Cisco Secure Network Analytics

x2xx 시리즈 하드웨어 어플라이언스 설치 설명서 7.4.1

목차

소개

개요

이 가이드에서는 Cisco Secure Network Analytics(이전 명칭 Stealthwatch) x2xx 시리즈 하드웨어 어플라이언스를 설치하는 방법을 설명합니다. 이 가이드는 또한 Secure Network Analytics 하드웨어의 장착 및 설치에 대해 설명합니다.

> ⚠ Secure Network Analytics x2xx 시리즈 어플라이언스를 설치하기 전 규정 및 컴플라이언스 및 안전 정보 문서를 읽어보십시오.

x2xx 시리즈의 하드웨어에는 다음이 포함됩니다.

어플라이언스	부품 번호
매니저 2210 (이전 명칭 Stealthwatch Management Console)	ST-SMC2210-K9
데이터스토어 6200 (데이터 노드 3개)	ST-DS6200-K9(ST-DNODE-G1 3개)
Flow Collector 4210	ST-FC4210-K9
Flow Collector 5210 엔진	ST-FC5210-E
Flow Collector 5210 데이터베이스	ST-FC5210-D
UDP Director 2210	ST-UDP2210-K9
Flow Sensor 1210	ST-FS1210-K9
Flow Sensor 3210	ST-FS3210-K9
Flow Sensor 4240	ST-FS4210-K9

대상

이 가이드는 Secure Network Analytics 하드웨어 설치 담당자를 위해 제작되었습니다. 사용자에게 네트워크 장비 설치에 대한 일반적인 이해가 이미 있는 것으로 가정합니다.

전문 설치자의 도움을 받길 원하는 경우 로컬 Cisco 파트너 또는 Cisco 지원팀에 문의하십시오.

어플라이언스 설치 및 시스템 구성

Secure Network Analytics 설치 및 구성에 대한 전체 워크플로를 참조하십시오.

1. **어플라이언스 설치**: 이 설치 가이드를 사용하여 Secure Network Analytics x2xx 시리즈 하드웨어(물리적) 어플라이언스를 설치합니다. 가상 버전 어플라이언스를 설치하려면 가상 버전 설치 가이드의 지침을 따르십시오.
2. **Secure Network Analytics 구성:** 하드웨어 및 가상 어플라이언스를 설치한 후에는 관리되는 시스템에서 Secure Network Analytics를 구성할 수 있습니다. Secure Network Analytics 시스템 구성 가이드 v7.4.1의 지침을 따르십시오.

관련 정보

Secure Network Analytics에 대한 자세한 내용은 다음 온라인 리소스를 참조하십시오.

- **규정 및 컴플라이언스 정보:** Secure Network Analytics x2xx 시리즈 어플라이언스를 설치하기 전 규정 및 컴플라이언스 및 안전 정보 문서를 읽어보십시오.
- **개요:** https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html
- **데이터 저장소 설계 가이드:** https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/stealthwatch-data-store-guide.pdf
- **하드웨어 및 소프트웨어 버전 지원 매트릭스:** https://www.cisco.com/c/en/us/support/security/stealthwatch/products-device-support-tables-list.html
- **어플라이언스 사양:** https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html

용어

이 가이드에서는 모든 Secure Network Analytics 제품에 대해 "**어플라이언스**"라는 용어를 사용합니다.

"**클러스터**"는 매니저에서 관리하는 Secure Network Analytics 어플라이언스의 그룹입니다.

일반 약어

이 가이드에 나오는 약어는 다음과 같습니다.

약어	설명
DMZ	비무장지대(경계 네트워크)
HTTPS	Hypertext Transfer Protocol(Secure)
ISE	Identity Services Engine
NIC	Network Interface Card(네트워크 인터페이스 카드)
NTP	Network Time Protocol(네트워크 타이밍 프로토콜)
PCIe	Peripheral Component Interconnect Express
SNMP	Simple Network Management Protocol
SPAN	스위치 포트 애널라이저
TAP	테스트 액세스 포트
UPS	무중단 전원 공급 장치
VLAN	Virtual Local Area Network

Secure Network Analytics 어플라이언스 정보

Secure Network Analytics 는 네트워크 성능 및 보안을 개선하기 위해 네트워크에 대한 정보를 수집, 분석 및 제공하는 여러 하드웨어 어플라이언스로 구성됩니다. 이 섹션에서는 각 Secure Network Analytics x2xx 시리즈 어플라이언스에 대해 설명합니다.

매니저 2210

매니저는 시스템의 다양한 구성 요소를 모두 관리, 조정, 구성 및 구성합니다. Secure Network Analytics 소프트웨어를 사용하면 웹 브라우저에 액세스할 수 있는 모든 컴퓨터에서 콘솔의 웹 UI에 액세스할 수 있습니다. 엔터프라이즈 전반의 중요한 세그먼트에 대한 실시간 보안 및 네트워크 정보에 쉽게 액세스할 수 있습니다. 자바 기반 플랫폼에 구애받지 않는 매니저에서는 다음 기능을 지원합니다.

- 최대 25개의 Secure Network Analytics 플로우 컬렉터에 대한 중앙 집중식 관리, 설정 및 보고
- 트래픽 시각화를 지원하는 그래픽 차트
- 문제 해결을 위한 드릴다운 분석
- 통합된 맞춤형 보고서
- 트렌드 분석
- 성능 모니터링
- 보안 침입 실시간 알림

데이터스토어를 구축하는 경우 증가된 처리량을 위한 eth0로서 10 Gbps SFP+DAC 인터페이스를 갖춘 매니저 2210을 구성할 수 있습니다. 데이터스토어를 구축하지 않은 경우 eth0로서 100Mbps/1Gbps/10Gbps 구리 인터페이스만 구성할 수 있습니다.

데이터스토어 6200

데이터스토어는 Flow Collector에서 수집한 네트워크의 텔레메트리를 저장할 중앙 저장소를 제공합니다. 데이터스토어는 각각 데이터의 일부를 포함하는 데이터 노드의 클러스터와 별도의 데이터 노드의 데이터 백업으로 구성됩니다. 모든 데이터가 하나의 중앙 집중식 데이터베이스에 있으므로 Flow Collector는 여러 매니저에 분산되어 있는 것과 달리 모든 데이터스토어를 개별적으로 쿼리하는 것보다 Flow Collector에서 쿼리 결과를 더 빠르게 검색할 수 있습니다. 데이터스토어 클러스터는 개선된 내결함성, 개선된 쿼리 응답, 더 빠른 그래프 및 차트 채우기를 제공합니다.

자세한 내용은 Secure Network Analytics 섹션을 참조하십시오.

플로우 컬렉터 4210 및 5210

플로우 컬렉터는 행동 기반 네트워크 보호를 제공하기 위해 NetFlow, cFlow, J-Flow, Packeteer 2, NetStream 및 IPFIX 데이터를 수집합니다.

Flow Collector는 엔드 투 엔드 보호를 제공하고 지리적으로 분산된 네트워크의 성능을 향상할 수 있도록 여러 네트워크 또는 네트워크 세그먼트에서 고속 네트워크 행동 데이터를 집계합니다.

데이터스토어를 구축하는 경우 증가된 처리량을 위한 eth0로서 10 Gbps SFP+DAC 인터페이스를 갖춘 플로우 컬렉터 4210을 구성할 수 있습니다. 데이터스토어를 구축하지 않은 경우 eth0로서 100Mbps/1Gbps/10Gbps 구리 인터페이스만 구성할 수 있습니다.

> Flow Collector는 데이터를 수신할 때 패킷 암호화 또는 프래그멘테이션과 관계없이 알려지거나 알려지지 않은 공격, 내부 오용 또는 잘못 구성된 네트워크 디바이스를 식별합니다. Secure Network Analytics가 행동을 식별하면 시스템은 그러한 행동 유형에 대해 구성한 작업이 있는 경우 해당 작업을 수행할 수 있습니다.

UDP Director 2210

UDP Director는 고속의 고성능 UDP 패킷 복제기입니다. UDP Director는 NetFlow, sFlow, syslog 또는 SNMP(Simple Network Management Protocol) 재배포에 매우 유용합니다. 연결되지 않은 UDP 애플리케이션에서 데이터를 수신한 다음, 이를 여러 대상에 다시 전송하고, 필요한 경우 데이터를 복제합니다.

UDP Director 고가용성(HA) 설정을 사용하는 경우 두 개의 UDP Director 어플라이언스를 크로스오버 케이블로 연결해야 합니다. 자세한 내용은 **2. 어플라이언스를 네트워크에 연결**을 참조해 주십시오.

플로우 센서 1210, 3210 및 4240

Flow Sensor는 SPAN(Switch Port Analyzer), 미러링 포트 또는 이더넷 TAP(Test Access Port)에 플러그인한다는 점에서 기존의 패킷 캡처 어플라이언스 또는 IDS와 유사하게 동작하는 네트워크 어플라이언스입니다. Flow Sensor는 다음의 네트워크 영역에 대한 가시성을 강화해 줍니다.

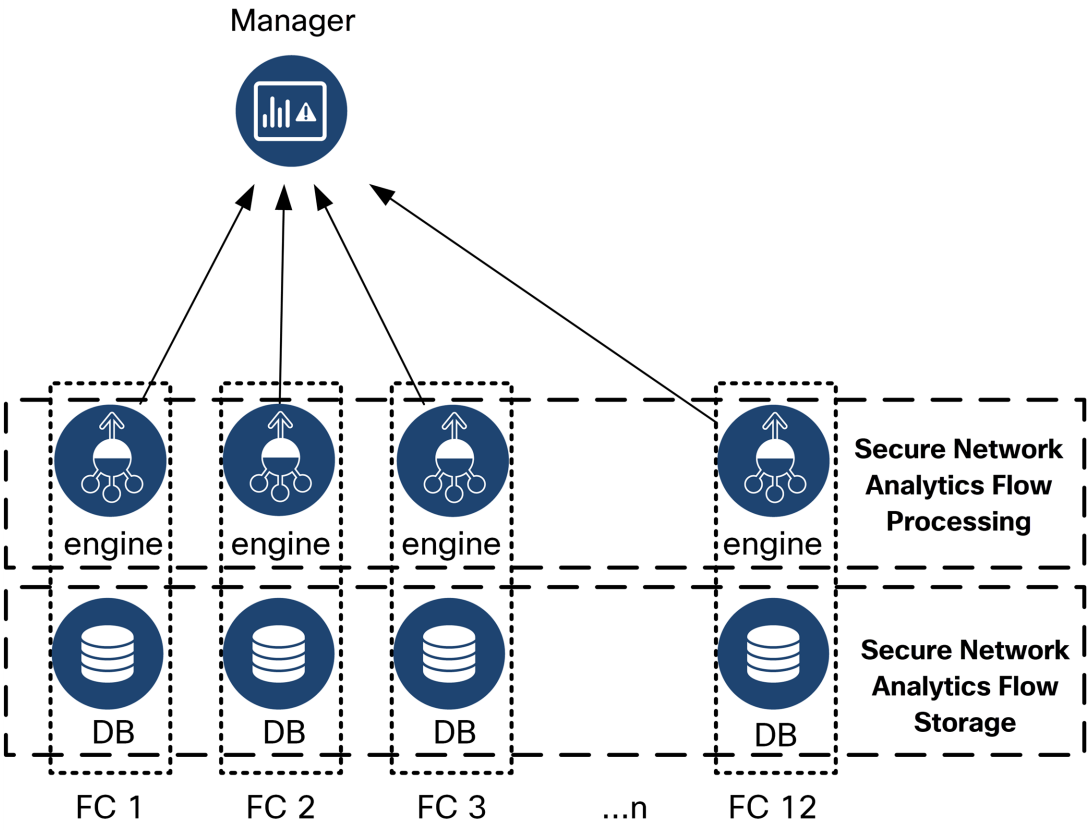
- NetFlow를 사용할 수 없는 경우.
- NetFlow를 사용할 수 있지만, 성능 메트릭 및 패킷 데이터에 대해 더욱 심층적인 가시성을 얻고자 하는 경우.

Flow Sensor를 NetFlow v9 지원 Flow Collector에 직접 연결함으로써 NetFlow에서 중요하고 자세한 트래픽 통계를 얻을 수 있습니다. 또한 Flow Sensor를 Secure Network Analytics 플로우 컬렉터와 함께 사용하면 성능 메트릭 및 행동 지표에 대한 상세 정보도 제공됩니다. 이러한 플로우 성능 지표는 네트워크 또는 서버 측 애플리케이션에서 시작된 모든 왕복 레이턴시에 대한 인사이트를 제공합니다.

Flow Sensor는 패킷 레벨 가시성을 제공하므로 TCP 세션에 대한 RTT(Round-Trip Time), SRT (Server Response Time) 및 패킷 손실을 계산할 수 있습니다. Flow Collector에 전송하는 NetFlow 레코드에 이러한 추가 필드가 모두 포함되어 있습니다.

Secure Network Analytics (데이터 저장소 없음)

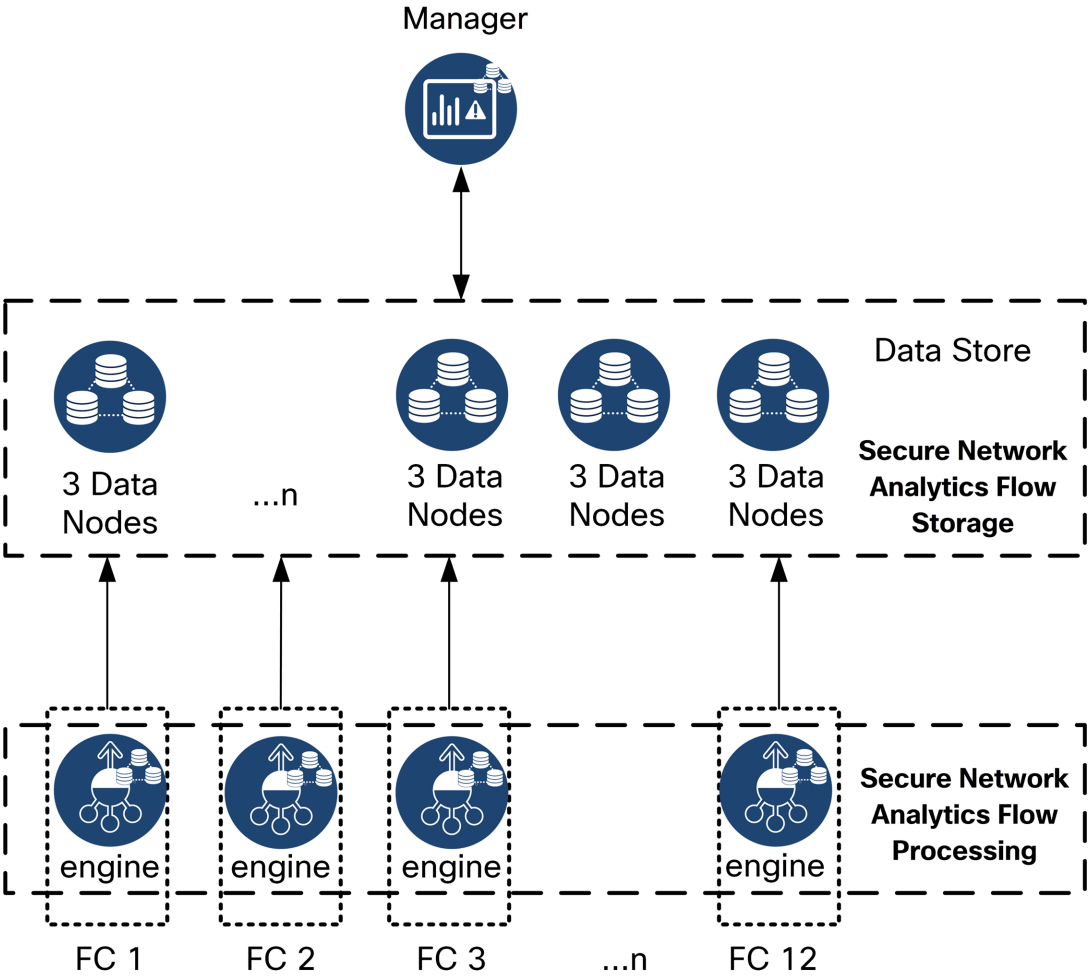
데이터스토어가 없는 Secure Network Analytics 구축에서는 하나 이상의 Flow Collector가 데이터를 수집 및 중복 제거하고 분석을 수행하며 데이터와 결과를 매니저에 직접 보고합니다. 매니저는 그래프 및 차트를 포함하여 사용자가 제출한 쿼리를 해결하기 위해 모든 관리되는 Flow Collector를 쿼리합니다. 각 Flow Collector는 일치하는 결과를 매니저에 반환합니다. 매니저는 서로 다른 결과 집합의 정보를 대조한 다음 결과를 표시하는 그래프 또는 차트를 생성합니다. 이 구축에서 각 Flow Collector는 로컬 데이터베이스에 데이터를 저장합니다. 다음 다이어그램의 예를 참조하십시오.



데이터 저장소가 있는

Secure Network Analytics

데이터스토어를 사용하는 Secure Network Analytics 구축에서는 데이터스토어 클러스터가 매니저와 플로우 컬렉터 사이에 있습니다. 하나 이상의 플로우 컬렉터가 플로우를 수집 및 중복 제거하고, 분석을 수행하고, 데이터와 결과를 데이터스토어에 직접 보고하여 모든 데이터 노드에 거의 동일하게 배포합니다. 데이터스토어는 데이터 스토리지를 용이하게 하고, 여러 플로우 컬렉터에 분산되지 않고 모든 트래픽을 중앙 집중식 위치에 유지하며, 여러 플로우 컬렉터보다 더 큰 스토리지 용량을 제공합니다. 다음 다이어그램의 예를 참조하십시오.



데이터스토어는 Flow Collector에서 수집한 네트워크의 텔레메트리를 저장할 중앙 저장소를 제공합니다. 데이터스토어는 각각 데이터의 일부를 포함하는 데이터 노드의 클러스터와 별도의 데이터 노드의 데이터 백업으로 구성됩니다. 모든 데이터가 하나의 중앙 집중식 데이터베이스에 있으므로 Flow Collector는 여러 매니저에 분산되어 있는 것과 달리 모든 데이터스토어를 개별적으로 쿼리하는 것보다 Flow Collector에서 쿼리 결과를 더 빠르게 검색할 수 있습니다. 데이터스토어 클러스터는 개선된 내결함성, 개선된 쿼리 응답, 더 빠른 그래프 및 차트 채우기를 제공합니다.

쿼리

그래프 및 차트를 포함하여 사용자가 제출한 쿼리를 해결하기 위해 매니저는 데이터스토어를 쿼리합니다. 데이터스토어는 쿼리와 관련된 열에서 일치하는 결과를 찾은 다음 일치하는 행을 검색하고 쿼리 결과를 매니저에 반환합니다. 매니저는 여러 Flow Collector의 여러 결과 집합을 대조할 필요 없이 그래프 또는 차트를 생성합니다. 이렇게 하면 여러 Flow Collector를 쿼리할 때와 비교하여 쿼리 비용이 감소하고 쿼리 성능이 향상됩니다.

데이터스토어 스토리지 및 내결함성

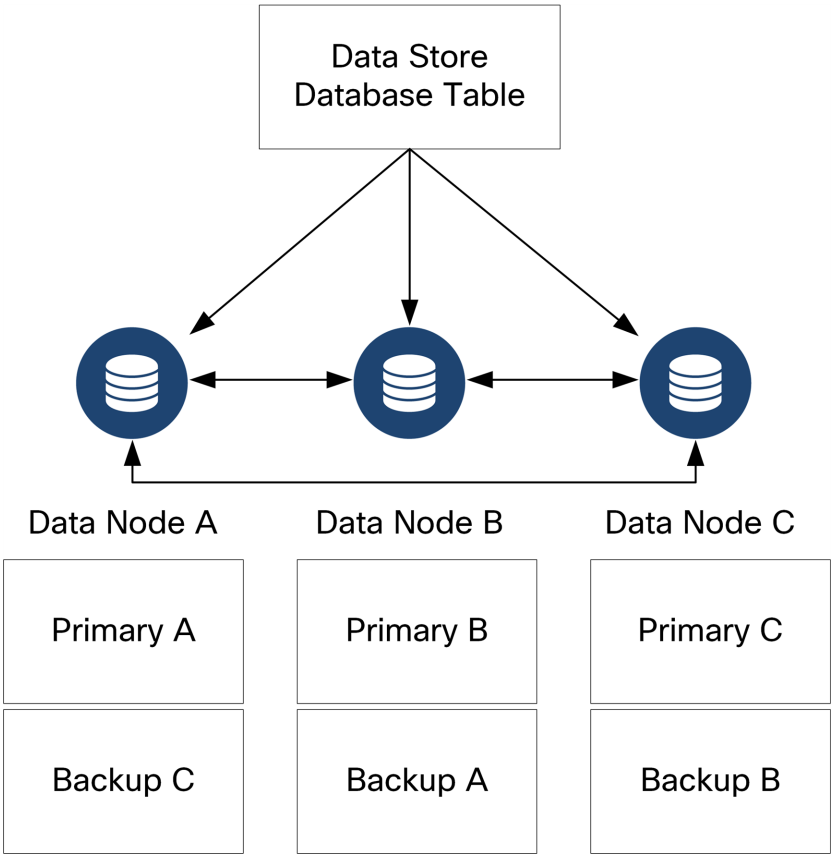
데이터스토어는 Flow Collector에서 데이터를 수집하여 클러스터 내의 데이터 노드에 동일하게 배포합니다. 전체 텔레메트리의 일부를 저장하는 것 외에도 각 데이터 노드는 다른 데이터 노드의 텔레메트리 백업도 저장합니다. 다음과 같은 방식으로 데이터를 저장합니다.

- 로드 밸런싱 지원
- 각 노드에 처리를 분산
- 데이터스토어로 수집된 모든 데이터에 내결함성을 위한 백업이 있는지 확인
- 데이터 노드의 수를 늘려 전체 스토리지 및 쿼리 성능을 개선 가능

데이터 저장소에 3개 이상의 데이터 노드가 있고 데이터 노드가 다운된 경우, 해당 백업을 포함하는 데이터 노드를 계속 사용할 수 있고 총 데이터 노드 개수의 절반 이상이 여전히 가동 중인 경우, 전체 데이터스토어는 가동 상태를 유지합니다. 이렇게 하면 다운된 연결 또는 결함 있는 하드웨어를 복구할 수 있습니다. 결함 있는 데이터 노드를 교체하면 데이터스토어는 인접 데이터 노드에 저장된 기존 백업에서 해당 노드의 데이터를 복원하고 이 데이터 노드에 데이터 백업을 생성합니다.

텔레메트리 스토리지 예

3개 데이터 노드가 텔레메트리를 저장하는 방법의 예는 다음 다이어그램을 참조하십시오.



일반 구축 요건

시작하기 전에 이 가이드를 검토하여 설치를 계획하는 데 필요한 준비, 시간, 리소스 등의 프로세스를 파악합니다.

하드웨어 및 소프트웨어 버전 릴리스 매트릭스

호환성 세부 정보는 하드웨어 및 소프트웨어 버전 릴리스 매트릭스를 검토하십시오. 매트릭스는 https://www.cisco.com/c/en/us/support/security/stealthwatch/products-device-support-tables-list.html에서 확인할 수 있습니다.

사양

설치할 각 어플라이언스의 사양 시트를 다운로드합니다. 사양은 https://www.cisco.com/c/en/us/support/security/stealthwatch/products-technical-reference-list.html에서 볼 수 있습니다.

CIMC(Cisco Integrated Management Controller)

어플라이언스를 설치한 후에는 서버 구성 및 가상 서버 콘솔에 대한 액세스를 활성화하도록 CIMC(Cisco Integrated Management Controller)를 구성해야 합니다. CIMC를 사용하여 하드웨어 상태를 모니터링할 수도 있습니다.

- **지침: CIMC를 사용하여 연결(원격 액세스에 필요)**을 참조하고 Cisco UCS C-Series 통합 관리 컨트롤러 GUI 구성 가이드의 지침을 따르십시오.
- **기본 비밀번호:** 초기 구성의 일부로 CIMC에 관리자로 로그인하고 **Password(비밀번호)** 필드에 비밀번호를 입력합니다.
- **비밀번호 요구 사항:** 로그인한 후에는 기본 비밀번호를 변경하여 네트워크 보안을 보호합니다.

표준 어플라이언스 요구 사항(데이터스토어 없음)

데이터스토어 없이 Secure Network Analytics를 설치하는 경우 다음 어플라이언스를 설치합니다.

어플라이언스	요건
매니저	• 최소 1개 매니저
Flow Collector	• 최소 1개 Flow Collector
Flow Sensor	선택 사항
UDP Director	선택 사항

데이터 저장소를 사용하는 Secure Network Analytics에 대한 어플라이언스 설치 요구 사항을 검토하려면 **데이터스토어 구축 요건**을 참조하십시오.

관리자 및 플로우 컬렉터 구축 요건

구축하는 각 매니저 및 Flow Collector에 대해 라우팅 가능한 IP 주소를 `eth0` 관리 포트에 할당합니다.

데이터스토어 구축 요건

데이터 저장소를 사용하여 Secure Network Analytics를 구축하려면 구축에 대한 다음 요구 사항 및 권장 사항을 검토하십시오.

어플라이언스 요구 사항(데이터 저장소 사용)

다음 표에서는 데이터스토어와 함께 Secure Network Analytics를 구축하는 데 필요한 어플라이언스에 대한 개요를 제공합니다.

어플라이언스	요건
매니저	• 최소 1개 매니저
데이터스토어	• 최소 1개 또는 3개 데이터 노드 • 데이터스토어 확장을 위한 3개 데이터 노드의 추가 세트(최대 36개 데이터 노드) • 클러스터에서 2개의 데이터 노드만 구축하는 것은 지원되지 않습니다.
Flow Collector	• 최소 1개 Flow Collector
UDP Director	선택 사항
Flow Sensor	선택 사항

> ⚠ 어플라이언스 기능에 문제가 발생할 수 있으므로 어플라이언스 BIOS를 업데이트하지 마십시오.

관리자 및 플로우 컬렉터 구축 요건

구축하는 각 매니저 및 Flow Collector에 대해 라우팅 가능한 IP 주소를 `eth0` 관리 포트에 할당합니다.

- **eth0 포트 설정:** 매니저 및 Flow Collector`eth0` 관리 포트에 대해 **BASE-T** 구리 1G/10G 포트 또는 SFP+ twinax 케이블 10G 포트의 사용을 구성할 수 있습니다.
- **처리량:** 데이터스토어 사용을 위해서는 10G 처리량의 BASE-T 구리 포트가 필요합니다. 데이터스토어를 구축하지 않은 경우 `eth0`로서 100Mbps/1Gbps/10Gbps 구리 인터페이스만 구성할 수 있습니다.

데이터 노드 구축 요건

각 데이터스토어는 데이터 노드로 구성됩니다.

- **하드웨어:** 각 하드웨어 데이터 노드는 전용 섀시입니다. 하드웨어 데이터스토어를 구매하면 해당 데이터스토어 모델에 표시된 노드 수에 해당하는 여러 데이터 노드 하드웨어 섀시를 받게 됩니다. 예를 들어 DS 6200 데이터스토어은 3개의 데이터 노드 하드웨어 섀시를 제공합니다.
- **가상 버전:** 가상 데이터스토어를 다운로드할 때 1개, 3개 또는 그 이상의 데이터 노드 가상 버전(3개 세트)을 구축할 수 있습니다.

> 데이터 노드는 모두 하드웨어 또는 모두 가상 버전이어야 합니다. 하드웨어 및 가상 데이터 노드의 혼합은 지원되지 않습니다.

다중 데이터 노드 구축

다중 데이터 노드 구축은 최대 성능 결과를 제공합니다. 예를 들어 3개 데이터 노드가 있는 데이터스토어 6200은 초당 약 500,000개의 플로우를 처리할 수 있으며 해당 데이터를 약 90일 동안 유지할 수 있습니다.

다음에 유의하십시오.

- **3개 세트**: 데이터 노드는 3개 세트(최소 3개에서 최대 36개)인 데이터스토어의 일부로 클러스터링될 수 있습니다. 클러스터에 2개의 데이터 노드만 구축하는 것은 지원되지 않습니다.
- **모두 하드웨어 또는 모두 가상**: 데이터 노드가 모두 하드웨어 또는 모두 가상 버전인지 확인합니다. 하드웨어 및 가상 데이터 노드의 혼합은 지원되지 않습니다.

단일 데이터 노드 구축

단일(1) 데이터 노드를 구축하도록 선택하는 경우:

- **플로우 컬렉터:**최대 4개 Flow Collector가 지원됩니다.
- **데이터 노드 추가:** 하나의 데이터 노드만 구축하는 경우 나중에 구축에 데이터 노드를 추가할 수 있습니다. 자세한 내용은 **다중 데이터 노드 구축**을 참조하십시오.

> 이러한 권장 사항은 텔레메트리만 고려합니다. 성능은 호스트 수, Flow Sensor 사용, 트래픽 프로파일 및 기타 네트워크 특성을 비롯한 추가 요인에 따라 달라질 수 있습니다. 크기 조정에 대한 지원이 필요한 경우 Cisco 지원팀에 문의하십시오.

> 현재 데이터스토어는 기본 데이터 노드가 다운되는 경우 예비 데이터 노드를 자동 교체로 구축하는 것을 지원하지 않습니다. 지침이 필요하면 Cisco 지원팀에 문의하십시오.

데이터 노드 구성 요구 사항

데이터스토어를 구축하려면 각 데이터 노드에 다음을 할당합니다. 준비하는 정보는 시스템 구성 가이드를 사용하는 최초 설정에서 구성됩니다.

- **라우팅 가능한 IP 주소(eth0):** Secure Network Analytics 어플라이언스와의 관리, 수집 및 쿼리 통신에 사용됩니다.
- **eth0 포트 구성:** `eth0` 관리 포트에 대해 **BASE-T** 구리 1G/10G 포트 또는 SFP+ twinax 케이블 10G 포트의 사용을 구성할 수 있습니다.
- **처리량:** 데이터스토어 사용을 위해서는 10G 처리량의 BASE-T 구리 포트가 필요합니다.
- **데이터 간 노드 통신:** 프라이빗 LAN 또는 데이터 노드간 통신에 사용할 VLAN 내의 `169.254.42.0/24` CIDR 블록에서 라우팅할 수 없는 IP 주소를 구성합니다.

  처리량 성능을 높이기 위해 는 데이터 노드 `eth2` 포트(또는 `eth2` 및 `eth3`을 포함하는 포트 채널)를 데이터 노드간 통신용 스위치에 연결합니다.데이터스토어의 일부로 데이터 노드는 서로 간에 통신합니다.
- **네트워크 연결:** 2개의 10G 네트워크 연결이 필요합니다. 하나는 관리, 수집 및 쿼리 통신용이고 다른 하나는 데이터 노드간 통신용입니다.
- **추가 연결 및 스위치:** 하드웨어 데이터 노드에서만 선택적으로, 네트워크 이중화 및 데이터 노드간 통신의 중요도를 위해 추가 10G 연결을 설치하고 데이터 노드에서 포트 채널을 설정하기 위한 추가 스위치를 설치합니다.

> 인접한 번호의 데이터 노드에 별도의 이중화 전원 공급 장치를 사용하여 전원을 공급하도록 데이터 노드를 구성합니다. 이 구성은 데이터 이중화 및 전반적인 데이터스토어 가동 시간을 개선합니다.

네트워킹 및 스위칭 고려 사항

다음 표에서는 데이터스토어를 사용하여 Secure Network Analytics를 구축하기 위한 네트워킹 및 스위칭 고려 사항에 대한 개요를 제공합니다.

네트워크 고려 사항	설명
데이터 노드간 통신	• 데이터 노드간에 권장되는 왕복 시간(RTT) 레이턴시를 200마이크로초 미만으로 설정합니다. • 데이터 노드간의 클럭 오차를 1초 이하로 유지합니다. • 데이터 노드간에 6.4Gbps 이상의 권장 처리량(10Gbps 전이중 스위치 연결)을 설정합니다. • 하드웨어 데이터 노드의 경우, 10G 처리량에 대해 `eth2` 포트를 구성하면 정상적인 데이터 노드간 통신에 충분합니다. 최대 20G 처리량을 지원하는 `eth2/eth3` 포트 채널을 생성하면 데이터 노드간의 통신이 더 빨라지고 데이터스토어에 데이터 노드 추가 또는 교체가 더 빨라집니다. 각각의 새 데이터 노드는 인접 데이터 노드에서 트래픽을 수신하여 데이터를 채우기 때문입니다.
데이터 노	• 하드웨어 데이터 노드에 예기치 않은 정전이 발생하면 데이터가 손상될

드 하드웨어 전원	수 있습니다. 무정전 전원 공급 장치의 별도 회로에서 두 전원 공급 장치를 모두 사용합니다. • 데이터스토어 클러스터를 초기화할 때 각 데이터 노드에서 사용하는 전원 공급 장치를 기반으로 데이터 노드 구성을 대체합니다. 이렇게 하면 정전 시 중단되는 데이터 노드의 수를 최소화하여 내결함성을 최적화할 수 있습니다.
데이터 노드 스위칭	• 데이터 노드간 통신을 허용하려면 데이터 노드에 고유한 레이어 2 VLAN 이 필요합니다. 하드웨어 데이터 노드는 공유 또는 전용 10G 스위치에 연결할 수 있습니다. • 스위치 중단 및 업그레이드 중에 지속적인 연결을 보장하려면 하드웨어 데이터 노드를 2개의 스위치에 연결하는 것이 좋습니다. 데이터 노드간 통신에 필요한 짧은 대기 시간으로 인해 Cisco는 이중 스위치 쌍을 권장합니다 .이 쌍은 두 스위치가 상호 연결되고 두 스위치에서 레이어 2 VLAN 을 전달합니다.
Secure Network Analytics 어플라이언스 통신	• 매니저 및 플로우 컬렉터는 모든 데이터 노드에 도달할 수 있어야 합니다. • 데이터 노드는 매니저, 모든 플로우 컬렉터 및 각 데이터 노드에 연결할 수 있어야 합니다.

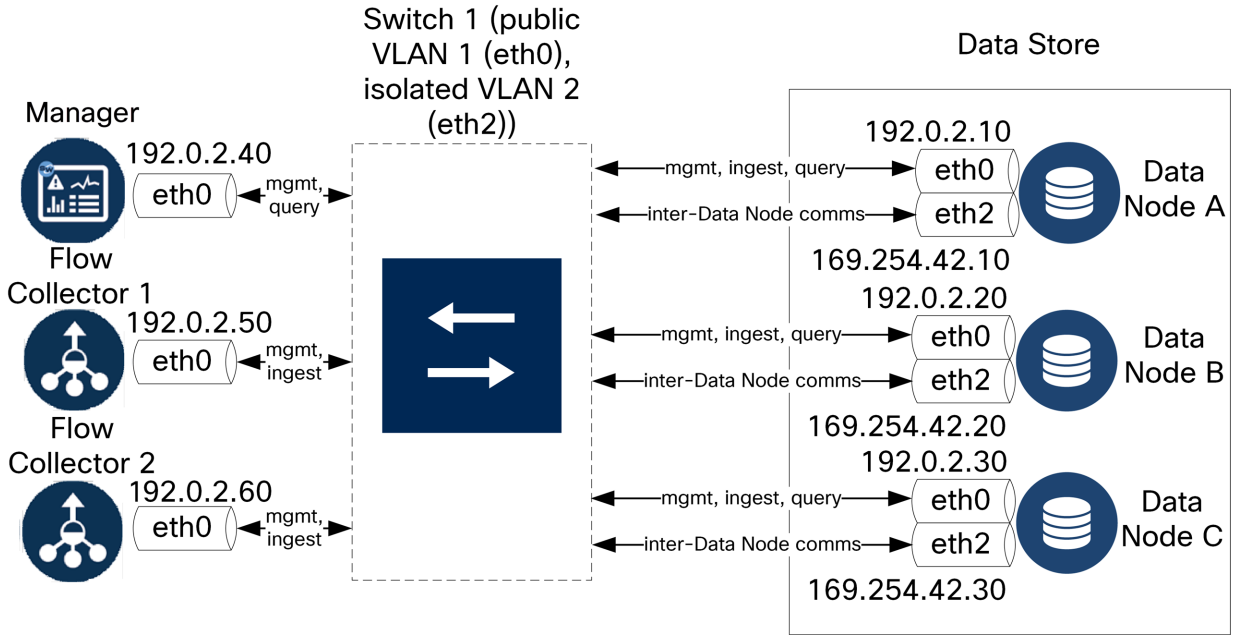
현재 데이터스토어는 기본 데이터 노드가 다운되는 경우 예비 데이터 노드를 자동 교체로 구축하는 것을 지원하지 않습니다. 지침이 필요하면 Cisco 지원팀에 문의하십시오.

하드웨어 스위치 예

`eth2`또는 `eth2/eth3`포트 채널을 데이터 노드간 통신을 활성화하려면 10G 속도를 지원하는 스위치 1개를 구축합니다.

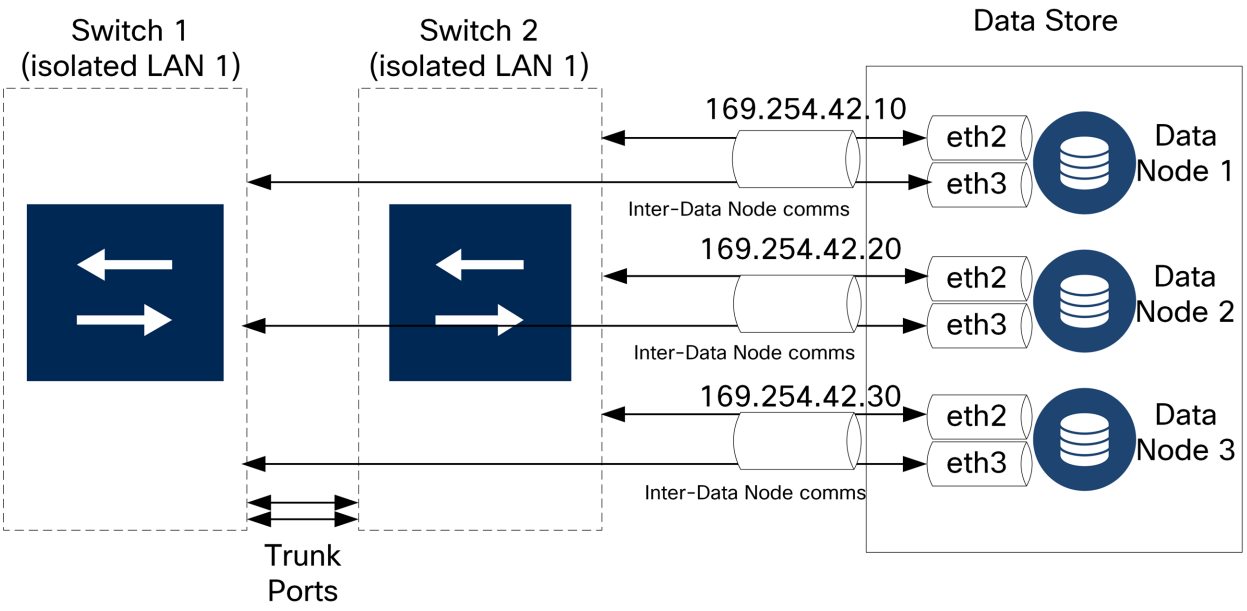
매니저 및 플로우 컬렉터와의 `eth0` 통신을 위해 데이터 노드에 대해 LAN 또는 VLAN을 구성하고, 데이터 노드간 통신을 위해 격리된 LAN 또는 VLAN을 구성합니다.

이러한 스위치를 다른 어플라이언스와 공유할 수 있지만 추가 어플라이언스 트래픽에 대해 별도의 LAN 또는 VLAN을 생성할 수 있습니다. 다음 다이어그램의 예를 참조하십시오.



데이터스토어 클러스터에는 격리된 VLAN 내의 노드 간에 지속적인 하트비트가 필요합니다. 이 하트비트가 없으면 데이터 노드가 오프라인이 될 수 있으며, 이로 인해 데이터스토어가 다운될 위험이 높아집니다.

스위치 업데이트 및 계획된 중단에 대한 계획을 위해 추가 네트워크 이중화를 원하는 경우 전용 데이터 노드간 통신용 포트 채널을 사용하여 데이터 노드를 구성해야 합니다. 각 물리적 포트를 서로 다른 스위치에 연결하여 모든 데이터 노드를 2개의 스위치에 연결합니다. 다음 다이어그램의 예를 참조하십시오.



구축 계획에 대한 지원을 받으려면 Cisco 전문 서비스에 문의하십시오.

데이터스토어배치 고려 사항

Flow Collector, 매니저, 다른 모든 데이터 노드와 통신할 수 있도록 각 데이터 노드를 배치합니다. 최상의 성능을 위해 데이터 노드과 Flow Collector를 함께 배치하여 통신 레이턴시를 최소화하고, 최적의 쿼리 성능을 위해 데이터 노드 및 매니저를 배치합니다.

- **방화벽:** NOC와 같은 방화벽 내부에 데이터 노드를 배치하는 것이 좋습니다.
- **전원:** 정전 또는 하드웨어 장애로 인해 데이터스토어가 중단되면 데이터 손상 및 데이터 손실의 위험이 증가합니다. 일정한 업타임을 염두에 두고 데이터 노드를 설치합니다.

예기치 않게 데이터 노드에 정전이 발생한 경우 어플라이언스를 재부팅하면 데이터 노드의 데이터베이스 인스턴스가 자동으로 재시작되지 않을 수 있습니다. 문제 해결 및 데이터베이스 수동 재시작에 대한 내용은 시스템 설정 가이드를 참조하십시오.

- **정책:** 하드웨어 데이터 노드 전원 복원 정책이 **Restore Last State(마지막 상태 복원)**로 설정되어 있는지 확인합니다. 이 설정은 정전 후 데이터 노드을 자동으로 재시작하고 실행 중인 프로세스의 복원을 시도합니다. CIMC에서 전원 복원 정책을 구성하는 방법에 대한 자세한 내용은 UCS C-Series GUI 구성 가이드를 참조하십시오.

1. 통신을 위한 방화벽

구성

어플라이언스가 제대로 통신하기 위해서는 방화벽 또는 ACL(Access Control List)이 필수 연결을 차단하지 않도록 네트워크를 구성해야 합니다. 이 섹션에 제공된 정보를 사용해 네트워크를 구성하면 어플라이언스가 네트워크를 통해 통신할 수 있습니다.

열린 포트(모든 어플라이언스)

어플라이언스(매니저, Flow Collector, 데이터 노드, Flow Sensor 및 UDP Director)에 다음 포트가 열려 있고 액세스에 제한이 없는지 확인하려면 네트워크 관리자에게 문의하십시오.

- TCP 22
- TCP 25
- TCP 389
- TCP 443
- TCP 2393
- TCP 8910
- UDP 53
- UDP 123
- UDP 161
- UDP 162
- UDP 389
- UDP 514
- UDP 2055
- UDP 6343

데이터 노드에 대한 추가 열린 포트

또한 데이터 노드를 네트워크에 구축하는 경우 다음 포트가 열려 있고 액세스에 제한이 없는지 확인하십시오.

- TCP 5433
- TCP 5444
- TCP 9450

통신 포트와 프로토콜

다음 표는 Secure Network Analytics에서 포트가 사용되는 방식을 보여줍니다.

발신(클라이언트)	수신(서버)	포트	프로토콜
관리 사용자 PC	모든 어플라이언스	TCP/443	HTTPS
모든 어플라이언스	네트워크 시간 소스	UDP/123	NTP
Active Directory	매니저	TCP/389, UDP/389	LDAP
Cisco ISE	매니저	TCP/443	HTTPS
Cisco ISE	매니저	TCP/8910	XMPP
외부 로그 소스	매니저	UDP/514	SYSLOG
Flow Collector	매니저	TCP/443	HTTPS
UDP Director	플로우 컬렉터(sFlow)	UDP/6343	sFlow
UDP Director	플로우 컬렉터(NetFlow)	UDP/2055*	NetFlow
UDP Director	서드파티 이벤트 관리 시스템	UDP/514	SYSLOG
Flow Sensor	매니저	TCP/443	HTTPS
Flow Sensor	플로우 컬렉터(NetFlow)	UDP/2055	NetFlow
Identity	매니저	TCP/2393	SSL
NetFlow Exporter	플로우 컬렉터(NetFlow)	UDP/2055*	NetFlow
sFlow Exporter	플로우 컬렉터(sFlow)	UDP/6343*	sFlow
매니저	Cisco ISE	TCP/443	HTTPS
매니저	Cisco ISE	TCP/8910	XMPP
매니저	DNS	UDP/53	DNS
매니저	Flow Collector	TCP/443	HTTPS
매니저	Flow Sensor	TCP/443	HTTPS
매니저	Identity	TCP/2393	SSL

발신(클라이언트)	수신(서버)	포트	프로토콜
매니저	Flow Exporter	UDP/161	SNMP
매니저	LDAP	TCP/636	TLS
사용자 PC	매니저	TCP/443	HTTPS

*이것은 기본 포트이지만, 모든 UDP 포트를 엑스포터에서 구성할 수 있습니다.

추가 개방형 포트 - 데이터스토어

다음은 데이터스토어를 구축하기 위해 방화벽에서 열리는 통신 포트를 나열합니다.

#	발신(클라이언트)	수신(서버)	포트	프로토콜 또는 목적
1	매니저	Flow Collector 및 데이터 노드	22/TCP	SSH, 데이터스토어 데이터베이스를 초기화하는 데 필요
1	데이터 노드s	기타 모든 데이터 노드	22/TCP	SSH, 데이터스토어 데이터베이스 초기화 및 데이터베이스 관리 작업에 필요
2	매니저, Flow Collector 및 데이터 노드	NTP 서버	123/UDP	NTP, 시간 동기화에 필요
2	NTP 서버	매니저, Flow Collector 및 데이터 노드	123/UDP	NTP, 시간 동기화에 필요
3	매니저	Flow Collector 및 데이터 노드	443/TCP	HTTPS, 어플라이언스 간 보안 통신에 필요
3	Flow Collectors	매니저	443/TCP	HTTPS, 어플라이언스 간 보안 통신에 필요
3	데이터 노드s	매니저	443/TCP	HTTPS, 어플라이언스 간 보안 통신에 필요
4	NetFlow Exporter	플로우 컬렉터 - NetFlow	2055/UDP	NetFlow 수집
5	데이터 노드s	기타 모든 데이터 노드	4803/TCP	데이터 노드간 메시징 서비스
6	데이터 노드	기타 모든 데이터 노드	4803/UDP	데이터 노드간 메시징 서비스
7	데이터 노드s	기타 모든 데이터 노드	4804/UDP	데이터 노드간 메시징 서비스

8	매니저, Flow Collector 및 데이터 노드	데이터 노드s	5433/TCP	Vertica 클라이언트 연결
9	데이터 노드	기타 모든 데이터 노드	5433/UDP	Vertica 메시징 서비스 모니터링
10	sFlow Exporter	플로우 컬렉터 (sFlow)	6343/UDP	sFlow 수집
11	데이터 노드s	기타 모든 데이터 노드	6543/UDP	데이터 노드간 메시징 서비스

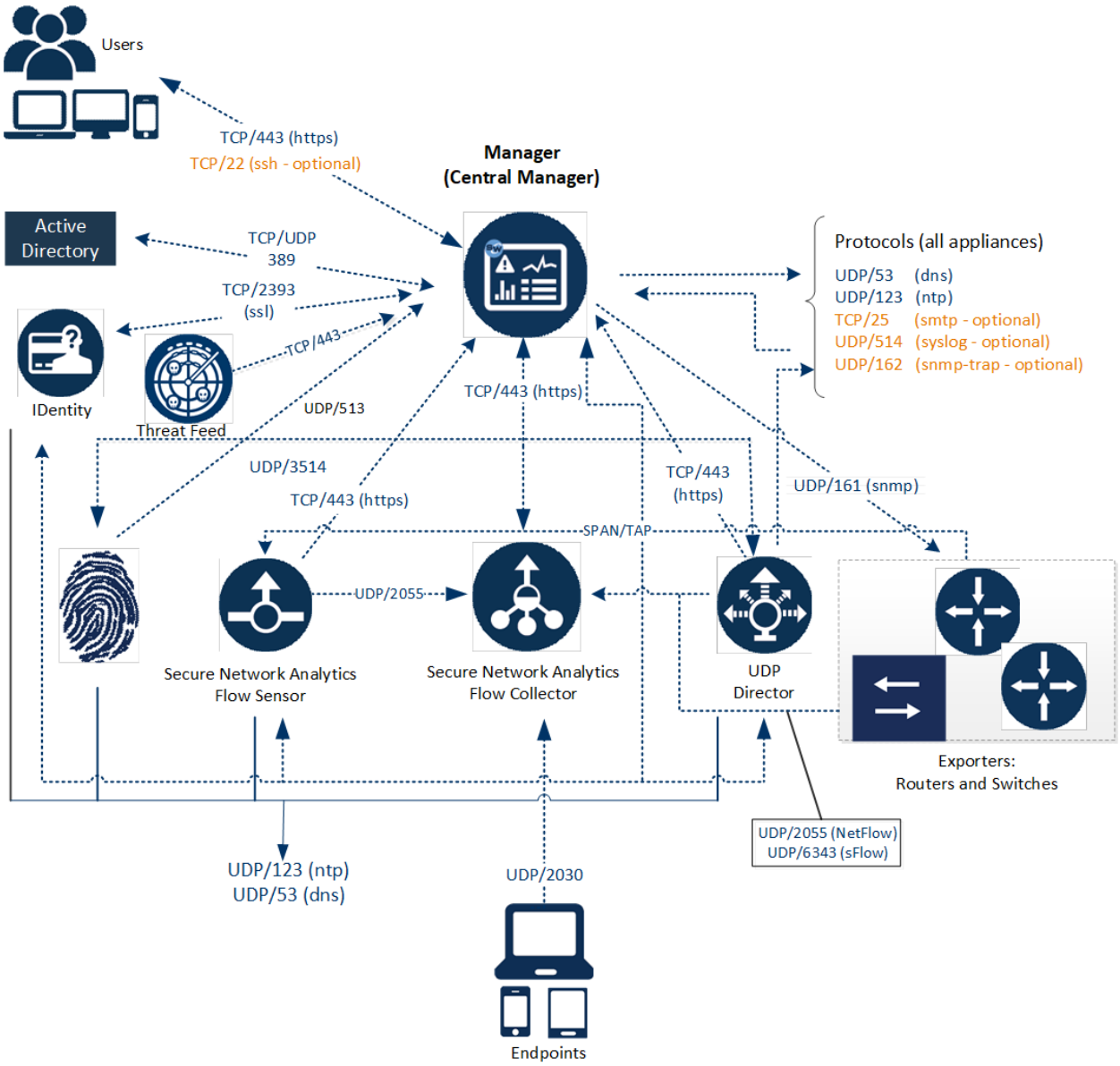
옵션 통신 포트

다음 표는 네트워크 요구 사항에 따라 결정된 컨피그레이션 옵션을 보여줍니다.

발신(클라이언트)	수신(서버)	포트	프로토콜
모든 어플라이언스	사용자 PC	TCP/22	SSH
매니저	서드파티 이벤트 관리 시스템	UDP/162	SNMP-trap
매니저	서드파티 이벤트 관리 시스템	UDP/514	SYSLOG
매니저	이메일 게이트웨이	TCP/25	SMTP
매니저	위협 피드	TCP/443	SSL
사용자 PC	모든 어플라이언스	TCP/22	SSH

Secure Network Analytics 구축 예

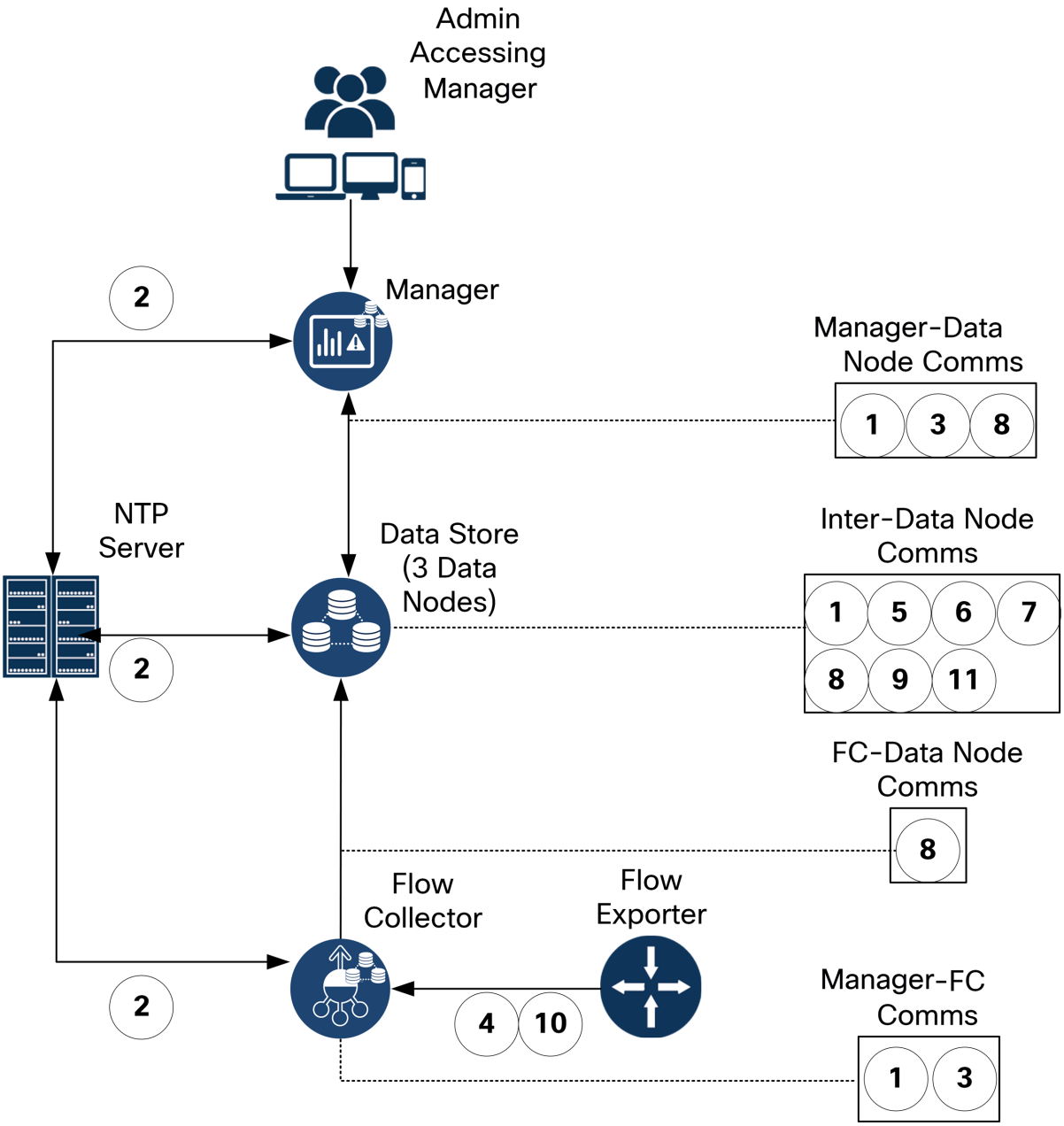
다음 다이어그램은 Secure Network Analytics에서 사용되는 다양한 연결을 보여줍니다. 이러한 포트 중 일부는 선택 사항입니다.



데이터스토어가 있는

Secure Network Analytics 구축 예

아래 그림과 같이 Secure Network Analytics 어플라이언스 제품을 전략적으로 구축하여 내부 네트워크 경계 또는 DMZ 등 네트워크 전반에 걸쳐 주요 네트워크 세그먼트 범위를 최적의 상태로 제공할 수 있습니다.



2. 설치 경고 및 지침

설치 경고

Secure Network Analytics x2xx 시리즈 어플라이언스를 설치하기 전 규정 및 컴플라이언스 및 안전 정보 문서를 읽어보십시오.

다음 경고에 유의하십시오.

명령문 1071 - 경고 정의

중요한 안전상의 지침

이 경고 기호는 위험을 의미합니다. 부상이 발생할 수 있는 상황입니다. 장비를 작동하기 전에 전기 관련 재해에 유의하고 사고 예방을 위해 표준 절차를 숙지하십시오. 각 경고의 끝에는 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾을 수 있도록 명령문 번호가 제공됩니다.

이 지침을 반드시 숙지하십시오.

명령문 1005 - 자동 차단기

이 제품은 건물의 단락(과전류) 차단 설비를 사용합니다. 보호 디바이스가 정격(미국: 120V, 15A/EU: 250V, 16A) 이하인지 확인하십시오.

명령문 1004 - 설치 지침

시스템 설치, 사용, 전원 연결 전 설치 안내를 읽으십시오.

명령문 12 - 전원 공급 장치 차단 경고

섀시 또는 전원 공급 장치 근처에서 작업 전 AC 장치의 전원 코드를 뽑거나 DC 장치의 자동 차단기에서 전원을 분리합니다.

명령문 43 - 장신구 착용 금지 경고

전원에 연결된 장비를 취급하기 전 장신구(반지, 목걸이, 시계 등)를 빼주십시오. 금속이 전원과 지면에 닿아 가열될 경우 심한 화상을 입거나 금속이 단자에 들러붙을 수 있습니다.

명령문 94 - 손목 스트랩 경고

이 작업 중에는 카드에 정전기 손상을 막기 위해 접지용 손목 스트랩을 착용하십시오. 손이나 금속 도구가 백플레인에 직접 닿지 않게 하십시오. 감전 사고가 발생할 수 있습니다.

명령문 1045 - 자동 차단기 보호

이 제품을 건물에 설치하려면 누전(과전류) 예방 조치가 필요합니다. 국가 및 지역의 배선 규정을 준수하여 설치하십시오.

명령문 1021 - SELV 회로

전기 충격을 방지하기 위해 안전초저압(SELV) 회로를 TNV(Telephone-Network Voltage) 회로에 연결하지 마십시오. LAN 포트는 SELV 회로를 포함하고, WAN 포트는 TNV 회로를 포함합니다. 모든 LAN 및 WAN 포트는 두 RJ-45 커넥터를 모두 사용합니다. 케이블을 연결하는 동안에는 주의를 기울이십시오.

명령문 1024 - 접지

이 장비는 접지가 필요합니다. 접지 컨덕터를 꺼놓거나 적절히 설치된 접지 컨덕터 없이 장비를 가동해서는 절대 안됩니다. 적절한 접지가 가능한지 확실치 않은 경우에는 해당 전기 검사 기관이나 전기 기사에게 문의하십시오.

명령문 1040 - 제품 폐기

이 제품을 최종 폐기할 때는 국가의 모든 법률 및 규정에 따라 처리해야 합니다.

명령문 1074 - 지역 및 국가의 전기 관련 법규 준수

이 장비를 설치할 때는 지역 및 국가의 전기 관련 법규를 준수해야 합니다.

명령문 19 - TN 전원 경고

이 디바이스는 TN 전원 시스템을 사용해 작동하도록 설계되었습니다.

설치 지침

다음 경고에 유의하십시오.

명령문 1047 - 과열 방지

시스템의 과열을 방지하려면 권장 최대 주변 온도인 5~35°C(41~95°F) 이상에서 작동하지 마십시오.

명령문 1019 - 기본 분리 장치

플러그-소켓 조합은 기본 분리 장치로서 항상 접근이 용이해야 합니다.

명령문 1005 - 자동 차단기

이 제품은 건물의 단락(과전류) 차단 설비를 사용합니다. 보호 디바이스가 정격(미국: 120V, 15A/EU: 250V, 16A) 이하인지 확인하십시오.

명령문 1074 - 지역 및 국가의 전기 관련 법규 준수

이 장비를 설치할 때는 지역 및 국가의 전기 관련 법규를 준수해야 합니다.

명령문 371 - 전원 케이블 및 AC 어댑터

제품을 설치할 때는 제공되거나 지정된 연결 케이블/전원 케이블/AC 어댑터/배터리를 사용합니다. 다른 케이블/어댑터를 사용하는 경우 제품이 오작동하거나 화재가 발생할 수 있습니다. 전자 기기 및 소재 안전법에 따라 코드에 "PSE"를 표시함으로써 준거법의 규제를 받지 않는 UL 인증 케이블(코드에 "UL" 또는 "CSA"가 표시됨)은 CISCO에서 지정한 제품 외의 기타 모든 전자 디바이스에 사용할 수 없습니다.

명령문 1073 - 사용자가 수리할 수 없는 부품

내부 부품은 사용자가 수리할 수 없습니다. 개봉하지 마십시오.

섀시를 설치할 때는 다음 지침을 따르십시오.

- 정비 작업 및 알맞은 공기 흐름 유지를 위해 섀시 주변에 적절한 공간을 확보해야 합니다. 섀시에서는 전면에서 후면으로 공기가 이동합니다.

적절한 공기 흐름을 유지하기 위해 레일 키트를 사용하여 섀시를 랙에 설치합니다. 레일 키트를 사용하지 않고 서버를 다른 장치 위에 두거나 “쌓아두면” 섀시 상단의 공기 배출구가 차단되어 과열되고 팬 속도가 빨라져 전력 소비량이 증가하게 됩니다. 레일을 사용하면 섀시 간에 필요한 최소 간격을 유지할 수 있으므로 섀시를 랙에 설치할 때

에는 레일 키트 위에 서버를 마운트하는 것이 좋습니다. 레일 키트를 사용하여 섀시를 마운트할 경우 섀시 간 추가 간격을 유지하지 않아도 됩니다.

- 공조 기능을 통해 섀시 온도를 5~35°C(41~95°F)로 유지할 수 있는지 확인하십시오.
- 캐비닛 또는 랙이 랙 요구 사항에 부합해야 합니다.
- 현장 전원이 어플라이언스의 사양 시트에 표시된 전력 요건을 충족하는지 확인합니다. 가능하다면 UPS를 사용하여 정전으로부터 보호할 수 있습니다.

철공진(ferroresonant) 기술을 사용하는 UPS 유형은 사용하지 마십시오. 이 UPS 유형은 이러한 시스템에서 불안정해질 수 있습니다. 그러면 데이터 트래픽 패턴의 변화에 따라 전류 요구량의 변동이 커질 수 있습니다.

보안 권장 사항

다음 정보를 참조하면 안전을 보장하고 섀시를 보호할 수 있습니다. 이 정보가 작업 환경의 잠재적으로 위험한 모든 상황을 해결하지는 못할 수 있으므로, 항상 신중한 자세로 올바른 판단을 내려야 합니다.

다음의 보안 지침을 따르십시오.

- 설치 전후와 설치 중 해당 구역을 깨끗이 치우고 먼지가 없는 상태로 유지하십시오.
- 사람들이 걸려 넘어질 수 있으므로 툴은 통로에서 떨어진 곳에 두십시오.
- 섀시에 걸릴 수 있는 귀걸이, 팔찌 또는 체인 등의 장식품이나 헐렁한 옷을 착용하지 마십시오.
- 눈에 위험할 수 있는 조건에서 작업 중인 경우 보안 안경을 착용하십시오.
- 사람에게 잠재적 위험을 유발하거나 장비를 안전하지 않게 만들 수 있는 어떠한 작업도 수행하지 마십시오.
- 한 사람에게 너무 무거울 수 있는 물체를 들어 올리려고 하지 마십시오.

전기의 안전 유지

⚠ 섀시 작업을 수행하기 전에 전력 코드를 뽑았는지 확인하십시오.

전기가 필요한 장비로 작업할 때는 다음 지침을 따르십시오.

- 작업 공간이 잠재적으로 위험할 수 있는 상황에서는 혼자서 작업하지 마십시오.
- 전원이 분리되었을 것이라고 가정하지 말고 항상 확인하십시오.
- 젖은 바닥, 비접지 전원 연장 케이블, 마모된 전력 코드, 안전 접지 누락 등 작업 구역의 가능한 위험 요소를 주의 깊게 점검하십시오.
- 전기 사고 발생 시:
  - 주의를 기울이고, 스스로 희생자가 되지 마십시오.
  - 시스템에서 전원을 분리하십시오.
  - 가능한 경우 의료 조치를 받을 수 있도록 다른 사람을 보내십시오. 그렇지 않으면 피해자의 상태를 확인하고 도움을 요청하십시오.
  - 인공호흡 또는 외부 심장 압박이 필요한지 확인한 후 적절한 조치를 취하십시오.
- 표시된 전기 등급 및 제품 사용 지침에 따라 섀시를 사용하십시오.

ESD 손상 방지

전자 구성 요소를 부적절하게 처리하면 ESD가 발생하며, 이로 인해 장비와 전기 회로가 손상되어 장비의 간헐적 장애 또는 완전한 장애가 발생할 수 있습니다.

구성 요소를 제거 및 교체할 때는 항상 ESD 방지 절차를 따르십시오. 섀시가 전기적으로 접지에 연결되었는지 확인합니다. ESD 방지 손목 스트랩을 착용하여 피부에 잘 접촉되도록 합니다. 접지 클립을 페인트하지 않은 섀시 프레임 표면에 연결하여 ESD 전압을 안전하게 접지합니

다. ESD 손상 및 충격으로부터 적절히 보호하려면 손목 스트랩과 코드가 효과적으로 작동해야 합니다. 손목 스트랩을 사용할 수 없는 경우 섀시의 금속 부분을 만져 스스로 접지해야 합니다.

안전을 위해 정전기 방지 스트랩의 저항 값(1~10메그옴)을 정기적으로 확인하십시오.

사이트 환경

장비 고장을 피하고 환경으로 인한 종료 가능성을 줄이려면 사이트 레이아웃 및 장비 위치를 신중하게 계획하십시오. 현재 장비의 종료 또는 기존 장비에서 비정상적으로 높은 오류율을 경험하는 경우 이러한 고려 사항은 고장의 원인을 파악하고 향후 문제를 방지하는 데 도움이 될 수 있습니다.

전원 공급 장치 고려 사항

섀시를 설치할 때 다음 사항을 고려하십시오.

- 섀시를 설치하기 전에 현장의 전원을 점검하여 스파이크와 노이즈가 없는지 확인합니다. 어플라이언스 입력 전압에서 적절한 전압 및 전력 수준을 유지하려면 필요 시 전력 조절기를 설치합니다.
- 번개 및 전류 급증으로 인한 손상을 방지할 수 있도록 사이트를 적절히 접지합니다.
- 섀시에는 사용자가 선택할 수 있는 작동 범위가 없습니다. 올바른 어플라이언스 입력 전원 요구 사항은 섀시의 레이블을 참조하십시오.
- 여러 가지 스타일의 AC 입력 전력 공급 장치 코드를 어플라이언스에 사용할 수 있습니다. 지역에 맞는 올바른 스타일이 있는지 확인하십시오.
- 듀얼 이중(1+1) 전력 공급 장치를 사용하는 경우에는 각 전력 공급 장치에 독립적인 전기 회로를 사용하는 것이 좋습니다.
- 가능하면 사이트용 UPS(uninterruptible power source)를 설치하십시오.

랙 구성 고려 사항

랙 구성을 계획할 때 다음 사항을 고려하십시오.

- 개방형 랙에 섀시를 마운트할 경우, 랙 프레임이 진입점 또는 배기구를 차단하지 않도록 해야 합니다.
- 밀폐된 랙에 적절한 환기구가 있는지 확인합니다. 각 섀시가 열을 생성하므로 랙이 너무 혼잡하지 않도록 해야 합니다. 밀폐된 랙에는 냉각 공기를 제공할 루버형 측면과 팬이 있어야 합니다.
- 상단에 환기 팬이 있는 밀폐된 랙에서는 랙의 하단 근처 장비에서 생성되는 열을 랙 위쪽에 있는 장비의 흡입 포트로 끌어올릴 수 있습니다. 랙의 하단에 있는 장비를 위한 적절한 환기구를 제공해야 합니다.
- 배플(Baffle)은 흡기 공기로부터 배출 공기를 분리하는 데 도움이 되며, 이는 또한 섀시를 통해 냉각 공기를 끌어오는 데 도움이 됩니다. 배플의 가장 좋은 위치는 랙의 공기 흐름 패턴에 따라 달라집니다. 배플을 효과적으로 배치하기 위해 여러 방식으로 실험해보십시오.

3. 어플라이언스 장착

표준 19" 랙 또는 캐비닛, 기타 적합한 캐비닛 또는 평평한 표면에 Secure Network Analytics 어플라이언스를 직접 장착할 수 있습니다. 랙 또는 캐비닛에 어플라이언스를 장착할 경우 레일 장착 키트에 포함된 지침을 따르십시오. 어플라이언스를 배치할 위치를 결정할 때는 다음과 같이 전면 패널과 후면 패널의 여유 공간을 확보해야 합니다.

- 전면 패널 표시기는 쉽게 읽을 수 있어야 합니다.
- 후면 패널 포트 액세스는 케이블 연결에 제약을 받지 않아야 합니다.
- 후면 패널 전원 유입구는 적합한 AC 전원이 닿는 곳에 있어야 합니다.
- 어플라이언스 주변과 통풍구를 통과하는 공기 흐름이 제한되지 않아야 합니다.

어플라이언스에 포함된 하드웨어

Secure Network Analytics 어플라이언스에는 다음과 같은 하드웨어가 포함되어 있습니다.

- AC 전원 코드
- 액세스 키(전면판 용)
- 랙 장착용 레일 키트 또는 소형 어플라이언스를 위한 마운팅 이어
- Flow Collector 5210의 경우 10GB SFP 케이블

추가 필수 하드웨어

다음과 같은 추가 필수 하드웨어를 제공해야 합니다.

- 표준 19" 랙용 고정 나사
- 설치하려는 각 어플라이언스용 UPS(무정전 전원 공급 장치)
- (선택 사항) 로컬에서 구성하려면 다음 방법 중 하나를 사용합니다.
    - 비디오 케이블과 USB 케이블(키보드용)을 사용하는 랩톱 컴퓨터
    - USB 케이블로 비디오 케이블 및 키보드가 포함 된 비디오 모니터

4. 어플라이언스를 네트워크에 연결

동일한 절차를 사용해 네트워크에 각 어플라이언스를 연결합니다. 연결에서 유일한 차이점은 보유한 어플라이언스의 유형입니다.

1. 사양 검토

동일한 절차를 사용해 네트워크에 각 어플라이언스를 연결합니다. 연결에서 유일한 차이점은 보유한 어플라이언스의 유형입니다.

- **사양 시트:** 각 어플라이언스에 대한 자세한 사양 정보는 Secure Network Analytics사양 시트를 참조하십시오.
- **UCS 플랫폼:** Cisco x2xx 하드웨어는 모두 동일한 USC 플랫폼인 UCSC-C220-M5SX를 사용하고, Flow Collector 5210 DB만 예외적으로 UCSC-C240-M5SX를 사용합니다. 어플라이언스에서 NIC 카드, 프로세서, 메모리, 스토리지, RAID를 변경할 수 있습니다.
- **Manager 2210:** 데이터스토어를 구축하는 경우 증가된 처리량을 위한 eth0로서 10 Gbps SFP+DAC 인터페이스를 갖춘 매니저 2210을 구성할 수 있습니다. 데이터스토어를 구축하지 않은 경우 eth0로서 100Mbps/1Gbps/10Gbps 구리 인터페이스만 구성할 수 있습니다.
- **플로우 컬렉터 4210:** 데이터스토어를 구축하는 경우 증가된 처리량을 위한 eth0로서 10 Gbps SFP+DAC 인터페이스를 갖춘 플로우 컬렉터 4210을 구성할 수 있습니다. 데이터스토어를 구축하지 않은 경우 eth0로서 100Mbps/1Gbps/10Gbps 구리 인터페이스만 구성할 수 있습니다.
- **플로우 컬렉터 5210:** Flow Collector 5210은 두 개의 연결된 서버(엔진 및 데이터베이스)로 구성되어 단일 어플라이언스로 작동합니다. 따라서 다른 어플라이언스와 설치 방법이 약간 다릅니다. 먼저 10G SFP+ DA 크로스 연결 케이블로 직접 연결합니다. 그 뒤 네트워크에 연결합니다.

> ⚠ 어플라이언스 기능에 문제가 발생할 수 있으므로 어플라이언스 BIOS를 업데이트하지 마십시오.

2. 어플라이언스를 네트워크에 연결

어플라이언스를 네트워크에 연결하려면 다음을 수행합니다.

1. 어플라이언스 뒷면의 관리 포트에 이더넷 케이블을 연결합니다.
2. Flow Sensor 및 UDP Director의 모니터링 포트를 하나 이상 연결합니다.

    - **UDP Director High Availability:** 두 개의 UDP Director를 크로스오버 케이블로 연결합니다. UDP Director 하나의 eth2 포트를 두 번째 UDP Director의 eth2 포트에 연결합니다. 마찬가지로 각 UDP Director의 eth3 포트를 두 번째 크로스오버 케이블로 연결합니다. 케이블은 파이버 또는 구리를 사용할 수 있습니다.

- **이더넷 레이블:** 각 포트에 대한 이더넷 레이블(eth2, eth3 등)을 확인하십시오. 이러한 레이블은 시스템 구성에서 사용되는 네트워크 인터페이스(eth2, eth3 등)에 해당합니다.

3. 이더넷 케이블의 다른 쪽 끝을 네트워크 스위치에 연결합니다.
4. 전원 코드를 전원 공급 장치에 연결합니다. 일부 어플라이언스는 전원 공급 장치 1 및 전원 공급 장치 2의 형태로 2개의 전원 연결을 제공합니다.

5. 어플라이언스에 연결

이 섹션에서는 시스템 구성을 위해 어플라이언스에 연결하는 방법을 설명합니다.

연결 절차를 선택합니다.

- **키보드 및 모니터를 사용해 연결**
- **시리얼 케이블 또는 시리얼 콘솔로 연결**
- **CIMC를 사용하여 연결(원격 액세스에 필요)** 원격 액세스를 위해 어플라이언스에 연결하려면 다음 절차를 사용합니다.

키보드 및 모니터를 사용해 연결

로컬에서 IP 주소를 설정하려면 다음 단계를 완료합니다.

1. 전원 케이블을 어플라이언스에 연결합니다.
2. 전원 버튼을 눌러 어플라이언스를 켭니다. 부팅이 완전히 완료될 때까지 기다리십시오. 부팅 프로세스를 중단하지 마십시오.

> 전원을 적용하려면 전면 패널을 제거해야 할 수 있습니다.
>
> 일부 모델의 경우 시스템 전원이 켜지지 않은 상태에서 전원 공급 장치 팬이 켜집니다. 전면 패널의 LED가 켜져 있는지 확인합니다.
>
> UPS(무정전 전원 공급 장치)에 어플라이언스가 연결되어 있는지 확인합니다. 전원 공급 장치에 전원이 연결되지 않은 경우 시스템에 오류가 표시됩니다.

3. 키보드를 연결합니다.
   - 표준 키보드인 경우 표준 키보드 커넥터에 연결합니다.
   - USB 키보드인 경우 USB 커넥터에 연결합니다.
4. 비디오 케이블을 비디오 커넥터에 연결합니다. 로그인 프롬프트가 표시됩니다.
5. 4로 **6. Secure Network Analytics 시스템 구성** 구성.

시리얼 케이블 또는 시리얼 콘솔로 연결

터미널 에뮬레이터가 있는 랩톱과 같은 시리얼 케이블 또는 시리얼 콘솔을 사용해 어플라이언스에 연결할 수도 있습니다. 지침에서는 노트북을 예로 들어 설명합니다.

1. 다음 방법 중 하나를 사용하여 랩톱을 어플라이언스에 연결합니다.
   - RS232 케이블을 랩톱의 DB9 직렬 포트 커넥터에서 어플라이언스의 콘솔 포트로 연결합니다.

- 크로스오버 케이블을 랩톱의 이더넷 포트에서 어플라이언스의 관리 포트로 연결합니다.

2. 전원 케이블을 어플라이언스에 연결합니다.
3. 전원 버튼을 눌러 어플라이언스를 켭니다. 부팅이 완전히 완료될 때까지 기다리십시오. 부팅 프로세스를 중단하지 마십시오.

> 전원을 적용하려면 전면 패널을 제거해야 할 수 있습니다.
>
> 일부 모델의 경우 시스템 전원이 켜지지 않은 상태에서 전원 공급 장치 팬이 켜집니다. 전면 패널의 LED가 켜져 있는지 확인합니다. UPS(무정전 전원 공급 장치)에 어플라이언스가 연결되어 있는지 확인합니다. 전원 공급 장치에 전원이 연결되지 않은 경우 시스템에 오류가 표시됩니다.

4. 랩톱에서 어플라이언스로 연결합니다.

   사용 가능한 모든 터미널 에뮬레이터를 사용해 어플라이언스와 통신할 수 있습니다.

5. 다음 설정을 적용합니다.

   - BPS: 115200
   - 데이터 비트: 8
   - 정지 비트: 1
   - 패리티: 없음
   - 플로우 제어: 없음

   로그인 화면과 로그인 프롬프트가 표시됩니다.

6. 4로 **6. Secure Network Analytics 시스템 구성** 구성.

CIMC를 사용하여 연결(원격 액세스에 필요)

Cisco Integrated Management Controller(CIMC)를 사용하면 서버 설정 및 가상 서버 콘솔 액세스는 물론 하드웨어 상태 모니터링도 가능합니다. 또한 Secure Network Analytics 시스템 구성에서 CIMC를 사용합니다.

1. Cisco UCS C-Series 통합 관리 컨트롤러 GUI 구성 가이드의 지침을 따르십시오.
2. CIMC에 관리자로 로그인하고 Password(비밀번호) 필드에 **비밀번호**를 입력합니다.
3. 기본 비밀번호를 변경하여 네트워크 보안을 보호합니다.
4. 4로 **6. Secure Network Analytics 시스템 구성** 구성.

6. Secure Network Analytics 시스템 구성

가상 버전 어플라이언스 및/또는 하드웨어 어플라이언스 설치를 완료했다면 관리되는 시스템에 Secure Network Analytics를 구성할 준비가 된 것입니다.

> ⚠ Secure Network Analytics를 구성하려면 Secure Network Analytics 시스템 구성 가이드 v7.4.1의 지침을 따르십시오. 이 단계는 시스템의 성공적인 구성 및 통신에 매우 중요합니다.

시스템 구성 요구 사항

CIMC를 통해 어플라이언스 콘솔에 액세스할 수 있는지 확인합니다.

다음 표를 사용하여 각 어플라이언스에 대한 필수 정보를 준비합니다.

설정 요구 사항	세부정보	어플라이언스
IP Address(IP 주소)	`eth0` 관리 포트에 라우팅 가능한 IP 주소를 할당합니다.	
Netmask		
게이트웨이		
브로드캐스트		
Host Name(호스트 이름)	각 어플라이언스에는 고유한 호스트 이름이 필요합니다. 다른 어플라이언스와 동일한 호스트 이름을 사용하여 어플라이언스를 구성할 수 없습니다. 또한 각 어플라이언스 호스트 이름이 인터넷 호스트에 대한 인터넷 표준 요구 사항을 충족하는지 확인합니다.	
도메인 이름	각 어플라이언스에는 정규화된 도메인 이름이 필요합니다. 빈 도메인을 사용하여 어플라이언스를 설치할 수 없습니다.	
DNS 서버	이름 확인용 내부 DNS 서버	
NTP 서버	서버 간 동기화를 위한 내부 시간 서버입니다. 각 어플라이언스에 최소 1개의 NTP 서버가 필요합니다. 서버 목록에 있는 경우 130.126.24.53 NTP	

	서버를 제거합니다. 이 서버는 문제가 있는 것으로 알려져 있으며 기본 NTP 서버 목록에서 더 이상 지원되지 않습니다.	
메일 릴레이 서버	알림을 보낼 SMTP 메일 서버	
Flow Collector 내보내기 포트	플로우 컬렉터에만 필요합니다. NetFlow 기본값: 2055	
프라이빗 LAN 또는 VLAN 내에서 라우팅할 수 없는 IP 주소(상호 데이터 노드통신용)	데이터 노드에만 필요합니다. • 하드웨어 eth2 또는 eth2와 eth3의 결합 • 가상 eth1 **IP 주소:** 제공된 IP 주소를 사용하거나 상호 데이터 노드통신에 대한 다음 요구 사항을 충족하는 값을 입력할 수 있습니다. • 169.254.42.2와 169.254.42.254 사이의 **169.254.42.0/24 CIDR 블록**의 **라우팅할 수 없는 IP 주소**. • **처음 3개의 옥텟:** 169.254.42 • **서브넷:** /24 • **순차**: 유지 관리의 편의를 위해 순차 IP 주소(예: 169.254.42.10, 169.254.42.11, 169.254.42.12)를 선택합니다. **넷마스크:** 넷마스크는 255.255.255.0으로 하드 코딩되어 있으며 수정할 수 없습니다.	
eth0 하드웨어 연결 포트	데이터스토어 하드웨어 어플라이언스가 있는 Secure Network Analytics의 경우에만 필요합니다. • 관리자 2210 • 플로우 컬렉터 4210 • 데이터 노드s eth0 하드웨어 연결 포트 옵션:	

	• **SFP+**: SFP+: 10G SFP+/DAC 파이버 포트(eth0용). • **BASE-T**: 100Mbs/1GbE/10GbE eth0에 대한 BASE-T 구리 포트입니다. BASE-T가 기본값입니다.	

지원 팀에 문의

기술 지원이 필요하면 다음 방법 중 하나를 선택하십시오.

- 현지 Cisco 파트너에게 문의합니다.
- Cisco 지원팀에 문의
- 웹에서 사례를 확인하려면 http://www.cisco.com/c/en/us/support/index.html을 참조합니다.
- 이메일로 사례를 확인하려면 tac@cisco.com을 이용합니다.
- 전화 지원: 1-800-553-2447(미국)
- 월드와이드 지원 번호: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

저작권 정보