하여, Context Explorer는 수동으로 업데이트되고 데이터에 대한 광범위한 컨텍스트를 제공하도록 설계되었으며 활성 사용자 탐색을 위해 설계된 일관적인 단일 레이아웃을 사용합니다.

eStreamer

이벤트 또는 관리되는 방어 센터에서 외부 디바이스으로 클라이언트 애플리케이션 데이터를 스트리밍할 수 있도록 하는 FireSIGHT System의 구성 요소.

Event Streamer

eStreamer을 참조하십시오.

FireAMP

Cisco악성코드 침투, 지속적인 위협 및 표적 공격을 발견, 이해 및 차단하는 엔터프라이즈급, 엔드포인트 기반 지능형 위협 분석 및 방지 솔루션입니다. 조직에 FireAMP 서브스크립션이 있는 경우 개별 사용자가 엔드포인트(컴퓨터, 모바일 디바이스)에 경량의 FireAMP 커넥터를 설치하면 이를 통해 Cisco 클라우드와 통신할 수 있습니다. 이렇게 하면 악성코드를 빠르게 식별 및 격리할 수 있을 뿐만 아니라 침투가 발생하는 즉시 식별할 수 있으며 전파 흔적을 추적하고 그로 인한 영향과 성공적으로 복구하는 방법을 이해할 수 있습니다. 또한 FireAMP 포털을 사용하여 사용자 정의 보호를 만들고 특정 애플리케이션의 실행을 차단하며 사용자 정의 화이트리스트를 작성할 수 있습니다. 네트워크 기반 AMP(Advanced Malware Protection)와 비교해 보십시오.

FireAMP 서브스크립션

조직이 FireAMP를 AMP(AMP(Advanced Malware Protection))를 솔루션으로 사용할 수 있도록 별도로 구매하는 서브스크립션. 관리되는 악성코드 라이센스에서 활성화하여 네트워크 기반 AMP를 수행하는 디바이스와 비교해 보십시오.

FireAMP 커넥터

서브스크립션 기반 FireAMP 구축의 사용자가 컴퓨터, 모바일 디바이스 등의 엔드포인트에 설치하는 경량 에이전트. 커넥터는 Cisco 클라우드와 통신하며, 조직 전체에서 악성코드를 빠르게 식별 및 격리하기 위해 사용할 수 있는 정보를 교환합니다.

FireAMP 포털

조직의 서브스크립션 기반 FireAMP 구축을 구성할 수 있는 웹사이트 http://amp.sourcefire.com/

FireSIGHT 라이센스

방어 센터, 호스트, 사용자 검색을 수행할 수 있도록 하는 애플리케이션의 기본 라이센스. 또한 FireSIGHT 라이센스에 따라 호스트 및 관리되는 방어 센터를 사용하여 모니터링할 수 있는 개별 디바이스 수 및 사용자 수와 액세스 제어 규칙을 수행하기 위해 사용자 제어에서 사용할 수 있는 액세스 제어 사용자 수가 결정됩니다.

GeoDB

위치정보 데이터베이스를 참조하십시오.

LDAP 인증

사용자 자격 증명을 LDAP(Lightweight Directory Access Protocol) 디렉토리 서버에 저장된 LDAP 디렉토리와 비교하여 검증하는 외부 인증 형식

LOM(Lights-Out-Management)

어플라이언스의 웹 인터페이스에 로그인하지 않고도 OOB(Out of Band) SOL(Serial over LAN) 관리 연결을 사용하여 어플라이언스를 원격으로 모니터링 또는 관리할 수 있는 Series 3 기능. 섀시 일련 번호를 확인하거나 팬 속도, 온도와 같은 조건을 모니터링하는 등의 제한적 작업을 수행할 수 있습니다.

NAT

사설 네트워크의 여러 호스트 사이에서 단일 인터넷 연결을 공유하기 위해 가장 일반적으로 사용되는 네트워크 주소 변환 기능. 검색을 사용하면 시스템에서 네트워크 디바이스를 논리적 인터페이스로 식별할 수 있습니다. 또한 FireSIGHT System의 레이어 3 구축에서 NAT을 사용하여 NAT 정책을 통한 라우팅을 구성할 수 있습니다.

NAT 정책

NAT 규칙을 사용하여 NAT를 통한 라우팅을 수행하는 정책

NetMod

해당 디바이스에 대한 디바이스가 포함된 관리되는 센싱 인터페이스의 섀시에 설치하는 모듈.

RADIUS 인증

RADIUS(Remote Authentication Dial In User Service)는 네트워크 리소스에 대한 사용자 액세스를 인증 및 승인하고 여기에 대응하는 데 사용되는 서비스입니다. FireSIGHT System 사용자가 RADIUS 서버를 통해 인증할 수 있도록 허용하는 외부 인증 객체를 만들 수 있습니다.

Series 2

Cisco 어플라이언스 모델의 두 번째 시리즈. 리소스, 아키텍처 및 라이센싱 제한으로 인해 Series 2 어플라이언스는 FireSIGHT System의 제한된 기능 집합을 지원합니다. Series 2 디바이스에는 3D500, 3D1000, 3D2000, 3D2100, 3D2500, 3D3500, 3D4500, 3D6500 및 3D9900이 포함됩니다. Series 2 방어 센터에는 DC500, DC1000 및 DC3000이 포함됩니다.

Series 3

Cisco 어플라이언스 모델의 세 번째 시리즈. Series 3 어플라이언스에는 7000 Series 및 8000 Series 디바이스와 DC750, DC1500, DC2000, DC3500, DC4000 방어 센터가 포함됩니다.

SFP 모듈

71xx 제품군 디바이스의 네트워크 모듈에 삽입된 소형 폼팩터 플러그형 트렌시버. SFP 모듈의 센싱 인터페이스는 구성 가능한 바이패스를 허용하지 않습니다.

URL 범주

악성코드 또는 소셜 네트워킹과 같은 URL의 일반 분류

URL 필터링

모니터링되는 호스트에서 요청하고 해당 URL에 대한 URL 평판 정보(액세스 제어 규칙가 URL 범주에서 얻음)와 Cisco 클라우드의 상관 관계를 분석한 URL을 기준으로 네트워크를 이동할 수 있는 트래픽을 결정하는 방어 센터를 작성할 수 있는 기능. 또한 허용하거나 차단할 개별 URL 또는 URL 그룹을 지정하여 웹 트래픽에서 더욱 세분화된 맞춤 제어를 달성할 수 있습니다.

URL 필터링 라이센스

URL 필터링 및 URL 평판 정보를 기준으로 URL 범주를 수행할 수 있도록 하는 라이센스. URL 필터링 라이센스는 만료될 수 있습니다.

UTC 시간

협정 세계시. GMT(Greenwich Mean Time)라고도 하며 전 세계 모든 위치에서 공통적인 표준시입니다. 표준 시간대 기능을 사용하여 로컬 시간을 설정할 수 있지만 FireSIGHT System에서는 UTC를 사용합니다.

VDB

취약성 데이터베이스를 참조하십시오.

VLAN

가상 LAN(Local Area Network). VLAN은 지리적 위치가 아닌 부문 또는 기본 용도와 같이 몇 가지 다른 기준으로 호스트를 매핑합니다. 모니터링되는 호스트의 호스트 프로필에는 호스트와 관련된 VLAN 정보가 표시됩니다. VLAN 정보도 이벤트를 트리거한 패킷의 가장 안쪽에 있는 VLAN 태그로 침입 이벤트에 포함됩니다. VLAN을 기준으로 침입 정책을 필터링하고 VLAN을 기준으로 대상 준수 화이트리스트를 정할 수 있습니다. 레이어 2 및 레이어 3 구축의 경우 관리되는 가상 스위치의 가상 라우터 및 디바이스가 VLAN 태그가 포함된 트래픽을 적절히 처리하도록 구성할 수 있습니다.

VPN

Cisco VPN의 가상 라우터 사이 또는 관리되는 디바이스에서 원격 디바이스 또는 기타 서드파티 VPN 관리되는 디바이스로 안전한 엔드포인트 터널을 구축할 수 있는 기능.

VPN 라이센스

Cisco VPN의 가상 라우터 사이 또는 관리되는 디바이스에서 원격 디바이스 또는 기타 서드파티 VPN 관리되는 디바이스로 안전한 엔드포인트 터널을 구축할 수 있도록 하는 라이센스.

VRT

Cisco VRT를 참조하십시오.

가상 디바이스

가상 호스팅 환경에서 자체 장비에 구축할 수 있는 관리되는 디바이스. 가상 디바이스를 가상 스위치 또는 가상 라우터로 구성할 수 없습니다.

가상 라우터

레이어 3 트래픽을 라우팅하는 라우팅 인터페이스의 그룹. 레이어 3 구축에서 대상 IP 주소에 따라 패킷 전달을 결정함으로써 가상 라우터에서 패킷을 라우팅하도록 구성할 수 있습니다. 정적 경로를 정의하고 RIP(Routing Information Protocol) 및 OSPF(Open Shortest Path First) 동적 라우팅 프로토콜을 구성하며 NAT(Network Address Translation)를 구현할 수 있습니다.

가상 방어 센터

가상 호스팅 환경에서 자체 장비에 구축할 수 있는 방어 센터

가상 스위치

네트워크에서 인바운드 및 아웃바운드 트래픽을 처리하는 스위치 인터페이스 그룹. 레이어 2 구축에서 네트워크를 논리적 세그먼트로 분할하여 관리되는 디바이스의 가상 스위치가 독립형 브로드캐스트 도메인으로 작동하도록 구성할 수 있습니다. 가상 스위치에서는 호스트의 MAC(Media Access Control) 주소를 사용하여 패킷을 보낼 대상을 결정합니다.

가져오기

어플라이언스에서 어플라이언스로 다양한 컨피그레이션을 전달하는 데 사용할 수 있는 방법. 이전에 동일한 유형의 다른 어플라이언스에서 내보낸 컨피그레이션을 가져올 수 있습니다.

검색

관리되는 디바이스를 사용하여 네트워크를 모니터링하고 네트워크에 대해 완전하고 지속적인 보기를 제공하는 FireSIGHT System의 구성 요소. 네트워크 검색을 통해 네트워크에 있는 호스트(네트워크 디바이스 및 모바일 디바이스 포함)의 수와 유형, 운영 체제, 활성 애플리케이션 및 해당 포트에서 개방된 포트에 대한 정보를 확인합니다. 또한 네트워크의 사용자 활동을 모니터링하도록 Cisco 관리되는 디바이스를 구성하여 정책 위반, 공격 또는 네트워크 취약성을 식별할 수 있습니다.

검색 정책

네트워크 검색 정책을 참조하십시오.

경고

시스템에서 특정 이벤트 를 생성했다는 알림. 침입 이벤트(해당 영향 플래그 포함), 검색 이벤트, 악성코드 이벤트, 상관 관계 정책 위반, 상태 변경, 특정 연결에서 로깅하는 액세스 제어 규칙을 기준으로 경고를 표시할 수 있습니다. 대부분의 경우 이메일, syslog 또는 SNMP 트랩을 통해 경보를 표시할 수 있습니다.

고가용성

이중화 물리적 방어 센터를 구성하여 디바이스 그룹을 관리하는 기능. 이벤트 데이터는 관리되는 디바이스에서 두 방어 센터로 스트리밍되며 대부분의 컨피그레이션 요소가 두 방어 센터에서 유지됩니다. 기본 방어 센터에 장애가 발생할 경우 보조 방어 센터를 사용하여 중단 없이 네트워크를 모니터링할 수 있습니다. 이중화 디바이스를 지정할 수 있는 클러스터링과 비교하십시오.

고급 설정

계속하려면 특정 전문 지식이 필요한 프리프로세서 또는 침입 정책. 고급 설정은 일반적으로 거의 또는 전혀 수정할 필요가 없으며 모든 구축에서 공통적으로 적용하지 않습니다.

관리 인터페이스

FireSIGHT System 어플라이언스를 관리하는 데 사용하는 네트워크 인터페이스. 부분의 구축에서 관리 인터페이스는 내부 보호된 네트워크에 연결되어 있습니다. 센싱 인터페이스와 비교해 보십시오.

관리 트래픽 채널

트래픽 채널을 참조하십시오.

관리되는 디바이스

디바이스를 참조하십시오.

구성 가능한 바이패스

인라인 세트를 구성할 수 있는 바이패스 모드의 특성

규칙

일반적으로 정책 내에서 네트워크 트래픽이 검사되는 기준을 제공하는 구문

규칙 동작

시스템이 규칙 조건을 충족하는 네트워크 트래픽을 처리하는 방식을 결정하는 설정. 액세스 제어 규칙 및 파일 규칙 동작을 참조하십시오.

규칙 상태

침입 규칙이 침입 정책 내에서 활성화(Generate Events(이벤트 생성) 또는 Drop and Generate Events(이벤트 삭제 및 생성)로 설정됨) 또는 비활성화(Disable(비활성화)로 설정됨)되었는지를 나타냅니다. 규칙을 활성화할 경우 네트워크 트래픽을 평가하는 데 사용되며 규칙을 비활성화할 경우 사용되지 않습니다.

규칙 업데이트

필요에 따라 업데이트되고 업데이트되었거나 새로운 표준 텍스트 규칙, 공유 객체 규칙 및 프리프로세서 규칙을 포함하는 침입 규칙 업데이트. 규칙 업데이트는 규칙을 삭제하거나 기본 침입 정책 설정을 수정하거나 시스템 변수 및 규칙 범주를 추가 또는 삭제할 수 있습니다.

기본 동작

액세스 제어 정책의 일부로 정책의 어떤 규칙 조건도 충족하지 않는 트래픽을 처리하는 방법을 결정합니다. 적용 또는 액세스 제어 규칙 설정이 포함되지 않은 액세스 제어 정책을 보안 인텔리전스할 경우 기본 정책 동작에 따라 네트워크에서 빠른 경로가 아닌 트래픽의 처리 방법이 결정됩니다. 추가 검사 없이 트래픽을 차단 또는 신뢰하거나 네트워크 검색 정책 또는 침입 정책을 사용하여 검사하는 기본 동작을 설정할 수 있습니다.

네트워크 검색

검색을 참조하십시오.

네트워크 검색 정책

정책 지원 디바이스에서 모니터링되는 네트워크를 포함하여, 시스템이 특정 네트워크 세그먼트에 대해 수집하는 검색 정책의 유형(호스트, 사용자, 애플리케이션 데이터 포함)을 지정하는 NetMod. 네트워크 검색 정책은 가져오기 해상도 기본 설정과 활성 탐지 소스 우선순위도 관리합니다.

네트워크 디바이스

FireSIGHT System에서 브리지, 호스트, 라우터 디바이스 또는 NAT로 식별되는 논리적 인터페이스

네트워크 맵

네트워크의 자세한 표시. 네트워크 맵을 사용하면 네트워크에서 실행되고 있는 호스트, 모바일 디바이스, 네트워크 디바이스뿐만 아니라 관련 호스트 특성, 애플리케이션 프로토콜, 취약성 측면에서 네트워크 토폴로지를 볼 수 있습니다.

네트워크 파일 경로

호스트가 네트워크에서 파일을 전송하는 경로의 시각적 표시. 전파 흔적 분석 맵은 관련 SHA256 해시값이 있는 파일에 대해 파일을 전송한 모든 호스트의 IP 주소, 파일이 감지된 시간, 파일의 악성코드 특성, 관련 파일 이벤트, 악성코드 이벤트 등을 표시합니다.

논리적 인터페이스

태그가 지정된 트래픽이 VLAN를 통과할 때 특정 물리적 인터페이스 태그가 포함된 트래픽을 처리하도록 정의하는 가상 하위 인터페이스

대시보드

시스템에서 수집 및 생성하는 이벤트에 대한 데이터를 포함하여 현재 시스템 상태를 간략하게 보여주는 디스플레이. 시스템에 기본 제공되는 대시보드를 보강하기 위해 사용자가 선택하는 대시보드 위젯으로 채워지는 여러 사용자 정의 대시보드를 만들 수 있습니다. 모니터링하는 네트워크의 모습과 동작을 광범위하고 개략적인 컬러 그림으로 보여주는 Context Explorer와 비교해 보십시오.

대시보드 위젯

FireSIGHT System의 측면에 대한 통찰력을 제공하는 작은 자체 포함 대시보드 구성 요소

데이터베이스 액세스

서드파티 클라이언트의 방어 센터 데이터베이스에 대한 읽기 전용 액세스를 허용하는 기능

디바이스

다양한 처리량을 제공하는 맞춤형 폴트 톨러런트(fault-tolerant) 어플라이언스. 디바이스에서 활성화하는 라이센스가 부여된 기능에 따라, 트래픽을 수동으로 모니터링하는 데 사용하여 네트워크 자산, 애플리케이션 트래픽, 사용자 활동에 대한 포괄적 맵을 구축하고 침입 탐지 및 방지 및 액세스 제어를 수행하고 스위칭 및 라우팅을 구성할 수 있습니다. 방어 센터를 사용하여 디바이스를 관리해야 합니다.

디바이스 스태킹

스태킹을 참조하십시오.

디바이스 클러스터링

클러스터링을 참조하십시오.

디코더

유입 패킷을 침입 탐지 및 방지가 이해할 수 있는 형식으로 변환하는 프리프로세서의 구성 요소

라우터

게이트웨이에 위치하며 네트워크 사이에서 패킷을 전달하는 네트워크 디바이스. 시스템에서는 네트워크 검색을 사용하여 라우터를 식별할 수 있습니다. 또한 관리되는 디바이스를 두 개 이상의 인터페이스 간 트래픽을 라우팅하는 가상 라우터로 구성할 수 있습니다.

라우팅 인터페이스

레이어 3 구축에서 트래픽을 라우팅하는 인터페이스. 태그가 지정되지 않은 VLAN 트래픽을 처리하기 위한 물리적 라우팅 인터페이스와 지정된 VLAN 태그가 포함된 트래픽을 처리하기 위한 논리적 라우팅 인터페이스를 설정할 수 있습니다. 또한 라우팅 인터페이스에 정적 ARP(Address Resolution Protocol) 항목을 추가할 수 있습니다.

레이어

침입 규칙 내 프리프로세서 규칙, 고급 설정, 침입 정책 컨피그레이션의 전체 집합. 사용자 정의 레이어를 기본 내장 레이어 또는 정책의 레이어에 추가할 수 있습니다. 침입 정책에서 더 높은 레이어의 설정이 더 낮은 레이어의 설정을 재정의합니다.

링크 상태 전파

바이패스 모드에서 인라인 세트의 인터페이스 중 하나에 장애가 발생할 경우 페어의 두 번째 인터페이스를 자동으로 비활성화하는 인라인 세트 옵션. 장애가 발생한 인터페이스가 복원되면 두 번째 인터페이스도 자동으로 활성화됩니다. 다시 말해, 쌍으로 연결된 인터페이스의 링크 상태가 변경되면 다른 인터페이스의 링크 상태도 이에 맞게 자동으로 변경됩니다.

명령행 인터페이스

Series 3 및 가상 디바이스의 제한적 텍스트 기반 인터페이스. CLI 사용자가 실행할 수 있는 명령은 사용자에게 할당된 액세스 수준에 따라 다릅니다.

모니터

액세스 제어 정책에서 보안 인텔리전스 블랙리스트 또는 액세스 제어 규칙과 일치하지만 시스템에서 트래픽을 즉시 허용하거나 차단하지 않고 계속해서 트래픽을 평가하도록 허용하는 트래픽 로깅 방법.

모바일 디바이스

FireSIGHT System에서 호스트 기능이 모바일 핸드헬드 디바이스로 식별한 검색(예: 휴대전화 또는 태블릿). 흔히 시스템에서 모바일 디바이스가 탈옥 상태인지 여부를 감지할 수 있습니다.

목록

보안 인텔리전스 목록을 참조하십시오.

물리적 인터페이스

NetMod에서 물리적 포트를 나타내는 인터페이스.

바이패스 모드

세트의 인라인 세트가 어떤 이유로든 실패하는 경우 트래픽이 계속 이동하도록 하는 센싱 인터페이스의 특성.

방어 센터

디바이스를 관리하고 여기에서 생성하는 이벤트를 자동으로 집계하고 상관 관계를 분석할 수 있는 중앙 관리 지점.

보안 영역

다양한 정책과 컨피그레이션에서 트래픽 흐름을 관리 및 분류하는 데 사용할 수 있는 하나 이상의 인라인, 수동, 스위치 또는 라우팅 인터페이스의 그룹. 단일 영역의 인터페이스를 여러 디바이스에서 사용할 수 있으며 복수 보안 영역을 단일 디바이스에 구성할 수도 있습니다. 보안 영역에서 트래픽을 처리하기 전에 인터페이스를 구성하여 해당 보안 영역에 할당해야 하며, 각 인터페이스는 하나의 보안 영역에만 속할 수 있습니다.

보안 인텔리전스

소스 또는 대상 IP 주소를 기준으로 액세스 제어 정책에 따라 네트워크를 이동할 수 있는 트래픽을 지정하도록 하는 기능. 이 기능은 액세스 제어 규칙에서 트래픽을 분석하기 전에 특정 IP 주소 사이에서 이동하는 트래픽을 블랙리스트에 추가(거부)하려는 경우에 특히 유용합니다. 선택적으로, 보안 인텔리전스 필터링에 대한 모니터 설정을 사용하면 시스템이 블랙리스트에 추가된 연결을 분석하고 일치 항목을 블랙리스트에 로깅할 수 있습니다.

보안 인텔리전스 목록

보안 인텔리전스 객체로 방어 센터에 수동으로 업로드하는 IP 주소의 단순한 정적 컬렉션. 이 목록을 사용하여 보안 인텔리전스 피드, 글로벌 블랙리스트, 글로벌 화이트리스트를 보강 및 세부 조정합니다.

보안 인텔리전스 피드

보안 인텔리전스 객체 유형 중 하나이며, 사용자가 구성하는 간격에 따라 시스템에서 정기적으로 다운로드하는 IP 주소의 동적 컬렉션. 피드는 정기적으로 업데이트되므로 피드를 사용할 경우 시스템에서 최신 정보를 바탕으로 보안 인텔리전스 기능을 사용하여 네트워크 트래픽을 필터링합니다. Cisco 인텔리전스 피드도 참조하십시오.

보안 정책

네트워크를 보호하기 위한 조직의 지침. 예를 들어, 보안 정책에서는 무선 액세스 포인트의 사용을 금지할 수 있습니다. 보안 정책에는 직원에게 조직 시스템을 사용할 수 있는 방법의 지침을 제공하는 AUP(Acceptable Use Policy)도 포함됩니다.

보안 정책 위반

네트워크의 보안 침입, 공격, 공격용 악성코드 또는 기타 오용.

보호 라이센스

Series 3, 가상 디바이스 및 침입 탐지 및 방지 필터링을 수행할 수 있는 파일 제어 및 보안 인텔리전스의 라이센스. 라이센스가 없을 경우 Series 2 디바이스가 보안 인텔리전스를 제외한 보호 기능을 자동으로 갖춥니다.

보호된 네트워크

방화벽과 같은 디바이스로 인해 다른 네트워크의 사용자로부터 보호되는 조직 내부 네트워크. FireSIGHT System에 기본 제공되는 대부분의 침입 규칙에서는 변수를 사용하여 보호된 네트워크와 보호되지 않는(또는 외부) 네트워크를 정의합니다.

복수 관리 인터페이스

트래픽을 트래픽 채널로 분리하여 성능을 개선하거나 방어 센터에서 다른 네트워크의 트래픽을 격리할 수 있도록 추가 네트워크에 대한 경로를 만들도록 구성할 수 있는 Series 3 어플라이언스의 추가 관리 인터페이스. 또한 트래픽 채널을 별도의 네트워크로 라우팅하여 처리량을 늘릴 수 있습니다. 관리 인터페이스를 참조하십시오.

비 바이패스 모드

인라인 세트의 인라인 세트에 어떤 이유로 장애가 발생할 경우 트래픽을 차단하는 센싱 인터페이스 특성

빠른 경로 규칙

제한된 기준 집합을 사용하여 규칙의 하드웨어 수준에서 구성하여 분석하지 않아도 되는 트래픽이 처리를 바이패스하도록 하는 디바이스

사용자

네트워크 활동이 관리되는 디바이스 또는 사용자 에이전트에서 감지되는 사용자

사용자 에이전트

네트워크에 로그인하거나 다른 이유로 Active Directory 자격 증명에 대해 인증할 때 사용자를 모니터링하기 위해 서버에 설치하는 에이전트. 액세스가 제어되는 사용자의 사용자 활동은 사용자 에이전트에서 보고할 경우에만 액세스 제어에 사용됩니다.

사용자 역할

FireSIGHT System의 사용자에게 부여된 액세스 수준. 예를 들어, 이벤트 분석가, FireSIGHT System 관리자, 서드파티 툴을 사용하여 방어 센터 데이터베이스에 액세스하는 사용자 등에게 웹 인터페이스에 대한 다른 액세스 권한을 부여할 수 있습니다. 또한 특수 액세스 권한이 있는 사용자 정의 역할을 만들 수도 있습니다.

사용자 인식

조직이 위협, 엔드포인트, 네트워크 인텔리전스와 사용자 ID 정보의 상관 관계를 분석하고 사용자 제어를 수행할 수 있는 기능

사용자 정의 사용자 역할

특별한 액세스 권한이 있는 사용자 역할. 사용자 정의 사용자 역할은 임의의 메뉴 기반 및 시스템 권한 집합을 보유할 수 있으며 사전 정의된 사용자 역할을 원래 그대로 유지하거나 이를 기준으로 변경할 수 있습니다.

사용자 제어

액세스 제어의 일환으로, 네트워크를 들어오고 나가거나 네트워크 안에서 이동할 수 있는 사용자 관련 트래픽을 지정 및 로깅할 수 있는 기능

사용자 활동

시스템이 사용자 로그인(선택적으로, 일부 실패한 로그인 시도 포함)을 감지하거나 이벤트 데이터베이스에서 사용자 레코드의 추가 또는 삭제를 감지할 경우 생성되는 방어 센터

상관 관계

네트워크 위협에 실시간으로 대응하는 상관 관계 정책을 구축하는 데 사용할 수 있는 기능. 상관 관계의 위협 요소 제거 구성 요소는 정책 위반에 대응하는 사용자 정의 위협 요소 제거 모듈을 생성하고 업로드할 수 있는 유연한 API를 제공합니다.

상태 모니터

구축 과정에서 지속적으로 어플라이언스의 성능을 모니터링하는 기능. 상태 모니터는 적용된 상태 모듈 내의 상태 정책을 사용하여 어플라이언스를 테스트합니다.

상태 모듈

구축에서 어플라이언스의 특정 성능 부문(예: CPU 사용량 또는 사용 가능한 디스크 공간)에 대한 테스트. 상태 모듈은 상태 정책에서 활성화하며 모니터링하는 성능 측면이 특정 수준에 도달하면 상태 이벤트를 생성합니다.

상태 정책

구축에서 어플라이언스의 상태를 확인할 때 사용되는 기준. 상태 정책은 상태 모듈을 사용하여 FireSIGHT System 하드웨어 및 소프트웨어가 올바르게 작동하는지 여부를 나타냅니다. 기본 상태 정책을 사용하거나 직접 만들 수 있습니다.

서버

애플리케이션 트래픽으로 식별되는 클라이언트 애플리케이션에 설치된 서버 호스트(애플리케이션 프로토콜과 비교)

센싱 인터페이스

네트워크 세그먼트를 모니터링하는 데 사용하는 디바이스의 네트워크 인터페이스. 관리 인터페이스와 비교해 보십시오.

수동 인터페이스

수동 구축의 트래픽을 분석하도록 구성된 센싱 인터페이스

수동 탐지

관리되는 검색 정책에서 수동적으로 수집되는 트래픽의 분석을 통한 디바이스의 컬렉션. 활성 탐지와 비교해 보십시오.

스위치

다중 포트 브리지 역할을 하는 네트워크 디바이스. 시스템에서는 네트워크 검색을 사용하여 스위치를 브리지로 식별합니다. 또한 관리되는 디바이스를 가상 스위치로 구성하여 2개 이상의 네트워크 사이에서 패킷 스위칭을 수행할 수 있습니다.

스위치 인터페이스

레이어 2 구축에서 트래픽을 전환하는 데 사용할 인터페이스. 태그가 지정되지 않은 VLAN 트래픽을 처리하기 위한 물리적 스위치 인터페이스와 지정된 VLAN 태그가 포함된 트래픽을 처리하기 위한 논리적 스위치 인터페이스를 설정할 수 있습니다.

스태킹

2~4개의 물리적 디바이스를 스태킹 컨피그레이션으로 연결하여 네트워크 세그먼트에서 검사하는 트래픽의 양을 늘릴 수 있는 기능. 스태킹된 컨피그레이션을 구축하면 각 스태킹된 디바이스의 리소스를 공유된 단일 컨피그레이션으로 결합합니다.

스택

탐지 리소스를 공유하는 2~4개의 연결된 디바이스

시스템 정책

메일 릴레이 호스트 기본 설정, 시간 동기화 설정과 같이 구축에서 여러 어플라이언스에 대해 일반적으로 유사한 설정. 방어 센터를 사용하여 방어 센터 자체와 관리되는 적용에 시스템 정책을 디바이스합니다.

악성코드 라이센스

네트워크 트래픽에서 AMP(AMP(Advanced Malware Protection))를 수행할 수 있도록 하는 라이센스. 파일 정책을 사용하면 관리되는 악성코드 클라우드 조회에서 감지된 특정 파일 유형에서 디바이스를 수행하도록 시스템을 구성할 수 있습니다. FireAMP 서브스크립션과 비교해 보십시오.

악성코드 방지

AMP(Advanced Malware Protection)을 참조하십시오.

악성코드 이벤트

Cisco의 이벤트 솔루션 중 하나에서 생성되는 AMP(Advanced Malware Protection). Cisco 클라우드에서 네트워크 트래픽에서 감지된 파일의 악성코드 특성을 반환하면 네트워크 기반 악성코드 이벤트가 생성되고, 해당 특성이 변경되면 소급적 악성코드 이벤트가 생성됩니다. 구축된 엔드포인트에서 위협을 감지하고 악성코드 실행을 차단하거나 악성코드를 격리 또는 격리에 실패할 경우 생성되는 FireAMP 커넥터 기반 악성코드 이벤트와 비교해 보십시오.

악성코드 차단

Cisco의 네트워크 기반 AMP(AMP(Advanced Malware Protection)) 솔루션의 구성 요소. 악성코드 탐지에서 감지된 파일에 대한 악성코드 특성을 확인하면 파일을 차단하거나 업로드 또는 다운로드를 허용할 수 있습니다. 이 기능을 FireAMP, Cisco의 엔드포인트 기반 AMP 툴(FireAMP 서브스크립션 필요)과 비교하십시오.

악성코드 클라우드 조회

방어 센터가 Cisco 클라우드와 통신하여 파일의 SHA256 해시값을 기준으로 네트워크 트래픽에서 감지된 파일의 악성코드 특성을 확인하는 프로세스.

악성코드 탐지

Cisco의 네트워크 기반 AMP(AMP(Advanced Malware Protection)) 솔루션의 구성 요소. 전반적인 디바이스 컨피그레이션 검사 네트워크 트래픽의 일부로 관리되는 액세스 제어에 적용되는 파일 정책. 그런 다음 방어 센터에서 감지된 특정 악성코드 클라우드 조회에 대해 파일 유형를 수행하고 파일의 악성코드 특성에 대해 경고하는 이벤트를 생성합니다. 이어서 AMP 악성코드 차단이 실행되고 파일을 차단하거나 업로드 또는 다운로드를 허용합니다. 이 기능을 FireAMP, Cisco의 엔드포인트 기반 AMP 툴(FireAMP 서브스크립션 필요)과 비교하십시오.

애플리케이션

액세스 제어 규칙을 작성할 수 있는 감지된 네트워크 자산, 통신 방법 또는 HTTP 콘텐츠. 시스템에서는 애플리케이션 프로토콜, 클라이언트 애플리케이션 및 웹 애플리케이션 등 세 가지 유형의 애플리케이션을 감지합니다.

애플리케이션 제어

액세스 제어의 일부로 네트워크를 이동할 수 있는 애플리케이션 트래픽을 지정할 수 있도록 하는 기능

애플리케이션 프로토콜

호스트의 서버 및 애플리케이션 애플리케이션 간 통신 중에 감지되는 애플리케이션 프로토콜 트래픽을 나타내는 클라이언트의 유형(예: SSH 또는 HTTP)

액세스 목록

시스템 정책에 구성되어 있고 호스트에 액세스할 수 있는 어플라이언스를 나타내는 IP 주소 목록. 기본적으로 누구나 포트 443(HTTPS)을 사용하여 어플라이언스의 웹 인터페이스에 액세스하고, 포트 22(SSH)를 사용하여 명령행에 액세스할 수 있습니다. 또한 포트 161을 사용하여 SNMP 액세스를 추가할 수 있습니다.

액세스 제어

네트워크를 이동할 수 있는 트래픽을 지정, 검사 및 로깅할 수 있는 FireSIGHT System의 기능. 액세스 제어에는 침입 탐지 및 방지, 파일 제어 및 AMP(Advanced Malware Protection) 기능이 포함되며, 이에 따라 검색 기능으로 검사할 수 있는 트래픽이 결정됩니다.

액세스 제어 규칙

FireSIGHT System에서 모니터링되는 네트워크 트래픽을 검사하고 세부적인 액세스 제어를 달성할 수 있는 조건의 집합. 액세스 제어 규칙은 액세스 제어 정책을 채우며 간단한 IP 주소 매칭을 수행하거나 다른 사용자, 연결, 포트 및 URL이 포함된 복잡한 애플리케이션의 특성을 파악할 수 있습니다. 액세스 제어 규칙 동작에 따라 시스템에서 규칙의 조건을 충족하는 트래픽을 처리하는 방법이 결정됩니다. 다른 규칙 설정은 연결이 로깅되는 방법과 로깅되는지 여부 및 침입 정책 또는 파일 정책에서 일치하는 트래픽을 검사하는지 여부를 결정합니다.

액세스 제어 정책

관리되는 정책가 모니터링하는 네트워크 트래픽에서 적용을 수행하기 위해 해당 디바이스에 디바이스하는 액세스 제어. 액세스 제어 정책에는 복수의 액세스 제어 규칙이 포함될 수 있으며, 해당 규칙의 기준을 충족하지 않는 트래픽에 대한 처리 및 기록을 결정하는 기본 동작도 지정합니다. 또한 액세스 제어 정책은 HTTP 응답 페이지, 보안 인텔리전스 및 기타 고급 설정을 지정할 수 있습니다.

어플라이언스

방어 센터 또는 관리되는 디바이스. 물리적 또는 가상 어플라이언스가 있습니다.

엔드포인트

사용자가 조직의 FireAMP 커넥터 전략의 일부로 AMP(Advanced Malware Protection)를 설치하는 컴퓨터 또는 모바일 디바이스

연결

두 호스트 사이에서 모니터링되는 세션. 디바이스의 관리되는 액세스 제어 정책에서 감지한 연결을 로깅할 수 있습니다. NetMod 연결 기록은 네트워크 검색 정책에서 구성합니다.

영역

보안 영역을 참조하십시오.

예약된 작업

한 번 또는 반복적으로 일정 간격마다 실행하도록 예약할 수 있는 관리 작업

웹 애플리케이션

HTTP 트래픽의 콘텐츠 또는 요청된 URL을 나타내는 애플리케이션의 유형

위젯

대시보드 위젯을 참조하십시오.

위치정보

연결 유형, 인터넷 서비스 제공자 등 모니터링되는 네트워크의 트래픽에서 감지된 라우팅 가능한 IP 주소의 지리적 소스에 대한 데이터를 제공하는 기능. 위치정보 데이터베이스, 연결 이벤트, 침입 이벤트, 파일 이벤트 및 악성코드 이벤트와 호스트 프로필에 저장된 위치정보를 볼 수 있습니다.

위치정보 데이터베이스

GeoDB라고도 하며, 라우팅 가능 IP 주소와 관련된 알려진 위치정보 데이터의 정기적으로 업데이트되는 데이터베이스.

위협 요소 제거

시스템에 대한 잠재적인 공격을 완화하는 작업. 위협 요소 제거를 구성하고 상관 관계 정책 내에서 이러한 요소와 상관 관계 규칙 및 규정준수 화이트리스트와 연결한 다음 트리거가 발생하면 방어 센터에서 위협 요소 제거를 시작할 수 있습니다. 이 기능은 문제를 즉시 해결할 수 없을 때 공격을 자동으로 완화할 뿐만 아니라 시스템이 조직의 보안 정책을 준수함을 보장할 수 있습니다. 방어 센터에는 사전 정의된 위협 요소 제거 모듈이 기본 제공되며 유연한 API를 사용하여 사용자 정의 위협 요소 제거를 만들 수 있습니다.

이벤트

워크플로를 사용하여 이벤트 뷰어에서 확인할 수 있는 특정 발생 상황에 대한 상세 정보의 컬렉션. 이벤트는 네트워크에서의 공격, 감지된 네트워크 자산의 변경 사항, 조직의 보안 및 네트워크 사용 정책 위반 등을 나타낼 수 있습니다. 시스템은 또한 어플라이언스의 변경되는 상태, 웹 인터페이스, 규칙 업데이트, 시작된 위협 요소 제거의 사용에 대한 정보를 포함하는 이벤트를 생성합니다. 마지막으로, 이러한 "이벤트"가 특정 발생 상황을 나타내지 않는 경우에도 시스템에서 기타 특정 정보를 이벤트로 표시합니다. 예를 들어, 이벤트 뷰어를 사용하여 감지된 호스트, 애플리케이션 및 해당 취약성에 대한 자세한 정보를 확인할 수 있습니다.

이벤트 뷰어

이벤트를 확인하고 조정할 수 있는 시스템 구성 요소. 이벤트 뷰어는 워크플로를 사용하여 광범위한 정보를 표시한 다음 관심이 있는 이벤트만 포함된 더욱 집중적인 이벤트 보기를 표시합니다. 워크플로를 드릴다운하거나 검색을 사용하여 이벤트 보기에 표시할 이벤트를 제한할 수 있습니다.

이벤트 트래픽 채널

트래픽 채널을 참조하십시오.

인라인 구축

관리되는 디바이스가 네트워크에서 인라인으로 배치되는 FireSIGHT System의 구축. 이 컨피그레이션에서는 디바이스가 스위칭, 라우팅, 액세스 제어 및 침입 탐지 및 방지를 사용하여 네트워크 트래픽 흐름에 영향을 미칠 수 있습니다.

인라인 세트

하나 이상의 인라인 인터페이스 쌍

인라인 인터페이스

센싱 인터페이스에서 트래픽을 처리하도록 구성된 인라인 구축. 인라인 인터페이스를 인라인 세트에 쌍으로 추가해야 합니다.

작업 대기열

어플라이언스에서 수행해야 하는 작업의 대기열. 적용을 정책하고 소프트웨어 업데이트를 설치한 후 기타 장기 실행 작업을 수행할 경우 작업이 대기열에 추가되고 Task Status(작업 상태) 페이지에 상태가 보고됩니다. Task Status(작업 상태) 페이지는 작업의 자세한 목록을 제공하고 10초마다 새로 고쳐져서 해당 상태를 업데이트합니다.

적용

정책 또는 해당 정책의 변경 사항이 유효하도록 하는 작업. 대부분의 정책은 방어 센터에서 관리되는 디바이스에 적용하지만, 상관 관계 정책은 관리되는 디바이스의 컨피그레이션 변경 사항이 포함되지 않으므로 사용자가 활성화 및 비활성화합니다.

정책

대부분 어플라이언스에 설정을 적용하기 위한 메커니즘. 액세스 제어 정책, 상관 관계 정책, 파일 정책, 상태 정책, 침입 정책, 네트워크 검색 정책 및 시스템 정책을 참조하십시오.

제어 라이센스

사용자와 사용자 제어 상태를 애플리케이션 제어에 추가하여 애플리케이션 및 액세스 제어 규칙를 구현할 수 있도록 하는 라이센스. 또한 이 라이센스를 통해 관리되는 디바이스가 스위칭 및 라우팅(DHCP 릴레이 및 NAT 포함)을 수행하도록 구성하고 관리되는 디바이스를 클러스터링할 수 있습니다.

취약성

호스트가 영향을 받기 쉬운 특정 감염에 대한 설명입니다. 방어 센터에서는 각 호스트가 취약해질 수 있는 취약성에 대한 정보를 해당 호스트의 호스트 프로필에 제공합니다. 또한 취약성 네트워크 맵을 사용하여 모니터링되는 전체 네트워크에서 감지된 취약성에 대한 전반적 정보를 볼 수 있습니다. 하나 이상의 호스트가 특정 감염에 대해 더 이상 취약하지 않다고 판단되면, 특정 취약성을 비활성화하거나 유효하지 않은 것으로 표시할 수 있습니다.

취약성 데이터베이스

VDB라고도 하며, 호스트가 영향을 받기 쉬운 알려진 취약성의 데이터베이스입니다. 시스템에서는 각 호스트에서 감지된 운영 체제, 애플리케이션 프로토콜 및 클라이언트와 VDB의 상관 관계를 분석하여 특정 호스트가 네트워크 감염 위험을 높이는지 여부를 판별합니다. VDB 업데이트에는 새 취약성 및 업데이트된 취약성과 새 애플리케이션 감지기 및 업데이트된 애플리케이션 감지기가 포함될 수 있습니다.

침입

네트워크에서 발생하는 보안 침입, 공격 또는 공격용 악성코드.

침입 규칙

모니터링되는 네트워크 트래픽에 적용할 경우 잠재적 침입, 보안 정책 위반 및 보안 침입을 식별하는 키워드와 인수의 집합. 시스템에서 규칙 조건과 패킷을 비교합니다. 패킷 데이터가 조건과 일치하면 규칙이 트리거되고 침입 이벤트가 생성됩니다. 침입 규칙에는 삭제 규칙과 통과 규칙이 포함됩니다.

침입 이벤트

이벤트 위반을 기록하는 침입 정책. 침입 이벤트 데이터에는 공격용 악성코드의 날짜, 시간, 유형과 공격 및 대상에 대한 기타 상황 정보가 포함됩니다.

침입 정책

네트워크 트래픽에서 침입 및 보안 정책 위반을 검사하기 위해 구성할 수 있는 다양한 구성 요소. 이러한 구성 요소에는 프로토콜 헤더 값, 페이로드 콘텐츠, 특정 패킷 크기 특성을 검사하는 침입 규칙, 침입 규칙에 일반적으로 사용되는 변수, FireSIGHT에서 권장하는 규칙 컨피그레이션, 고급 설정 및 기타 탐지 및 성능 기능과 같은 프리프로세서, 관련 프리프로세서 옵션에 대한 이벤트를 생성할 수 있는 프리프로세서 규칙이 있습니다. 네트워크 트래픽이 액세스 제어 규칙의 조건을 충족할 경우 침입 정책으로 해당 트래픽을 검사할 수 있습니다. 또한 침입 정책을 기본 동작과 연계할 수 있습니다.

침입 탐지 및 방지

네트워크 트래픽에서 보안 정책 위반을 모니터링하고 인라인 구축의 경우 악성 트래픽을 차단 또는 변경하는 기능. FireSIGHT System의 경우 침입 정책을 액세스 제어 규칙 또는 기본 동작과 연결할 때 침입 탐지 및 방지를 수행합니다.

컨텍스트 메뉴

웹 인터페이스의 많은 페이지에서 사용 가능하며 바로가기를 사용하여 FireSIGHT System의 다른 기능에 액세스할 수 있는 팝업 메뉴. 메뉴의 콘텐츠는 보고 있는 페이지, 조사 중인 특정 데이터, 사용자 역할 등의 여러 요소에 따라 다릅니다. 컨텍스트 메뉴 옵션에는 침입 규칙, 이벤트 및 호스트 정보에 대한 링크, 다양한 침입 규칙 설정, Context Explorer에 대한 빠른 링크, 호스트를 IP 주소별 보안 인텔리전스 글로벌 블랙리스트 또는 글로벌 화이트리스트에 추가하는 옵션, 파일을 SHA-256 해시값을 기준으로 글로벌 화이트리스트에 추가하는 옵션 등이 있습니다.

클라이언트

클라이언트 애플리케이션이라고도 하며, 한 애플리케이션에서 실행되고 다른 호스트(호스트)에 의존하여 일부 작업을 수행하는 서버. 예를 들어, 이메일 클라이언트를 사용하여 이메일을 전송 및 수신할 수 있습니다. 호스트의 사용자가 특정 클라이언트를 사용하여 다른 호스트에 액세스하는 것을 시스템에서 감지하면 클라이언트의 이름과 버전(확인 가능한 경우)을 포함하여 호스트 프로필 및 네트워크 맵에 있는 해당 정보를 보고합니다.

클라이언트 애플리케이션

클라이언트를 참조하십시오.

클러스터링

두 개의 피어 디바이스 Series 3 또는 스택 사이에서 네트워킹 기능 및 컨피그레이션 데이터의 이중화를 달성할 수 있는 기능. 클러스터링은 정책 적용, 시스템 업데이트 및 등록을 위한 하나의 논리적 시스템을 제공합니다. 이중화 고가용성을 구성할 수 있는 방어 센터와 비교하십시오.

탭 모드

트래픽을 인라인 세트로 통과시키지 않으면서 각 패킷의 복사본을 분석하고 네트워크 트래픽 흐름을 방해하지 않는 3D9900 및 Series 3 디바이스에서 사용 가능한 고급 디바이스 옵션. 패킷 자체가 아닌 패킷의 복사본으로 작업하므로 트래픽을 삭제, 수정, 차단하기 위한 액세스 제어 및 침입 정책을 구성하는 경우에도 디바이스가 패킷 스트림에 영향을 미칠 수 없습니다.

투명한 인라인 모드

트래픽의 소스 및 대상과 상관없이 인라인 세트가 "bump in the wire"의 역할을 하고 확인하는 모든 네트워크 트래픽을 전달하도록 하는 고급 디바이스 옵션

트래픽 채널

Series 3 어플라이언스 또는 가상 방어 센터의 관리 인터페이스에 구성하여 관리 또는 이벤트 트래픽을 운반하도록 구성할 수 있는 연결. 이벤트 트래픽 채널은 외부에서 생성된 트래픽(웹 브라우저 등)만 운반하며 관리 트래픽 채널은 내부에서 생성된 트래픽(즉, 방어 센터와 디바이스 간 관리 트래픽)만 운반합니다. 복수 관리 인터페이스를 참조하십시오.

파일 경로

네트워크 파일 경로를 참조하십시오.

파일 유형

PDF, EXE, MP3와 같은 특정 유형의 파일 형식

파일 정책

시스템에서 정책 및 파일 제어를 수행하기 위해 사용하는 AMP(Advanced Malware Protection). 파일 정책은 파일 규칙으로 채워지며 액세스 제어 규칙 내의 액세스 제어 정책에서 호출됩니다.

파일 제어

액세스 제어의 일부로 네트워크를 이동할 수 있는 파일의 유형을 지정 및 로깅할 수 있는 기능.

평판(IP 주소)

보안 인텔리전스를 참조하십시오.

표 보기

열마다 데이터베이스 테이블의 각 필드를 포함하여 이벤트 정보를 표시하는 워크플로 페이지의 유형. 이벤트 분석을 수행할 경우 관심 이벤트에 대한 상세 정보를 표시하는 표 보기로 이동하기 전에 드릴다운 페이지를 사용하여 조사하려는 이벤트만 포함할 수 있습니다. 표 보기는 시스템에 기본 제공되는 워크플로의 마지막에서 두 번째 페이지인 경우가 많습니다.

프리프로세서

침입 정책에서 검사한 트래픽을 정규화하고 부적절한 헤더 옵션 식별, IP 데이터그램 조각 모으기, 상태 정보를 저장하는 TCP 검사 및 스트림 어셈블리 제공, 체크섬 검증을 통해 네트워크 계층 및 전송 계층 프로토콜 이상 현상을 식별하는 기능. 또한 프리프로세서는 시스템에서 분석할 수 있는 형식으로 특정 유형의 패킷 데이터를 렌더링합니다. 이러한 프리프로세서를 데이터 정규화 프리프로세서 또는 애플리케이션 레이어 프로토콜 프리프로세서라고 합니다. 애플리케이션 레이어 프로토콜 인코딩을 정규화하면 시스템에서 데이터가 다르게 표현된 패킷에 동일한 콘텐츠 관련 침입 규칙을 효과적으로 적용하고 의미 있는 결과를 얻을 수 있습니다. 패킷이 사용자가 구성하는 프리프로세서 옵션을 트리거할 때마다 프리프로세서에서 프리프로세서 규칙을 생성합니다.

프리프로세서 규칙

침입 규칙 또는 포트 스캔 흐름 감지기와 관련된 프리프로세서. 프리프로세서 규칙에서 이벤트를 생성하도록 하려면 해당 규칙을 활성화해야 합니다. 프리프로세서 규칙에는 프리프로세서별 GID(Generator ID)가 있습니다.

피드

보안 인텔리전스 피드를 참조하십시오.

하이브리드 인터페이스

시스템이 논리적 인터페이스와 디바이스 사이의 트래픽을 브리징할 수 있도록 하는 관리되는 가상 라우터의 가상 스위치

호스트

네트워크에 연결되고 고유한 IP 주소가 있는 디바이스. FireSIGHT System에 대해, 호스트는 모바일 디바이스, 라우터, 브리지, NAT 디바이스 또는 논리적 인터페이스로 분류되지 않은 식별된 모든 호스트입니다.

호스트 입력

스크립트 또는 명령행 파일을 사용하여 서드파티 소스에서 데이터를 가져오기하여 네트워크 맵의 정보를 확장할 수 있는 기능. 또한 웹 인터페이스는 몇 가지 호스트 입력 기능을 제공합니다. 운영 체제 또는 애플리케이션 프로토콜 ID를 수정하거나 취약성을 식별, 검증 또는 무효화하며 클라이언트 및 서버 포트를 포함한 네트워크 맵에서 다양한 항목을 삭제할 수 있습니다.