Cisco Security Packet Analyzer 2400 어플라이언스

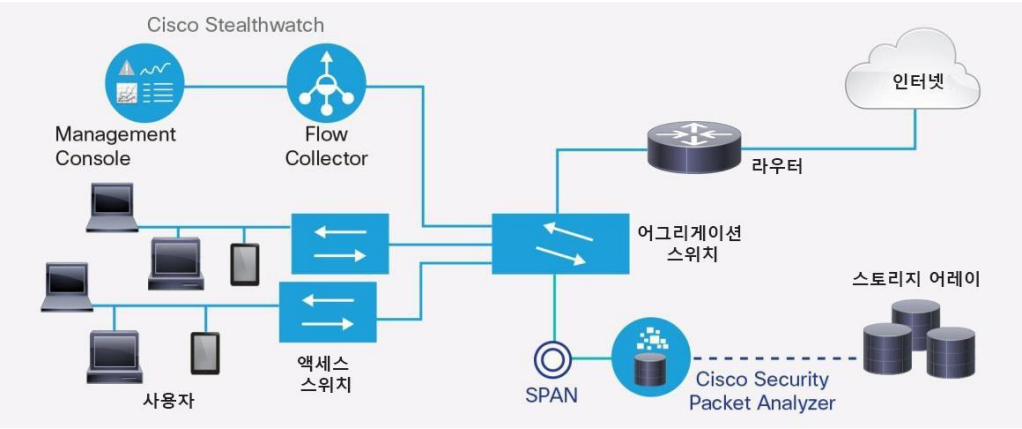
Cisco® Security Packet Analyzer는 위협 '탐지 및 대응' 기능을 강화하여 네트워크를 보호합니다. 비정상적인 네트워크 활동 및 보안 이벤트를 심층적으로 분석하여 전체 네트워크의 상태를 확보합니다.

네트워크 위협 및 사이버 범죄가 점점 똑똑해지고 있습니다. 문제는 네트워크에 보안 침해가 발생할지 여부가 아니라, 언제 발생할 것인지가 관건입니다. 네트워크의 가시성을 확보하고 지능형 위협에 빠르게 대응해야 할 필요성이 그 어느 때보다 커졌습니다. 대부분의 조직은 어느 정도의 보안 모니터링 및 사고 대응 능력을 갖추고 있습니다. 보안 전문가는 여러 가지 방법으로 사고 대응 속도를 단축할 수 있습니다. 일반적인 방법은 네트워크를 통과하는 모든 정보를 수집하고 저장할 수 있는 패킷 캡처 솔루션을 사용하는 것입니다.

더 나은 사고 대응을 위한 패킷 캡처 사용

네트워크 포렌식은 네트워크를 통해 이동하는 데이터를 모니터링하고 분석하며 이러한 결과를 이용하여 비정상적인 활동을 조사하는 프로세스입니다. Security Packet Analyzer는 이 포렌식 프로세스를 지원합니다. Cisco Security Packet Analyzer는 Cisco Stealthwatch와 함께 이용할 수 있습니다. 이렇게 하면 캡처된 데이터 패킷에 Stealthwatch NetFlow와 상황 정보 보안 분석 기능이 적용되므로 네트워크 세션의 상황 정보와 콘텐츠를 거의 실시간으로 검토할 수 있습니다. (그림 1 참조)

그림 1. 샘플 Packet Analyzer 및 Stealthwatch 구축



제품 개요

Security Packet Analyzer는 포트 미러링이라고 불리는 기능인 SPAN(Switched Port Analyzer) 또는 TAP(Test Access Point)를 통해 고객 네트워크에 연결됩니다. 네트워크의 해당 시점부터 패킷 트래픽 사본이 생성됩니다. Security Packet Analyzer는 이러한 네트워크 패킷의 전체 사본을 저장합니다. 저장된 사본은 향후 더욱 자세한 분석을 위해 솔루션에 포함된 패킷 분석 소프트웨어나 서드파티 분석 툴을 사용하여 검색할 수 있습니다.

그림 2. Cisco Security Packet Analyzer 2400

기능 및 이점

기능	이점
고성능 패킷 캡처	• 실시간 4 x 1GE 및 2 x 10GE 네트워크 성능이 추가되어 일반적으로 표준 NIC(Network Interface Card)에서 버리는 프레임을 포함한 모든 프레임 캡처
온프레미스 어플라이언스	• 데이터 기밀을 유지하기 위해 안전하고 고도의 보안이 된 온프레미스 캡처 및 스토리지 기능 제공
Stealthwatch와 통합	• Stealthwatch 플로우 데이터 분석을 사용하여 데이터 스트림에서 특정 지점을 찾고 Packet Analyzer에서 특정 패킷을 찾는 데 사용하는 상세 검색 쿼리 생성
API	• 기존 보안 및 네트워크 인프라에서 신속하고 간편하게 위협 인텔리전스 운용
업계 표준 스토리지	• Security Packet Analyzer는 업계 표준 패킷 캡처 형식으로 데이터를 저장하여 패킷 캡처나 WinPcap을 통해 고성능 패킷 캡처 가능

Cisco Security Packet Analyzer는 Cisco NAM(Network Analysis Module)에서 사용하기 위해 개발된 기술을 기반으로 합니다. NAM 버전 6.2의 기능 및 개선 사항을 바탕으로 하여 개발되었습니다. 여기에는 RISE(Remote Integrated Services Engine) 기술 지원이 포함되며, 이를 통해 스위치(Cisco Nexus® 7000 시리즈 등)에서 Packet Analyzer 어플라이언스를 블레이드로 "볼" 수 있습니다. 또 다른 중요 사항으로는 트래픽 캡처 기능을 확장하기 위해 데이터 포트에서 사용하던 ERSPAN(Encapsulated Remote SPAN)이 종료되었습니다. 데이터 포트에서의 고속 ERSPAN이 종료됨으로써, Packet Analyzer가 Type III ERSPAN 헤더에 액세스하고 더 빠른 속도로 ERSPAN을 처리할 수 있게 되었습니다.

Cisco UCS®(Unified Computing System™) C240 랙 마운트 서버 플랫폼을 최대로 활용하는 Security Packet Analyzer 어플라이언스는 높은 수준의 성능, 안정성 및 관리 효율성을 제공합니다. Security Packet Analyzer 어플라이언스는 네 개의 기가비트 이더넷 또는 두 개의 10기가비트 이더넷 모니터링용 구리(RJ-45) 또는 광학(소형 폼 팩터 플러그 또는 SFP) 인터페이스와 100/1000 RJ-45 이더넷 관리 포트로 구성할 수 있습니다. 이 어플라이언스 솔루션에는 128GB의 DRAM 및 운영 중 교체 가능한 48TB의 엔터프라이즈급 SAS 스토리지가 포함됩니다. 스토리지는 외부 SAS 포트를 통해 확장할 수 있습니다.

제품 사양

표 1. 제품 사양

Packet Analyzer 기능	설명
섀시	랙 유닛 2개(2RU)
프로세서	Intel® Xeon® E5-2660 프로세서 2개
메모리	128GB 업계 표준 DDR4(Double Data Rate) 주 메모리
저장	48TB(24 x 2TB) SAS 드라이브
스토리지 확장	마더보드의 SAS 포트 및 mLOM(modular LAN on motherboard)

Packet Analyzer 기능	설명
모니터링 포트(하나 선택)	• 4 x 1GE RJ-45 • 4 x 1GE SFP • 2 x 10GE SFP+
관리 포트	10/100/1000 RJ-45
물리적 크기	2RU: 3.43 x 17.65 x 29.0in.(8.71 x 44.83 x 73.66cm) 핸들 제외 3.43 x 18.96 x 30.18in.(8.71 x 48.16 x 76.66cm) 핸들 포함
온도: 작동	41~95°F(5~35°C)(해발 높이에서 작동, 팬 고장(fan fail) 없음, CPU 속도 제한 없음, 터보 모드)

규제 표준

표 2에는 규제 표준 컴플라이언스 정보가 나와 있습니다.

표 2. 규제 표준 컴플라이언스: 안전 및 EMC

사양	설명
안전	• UL 60950-1 No. 21CFR1040 Second Edition • CAN/CSA-C22.2 No. 60950-1 Second Edition • IEC 60950-1 Second Edition • EN 60950-1 Second Edition • IEC 60950-1 Second Edition • AS/NZS 60950-1 • GB4943 2001
EMC: 배출	• 47CFR Part 15(CFR 47) Class A • AS/NZS CISPR22 Class A • CISPR2 2 Class A • EN55022 Class A • ICES003 Class A • VCCI Class A • EN61000-3-2 • EN61000-3-3 • KN22 Class A • CNS13438 Class A
EMC: 내성	• EN55024 • CISPR24 • EN300386 • KN24

워런티 정보

워런티 정보는 Cisco.com의 제품 워런티 페이지에서 확인하십시오.

주문 정보

제품을 주문하려면 Cisco 주문 홈페이지를 방문하십시오.소프트웨어를 다운로드하려면 Cisco Software Center를 방문하십시오. 주문 정보는 표 3을 참조하십시오.

표 3. Cisco Security Packet Analyzer 주문 정보

제품 이름	부품 번호
Cisco Security Packet Analyzer 2400	SEC-PA-2400-K9

Cisco Security Packet Analyzer를 주문할 때 주문 편의를 위해 Cisco 주문 홈페이지에서 SFP 부품 번호(표 4)를 확인할 수 있습니다.

표 4. SFP 주문 정보

제품 이름	부품 번호	주문 정보
MMF용 10GBASE-SR SFP+ 모듈	SFP-10G-SR=	Cisco SFP+ 모듈 및 관련 케이블에 관한 주문 정보는 Cisco 10GBASE SFP+ 모듈 데이터 시트를 참조하십시오.
SMF용 10GBASE-LR SFP+ 모듈	SFP-10G-LR=	
SMF용 10GBASE-ER SFP+ 모듈	SFP-10G-ER=	
1000BASE-T 표준	GLC-T=	Cisco SFP 모듈에 관한 주문 정보는 Cisco SFP 모듈 데이터 시트를 참조하십시오.
1000BASE-SX 단파장, DOM 사용	GLC-SX-MMD=	
1000BASE-LX/LH 장파장, DOM 사용	GLC-LH-SMD=	

Cisco Services

Cisco 및 파트너의 제공 서비스

Cisco 및 Cisco의 파트너가 제공하는 지능형 맞춤 서비스를 사용하여 기술 투자의 비즈니스 가치를 최대한 실현하십시오. 심층적인 네트워킹 전문 기술과 다양한 파트너 생태계를 갖춘 Cisco Services는 고객이 네트워크를 성공적으로 계획 및 구축하여 강력한 비즈니스 플랫폼으로 운영할 수 있도록 지원합니다. 높아지는 고객 기대치를 충족시키기 위한 새로운 기회를 빠르게 포착, 운영 효율성 개선을 통한 비용 절감, 위험 완화, 성장 가속화 등의 요구사항을 지원하는 서비스를 제공합니다. Cisco Services에 대한 자세한 내용을 보려면 http://www.cisco.com/go/services를 참조하십시오. 표 5에서는 Cisco Security Packet Analyzer에서 권장되는 기술 지원 서비스를 보여줍니다.

표 5. Cisco Technical Services

Technical Services(기술 지원 서비스)
Cisco Smart Net Total Care™ 서비스는 다음과 같은 기능을 제공합니다. • 전 세계 어디서든 Cisco TAC(Technical Assistance Center)에 24시간 액세스 • 온라인 기술 자료, 커뮤니티 및 툴 액세스 • 2시간, 4시간 및 익영업일* 서비스를 포함한 하드웨어 교체 옵션 • 지속적인 운영 체제 소프트웨어 업데이트** • Smart Call Home으로 가능해진 디바이스에 대한 스마트한 예방적 진단 및 실시간 알림

* 장애 제품 선교체는 다양한 서비스 레벨을 조합하여 사용할 수 있습니다. 예를 들어 "8x5xNBD"는 표준 영업일(해당 지역에서 일반적으로 인정되는 영업일)당 8시간, 주 5일, NBD(익영업일)에 출고가 시작된다는 것을 의미합니다. 익영업일 배송이 불가능한 경우 당일 출고됩니다.
이 경우 제한 사항이 적용됩니다. 자세한 내용은 해당 서비스 설명을 검토하십시오.

** Cisco 운영체제 업데이트에는 라이선스 기능 세트 범위 내의 유지 관리 릴리스, 주요 업데이트 및 사소한 업데이트가 포함됩니다.

Cisco Capital

목표 달성을 지원하는 파이낸싱

Cisco Capital이 목표 달성과 경쟁력 유지에 필요한 기술 도입을 도와드리겠습니다. 고객의 설비 투자 부담을 줄여드립니다. 성장을 가속화하십시오. 투자 및 ROI를 최적화하십시오. Cisco Capital 파이낸싱은 하드웨어, 소프트웨어, 서비스, 보완적인 서드파티 장비 도입 편의성을 제공합니다. 또한, 정해진 일자에 비용 결제를 한 번만 하면 됩니다. Cisco Capital은 100여 개 국가에서 이용 가능합니다. 자세히 알아보십시오.

추가 정보

Cisco Security Packet Analyzer 어플라이언스에 대한 자세한 내용을 알아보려면 해당 지역 어카운트 담당자를 방문하거나 Cisco Security Product Analyzer 제품 마케팅 그룹 이메일(secpa-info@cisco.com)로 문의해 주십시오.

미주 지역 본부
Cisco Systems, Inc.
San Jose CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco는 전 세계에 200여 개 이상의 지사가 있습니다. 각 지사의 주소, 전화 번호 및 팩스 번호는 Cisco 웹 사이트 **www.cisco.com/go/offices**에서 확인하십시오.

Printed in USA C78-737589-01 08/16