Cisco Cyber Threat Defense v2.0
한 눈에 보는 설계 가이드

최종 업데이트: 2016-10-17

목차

소개

이 문서의 목표

보안 전문가들은 최근 기존의 방어가 다양한 일반 위협에 대해서는 여전히 효과적이지만 더욱 지능화되고 단호한 공격자에게는 취약하다는 사실을 차츰 인식하게 되었습니다. 실제로 효율성이 98% 또는 99%인 방어 기능이 사용 가능한 최고의 기능으로 간주되는데, 이는 모든 공격 중 1-2%가 여전히 방어를 우회하는 데 성공하고 가장 위험한 위협을 포함하고 있음을 의미합니다. 설상가상으로 대부분의 방어 기능은 일반적으로 네트워크 경계에 집중되어 있기 때문에 진입에 성공한 위험한 공격을 탐지하지 못하는 일이 흔히 발생합니다.

Cisco CTD(Cyber Threat Defense) 솔루션에서는 이러한 최신 지능형 위협에 맞서는 심층 방어를 위해 통합 및 검증된 아키텍처를 제공합니다. Cisco 접근 방식의 핵심은 진입 시뿐만 아니라 엔터프라이즈 전체에서 가시성과 제어 기능을 제공하는 네트워크 인프라의 중심성입니다. 총체적인 통합 아키텍처 접근 방식만이 전체 공격 라이프사이클의 전 범위(공격 전, 공격 중, 공격 후)에 대한 포괄적 커버리지를 제공할 수 있습니다. 이 설계 가이드에서는 Cisco Cyber Threat Defense 솔루션에 대한 주요 업데이트인 버전 2.0을 소개합니다.

대상

이 문서는 강력한 분산형 보안 아키텍처를 구축하는 방법을 숙지하여 최신 지능형 위협을 해결하고자 하고, 지속적인 유연성을 토대로 가상 및 물리적 워크로드를 운영하려고 하며, 기존 모드에서 업무를 수행 중이거나 클라우드 운영 모델로 마이그레이션한 보안 설계자, 시스템 설계자, 네트워크 설계 엔지니어, 시스템 엔지니어, 현장 컨설턴트, Advanced Services 전문가 및 고객을 대상으로 하며 이에 국한되지는 않습니다. 또한 이 문서에서는 별도의 설계 및 구축 가이드에 설명된 추가적인 보완 솔루션을 활용합니다. 이 문서에서는 독자가 IP 프로토콜, QoS(Quality of Service), HA(High Availability), 보안 기술의 기본 개념을 잘 알고 있다는 것을 전제로 합니다. 또한 독자가 일반적인 시스템 요건을 잘 알고 있고 엔터프라이즈 네트워크 및 데이터 센터 아키텍처에 대한 지식을 갖추고 있다고 전제합니다.

Executive Summary

초기 버전의 Cisco Cyber Threat Defense 솔루션은 2013년 도입되었으며, CVD(Cisco Validated Design)를 사용하여 Cisco 네트워크 인프라의 NetFlow 텔레메트리, 사용자 및 디바이스 신원에 대한 ISE(Identity Services Engine) 및 Lancope, Inc.와의 파트너십을 통한 StealthWatch System을 통합하여 네트워크 내부에서 네트워크 동작 분석 및 위협 탐지를 제공했습니다.

이 문서에서는 이전 솔루션의 네트워크 가시성을 기반으로 구축된 Cisco Cyber Threat Defense 아키텍처의 주요 업데이트 및 확장을 소개합니다. 버전 2.0에는 Cisco가 2013년 후반에 인수한 Sourcefire(현재는 Cisco FirePOWER로 알려져 있음)의 업계를 선도하는 NGIPS(Next Generation Intrusion Prevention Systems) 및 AMP(Advanced Malware Protection) 구성 요소가 통합되어 있습니다. 이 솔루션에는 이메일 및 웹 콘텐츠 보안과 같은 Cisco 보안 포트폴리오의 기타 요소와 ISE 버전 1.3의 Cisco TrustSec 및 EPS(Endpoint Protection Services)를 사용하여 네트워크 자체를 정책 시행 포인트로 활용할 수 있는 기능이 포함되어 있습니다.

솔루션 개요

솔루션 설계

그림 1에서는 네트워크 에지 구축에 대해 너무 많은 세부 사항을 검토하지 않고 다른 CVD의 모범 사례를 기반으로 구축한 Cisco Cyber Threat Defense 솔루션의 개괄적인 아키텍처를 보여줍니다. Cyber Threat Defense 솔루션의 목표는 위협이 네트워크 내부에 침투한 후 위협을 쉽게 검색, 억제, 조치할 수 있는 설계 및 아키텍처를 소개하는 것입니다. 데이터 센터 고려 사항은 Secure Data Center CVD에 대한 Cyber Threat Defense 솔루션에 작성되어 있습니다.

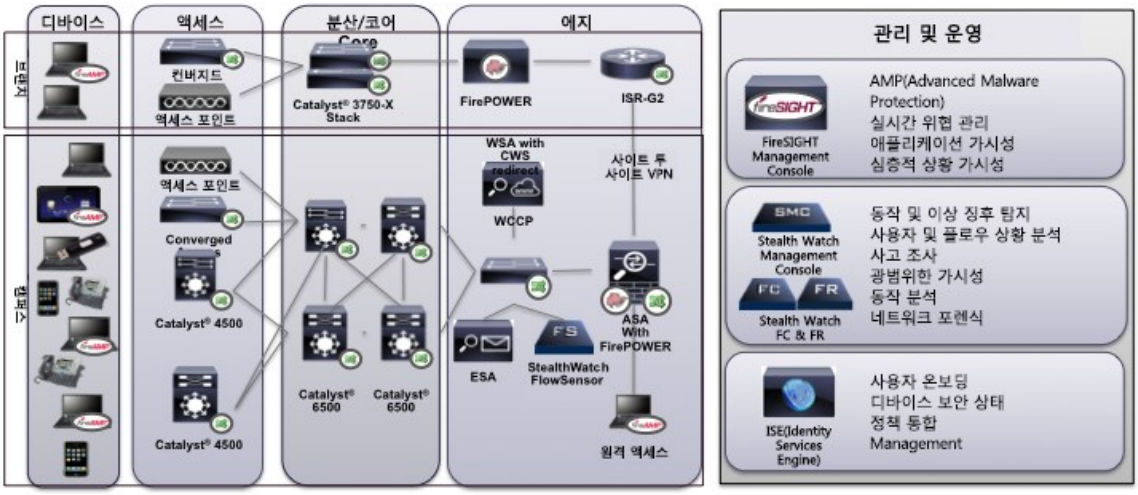


그림 1 - Cisco Cyber Threat Defense 솔루션의 개괄적인 아키텍처

Cisco Cyber Threat Defense 솔루션 버전 2.0에서는 다음과 같은 몇 가지 솔루션을 사용하여 목표를 달성합니다.

- NetFlow 및 StealthWatch System:
  - 광범위한 가시성
  - 사용자 및 플로우 상황 분석
  - 네트워크 동작 및 이상 징후 탐지
  - 사고 대응 및 네트워크 포렌식
- Cisco FirePOWER 및 FireSIGHT
  - 실시간 위협 관리
  - 경계를 우회하는 위협에 대한 심층적인 상황 가시성
  - URL 제어
- AMP(Advanced Malware Protection)
  - AMP for Endpoints로 엔드포인트 제어
  - AMP for Networks 및 AMP for Content로 악성코드 제어
- Content Security Appliances and Services
  - Cisco WSA(Web Security Appliance) 및 CWS(Cloud Web Security)
    - 웹 트래픽에 대한 동적 위협 제어
    - 아웃바운드 URL 분석 및 데이터 전송 제어
    - 의심스러운 웹 활동 탐지
  - Cisco ESA(Email Security Appliance)
    - 이메일 트래픽에 대한 동적 위협 제어
    - 의심스러운 이메일 활동 탐지
- Cisco ISE(Identity Services Engine)
  - StealthWatch와 사용자 및 디바이스 신원 통합
  - pxGrid를 사용한 조치 정책 실행

경계를 뛰어넘는 사고

거의 매일 대기업, 엔터프라이즈 및 정부에 대한 사이버 기반 데이터 유출과 절도가 새롭게 보고되고 있습니다. 이러한 사고의 경우 대부분 엔터프라이즈는 공격자의 직접 대상이 되며 최초 유출은 절도 발견 수개월 전에 발생한 것으로 나타납니다. 과거에는 업계에서 이러한 공격 유형을 지칭할 때 APT(Advanced Persistent Threat)라는 용어를 (과도하게) 사용했습니다. 업계에서 이 용어가 본래 의미를 거의 잃어버릴 정도로 과도하게 사용되었지만 다음과 같은 정의를 다시 재고할 필요가 있습니다.

> *APT(Advanced Persistent Threat): 공격자가 여러 공격 벡터(예: 사이버, 물리적, 기만)를 사용하여 목표를 달성하기 위한 기회를 만들 수 있는 정교한 수준의 전문 지식과 상당한 리소스를 보유한 상대.* [NIST IR 7298 Rev 2]

이 정의의 일부는 특별히 주목할 가치가 있습니다. 첫 번째 가장 중요한 부분은 *공격자*를 지칭하고 있다는 사실입니다. 즉, APT가 단순히 한 번의 공격, 익스플로잇 또는 하나의 악성코드가 아니라 단호한 공격자가 대상 엔티티에 대해 가하는 전체 캠페인을 의미한다는 사실입니다. 두 번째는 공격자는 둘 이상의 방법을 사용한다는 사실입니다. 그러므로 공격자의 보안 침해 시도를 여러 번 성공적으로 차단하더라도 공격자는 한 가지 방법이라도 성공할 때까지 계속해서 다른 방법을 시도할 수 있습니다.

따라서 APT에 대한 보호에는 대상 엔티티에 침투하여 목적을 달성하기 위해 논리와 기술을 사용하는 단호한 공격자에 대한 방어 기능이 포함됩니다. 이러한 공격자를 방어하기 위해서는 공격자가 어느 지점에서 경계를 뚫고 네트워크에 작업 공간을 확보할 수 있다는 사실을 인식해야 합니다. Cisco Cyber Threat Defense 솔루션의 주요 목표는 보안 운영자가 네트워크 내부에 발을 들여 놓은 공격자의 존재를 발견할 수 있도록 네트워크 내부에 기능을 추가하는 것입니다.

보안 침해 지표

APT 및 최신 위협의 특징은 공격의 시작과 마지막 실행 단계 사이에 상당한 시간차가 있다는 점입니다. 따라서 공격을 발견할 수 있는 새로운 접근법이 필요합니다. 이전의 레거시 위협 시스템에서는 대부분 공격으로 보이는 모든 활동을 탐지하는 접근법을 기반으로 수천 개의 알림을 생성합니다. 새로운 접근법은 IOC(Indicators of Compromise)를 활용하는 것입니다.

> *지표: 사고가 발생했거나 현재 발생하고 있을 가능성이 있다는 신호입니다.* [NIST SP 800-61]

IOC 접근법은 단호한 상대 또는 동기 부여된 공격자가 보안 경계를 우회하여 네트워크상에서 작업 공간을 확보하려는 위치를 찾아냄으로써 정확한 양의 툴을 적소에 가져와서 공격자의 존재 여부뿐만 아니라 그들의 작업 방식까지 알아내는 것입니다. 이러한 접근 방식은 어떤 징후가 나타났는지에 대해 더욱 폭넓고 정확한 분석을 제공하는 요소로 이루어지며, 다음 항목이 포함될 수 있습니다.

- 어떤 공격인지 (예: 알려진 유형 또는 범주)
- 구체적인 공격 내용은 무엇인지 공격의 실행 방법은 어떤 것인지 대상 엔드포인트 및 기타 항목에 변경된 사항이 있는지
- 공격의 출처는 어디인지
- 어떤 유해성이 있는지
- 대상은 무엇인지 어느 호스트인지 사용자는 누구인지
- 이 디바이스에서 접촉한 다른 시스템/사용자는 무엇인지
- 대상 애플리케이션 또는 데이터는 무엇인지
- 그 대상은 이 이벤트의 영향을 받을 가능성이 있는지
- 이는 새로운 문제인지 아니면 BYOD(Bring-Your-Own-Device) 같은 외부 소스를 통해 일어난 문제인지
- 현재 공격 호스트가 네트워크 내부에 있습니까 외부에 있는지
- 근본 원인은 무엇인지
- 시스템에서는 이러한 위협에 취약한 호스트 또는 네트워크 디바이스가 몇 개인지 즉시 확인할 수 있는지
- 이 공격이 차단될 경우, 시스템에서는 이러한 알림이 오탐인지 또는 실제 공격인지 여부를 어떻게 확인할 수 있는지

지능형 보안 침해 지표 기능을 구현하려면 이벤트를 다음 항목과 연관 지어 상관관계를 파악해야 합니다.

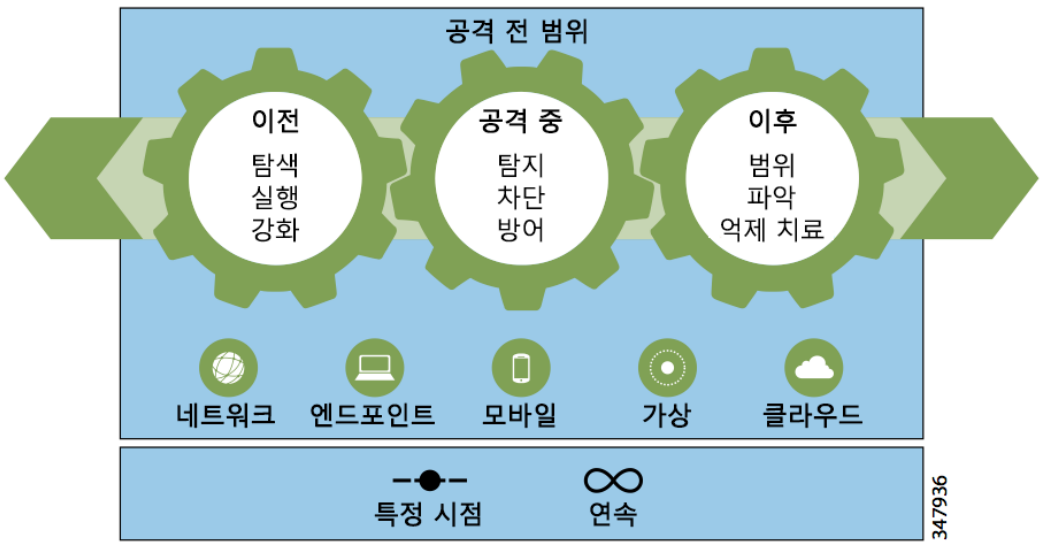
- 악성코드 활동
- 침입 탐지
- 네트워크 연결
- 네트워크 파일 전파 흔적
- 디바이스 전파 흔적
- 디바이스 네트워크 플로우(좌우 이동, 상위-하위 관계, 컨텍스트가 포함되며 이에 국한되지 않음)

위에 제시된 모든 항목의 목표는 네트워크, 엔드포인트, 애플리케이션, 사용자 컨텍스트와의 상관성을 분석하는 것입니다. 결과 데이터는 전체 네트워크에 걸쳐 즉시 실행 가능할 정도로 확실하고 정확한 보안 침해 지표를 제공할 수 있는 고유한 역량을 제공합니다.

네트워크 통합 보안을 활용하는 보안 모델

단호한 공격자의 특성으로 인해 엔터프라이즈에 영향을 미치는 위협에 대한 포괄적인 대응 방법을 개발하기 위해서는 새로운 툴과 기술이 필요합니다. 이는 복잡성을 최소화하고 지속적인 방식으로 비즈니스 자산을 보호하는 모델을 사용하는 동시에, 비즈니스 모델의 변경 사항(예: any-to-any)을 해결해야 합니다. 보안 시스템을 네트워크 패브릭에 직접 통합하여 효율성과 기능을 극대화하는 동시에, 네트워크를 인식하지 못하는 별도의 보안 제어를 추가하는 것과 관련하여 발생하는 위험을 최소화해야 합니다. 이러한 시스템을 설계하려면 특히 데이터 센터에서 이러한 통합이 올바르게 이루어지도록 보장하는 오차 범위가 아주 작은 새로운 모델이 필요합니다. 이러한 새 모델은 모든 유형의 네트워크를 위한 포괄적인 보안 솔루션을 개발할 때 유용한 참조가 될 수 있습니다. 새로운 모델에서는 공격의 전 범위라는 주요 구성 요소를 보여주며, 이는 완벽한 보안 시스템에 필수적인 각각의 중요 메커니즘 및 프로세스를 식별합니다.

새로운 보안 모델



이 모델에서는 공격의 전, 중, 후 전 범위에 걸쳐 수행해야 하는 조치 및 광범위한 공격 벡터(엔드포인트, 모바일 디바이스, 데이터 센터 자산, 가상 머신, 클라우드)를 살펴봄으로써 위협을 해결합니다. 대부분의 보안 솔루션은 특정 시점의 위협에 대응하는 경향이 있으므로, 지속적인 주기로 위협을 살펴보는 것이 중요합니다.

공격 전

상황 인식 공격자를 막아내기 위해서는 상황 인식 보안이 필요합니다. 조직은 인프라를 보호하려고 노력하는 방어자보다 조직의 인프라에 대해 더 많은 정보를 가지고 있는 공격자를 상대로 싸우고 있습니다. 공격자보다 정보 측면에서 우위를 차지하고 공격이 발생하기 전에 방어하기 위해서는 조직의 환경(물리적 및 가상 호스트, 운영 체제, 애플리케이션, 서비스, 프로토콜, 사용자, 콘텐츠, 네트워크 동작을 포함하되 이에 국한되지 않음)에 대한 완벽한 가시성이 필요합니다. 방어자들은 대상 값, 공격의 합법성, 이력을 기준으로 인프라에 대한 위험을 이해해야 합니다. 방어자가 보호하려는 대상을 이해하지 못할 경우, 방어를 위한 보안 기술을 구성할 준비를 할 수 없습니다. 가시성은 엔드포인트, 이메일 및 웹 게이트웨이, 가상 환경, 모바일 디바이스, 데이터 센터를 포함하여 네트워크 전체를 포괄해야 합니다. 이러한 가시성으로부터 방어자들이 정보에 기반을 둔 의사 결정을 할 수 있도록 실행 가능한 알림을 생성해야 합니다.

공격 중

집요한 공격과 복합적인 위협은 한 시점에만 발생하지 않습니다. 이러한 공격과 위협은 지속적인 활동이며 끊임없는 보안이 필요합니다. 기존 보안 기술은 공격의 단일 데이터 포인트 자체를 기준으로 특정 시점의 공격만 평가할 수 있습니다. 이 접근 방식은 더 이상 지능형 공격에 적합하지 않습니다.

대신, 인식 개념을 기준으로 한 보안 인프라, 즉, 지금까지의 패턴과 전반적인 공격 정보를 이용하여 확장된 네트워크에 걸쳐서 데이터를 취합하고 상관관계를 분석하여 컨텍스트를 제공하고 활성화된 공격, 유출, 정찰과 단순한 배경 활동을 구분할 수 있는 인프라가 필요합니다. 여기에는 특정 시점의 실행부터 연속적 분석, 의사결정에 이르는 보안이 포함됩니다. 안전하게 통과될 수 있는 파일로 간주되었으나 나중에 악의적인 동작이 나타나는 경우, 조직에서는 조치를 취할 수 있습니다. 이러한 실시간 통찰력으로 보안 전문가는 지능형 자동화를 채택하여 수동 개입 없이 보안 정책을 구현할 수 있습니다.

공격 후

조직이 공격의 전 범위에 대응하려면 회귀적 보안이 필요합니다. 회귀적 보안은 빅 데이터로 해결해야 할 과제이며 이 역량을 제공할 수 있는 조직은 거의 없습니다. 데이터를 지속적으로 수집하고 분석하여 보안 인텔리전스를 생성할 수 있는 인프라를 통해 보안 팀은 보안 침해 지표를 자동으로 식별하며, 탐지를 회피하는 동작을 수정할 수 있을 만큼 정교한 악성코드를 탐지한 후 문제를 해결할 수 있습니다.

몇 주 또는 몇 개월 동안 탐지되지 않았을 보안 침해 사항을 신속하게 식별, 조사, 방지, 해결할 수 있습니다. 조직은 이러한 위협 중심 보안 모델을 통해 모든 공격 벡터에서 공격의 전 범위에 대처하고 언제든지 실시간으로 대응할 수 있습니다.

참고: Cyber Threat Defense 2.0 솔루션은 공격 전 범위에서 "공격 중" 및 "공격 후" 단계에 1차적인 중점을 두고 있습니다. 추가 보안 솔루션은 Cisco DesignZone 웹 사이트에 있습니다.

솔루션 구성 요소

NetFlow

NetFlow는 Cisco Cyber Threat Defense 솔루션 최초 버전의 핵심 요소로, 이번 2세대 업데이트에서도 계속 중요한 역할을 수행합니다.

NetFlow는 Cisco IOS 소프트웨어에 내장된 계측 기능으로 연결 데이터를 검토하여 네트워크 운영의 특성을 묘사합니다. IPFix 프로토콜의 RFC 프로세스를 통해 표준화한 다양한 버전의 NetFlow는 Arista, Citrix, Huawei, Juniper, Palo Alto와 같은 벤더의 네트워크 장비 및 다양한 오픈 소스 Linux 운영 체제 배포판에서 사용할 수 있습니다.

NetFlow는 트래픽 플로우의 IP 네트워크 트래픽 특성을 측정하는 Cisco 애플리케이션입니다. 플로우는 Cisco 디바이스를 통과할 때 지정된 소스와 대상 사이의 단방향 패킷 스트림으로 식별됩니다. NetFlow는 초기에 대역폭, 애플리케이션 성능, 활용과 같은 네트워크 트래픽 특성을 측정하기 위해 만들어졌습니다. NetFlow는 일반적으로 청구 및 회계, 네트워크 용량 계획, 가용성 모니터링에 사용되었습니다.

NetFlow는 보고 기술입니다. NetFlow 지원 네트워크 디바이스로 트래픽을 처리하면 디바이스에서 트래픽 플로우에 대한 데이터를 수집하고 해당 데이터를 정의된 컬렉터로 보고하거나 내보냅니다. 이전 버전의 NetFlow에서는 연결을 종료한 후에만 데이터를 내보냈습니다. 이후의 NetFlow 구현에서는 하나 이상의 만료 타이머(활성 또는 비활성) 또는 조건(연결 완료 또는 캐시 가득참)을 정의할 수 있는 기능을 추가했습니다. NetFlow 보고의 특징은 부인 방지, 변칙 탐지, 조사 기능을 제공하는 기능 등 매우 다양한 보안 애플리케이션이 포함된다는 점입니다.

NetFlow는 처음 출시된 이후 다음 표에 표시된 것처럼 여러 버전을 거쳐왔습니다. 고정된 내보내기 형식의 버전(1, 5, 7, 8)은 유연하거나 조정 가능하지 않으며 각각의 새 버전에는 이전 버전과 호환되지 않는 새로운 내보내기 필드가 있습니다. NetFlow 버전 9에서는 수집 및 내보내기 프로세스를 완전히 분리하여 NetFlow 수집을 사용자 지정할 수 있습니다.

표 1 - NetFlow 버전

버전	상태
1	원본, 버전 5와 비슷하지만 시퀀스 번호 또는 BGP 정보가 없음
2	릴리스되지 않음
3	릴리스되지 않음
4	릴리스되지 않음
5	고정된 형식, 프로덕션에 가장 많이 사용되는 버전
6	릴리스되지 않음
7	버전 5와 비슷하지만 AS 인터페이스, TCP 플래그, TOS 정보가 포함되지 않으며, Cisco Catalyst 6500 및 7600에 한정됨
8	11개의 집계 방식 선택 가능, 엔터프라이즈에서 널리 사용되지 않음
9	추가 필드 및 기술을 지원할 수 있는 유연하고 확장 가능한 내보내기 형식
IPFIX	버전 9와 비슷하지만 표준화되었으며 가변 길이 필드가 있음
Flexible NetFlow	기존의 NetFlow를 뛰어넘는 플로우 데이터의 유연성 및 확장성 AVC를 통해 1000개 이상의 애플리케이션을 식별하고 분류할 수 있는 기능

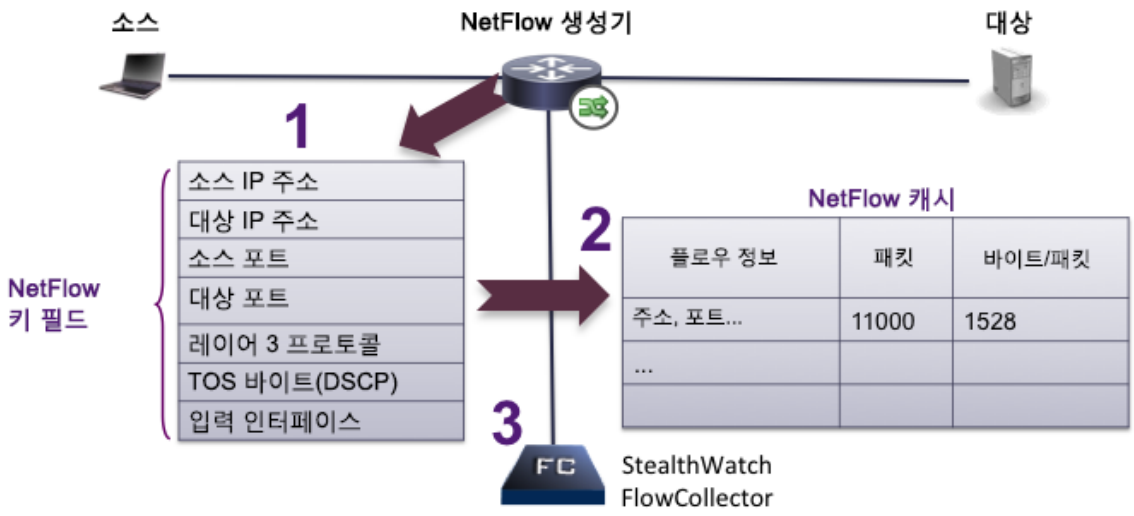
Cisco Cyber Threat Defense 솔루션에서는 Cisco IOS의 Flexible NetFlow 기능을 사용자 지정할 수 있다는 점을 활용하여 NetFlow 버전 9 레코드를 사용자 지정할 수 있습니다. 이러한 접근 방식을 사용하여 Cisco Cyber Threat Defense 솔루션을 위한 CVD에서는 차세대 NBAR2(Network Based Application Recognition) 및 Cisco AVC(Application Visibility and Control)를 사용하여 패킷 필드(TCP 플래그, TTL[Time-To-Live] 값, 프로토콜, 애플리케이션 이름 등)를 수집함으로써 각 디바이스의 보안 모니터링 잠재력을 극대화하도록 각 솔루션 디바이스에 대해 NetFlow 레코드를 정의했습니다. 이러한 필드 대부분은 이전 버전의 NetFlow 프로토콜에서 사용할 수 없습니다. 해당 필드가 없으면 Cisco Cyber Threat Defense 솔루션에 포함되어 사용되며 미세하게 조정된 일부 탐지 알고리즘에서 제공하는 장점 중 몇 가지가 사라지거나 최소화됩니다.

Cisco에서 개발한 NetFlow의 최신 버전은 Flexible NetFlow입니다. Flexible NetFlow에서는 NetFlow 버전 9의 기능을 확장하여 고객이 리소스 사용을 최적화하고, 네트워크 성능을 계획하고, QoS(Quality of Service)를 위한 최적의 애플리케이션 레이어를 식별하는 방법을 결정할 수 있도록 지원합니다. Flexible NetFlow는 DoS(denial-of-service) 공격과 네트워크에서 전파되는 웜을 탐지함으로써 네트워크 보안에서 중대한 역할을 합니다.

모범 사례: 가능한 경우 Cisco IOS Flexible NetFlow 기능을 사용합니다.

다음 그림에서는 Cisco 디바이스의 NetFlow 작업을 설명합니다.

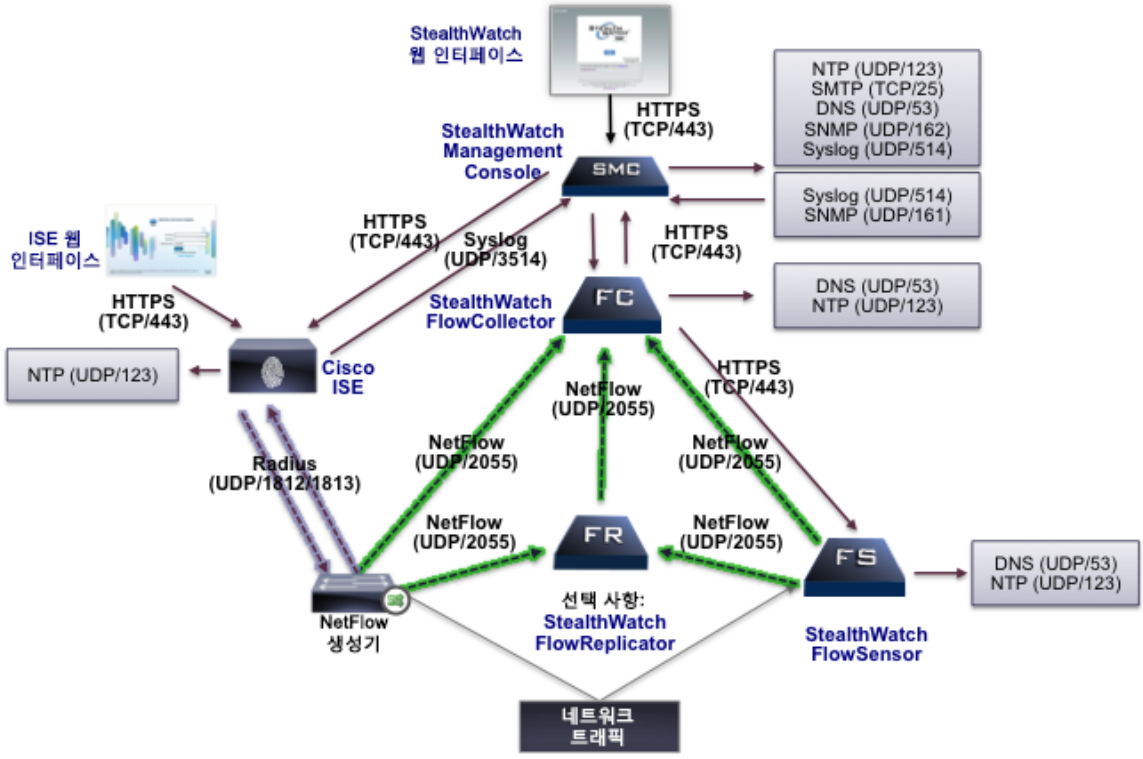
(1) 데이터가 NetFlow 지원 디바이스(NetFlow Generator)를 통과하면서 디바이스 연결 테이블이 추출되고 NetFlow 키 데이터 필드가 추출됩니다.
(2) 키 필드는 새 플로우 데이터를 식별한 후 기존 플로우와의 상관성을 분석하고 디바이스에서 유지되는 플로우 데이터베이스인 NetFlow 캐시에 새 항목을 만드는 데 사용됩니다. Cisco 디바이스에서는 키 필드 이외에도 추가 구성된 수집 필드(TCP 플래그, 바이트 카운터, 시작 및 종료 시간 등)를 수집하고 이러한 정보를 해당 플로우에 대한 NetFlow 캐시 항목에 저장합니다.
(3) 플로우가 종료되거나 시간 초과 이벤트가 발생하면 플로우 레코드라고 하는 NetFlow PDU(Protocol Data Unit)를 생성하여 플로우 컬렉터로 내보냅니다.



StealthWatch System

Cisco에서 제공하는 StealthWatch 시스템은 특수 제작된 고성능 네트워크 가시성 및 보안 인텔리전스 솔루션입니다. StealthWatch 시스템에서는 기타 상황 인식 데이터 소스(Cisco ISE의 신원 데이터 등), 시스템별 데이터(시스템 로그 및 SNMP 등), NBAR2 및 Cisco AVC를 통한 애플리케이션 데이터와 함께 NetFlow 데이터를 수집, 집계, 분석하여 보안 운영자가 네트워크의 모든 사용자, 디바이스, 트래픽에 대한 상황을 실시간으로 인식할 수 있도록 지원합니다. 또한 StealthWatch 시스템에서는 모든 네트워크 트래픽에 대한 보기 및 실시간 포렌식을 지속적으로 제공하여 보안 운영자가 보안 사고 발생 전, 발생 중, 발생 후 위협에 빠르고 효과적으로 대응할 수 있습니다.

StealthWatch 시스템은 Cisco Cyber Threat Defense 솔루션의 구성 요소로, 다음 다이어그램과 표에 표시된 것처럼 여러 개의 개별 구성 요소가 연결되어 구성됩니다.



구성 요소	설명
StealthWatch Management Console	모든 StealthWatch 어플라이언스에서 엔터프라이즈 전반에 걸쳐 보안 및 네트워크 인텔리전스의 상관성을 분석하도록 관리, 조정, 구성합니다. Cisco Identity Services Engine에서 인증된 세션 정보를 검색하여 플로우와 신원의 상관성을 분석합니다.
StealthWatch FlowCollector	NetFlow 지원 디바이스로 생성한 플로우 데이터의 중앙 컬렉터 역할을 합니다. StealthWatch FlowCollector에서는 네트워크 트래픽을 모니터링, 분류, 분석하여 네트워크 및 호스트 레벨 모두에서 포괄적인 보안 인텔리전스를 만듭니다.
StealthWatch UDP Director(FlowReplicator라고도 함)	고속의 단일 어플라이언스에서 NetFlow, 시스템 로그, SNMP 정보를 집계합니다. 이러한 고속 UDP 패킷 복제기에서는 여러 위치에서 필수 네트워크 최적화 및 보안 정보를 수집한 다음 이 정보를 단일 데이터 스트림으로 하나 이상의 StealthWatch FlowCollector 어플라이언스에 전달합니다.
StealthWatch FlowSensor	모든 호스트 및 서버 통신과 네트워크 트래픽 통계를 수동적으로 모니터링하고 FlowCollector로 전송되는 플로우 레코드로 변환합니다.
StealthWatch FlowSensor VE	가상 어플라이언스는 가상 서버 내에서 실행되도록 설계되었습니다. FlowSensor VE에서는 VM 내 트래픽을 수동적으로 모니터링하고 FlowCollector로 전송되는 플로우 레코드로 변환합니다.

차세대 침입 방지 시스템

Cisco의 NGIPS(Next-Generation IPS) 솔루션에서는 지능형 위협 방지를 위해 필수적이면서도 진보적인 기능 구조를 제공합니다. Cisco NGIPS에서는 실시간 상황 인식 및 보안 자동화 기능을 통해 보안 인텔리전스를 네트워크 패브릭에 통합합니다. 또한 위협을 평가 및 완화하고, 응답에 일관성 및 프로세스를 제공하며, 조직의 보안 비용을 절감할 수 있도록 상황 정보 및 인식을 활용하여 세부 정보(네트워크 활동, 운영 체제, 애플리케이션, 사용자 등)를 제공합니다. 보고 및 고도의 분석과 알림 기능을 활용하는 것 이외에도 위협 환경이 계속 진화함에 따라 공격 및 포렌식 기능을 포착하는 것은 물론 이해하는 것도 중요해졌습니다. Cisco NGIPS 솔루션에서 사용할 수 있는 이러한 이해 및 완화

솔루션이 등장하면서 이제 공격을 탐지할 수 있는 기능뿐만 아니라 공격을 방지할 수 있는 기능도 제공하게 되었습니다.

공간, 전원, 운영 관리 및 효율성과 같은 환경 요인이 진화하면서 이러한 환경 역동성을 이해할 수 있는 기능과 구축 유연성을 제공하는 다기능 보안 디바이스의 출현을 촉발시켰습니다. 다음은 Cisco NGIPS 솔루션의 주요 특성입니다.

- 다양한 클라이언트 애플리케이션 및 활동을 확인, 모니터링, 검사하고, Cisco AVC(Application, Visibility, Control)를 활용하는 한편 해당 정보에 정책을 시행할 수 있습니다.
- 환경 내부 및 외부(상관성 분석을 위해 외부적으로 사용할 수 있는 요인/정보를 참조하는 기능의 경우)에 있는 다양한 유형의 상황 데이터에 즉시 액세스하여 네트워크 동작, 사용자 신원, 네트워크 리소스, 공격 트렌드 및 벡터, 트래픽 프로필 등을 확인할 수 있습니다.
- 인라인에 있을 수 있지만 네트워크 운영을 방해하지 않습니다.
- 취약성과 위협 중심 시그너처 및 벡터를 지원할 수 있습니다.
- 프로토콜에 관계없이 통과 트래픽에 콘텐츠 인식 및 데이터 유출 방지 기능을 지원할 수 있습니다. 여기에는 인바운드 및 아웃바운드 파일과 실행 가능 파일에서 PDF 및 오피스 파일에 이르는 첨부 파일을 검사하고 분류할 수 있는 기능과 URL 필터링이 포함됩니다.
- 인텔리전스 수집을 지원하여 상황 인식 기능을 사용하거나, 통과 트래픽에 대한 차단/필터링 및/또는 경고와 관련된 의사 결정을 효과적으로 개선할 수 있도록 다양한 소스에서 정보를 가져올 수 있습니다.

FirePOWER

Cisco ASA with FirePOWER Services는 업계 최초의 적응형 위협 중심 NGFW (Next-Generation Firewall)로, Cisco ASA의 업계 최고 방화벽 기능과 업계 최고의 Cisco FirePOWERthreat 및 Advanced Malware Protection을 결합하여 공격 전 범위에 대해 통합 위협 방어를 제공합니다.

Cisco ASA에서는 스테이트풀 검사, NAT, VPN 라우팅 서비스 등을 계속 지원하면서 이제 Cisco FirePOWER Services를 패킷 플로우 경로에 통합합니다. FirePOWER Services 기능은 NGIPS 서비스 모듈 및 Advanced Malware Protection을 통해 URL 필터링, AVC, 위협 차단을 처리합니다. Cisco ASA 및 FirePOWER Services는 공동으로 아래 묘사된 바와 같이 완벽히 통합된 위협 중심 NGIPS/NGFW 솔루션을 제공합니다.

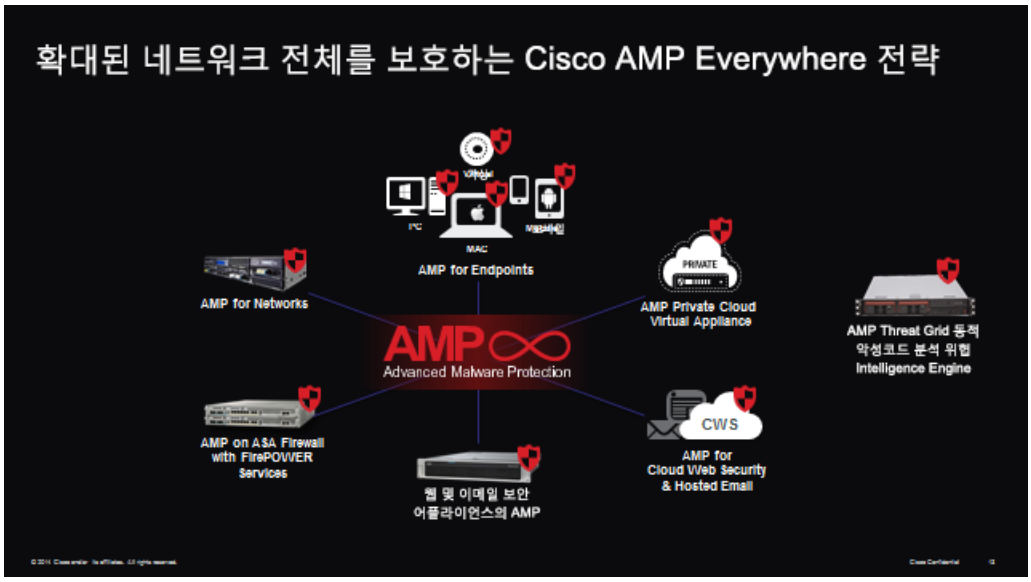
Cisco Advanced Malware Protection

Cisco AMP를 사용하면 사용자에게 확장된 네트워크와 공격 전, 중, 후 전 범위에 걸쳐 악성코드를 물리칠 수 있는 지속적인 가시성과 제어 기능을 제공할 수 있습니다.

- **공격 전:** 알려진 악성코드, 정책을 위반하는 파일 유형, 통신이 확장된 네트워크에 들어오는 것을 방지합니다.
- **공격 중:** 지속적으로 파일 및 네트워크 트래픽을 분석하여 1차 방어선을 통과한 위협을 찾아냅니다.
- **공격 후:** 활성 상태의 공격을 신속하고 효율적으로 파악하고 그 범위를 규정하고 억제하며 해결합니다.

Cisco AMP는 가장 광범위한 공격 벡터로부터 보호하며 다음과 같이 구축할 수 있습니다.

- 전용 Cisco ASA Firewall 및 Cisco FirePOWER 네트워크 보안 어플라이언스에 통합된 네트워크 기반 솔루션
- PC, Mac, 모바일 디바이스, 가상 환경의 엔드포인트 솔루션
- 개인 정보 보호 요건이 까다로운 환경에 적합한 온프레미스 프라이빗 클라우드 가상 어플라이언스
- Cisco Cloud Web Security Appliance 또는 Cisco Web & Email Security Appliance에 통합된 기능



Cisco AMP에서는 Cisco Talos Security Intellgence and Research Group은 물론 Cisco Collective Security Intelligence Ecosystem의 방대한 클라우드 보안 인텔리전스를 모두 활용하여 지능형 방어를 제공합니다. 또한 Cisco AMP는 Cisco AMP Thread Grid 동적 악성코드 분석과 위협 인텔리전스 기술을 통합하여 포착하기 어려운 지능형 사이버 위협을 식별하도록 데이터 집계 및 상관성 분석 기능을 강화합니다.

Cisco AMP에서는 다음과 같은 기능을 사용하여 지속적인 분석과 회귀적 알림 기능을 제공합니다.

- 파일 평판 – 파일 페이로드가 네트워크를 통과할 때 이를 인라인으로 분석하고, 기존 Cisco Web 또는 Email Security 사용자 인터페이스 및 유사한 정책 보고 프레임워크를 사용하여 사용자에게 악성 파일을 자동으로 차단하고 관리자 정의 정책을 적용하는 데 필요한 통찰력을 제공합니다.
- 파일 샌드박싱 – 높은 수준의 보안 샌드박스 환경을 활용하여 네트워크를 통과하는 알 수 없는 파일의 실제 동작을 분석하고 이해합니다. 이를 통해 AMP에서는 파일에 대한 더 세분화된 동작 기반 정보를 수집하고 해당 데이터를 세부적인 인적 및 머신 분석 정보와 결합하여 파일의 위협 레벨을 파악할 수 있습니다.
- 파일 회귀 분석 – 경계 방어를 통과하지만 나중에 위협으로 파악되는 악성 파일 문제를 해결합니다. 모든 시점 탐지는 100% 미만입니다. 파일 회귀 분석은 특정 시점에만 실행되는 것이 아니라 AMP 클라우드 기반 인텔리전스 네트워크의 실시간 업데이트를 사용하여 변화하는 위협 레벨을 따라가며 지속적으로 분석합니다. 따라서 AMP를 사용하여 공격이 확산되기 전에 빠르게 이를 식별하여 해결할 수 있습니다.

AMP for Networks

Cisco AMP for Networks는 FirePOWER Services for ASA를 포함한 모든 FirePOWER 어플라이언스에서 실행할 수 있습니다. HTTP, SMTP, IMAP, FTP, NBT를 포함한 일반 파일 전송 메커니즘에 실시간 및 회귀적으로 악성코드 탐지 기능을 제공합니다.

콘텐츠용 AMP

Email 및 Web 액세스는 업무/회사 용도와 개인 용도를 조합하는 필수 제품입니다. 최신 Web 2.0 제품과 최종 사용자 디바이스의 모바일 사용을 혼합한 특성으로 인해 관리자는 모든 비업무용 액세스를 차단할 수 없습니다. AMP의 전원은 WSA, ESA, CWS에도 사용할 수 있습니다. 콘텐츠 보안 게이트웨이에서는 IP 평판 및 파일 기반 평판은 물론 메일 또는 웹 플로우의 전체 컨텍스트를 활용하여 네트워크 에지에서 혼합형 공격의 가시성을 실행 및 확보할 수 있습니다.

AMP for Endpoints

Cisco AMP for Endpoints는 Microsoft Windows, Mac OS X, 안드로이드 모바일 디바이스에 설치하여 엔드포인트 자체에 탁월한 위협 방어 기능을 제공할 수 있습니다.

FireSIGHT Management Center

FMC(FireSIGHT Management Center)에서는 FirePOWER 및 AMP의 위협 정보를 디바이스에 대한 상황 정보(물리적 호스트 및 가상 호스트, 운영 체제, 애플리케이션, 서비스, 프로토콜, 사용자, 지리적 위치 정보, 콘텐츠, 네트워크 동작 등)와 결합하는 네트워크 연결 디바이스에 대한 가시성을 제공합니다. 또한 FireSIGHT에서는 인텔리전스 소스 및 정보는 물론 자동화된 기능을 통합하여 운영 효율성을 높일 수 있는 기능에 대한 액세스를 제공하는데, 이는 해당 환경에 대해 정확한 의사 결정을 내릴 수 있도록 이벤트 및 인텔리전스 데이터의 상관성을 분석하는 기능을 제공함으로써 가능합니다. NGIPS 및 AMP 솔루션의 관리 콘솔이자 데이터베이스 저장소인 FMC는 보안 운영을 위한 이벤트 및 정책 관리의 중앙 지점을 제공합니다. 네트워크 전반에 구축된 Cisco FirePOWER 물리적 또는 가상 어플라이언스 및 Cisco ASA with FirePOWER Services에서 생성한 다양한 정보를 자동으로 집계 및 연계할 수 있습니다.

FireSIGHT의 중앙 관리 기능을 통해 이벤트 모니터링, 분석, 사고 우선 순위, 보고를 포함한 모든 네트워크 보안 및 운영 기능을 중앙에서 관리할 수 있습니다.

콘텐츠 보안 제어

업무 및 개인 용도에 모두 앞서 말한 디바이스를 혼용하는 것은 물론 오늘날 앤드 디바이스의 모바일 특성으로 인해 이메일 및 웹 콘텐츠 보안은 위협 방어 아키텍처의 중요한 구성 요소가 되었습니다. 디바이스/사용자가 특정 엔드포인트와 통신할 수 있는 항목을 잠그는 데 적용할 수 있는 보안 방식의 기타 애플리케이션 및 디바이스와 달리, 콘텐츠 보안에서는 다른 서버 및 사용자에게 유비쿼터스 레벨의 액세스를 허용해야 합니다. 범죄 에코시스템은 이 액세스 레벨에 따라 달라집니다. 인바운드 플로우의 콘텐츠 보안 값에 대해 많은 논문과 가이드가 작성되고 전파되었지만 이 섹션에서는 아웃바운드를 중점적으로 다룹니다.

웹 보안

지능적인 공격자들은 모바일 디바이스, 웹 지원 애플리케이션 및 모바일 애플리케이션, 웹 브라우저 등의 새로운 공격 벡터를 활용하여 공격하고 있습니다. 이렇게 새로운 환경에서는 조직의 모두가 언제 어디서든 공격을 받을 수 있습니다. 여기에는 다음과 같은 두 가지 이유가 있습니다.

- **범죄자에게 웹은 인기 있는 공격 벡터입니다**. - 공격자는 조직화되어 있으며 웹을 통한 전술은 교활합니다. 워터링 홀(Watering hole) 공격은 회원 기반 사이트에 악성코드를 숨기고, 개인 정보가 있는 대상 개인의 신원 정보를 도용하여, 봇넷에서 피해자 디바이스를 제어합니다. 이러한 위협을 가하는 사이트는 소수가 아닙니다. 고객 네트워크 중 93%가 악성코드에 감염된 웹 사이트에 액세스합니다.[1] 웹 기반 공격은 계속 변화하고 있으며 전보다 더 탐지하기 어렵고 더 큰 손상을 주고 있습니다.
- **적절하게 제어하지 않으면 자체 사용자가 비즈니스를 위험에 처하게 할 수 있습니다.** - 지사, 개별 직원은 물론 게스트 사용자도 대역폭을 과도하게 사용하여 SaaS(Software-as-a-service) 애플리케이션 사용과 기타 우선 순위가 높은 비즈니스 업무 기능을 제한할 수 있습니다. 이들은 또한 소셜 미디어, 인터넷 비디오, 개인 SaaS 애플리케이션과 같이 제한적 사용 정책을 벗어나는 콘텐츠에 액세스하여 기업 IT 거버넌스 및 기존 보안 솔루션의 보호를 벗어나는 섀도우 IT 인프라를 만들 수도 있습니다.

---

[1] Cisco 연례 보안 보고서

보안은 단순히 더 큰 벽을 만들고 일회성 솔루션을 추가하는 작업이 아닙니다. 범죄자를 막고 사용을 제어하려면 해당 인프라에 적합하고, 비즈니스와 함께 성장하며, 변화하는 위협에 즉각적으로 적응하는 솔루션이 필요합니다. 솔루션에서는 최신 악성코드 방어를 제공하고 유출이 발생하는 경우 이를 관리할 수 있는 툴을 제공해야 합니다.

다음은 Cisco CTD 버전 2.0에 구축된 Web Security 포트폴리오의 주요 구성 요소입니다.

- 인바운드 플로우의 Advanced Malware Protection 및 샌드박싱 및 회귀 분석 관련 위협 추적. 기타 AMP 구성 요소와 동일한 설명을 따르지만 현재 AMP에서는 아웃바운드 플로우만 검사합니다. CTD에서 회귀 분석 후 감염됐을 가능성이 있는 클라이언트를 발견하는 작업에 해당합니다. 악의적인 코드와 상호작용한 모든 클라이언트와 해당 콘텐츠의 출처로 구성된 클린 목록에는 최초 감염자에 대한 세부 정보와 감염 소스가 있습니다.
- 시그너처 기반 보안. 아웃바운드 플로우에 대해 안티 바이러스 검사를 사용하면 관리자가 분산된 공격의 일부로 사용되는 사용자 층의 감염 및 감염 가능성을 쉽게 확인할 수 있습니다.
- C&C 사이트로의 아웃바운드 플로우에 대한 행동 분석은 L4TM으로 쉽게 검색할 수 있습니다. WSA에서는 모든 아웃바운드 TCP 및 UDP 플로우를 검사하여 C&C 서버에 대한 해당 통신을 모니터링하고 차단할 수 있습니다. Cisco CTD 버전 2.0의 다른 측면과 함께 이 중요 데이터는 IoC를 발견하는 데 도움이 될 수 있습니다.

이메일 보안

이메일 위협 환경에서는 정교한 지능형 위협과 표적 공격이 늘어나고 있습니다. 대량 스팸 및 안전하지 않은 이메일 첨부 파일은 더 이상 기본 보안 문제가 아닙니다. 공격자는 이제 소셜 미디어 웹 사이트를 샅샅이 뒤져 의도한 피해자에 대한 정보를 찾아내고 스피어 피싱 이메일을 고안합니다. 이러한 공격에서는 흔히 글로벌 뉴스 이벤트와 연결된 개인 정보 및 사회 공학 전술을 사용하여 악성코드를 제공하는 악성 링크로 사용자를 속입니다. 그 어느 때보다 공격할 기회가 늘어났습니다. 이전에는 직원이 회사 방화벽 뒤의 워크스테이션에서 텍스트 기반의 이메일을 확인했으나, 이제는 다양한 디바이스에서 언제 어디에서든 리치 HTML 메시지를 주고받는 환경이 되었습니다. 유비쿼터스 액세스는 이전에는 세분화되었던 보안 레이어의 경계를 모호하게 하는 새로운 네트워크 진입점을 만듭니다.

CES(Cisco Email Security)는 진화하는 위협 환경의 선두 주자입니다. 스팸에 사용 가능한 최고 차단율과 최저 오탐지율을 자랑합니다. Cisco는 업계 유일의 검증된 제로 아워(zero-hour) 안티바이러스 솔루션을 보유하여 60분 이내에 신종 바이러스를 방어합니다. 이 솔루션을 기존 검사 엔진과 결합한 것을 스팸 및 바이러스에 대한 심층 방어라고 합니다. 동일한 솔루션에서 아웃바운드 이메일도 검사하여 데이터 유출 방지 규정준수 요구 사항을 따르도록 합니다. 주민등록 번호, 신용카드 번호, 환자의 건강 정보 등의 아웃바운드 이메일을 자동으로 검사할 수 있습니다. 해당 메시지를 자동으로 암호화하여 수신자가 인증 절차를 거쳐야 내용을 열어 볼 수 있도록 하여 즉각적인 규정준수를 제공합니다.
또한 최고의 성능을 최저 총 소유 비용으로 제공합니다. Cisco는 자사의 완벽한 보안 아키텍처를 이용하여 미래에 Cisco의 모든 보안 기술이 함께 작동하여 귀사의 보안을 강화할 수 있도록 하는 데 주력하고 있습니다.

다음은 Cisco CTD 버전 2.0에 구축된 Email Security 포트폴리오의 주요 구성 요소입니다.

- 인바운드 플로우의 Advanced Malware Protection 및 샌드박싱 및 회귀 분석 관련 위협 추적.
- 서명 기반 보안. 아웃바운드 플로우에 대한 안티스팸 및 안티바이러스 검사.
- C&C 사이트로의 아웃바운드 플로우 또는 아웃바운드 스팸 공격의 일부인 플로우에 대한 행동 분석. 정상적인 사항 또는 예상되는 사항의 베이스라인에 대한 아웃바운드 플로우를 모니터링하면 관리자가 감염이 발생한 위치를 신속하게 파악하고 정리하는 데 도움이 될 수 있습니다.

TrustSec 및 Identity Services Engine

Cisco ISE는 업계 최고의 보안 정책 관리 플랫폼으로서 자동화된 통합 액세스 제어를 통해 사용자가 선택한 연결 방식(유선, 무선 또는 VPN)에 구애받지 않고 능동적으로 엔터프라이즈 네트워크 및 리소스에 대한 역할 기반의 액세스를 적용합니다.

Cisco ISE에서는 Cisco pxGrid(Platform Exchange Grid) 기술을 사용하여 기타 Cisco 플랫폼 및 통합 파트너 에코시스템 솔루션과 다양한 상황 인식 데이터를 공유합니다. 이 기술을 사용하면 전보다 더 쉽게 네트워크 전체의 보안 위협을 식별, 완화, 교정하는 기능을 추가할 수 있습니다. 전체적으로는 보안 액세스 제어를 중앙 집중화하고 간소화하여 중요한 비즈니스 서비스를 안전하게 제공하고 인프라 보안을 개선하고 규정 준수를 시행하며 서비스 운영을 간소화할 수 있습니다.

Cisco TrustSec에서는 네트워크 서비스 및 애플리케이션에 대한 보안 액세스의 프로비저닝 및 관리를 간소화합니다. 네트워크 토폴로지를 기반으로 한 액세스 제어 메커니즘과 달리 Cisco TrustSec에서는 논리적 정책 그룹화를 사용하여 정책을 정의하므로 모바일 및 가상 네트워크에서 리소스가 이동하는 경우에도 보안 액세스가 지속적으로 유지됩니다. IP 주소 및 VLAN에서 액세스 엔타이틀먼트를 분리하면 보안 정책 유지보수 작업이 간소화되고, 운영 비용이 절감되며, 일반 액세스 정책을 유무선 액세스 및 VPN 액세스에 일관적으로 적용할 수 있습니다.

Cisco TrustSec의 분류 및 정책 시행 기능은 Cisco 스위칭, 라우팅, 무선 LAN, 방화벽 제품에 내장되어 있습니다. Cisco TrustSec에서는 엔드포인트-IP 주소의 컨텍스트 신원에 따라 트래픽을 분류하여 동적 네트워크 환경 및 데이터 센터에 대한 액세스를 더 유연하게 제어할 수 있습니다.

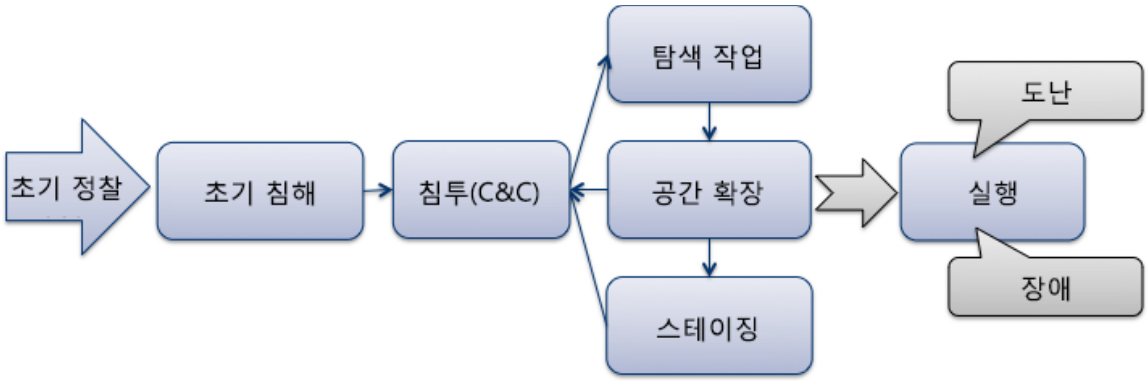
네트워크 액세스 지점에서 SGT(Security Group Tag)라는 일반적으로 해당 엔드포인트의 사용자, 디바이스, 위치 특성에 따라 Cisco TrustSec 정책 그룹을 엔드포인트에 할당합니다. SGT는 엔드포인트의 액세스 엔타이틀먼트를 표시하고 해당 엔드포인트의 모든 트래픽에서 SGT 정보를 전달합니다. SGT는 스위치, 라우터, 방화벽에서 전송 결정을 내리는 데 사용됩니다. SGT를 할당하면 비즈니스 역할과 기능을 표시할 수 있으므로, Cisco TrustSec 제어를 기본적인 네트워킹 세부 사항이 아닌 비즈니스 요구 사항 측면에서 정의할 수 있습니다.

유출을 가정한 상황의 작동

우수한 모든 보안 제어에도 불구하고 단호하고 동기 부여된 공격자가 목표를 위해 네트워크에서 실행할 작업 공간을 확보합니다. 공격자는 자신의 목표를 알고 많은 면에서 유리한 반면, 방어자는 공격자의 존재를 확인할 수 있어야 하는데 이는 간단한 작업이 아닙니다. 이 섹션에서는 먼저 공격 라이프사이클을 분석하고, 방어자가 Cyber Threat Defense 솔루션 구성 요소에서 데이터를 운영하여 공격자의 존재를 확인하고 중요한 자산을 보호할 수 있는 방법을 설명합니다.

공격 라이프사이클 분석

공격 라이프사이클은 공격자가 처음부터 목표를 실행할 수 있을 때까지 거치는 단계에 주로 초점을 맞춥니다. 모든 단계에는 기술 및 비기술적 실행 수단이 포함되며, 일부 초기 단계는 피해자 조직의 영역을 완전히 벗어난 곳에서 발생할 수 있습니다. 각 단계는 아래 그림과 같이 나눌 수 있습니다.



초기 정찰

이 단계에서는 공격자가 대상 조직에 대한 정보를 수집합니다. 여기에는 공개 정보 활용, 소셜 미디어를 사용하여 대상 직원 찾기, 대상 조직에서 사용 중인 기술 및 초기 공격을 위한 일반적인 준비 확인이 포함됩니다.

초기 침해

이 단계에서는 공격자가 피해자 조직 내부에 작업 공간을 확보합니다. 침해는 맞춤 제작한 악성코드인 제로데이를 활용하거나, 알려진 악성코드를 사용하거나, 사회 공학과 같은 비기술적 방법을 사용하여 수행될 수도 있습니다. 어느 쪽이든 이 단계를 완료하면 공격자는 조직에 성공적으로 침투하게 됩니다.

침투

이전 단계를 마치면 공격자는 조직에 성공적으로 침투하게 됩니다. 이 단계에서는 POP(Point of Presence)를 유지할 수 있습니다. 예를 들어 이전 단계에서 공격자가 사용자 이름과 암호를 검색할 수 있었다면 이 단계에서 공격자는 조직에 대한 원격 연결을 엽니다. 초기 침해에서 직원이 소유한 개인 컴퓨터에 악성코드 조각을 설치한 경우 이 단계에서는 해당 악성코드를 사용하여 C&C(Command-and-Control) 채널을 엽니다.

탐색 작업

이 시점에서 공격자는 조직 내부에서 목표와 관련된 리소스를 찾기 시작합니다. 공격자가 여기서 수행하는 작업은 공격자, 공격자의 목표 및 조직에 침투할 수 있었던 방법에 따라 달라집니다. 일반적으로 공격자는 취약할 수 있는 다른 리소스를 찾기 위해 네트워크 내부를 검사하거나 공격자가 익스플로잇에 관심이 있는 데이터를 호스팅하기 시작합니다. 이 단계에서 공격자는 적합한 자격 증명(예: 사용자 이름과 암호)을 복구하려고 할 수 있습니다.

공간 확장

이 시점까지 공격자는 실질적으로 하나의 조직 침투 지점(예: 머신을 감염시킨 단일 악성코드, 하나의 도난 자격 증명 집합)만 확보한 상태입니다. 이 단계에서 공격자는 기존의 지점을 확장하여 조직 내부에 여러 개의 침투 지점 및/또는 POP(Point of Presence)를 만들게 됩니다. 다이어그램에서 침투 단계로 돌아가는 것은 새 리소스에 대한 원격 연결을 나타냅니다.

스테이징

이 단계에서는 공격자가 마지막 실행 단계를 준비합니다. 이 단계의 결과는 공격자의 목표에 따라 달라집니다. 공격자의 목표가 데이터를 얻거나 또는 훔치는 것인 경우 이 단계에서 조직 내부의 다양한 리소스에서 데이터를 느리게 수집할 수 있습니다. 공격자의 목표가 중단인 경우 이 단계에서 필요한 모든 대상에 작업 공간을 확보하도록 할 수 있습니다. 다이어그램에서 침투 단계로 돌아가는 것은 공격자가 침투 지점으로 사용하고 있는 원격 연결 또는 자격 증명을 나타냅니다.

실행

공격의 마지막 단계입니다. 이 단계에서는 공격자가 자신의 임무가 완료되고 목적 및 목표가 달성되었는지 확인합니다. 공격자의 목표는 주로 데이터 도난 또는 활동 중단이라는 2가지 카테고리에 속합니다.

네트워크에 복원력 구축

네트워크에 복원력을 구축하려면 가장 먼저 공격의 라이프사이클 단계를 이해해야 합니다. 복원력 구축의 목표는 공격자의 존재를 신속하게 확인하고 공격을 관리할 수 있는 올바른 도구를 적소에 배치하는 것입니다. 이 섹션에서는 Cisco Cyber Threat Defense 솔루션의 다양한 요소 및 이러한 요소를 사용하여 다양한 공격 라이프사이클 단계를 식별하고 관리하는 방법을 살펴봅니다.

NGIPS를 사용하여 알려진 공격 차단

네트워크에 복원력을 구축하는 첫 번째 단계는 네트워크에 대한 액세스를 제어할 수 있는 정확한 기술 조합을 구축하는 것입니다. 이를 위해서는 기타 Cisco 모범 사례 및 검증된 설계를 준수하여 구내 및 데이터 센터 모두에 대해 보안 액세스 제어 및 네트워크 에지를 구성해야 합니다.

Cisco Cyber Threat Defense 솔루션에서는 www.cisco.com/go/designzone의 다음 CVD에 있는 모범 사례 및 원칙을 따를 것을 권장합니다.

- 차세대 IPS를 사용하는 Cisco Threat Management
- 방화벽 및 IPS 기술 설계 가이드
    - 일부 설계 가이드는 기존의 Cisco IPS 대신 FirePOWER를 사용하도록 아직 업데이트되지 않았을 수 있습니다.
- Cisco TrustSec 2.0 설계 및 구현 가이드

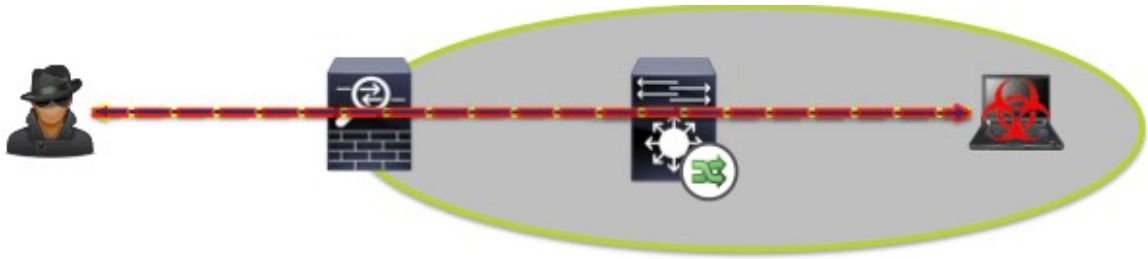
위 내용을 준수하면 액세스를 충분히 제어할 수 있고 위협 관리 솔루션을 적소에 배치하여 공격 표면을 제한하는 네트워크가 조성되어 공격자가 조직에 대해 알려진 익스플로잇을 실행하기 더 어려워집니다. 다음과 같은 결과가 발생합니다.

- NGIPS에서 알려진 악성코드 차단
- ESA에서 SMTP를 통한 알려진 악성코드 차단
- WSA에서 HTTP를 통한 악성코드 차단
- ISE에서 네트워크에 연결된 디바이스에 상태 확인 및 정책 시행 수행

또한 이 가이드에서는 네트워크 및 액세스 에지가 적소에 위치해 있으며, Cisco Cyber Threat Defense 솔루션의 기타 사용 사례를 지원하기 위해 텔레메트리를 용이하게 하도록 작동된다고 가정합니다.

커맨드 앤 컨트롤 탐지

운영상 공격자의 C&C 채널은 네트워크 내부(내부의 신뢰할 수 있고 인증된 영역) 호스트에서 외부 호스트로 향하는 통신 채널입니다. 이러한 채널은 악성코드에 감염된 호스트에서 C&C 서버로의 통신 채널 또는 도난당한 자격 증명을 사용하는 VPN 연결과 같이 다양한 형식으로 존재할 수 있습니다. 아래 그림에서는 C&C 채널이 의미하는 바를 개념적으로 보여줍니다(네트워크 내부에 있는 리소스와 네트워크 외부의 공격자 제어 지점 간 레이어 3 또는 4 연결).



C&C 채널을 탐지 및 방어하고 공격자의 침투 지점을 교정하기 위해서는 먼저 채널 자체를 살펴보고 채널을 표시할 수 있는 다양한 방법과 네트워크 및 프로토콜 측면에서 채널을 탐지하기 위해 수행할 수 있는 사항을 이해해야 합니다. 다음은 C&C 채널을 탐지하는 경우 분석할 항목의 예로, 완전한 목록은 아닙니다.

- 개국
- 애플리케이션
- 업로드/다운로드 속도
- 시각
- 반복된 연결 수
- 비커닝 - 반복적으로 끊긴 연결 수
- 장기 플로우 수
- 알려진 C&C 서버 수
- 웹 요청/URL 수
- 의심스러운 사용자 로그인 활동

Cisco Cyber Threat Defense 솔루션에는 위 항목 중 일부를 자동화하는 데 도움이 되고, C&C 채널의 동작 또는 이상 징후를 탐지하고, 보안 운영자가 해당 환경에서 C&C 활동을 수동으로 검색할 수 있도록 가시성을 제공할 수 있는 있는 기술이 포함되어 있습니다. 다음은 Cisco Cyber Threat Defense 솔루션 기술 및 해당 기술이 C&C 활동을 탐지 및 교정(가능한 경우)할 수 있는 방법에 대한 목록입니다.

StealthWatch: 네트워크 및 주변 디바이스의 NetFlow 데이터를 활용하여 네트워크를 출입하는 모든 트래픽 플로우에 대한 가시성을 확보할 수 있습니다. 일부 동작 및 이상 징후를 이용한 알고리즘에서는 네트워크 트래픽을 분석하여 의심스러운 트래픽 플로우를 기반으로 한 비밀 채널을 확인합니다. 또한 SLIC(StealthWatch Labs Information Center) 위협 피드에서는 해당 서버로의 통신이 탐지되는 경우 경보를 생성하도록 알려진 C&C 서버 목록을 StealthWatch 시스템에 제공합니다. (참고: 알려진 C&C 서버는 IP 주소 또는 URL이 될 수 있습니다.) 이 밖에도 모든 통신에 대한 레코드를 유지하여 보안 운영자가 새로운 정보 및 IoC를 발견하는 경우 포렌식의 룩백(look-back) 옵션에서 비밀 채널과 손상된 디바이스를 식별할 수 있습니다.

Cisco Web Security Appliance: Cisco WSA에서는 트래픽이 어플라이언스를 통과할 때 URL 검사를 통해 평판이 낮은 웹 서버를 대상으로 하는 HTTP 및 HTTPS 트래픽을 자동으로 인라인 차단할 수 있습니다. 대부분 낮은 평판의 웹 서버는 알려진 봇넷 C&C 서버가 될 수 있습니다.

Cisco FirePOWER: Cisco FirePOWER에서는 트래픽이 NGIPS 센서를 통과할 때 URL 검사를 통해 평판이 낮은 웹 서버를 대상으로 하는 트래픽을 자동으로 인라인 차단할 수 있습니다. 대부분 낮은 평판의 웹 서버는 알려진 봇넷 C&C 서버가 될 수 있습니다.

CTA(Cognitive Threat Analytics)를 사용하는 Cisco CWS(Cloud Web Security): Cisco CWS 프리미엄의 CTA 서비스에서는 URL 활동을 모니터링하여 C&C 채널을 분석하고 이상 징후를 탐지합니다. 이 서비스는 이전에는 발견하지 못했을 수 있거나 단일 조직을 표적으로 하는 방식으로 집중되던 C&C 서버를 식별하는 데 도움이 됩니다.

내부 정찰에 대한 방어

> *정찰: 주로 인터넷 웹사이트를 샅샅이 뒤져서 나오는 회의 기록, 이메일 주소가 있는 메일링 목록, 대인 관계, 특정 기술에 대한 정보 같은 표적을 조사, 식별하고 선정합니다.* [Lockheed Martin, "Intelligence-Driven Computer Network Defense"]

네트워크 내부 관점에서 이러한 동작에 대한 공격자의 활동은 레이어 3 및 4 프로토콜을 사용하여 관심 있는 다른 리소스를 식별하고자 하는 시도로 표시됩니다. 아래 그림에서는 내부 정찰을 뒷받침하는 개념을 보여줍니다.

활동의 예로는 ICMP 에코 요청 메시지를 임의의 내부 IP 주소로 전송, 개방형 서비스 또는 포트가 있는 디바이스를 식별하기 위해 광범위한 네트워크 주소 블록 검사 등이 있습니다. 이러한 정찰 기법은 상당히 소란스러울 수 있고 더 교묘하고 공격적인 공격자는 "조용히 느리게" 작업하지만, 일반적으로 방법론은 동일합니다 (기존의 POP(Point of Presence)를 사용하여 공격자는 네트워크 프로토콜을 사용하는 네트워크에서 다른 리소스를 찾으려고 시도). 다음은 네트워크 내부의 정찰 활동을 식별하기 위해 분석할 수 있는 항목의 예로, 완전한 목록은 아닙니다.

- 다수의 플로우
- 높은 클라이언트 바이트 비율
- 단방향 또는 응답하지 않는 플로우
- 서브넷/논리 그룹 내의 플로우
- 존재하지 않는 IP로의 플로우
- 플로우 패턴
- 비정상적인 동작(예: 안전한 데이터 센터에 대한 연결 시도)
- 의심스러운 플로우 유형(예: ICMP)

Cisco Cyber Threat Defense 솔루션에는 위 항목 중 일부를 자동화하는 데 도움이 되고, 내부 정찰 활동의 동작 또는 이상 징후를 탐지하고, 보안 운영자가 해당 환경에서 내부 활동을 수동으로 검색할 수 있도록 가시성을 제공하는 기술이 포함되어 있습니다. 다음은 Cisco Cyber Threat Defense 솔루션 기술 및 해당 기술이 내부 정찰 활동을 방지, 탐지, 교정(가능한 경우)할 수 있는 방법에 대한 목록입니다.

StealthWatch: 네트워크의 모든 레이어에 걸쳐 네트워크 디바이스의 NetFlow 데이터를 활용하여(액세스, 배포, 코어, 에지) 네트워크의 모든 트래픽 플로우에 대한 완벽한 가시성을 제공합니다. 이러한 가시성을 통해 네트워크 디바이스를 통과하는 모든 통신에 대한 메타데이터 레코드를 유지할 수 있습니다. 이렇게 집계된 데이터를 분석하여 의심스러운 활동 패턴이 있는 호스트를 식별할 수 있습니다. StealthWatch에는 다양한 알고리즘으로 동작을 감시하고 의심스러운 활동을 식별하는 특정 "정찰" 알람 카테고리가 있습니다. 이외에도 StealthWatch에서는 회귀적 활동에 대한 기록 룩백 기능을 지원하여 운영자가 다른 시스템에서 IOC를 발견한 다음 호스트를 조사할 수 있습니다.

Cisco NGIPS: Cisco NGIPS가 구축된 주요 세그멘테이션 지점에서 검색 활동에 사용된 특정 애플리케이션을 탐지 및 차단하는 데 사용할 수 있습니다. 예를 들면 Cisco NGIPS를 사용하여 구내 네트워크와 데이터 센터 간의 ICMP 메시지를 차단할 수 있습니다.

Cisco TrustSec: 정책을 활용하여 보안 그룹을 이용한 세그멘테이션으로 내부 정찰 활동의 효과를 제한하고 활동을 드러낼 수 있습니다. 동일한 보안 그룹에 속하는 호스트 간 P2P 네트워크 트래픽을 업무상 중요한 애플리케이션으로 제한하는 정책을 구현하면 네트워크 레벨의 정찰 활동이 발생하는 것을 네트워크에서 적극적으로 방지할 수 있습니다.

내부 APT 전파에 대한 방어

추가 또는 대상 리소스를 식별하고 나면 공격자는 악성코드를 활용하여 대상에 작업 공간을 확산하도록 선택할 수 있습니다. 아래 그림에서는 이러한 확산을 개념적으로 설명합니다. 운영상 악성코드 확산은 대상 호스트로 전송할 데이터 볼륨이 있는 2개의 호스트 간 레이어 4 통신처럼 보입니다. 그러면 대상 호스트에서 네트워크 정찰 및 심지어 악성코드 전파와 같은 의심스러운 활동을 표시하기 시작할 수 있습니다.

이러한 악성코드 전파의 예를 들면 다음과 같습니다.

- 자체적으로 전파되는 악성코드 변종으로, 특정 취약성에 민감한 호스트를 검사한 다음 해당 취약성을 악용
- 적합한 자격 증명을 사용하는 공격자가 원격 리소스에 연결하여 실행 파일을 전송하고 실행

내부 악성코드 전파를 방어하기 위해서는 네트워크 트래픽 분석, 파일 분석, 추적을 조합해야 합니다. 다음은 내부 악성코드 전파를 식별하기 위해 분석할 수 있는 항목의 예로, 완전한 목록은 아닙니다.

- 다수의 플로우
- 높은 클라이언트 바이트 비율
- 서브넷/호스트 그룹 내 연결 수
- 플로우 패턴
- 비정상적인 동작
- 알려진 취약점(규칙 일치)
- 파일 경로 및 이동
- 프로토콜 미준수
- 터널링된 플로우 수
- 실행 가능 분석

Cisco Cyber Threat Defense 솔루션에는 위 항목 중 일부를 자동화하는 데 도움이 되고, 악성코드 전파의 동작 또는 이상 징후를 탐지하고, 보안 운영자가 해당 환경에서 악성코드 활동을 수동으로 검색할 수 있도록 가시성을 제공하는 기술이 포함되어 있습니다. 다음은 Cisco Cyber Threat Defense 솔루션 기술 및 해당 기술이 내부 악성코드의 전파를 방지, 탐지, 교정(가능한 경우)할 수 있는 방법에 대한 목록입니다.

StealthWatch: 네트워크의 모든 레이어에 걸쳐 네트워크 디바이스의 NetFlow 데이터를 활용하여(액세스, 배포, 코어, 에지) 네트워크의 모든 트래픽 플로우에 대한 완벽한 가시성을 제공합니다. 이러한 가시성을 통해 네트워크 디바이스를 통과하는 모든 통신에 대한 메타데이터 레코드를 유지할 수 있습니다. 이렇게 집계된 데이터를 분석하여 의심스러운 활동 패턴이 있는 호스트를 식별할 수 있습니다. StealthWatch에는 다양한 알고리즘으로 동작을 감시하고 의심스러운 활동을 식별하는, 악성코드 확산에 대한 특정 알람 카테고리가 있습니다. 또한 네트워크의 의심스러운 활동을 통해 악성코드 확산을 추적하는 웜 추적기(아래 그림)로 알려진 기능도 있습니다. 이외에도 StealthWatch에서는 회귀적 활동에 대한 기록 룩백 기능을 지원하여 운영자가 다른 시스템에서 IOC를 발견한 다음 호스트를 조사할 수 있습니다.

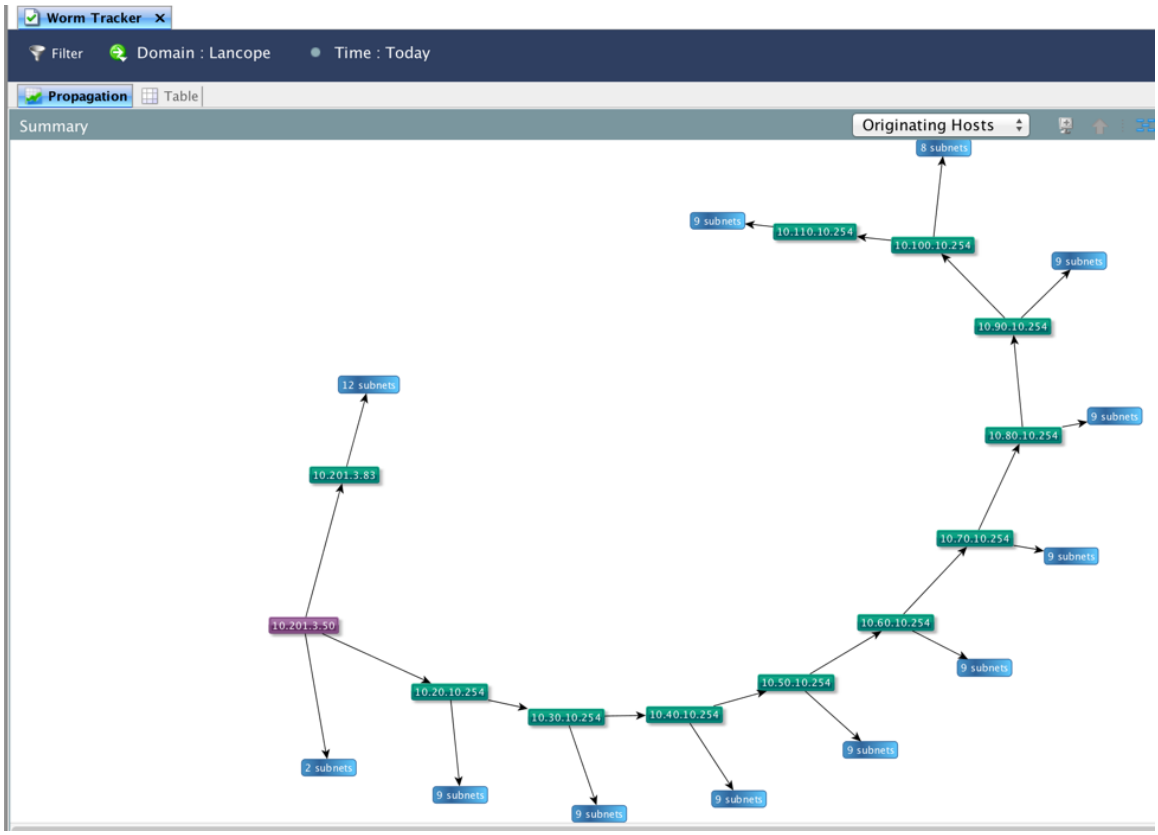
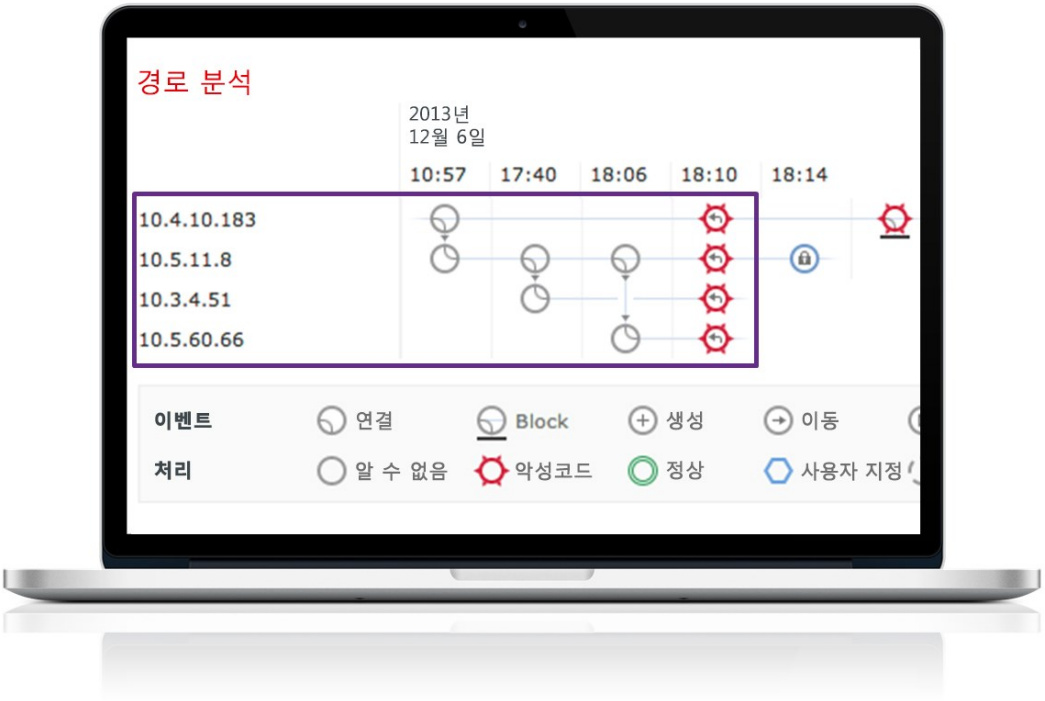


그림 2 - StealthWatch를 사용한 의심스러운 동작 추적

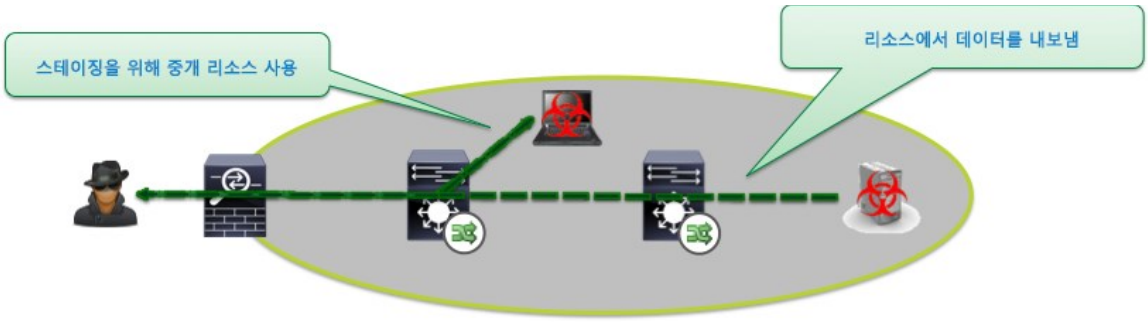
Advanced Malware Protection: Cisco AMP for Endpoints에서는 파일을 엔드포인트로 전송할 때 파일 일치 분석을 제공하여 의심스러운 파일을 식별합니다. AMP에서는 의심스러운 파일은 자동으로 차단할 뿐만 아니라 파일 경로(아래 그림)라는 기능을 사용하여 네트워크 전체에서 파일의 확산을 추적하는 기능을 제공합니다.



Cisco TrustSec: 정책을 활용하여 보안 그룹을 이용한 세그멘테이션으로 공격의 가능한 측면 이동에 대한 네트워크 레벨의 보호를 제공할 수 있습니다. 사용자-서버 트래픽에 영향을 미치지 않고 사용자 디바이스 간의 네트워크 레벨 통신을 제한하도록 정책을 구현할 수 있습니다.

데이터 손실 또는 유출에 대한 방어

대부분의 경우 공격자의 최종 목표는 대상 조직에서 데이터를 훔치는 것입니다. 이러한 데이터는 거래 또는 국가 기밀, 지적 재산, 고객 신용카드 데이터를 포함한 고객 정보 등 다양한 형태가 될 수 있습니다. 운영상 데이터 손실은 네트워크 내부에서 네트워크 외부로의 전송 또는 애플리케이션 레이어 프로토콜을 사용하는 데이터 전송으로 보일 수 있습니다. 공격자가 빠져나오기 전에 중간 디바이스를 사용하여 데이터를 임시로 저장하는 경우 데이터 스테이징 또는 데이터 호딩(Data Hoarding)으로 알려진 중간 단계도 발생할 수 있습니다.



데이터의 불균형(값의 데이터를 인식하기 어려움) 및 해당 데이터에 도달할 수 있는 여러 개의 공격 벡터 때문에(공격 표면이 지리적으로 분산되어 있기 때문일 수 있음(다중 판매 시점 터미널이 있는 대형 소매 업체 등)) 데이터 손실을 차단하는 일은 대부분의 조직이 당면한 중요한 과제입니다. 공격 라이프사이클의 최종 단계로서, 대부분의 경우 탐지는 일부 데이터가 이미 유출된 후 발생하므로 데이터 손실 이벤트가 발생하기 전에 공격을 탐지하도록 시스템을 운영하는 것뿐만 아니라 이러한 도난을 회귀적으로 분석할 수 있는 적절한 기술을 적소에 배치해야 합니다. 결과적으로 데이터 손실을 차단하는 작업은 여러 단계의 당면 과제이며 데이터 손실 이벤트를 검색하는 데는 다양한 기술이 필요할 수 있습니다. 다음은 데이터 손실을 식별하기 위해 분석할 수 있는 항목의 예로, 완전한 목록은 아닙니다.

- 기록 데이터 전송 동작
- 애플리케이션
- 시각
- 개국
- 데이터의 양 – 단일 및 집계
- 기간
- 비대칭 트래픽 패턴
- 기능 그룹 간의 트래픽

Cisco Cyber Threat Defense 솔루션에는 위 항목 중 일부를 자동화하는 데 도움이 되고, 데이터 도난 활동의 동작 또는 이상 징후를 탐지하고, 보안 운영자가 해당 환경에서 내부 활동을 수동으로 검색할 수 있도록 가시성을 제공하는 기술이 포함되어 있습니다. 다음은 Cisco Cyber Threat Defense 솔루션 기술 및 해당 기술이 내부 악성코드의 전파를 방지, 탐지, 교정(가능한 경우)할 수 있는 방법에 대한 목록입니다.

StealthWatch: 네트워크의 모든 레이어에 걸쳐 네트워크 디바이스의 NetFlow 데이터를 활용하여(액세스, 배포, 코어, 에지) 네트워크의 모든 트래픽 플로우에 대한 완벽한 가시성을 제공합니다. 이러한 가시성을 통해 네트워크 디바이스를 통과하는 모든 통신에 대한 메타데이터 레코드를 유지할 수 있어, 데이터 유출 이벤트 경우 포렌식 감사 내역이 존재할 수 있습니다. 또한 StealthWatch는 위 고려 사항 중 대부분에 대한 분석을 자동화하고, 데이터 호딩 및 데이터 유출 이벤트 모두에 대해 동작 및 이상 징후 알람 카테고리가 있습니다. 호스트 그룹을 생성하면 데이터가 네트워크의 다른 영역으로 이동하는 것을 모니터링하는 기능을 지원하고(다음 섹션에서 자세히 설명), 데이터가 중요 서버에서 의심스러운 위치로 유출되고 있을 때 적극적으로 모니터링할 수 있는 기능을 지원합니다. 이외에도 StealthWatch에서는 회귀적 활동에 대한 기록 룩백 기능을 지원하여 운영자가 다른 시스템에서 IOC를 발견한 다음 호스트를 조사할 수 있습니다.

중요 자산의 지속적인 모니터링

네트워크에 연결된 모든 디바이스에 동일한 값이 있는 것은 아닙니다. 일부 디바이스는 비즈니스 프로세스 및/또는 운영에 매우 중요하며 민감한 데이터를 보관하고 있을 수 있습니다. 이러한 디바이스, 호스트, 사용자는 모두 해당 사용 및 잠재적 오용을 모니터링할 때 특별히 주의해야 합니다. 중요한 자산의 네트워크 활동을 모니터링하는 작업은 필수적이며, 의심스럽거나 악의적인 활동을 식별하고 사고 대응 및 억제 프로세스의 속도를 높이는 데 도움이 되며, 조직의 위험 노출을 최소화합니다.

모든 조직은 "크라운주얼(Crown Jewel)"을 만들고 중요 자산을 구성하는 데 있어 서로 다른 우선 순위를 가지고 있습니다. 이러한 자산을 식별하는 접근법은 대상과 해당 정보의 위험 및 인식된 가치를 기반으로 판단할 수 있습니다. 다음은 "크라운주얼"을 식별하는 데 도움이 되는 항목의 예로, 완전한 목록은 아닙니다.

- 비즈니스 영향 분석
    - 비즈니스 작업에 직접적으로 관련되는 시스템
- 매출에 미치는 영향
    - 주문 및 배송에 이용되는 시스템
- 비용에 미치는 영향
    - 계약상의 의무를 관리하는 시스템
- 법적 요구 사항
    - 보호할 정보 및 시스템을 강조하는 법령 및 계약(예: 규정준수 요구 사항)

- 민감도 프로필
    - 권한이 있거나 제한된 정보에 액세스하는 시스템
- 리스크 프로필
    - 자체 특성으로 인해 보호를 받는 시스템(예: 기존 시스템)
- 가시성 프로필
    - 공격하는 경우 조직이 당혹스러워할 수 있는 눈에 잘 띄는 시스템

Cisco Cyber Threat Defense 솔루션을 구성하는 기술을 사용하여 모든 주요 자산에 대한 활성 모니터링을 제공할 수 있습니다. NetFlow 및 StealthWatch에서 제공하는 폭넓은 가시성을 통해 네트워크에 연결된 디바이스의 모든 엔드 투 엔드 통신을 감사할 수 있습니다. Cisco NGIPS 및 FMC에서 제공하는 심층적인 가시성을 통해 중요한 자산에서 또는 해당 자산에 사용 중인 악성 파일에 대한 가시성이 깊어지고 관련성이 강화되었습니다.

다음 그림에서는 호스트 그룹 및 StealthWatch의 사용자 지정 맵 기능을 사용하여 조직의 PCI 영역을 적극적으로 모니터링하는 방법을 보여줍니다. 이 예제에서는 PCI 영역의 각 주요 구성 요소에 대한 호스트 그룹을 정의하고, 해당 영역 간 관계 속성 및 정책을 정의 및 매핑한 후 네트워크에서 정책을 위반하는 트래픽이 나타나면 경고하는 사용자 지정 규칙을 개발합니다.

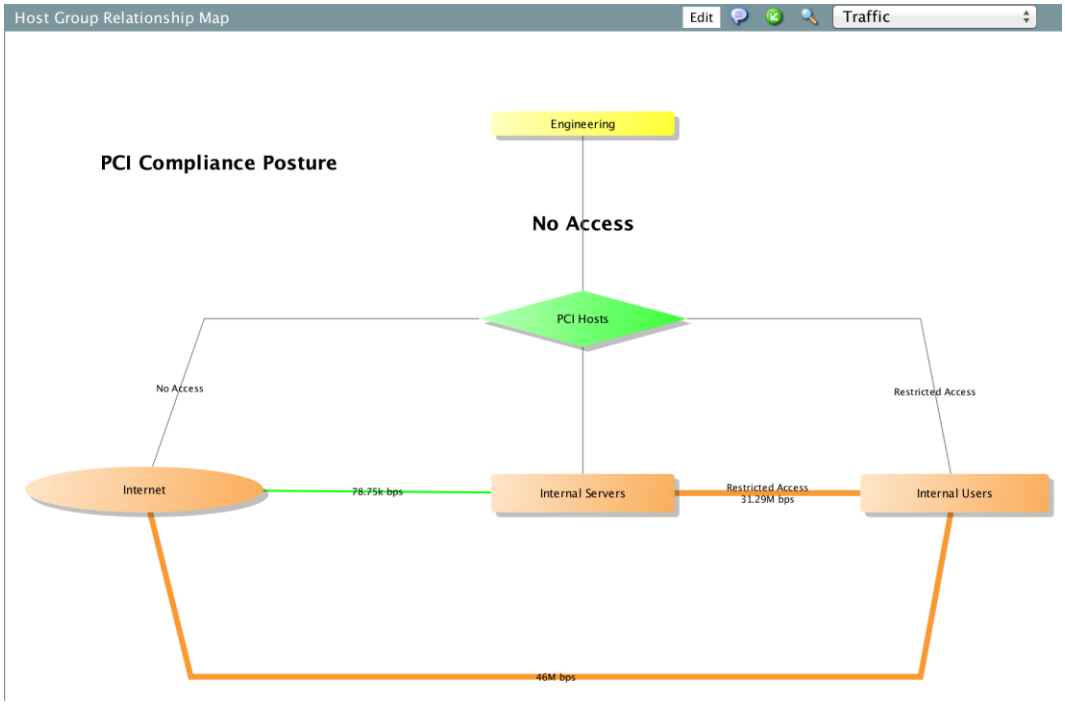


그림 3 - NetFlow 및 StealthWatch를 사용하는 세그멘테이션 모니터링

또한 네트워크 인프라 자체도 공격의 대상이 될 수 있으므로 활성 정책 모니터링을 적소에 배치하여 네트워크 인프라의 통신을 모니터링할 수 있습니다(다음 그림 참조).

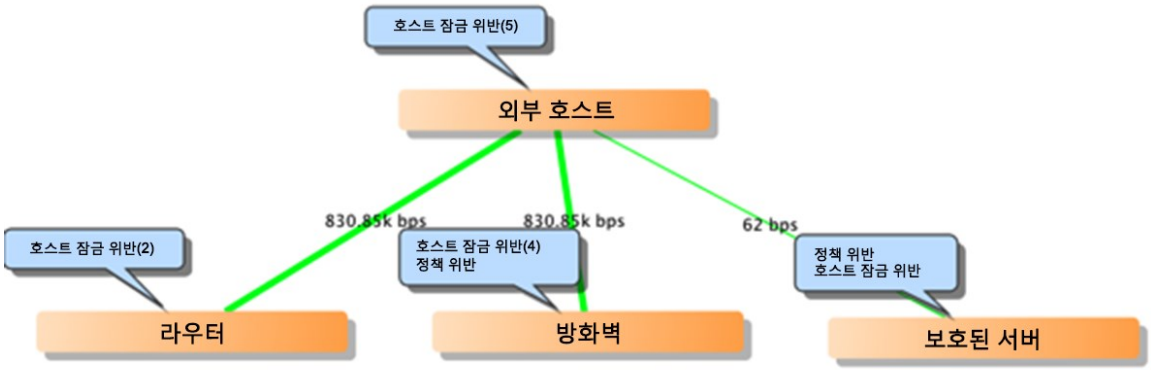


그림 4 - NetFlow 및 StealthWatch를 사용하는 네트워크 제어 플레인 모니터링

설계 고려 사항

NetFlow 및 StealthWatch 시스템

StealthWatch System

절차 1 (선택 사항) StealthWatch FlowSensor 추가

네트워크 장비에서 NetFlow 생성을 수행할 수 없는 경우 StealthWatch FlowSensor 및 FlowSensor VE를 사용하여 통신을 플로우 레코드로 변환할 수 있습니다. 이렇게 하면 이 가이드에 지정되지 않은 네트워킹 장비가 Cisco Cyber Threat Defense 솔루션 버전 1.1 구축에 참여할 수 있습니다. 또한 StealthWatch FlowSensor를 사용하여 네트워크의 핵심 영역에 대해 패킷 레벨 애플리케이션 식별 및 성능 메트릭을 추가할 수 있습니다. Cisco Cyber Threat Defense 솔루션 버전 1.1 구축에 StealthWatch FlowSensor를 추가하도록 고려하는 경우 다음 단계를 수행합니다.

1단계 StealthWatch FlowSensor 선택

StealthWatch FlowSensor를 선택하는 경우 FlowSensor로 전송되는 트래픽 레벨을 FlowSensor에서 처리할 수 있어야 하므로 모니터링 지점의 예상 트래픽 프로필을 고려하십시오. Cisco Cyber Threat Defense 솔루션 버전 1.1의 다른 NetFlow 생성 디바이스와 마찬가지로 FlowSensor를 최대한 액세스 레이어 가까이 구축하는 것이 좋습니다.

다음 표에는 StealthWatch FlowSensor 어플라이언스 모델 및 해당 사양이 있습니다. 표시된 처리 용량은 지원되는 지속 비율입니다. FlowSensor에서는 나열된 용량 이상의 단기 버스트를 처리할 수 있습니다. 모든 NetFlow 생성기와 마찬가지로 StealthWatch FlowSensor에서 생성되는 NetFlow 트래픽 볼륨은 모니터링되는 트래픽 프로필에 따라 달라집니다.

StealthWatch FlowSensor 어플라이언스 사양

모델	처리 용량	인터페이스	속도	물리적 레이어	폼 팩터	전원
250	100Mbps	2	10/100/100	구리	1RU-short	비이중화
1000	1Gbps	3	10/100/1000	구리	1RU-short	비이중화
2000	60,000	5	10/100/1000	구리 또는 파이버	1RU	이중
3000	120,000	1 또는 2	1GB	파이버	1RU	이중

참고: 단일 StealthWatch FlowSensor의 처리 용량에 도달하면 적절한 이더넷 로드 밸런서를 사용하여 여러 개의 FlowSensor를 추가할 수 있습니다.

StealthWatch FlowSensor VE는 vSphere/ESX 호스트 내에 설치하여 해당 호스트의 VM 간 트래픽에 대한 NetFlow 레코드를 생성하는 데 사용할 수 있는 가상 어플라이언스입니다. FlowSensor VE는 가상 스위치에서 promiscuous 모드로 연결됩니다. 관찰하는 트래픽에서 이더넷 프레임을 수동적으로 캡처한 후 대화 형식 쌍, 비트 속도, 패킷 속도에 해당하는 중요 세션 통계를 포함하는 플로우 레코드를 만듭니다. 그러면 FlowSensor VE에서 이러한 레코드를 StealthWatch

FlowCollector에 전송합니다. 다음 표에서는 StealthWatch FlowCollector VE 구축을 위한 요구 사항을 설명합니다.

StealthWatch FlowSensor VE 사양

디스크 공간 요구 사항	플로우 내보내기 형식	최소 CPU 요구 사항	최소 메모리 요구 사항	인터페이스
1.4 GB	NetFlow v9	2GHz 프로세서	512 MB 애플리케이션 검사용 1024MB	최대 16개의 vNIC

2단계 네트워크에 StealthWatch FlowSensor 통합

StealthWatch FlowSensor는 모니터링 지점에 인접하도록 레이어 1 또는 레이어 2에 배치해야 합니다. 샘플 구축 모드에는 TAP(Test Access Port), SPAN(Switched Port Analyzer) 포트 또는 네트워크 허브 사용이 포함됩니다. 네트워크에 *StealthWatch FlowSensor*를 통합하는 방법에 대한 자세한 내용은 StealthWatch 설명서 CD에서 *시스템 하드웨어 설치 가이드*를 참조하십시오.

절차 2 StealthWatch FlowCollector 선택

StealthWatch FlowCollector 서비스는 Cisco Cyber Threat Defense 솔루션 버전 1.1의 모든 NetFlow 생성기에서 생성한 NetFlow 데이터에 대한 중앙 수집 및 분석 지점 역할을 합니다. 솔루션 구축 시에는 다음 요인에 따라 StealthWatch FlowCollector의 번호 및 모델을 선택해야 합니다.

- StealthWatch FlowCollector에 도달할 초당 플로우 볼륨에 영향을 미치는 이전 섹션의 결정 내용
- StealthWatch FlowCollector 구축 전략
- 각 StealthWatch FlowCollector의 물리적 용량

1단계 StealthWatch FlowCollector 구축 전략 결정

StealthWatch FlowCollector는 분산형 또는 중앙 집중형으로 구축할 수 있습니다. 분산형 구축에서는 FlowCollector를 여러 장소에 구축하며 일반적으로 가장 많은 NetFlow 레코드를 생산하는 소스 가까이 배치합니다. 이 구축에는 NetFlow로 도입되는 오버헤드를 제한한다는 이점이 있습니다. 중앙 집중형 구축에서 모든

StealthWatch FlowCollector는 하나의 데이터 센터에 배치되어(가능한 경우 로드 밸런서 뒤) NetFlow 수집을 위해 전역적으로 단일 수집 위치 및 단일 IP 주소(가능한 경우)의 이점을 제공합니다. 이 구축은 NetFlow 생성기가 멀리 떨어져 있는 환경에 유리합니다.

또한 장소 간 대역폭에 고려해야 할 제한 사항(WAN을 통해 등)이 있을 수 있습니다. 일반적으로는 가급적 많은 관련 트래픽에 단일 FlowCollector를 사용해야 합니다. 중앙 집중형 수집은 트래픽이 유사하지 않은 경우 그 이점이 감소합니다.

특정 FlowCollector에서 수신하는 이중 플로우 레코드에 대한 플로우 데이터를 수신하면 이 플로우를 위한 단일 데이터베이스 항목을 만듭니다. 이 중복 제거 프로세스를 통해 FlowCollector는 가장 효율적인 방법으로 플로우 데이터를 저장하면서도 각 플로우 내보내기에 대한 세부 정보를 유지하고 폭등한 트래픽 볼륨에 대한 보고를 제거할 수 있습니다.

이상적인 구현은 특정 플로우와 관련된 데이터를 내보내는 모든 라우터에서 해당 데이터를 동일한 FlowCollector로 보내는 것입니다. 그러나 각각의 고유한 호스트 쌍(또는 대화)에서 FlowCollector에 추가 리소스를 사용합니다. 동시 연결 수가 너무 커지면 플로우 레코드가 메모리에서 삭제됩니다. 대화가 한동안 유휴 상태를 거친 후까지 레코드를 삭제하지 않고 모든 활성 대화의 상태를 유지하려면 구축을 계획할 때 각 FlowCollector에 충분한 리소스가 있는지 확인합니다.

모범 사례: 하나의 플로우에 속하는 모든 NetFlow 레코드를 동일한 StealthWatch FlowCollector로 전송해야 합니다.

2단계 성능 고려 사항

각 StealthWatch FlowCollector에서는 이 단계의 끝에 있는 표에 설명된 대로 보증되는 최소한의 플로우 볼륨을 지원할 수 있습니다. 또한 Cisco Cyber Threat Defense 솔루션 버전 1.1에 사용할 StealthWatch FlowCollector를 선택할 때 다음 요인도 고려합니다.

- 내보내기 수 - 각 StealthWatch FlowCollector에서 수락할 수 있는 NetFlow 생성 디바이스의 수입니다.
- 데이터 속도 - StealthWatch FlowCollector에서 수신하는 속도(fps)입니다.

- 호스트 수 - StealthWatch FlowCollector에서 상태를 유지할 수 있는 호스트 수(네트워크 내부 및 외부 모두)입니다. Cisco에서는 내부 호스트의 수가 호스트 수 값의 60%를 초과하지 않을 것을 권장합니다.
- 플로우 스토리지 - 네트워크의 특정 위치에 필요한 정밀한 플로우 데이터의 양입니다.

참고: 특정 섀시에 대해 최대 내보내기 수 및 최대 데이터 속도에 모두 근접하는 시스템에서는 성능 문제가 발생할 수 있습니다. 예를 들면 최대 내보내기 수에서 최대 데이터 속도가 약 10%에서 20% 감소할 수 있습니다.

StealthWatch FlowCollector 어플라이언스 사양

모델	초당 플로우 수	내보내기	호스트 수	스토리지
StealthWatch FlowCollector 1000	최대 30,000	최대 500	최대 250,000	1.0TB
StealthWatch FlowCollector 2000	최대 60,000	최대 1,000명	최대 500,000	2.0TB
StealthWatch FlowCollector 4000	최대 120,000	최대 2000	최대 1,000,000	4.0TB

다음 표에서는 VM용 CPU 수 및 예약된 메모리의 양을 기반으로 StealthWatch FlowCollector VE에 대한 지원을 보여줍니다.

StealthWatch FlowCollector VE 사양

초당 플로우 수	내보내기	호스트 수	예약된 메모리	예약된 CPU
최대 4500	최대 250	최대 125,000	4GB	2
최대 15,000	최대 500	최대 250,000	8GB	3
최대 22,500	최대 1,000명	최대 500,000	16GB	4
최대 30,000	최대 1,000명	최대 500,000	32GB	5

절차 3 StealthWatch 관리 콘솔 선택

SMC(StealthWatch Management Console)는 전체 StealthWatch 시스템 설치를 관리하고, 연결된 FlowCollector의 수 및 전체 시스템에서 모니터링하는 총 플로우 볼륨에 따라 사용할 수 있습니다.

아래의 첫 번째 표에는 SMC 모델 및 해당 모델에서 지원 가능한 StealthWatch FlowCollector 수가 있습니다. 두 번째 표에는 SMC VE에서 지원할 수 있는 예약된 메모리 및 CPU에 따른 FlowCollector 및 동시 사용자 수가 제시되어 있습니다.

SMC 어플라이언스 사양

SMC 모델	최대 FlowCollector 수	크기	스토리지	메모리
SMC 1000	5	1RU	1.0TB	8GB
SMC 2000	25	2 RU	2.0TB	16GB

SMC VE 사양

ector 수	동시 사용자 수	예약된 메모리	예약된 CPU
1	2	4GB	2
3	5	8GB	3
5	10	16GB	4

참고: 구축에 다수의 호스트 그룹 및 모니터링되는 인터페이스가 필요한 경우 SMC로 전송할 데이터 양이 해당 구축에서 증가할 수 있으므로 고성능 SMC를 고려해야 합니다.

절차 4 (선택 사항) StealthWatch FlowReplicator 선택

StealthWatch FlowReplicator에서는 UDP 패킷을 수신 및 모니터링하고, 해당 패킷의 복사본을 생성하여 하나 이상의 새 대상으로 전송한 후 복사본이 어플라이언스를 통과할 때 원본 소스에서 전송한 것처럼 보이도록 패킷을 수정합니다. 각 FlowReplicator에는 2개의 활성 인터페이스가 제공되는데, 하나는 패킷 복사본의 관리, 모니터링, 생성을 위해 IP 주소가 할당되고, 다른 하나는 모니터링을 위해 무작위 모드로 설정할 수 있습니다.

각 FlowReplicator는 초당 패킷 수(pps) 측면에서 특정 입력 및 출력 볼륨으로 평가되었습니다. 각각 패킷당 2 - 3개의 복사본을 생성하도록 테스트했지만 필요한 경우 추가 대상을 지원할 수 있습니다. 다음 표에는 StealthWatch FlowReplicator 모델 및 사양이 있습니다.

StealthWatch FlowReplicator 어플라이언스 사양

FlowReplicator 모델	처리 용량	물리적 레이어	폼 팩터	전원	고장 허용 범위
1000	10,000pps 입력 20,000pps 출력	구리	1RU-short	비이중화	아니오
2000	20,000pps 입력 60,000pps 출력	구리 또는 파이버	1RU	이중	예

참고: 어플라이언스의 물리적 한도를 초과하여 해당 링크에 대해 복사본이 너무 많이 생성되면 패킷이 삭제됩니다.

NetFlow

플랫폼	하드웨어 정보	소프트웨어 세부 사항	NetFlow 세부 사항	CTD 버전 1에 포함 여부
Catalyst 3K-X	3560-X/ 3750-X with SM	IOS 15.0.(2) SE7	FNF(v9)	예
Catalyst 3850/3650	3850/3650	IOS-XE 3.3.5SE	FNF(v9)	일부(1.1.2의 3850)
Catalyst 4500	Sup7-E Sup8-E	IOS-XE 3.4.5SG IOS-XE 3.3.2XO	FNF(v9)	일부 (Sup7-E)
Catalyst 6500	Sup2T	IOS 15.0.(1) SY7a	FNF(v9)	예
Catalyst 2960-X (NetFlow Lite)	2960-X	IOS 15.0.(2) EX	NetFlow Lite (sampled V9)	아니오

ISR G2	2901, 2911	IOS 15.3(3)M4	FNF(v9)	예
ASR 1000	ASR 1001/ 1002F	IOS-XE 3.10.xS	FNF(v9)	예
ASA 5500	ASA 5505, 5510	ASA 9.0.4	NSEL(v9)	예
ASA 5500-X with FirePOWER Services	ASA 5515-X, 5545-X	ASA 9.3.2 FirePOWER 5.3.1	NSEL(v9)	아니오
Netflow Generation Appliance (NGA)	NGA 3240	1.0.2	FNF(v9)	예(3140)
UCS VIC	VIC 1240/ 1280/1225	2.2(2e)	FNF(v9)	아니오

차세대 침입 방지 시스템

FirePOWER 구축 옵션

보안 네트워크를 설계하려면 기본 네트워크를 신뢰할 수 있고 사용할 수 있는 경우에만 적용할 수 있는 잘 계획된 보안 정책이 있어야 합니다. Cisco ASA에서는 서비스를 보장하기 위해 고가용성 및 로드 밸런싱 컨피그레이션을 오랫동안 지원해왔습니다.

Cisco ASA with FirePOWER Services는 다음과 같은 구축 모드로 지원됩니다.

- 고가용성이 주요 관심사인 위치의 경우 **활성/대기**
- 다음 사항이 적용되는 위치의 경우 **클러스터링**
  - 비대칭이 문제임
  - HA(High Availability) 필요
  - 수평 수행 확장 필요
- 논리적 및 물리적 인터페이스에 따라 정책을 분리하는 경우 **다중 컨텍스트**

참고: 단일 또는 다수의 Cisco ASA 고가용성 구축의 경우 Cisco ASA의 FirePOWER Services가 투명 및 라우팅된(L3) 모드로 지원됩니다.

고가용성을 위한 활성/대기 모드

활성/대기 모델을 사용하는 HA(High Availability)는 Cisco ASA 5500-X 및 Cisco ASA 5585-X 플랫폼에서 지원됩니다. 활성/대기에서는 HA 쌍에 1개의 디바이스를 기본(활성)으로 정의하고 다른 하나를 보조(대기)로 정의합니다. 신속하고 용이하게 페일오버를 수행하기 위해 방화벽 간에 연결 정보를 포함한 Cisco ASA의 상태를 공유합니다. 이를 상태 보존형 페일오버라고 합니다. 그러나 FirePOWER 상태 정보는 페일오버 쌍의 FirePOWER 모듈 간에 공유되지 않습니다.

FirePOWER Services 모듈은 표준화 이후 Cisco ASA 패킷 처리 경로에 삽입됩니다. TCP/IP 표준화 서비스에서는 비정상적인 패킷이 탐지되면 Cisco ASA에서 조치를 취할 수 있는 패킷을 식별합니다.

일반적인 활성/대기 구축은 아래와 같습니다.

ASA with FirePOWER Services 구축

- ASA 5500-X 및 ASA5585-X에서 사용 가능
- L2 투명 또는 L3 라우팅된 구축 옵션
- 페일오버 링크
- ASA에서 FirePOWER 모듈에 유효하고 표준화된 플로우 제공
- 고가용성을 위한 방화벽 간 상태 공유
  - 참고: FirePOWER Services 모듈 간에는 상태 공유가 발생하지 않습니다.

클러스터링 구축

클러스터에는 확장성을 위해 FirePOWER Services 모듈과 함께 최대 16개의 Cisco ASA 5585-X 방화벽이 포함될 수 있습니다. Cisco ASA 5500-X에서는 2개의 유닛으로 된 클러스터를 지원합니다.

Cisco ASA 클러스터링에서 제공하는 이점은 다음과 같습니다.

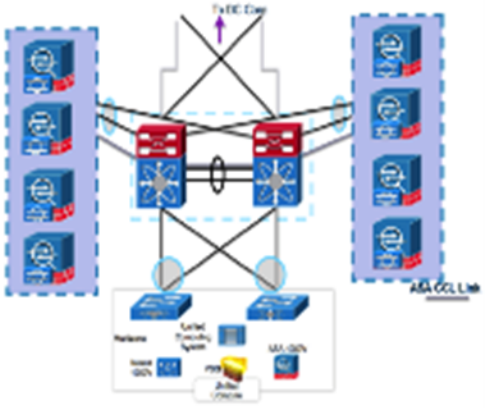
- 더 높은 처리량을 달성하기 위해 트래픽을 집계하는 기능
- Cisco ASA 어플라이언스 수를 데이터 센터 아키텍처 내에서 하나의 논리적 방화벽으로 조정
- 진정한 활성/활성 모델(다중 컨텍스트 모드에서 클러스터의 모든 컨텍스트에 대한 모든 멤버가 모든 트래픽 플로우를 전달할 수 있는 경우)
- 플로우를 소유하지 않은 ASA에서 보낸 패킷을 CCL(Cluster Control Link)을 통해 실제 소유자에게 전송하여 비대칭성을 제거합니다.
- 레이어 2 및 레이어 3 모드 중 하나로 작동
- 단일 및 다중 컨텍스트 지원(방화벽 가상화)
- 리소스 사용량을 추적할 수 있도록 클러스터 전체에 대한 통계 제공
- 자동 컨피그레이션 동기화를 사용하여 클러스터의 모든 유닛에서 하나의 Cisco ASA 컨피그레이션 유지

참고: Cisco ASA 클러스터 내의 FirePOWER Services 모듈 간에는 상태 공유가 발생하지 않습니다. 따라서 클러스터 내의 FirePOWER 컨피그레이션이 동기화되지 않습니다.

일반적인 클러스터 구축은 아래와 같습니다.

ASA with FirePOWER Services 구축

- 최대 16개의 ASA5585-X with FirePOWER Services
- 외부 스위치에 의한 ASA로의 상태 비저장 부하분산
- L2 투명 또는 L3 라우팅된 구축 옵션
- vPC, VSS 및 LACP 지원
- 클러스터 제어 프로토콜/링크
- 대칭 및 고가용성을 위한 방화벽 간 상태 공유
  - 참고: FirePOWER Services 모듈 간에는 상태 공유가 발생하지 않습니다.
- 각 세션에는 기본 소유자 및 책임자가 있음
- ASA에서 FirePOWER 모듈에 트래픽 대칭 제공



다중 컨텍스트 구축

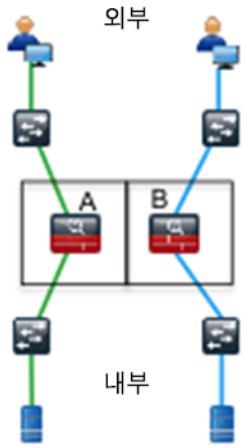
Cisco ASA를 통해 트래픽을 세분화하는 일반적인 방법은 다중 컨텍스트 모드를 구성하는 것입니다. 이렇게 하면 별도의 가상 보안 상황 각각에 고유한 보안 정책을 시행할 수 있습니다. 다음은 Cisco ASA의 다중 컨텍스트 모드에 대한 몇 가지 전형적인 사용예입니다.

- 통신 사업자가 수많은 고객에게 보안 서비스 지원
- 부서를 완전히 별도로 유지해야 하는 대기업 또는 대학 캠퍼스
- 부서별로 각기 다른 보안 정책을 제공해야 하는 기업
- Cisco ASA가 2개 이상 필요하지만 예산이 제한된 네트워크

다중 컨텍스트 모드에서는 Cisco ASA 인터페이스 및 하위 인터페이스가 각 컨텍스트에 할당됩니다. FirePOWER Services를 Cisco ASA에 다중 컨텍스트 모드로 구축하면 각 컨텍스트와 관련된 인터페이스를 보안 영역으로 그룹화할 수 있습니다. 그러면 다양한 FirePOWER 정책을 각 영역에 적용할 수 있습니다. 예를 들면 컨텍스트 A/인터페이스 외부 - 컨텍스트 A/인터페이스 내부에 하나의 정책이 적용됩니다.

일반적인 다중 컨텍스트 구축은 아래와 같습니다.

- ASA는 ASA를 통해 이동하는 트래픽에 다양한 정책을 할당할 수 있는 다중 컨텍스트 모드로 구성할 수 있습니다.
- 이러한 인터페이스는 FirePOWER 블레이드에 보고하고, 차별화된 정책에 사용할 수 있는 보안 영역에 할당할 수 있습니다.
- 다음 예제에서는 컨텍스트 A 외부에서 컨텍스트 A 내부로 이동하는 트래픽에 대해 하나의 정책을 만들 수 있습니다. 그런 다음 컨텍스트 B 외부에서 컨텍스트 B 내부로 이동하는 트래픽에 대해 다른 정책 정책을 만듭니다.
- 참고: ASA 컨피그레이션 내부의 컨텍스트 개념과 유사한 FirePOWER 모듈 내부에는 관리 세그멘테이션이 없습니다.



FirePOWER 어플라이언스에서는 다양한 구축 옵션을 사용할 수 있습니다. 예를 들면 다음과 같습니다.

- 수동-수동 모드에서는 센서가 네트워크 TAP 또는 스위치의 SPAN 포트에서 들어오는 패킷을 검사할 수 있습니다. 어플라이언스는 패킷 플로우에 속하지 않으므로(패킷은 복사본이며 원본이 아님) 레이턴시 또는 오류 시나리오의 네트워크에 영향을 미치지 않습니다. 단점은 디바이스가 수동 모드에 있기 때문에 원래 패킷을 사용하여 작동하지 않으며, 따라서 대상에 도달하기 전에 악의적인 트래픽을 삭제할 수 없습니다.
- 인터페이스 페어링 - 인터페이스 페어링 모드는 어플라이언스가 유선처럼 작동하고 하나의 인터페이스에서 패킷을 가져와 해당 패킷을 검사하여 다른 인터페이스를 전송하고, 그 반대의 경우도 마찬가지인 일반적인 IPS 모드입니다. 어플라이언스가 인라인이기 때문에 단일 패킷을 포함하여 악의적인 트래픽을 차단할 수 있지만, 트래픽이 어플라이언스를 통과해야 하므로 약간의 레이턴시가 추가되며, 오류 시나리오를 고려해야 합니다. 이러한 이유로 고장이 나면 개방 인터페이스와 같은 기능이 일반적으로 사용됩니다.
- 가상 스위치 - 이 모드에서는 센서가 가상 스위치 역할을 하고 레이어 2 스위치 역할을 하는 하나 이상의 가상 인터페이스로 들어오는 패킷을 검사할 수 있습니다. 이 모드에서는 인터페이스 페어링 모드처럼 디바이스에서 패킷을 삭제할 수 있습니다.
- 라우팅된 모드 - 이 모드에서는 디바이스를 각 인터페이스에 IP 주소가 있는 네트워크에 레이어 3 디바이스로 배치합니다. 이 모드는 일반적으로 디바이스가 방화벽 역할을 하는 경우 사용되며, IPS, AVC, URL 정책뿐만 아니라 레이어 3 및 레이어 4 정책도 적용합니다.

다양한 성능 레벨의 다양한 어플라이언스를 사용할 수 있습니다. 또한 인터페이스 유형에 따라 수많은 옵션이 있습니다.
어플라이언스는 원하는 결과에 따라 Failopen(고장 시 개방) 또는 Failclosed(고장 시 폐쇄) 모드로 설정할 수 있습니다.

FireSIGHT Management Center

FMC(FireSIGHT Management Center)는 어플라이언스 및 가상 폼 팩터, 두 가지로 제공됩니다. 둘 다 동일한 기능을 제공하지만 성능에 있어 다릅니다. 어플라이언스 버전은 모든 유형의 FirePOWER 센서를 관리할 수 있습니다. 가상 FMC에는 두 가지 유형이 있는데, 하나는 모든 센서 유형을 관리하는 전체 버전이고 다른 하나는 Cisco ASA 센서에 대해 FirePOWER Services만 관리하는 유형입니다.

고가용성은 FMC에서 사용할 수 있는 기능입니다. 고가용성을 통해 Management Center에서 라이센싱을 공유하고 컨피그레이션을 동기화된 상태로 유지할 수 있습니다. 가상 디바이스에서는 가상 솔루션에 일반적인 내장된 복구 방법을 사용해야 합니다.

AMP(Advanced Malware Protection)

Cisco AMP는 가장 광범위한 공격 벡터로부터 보호하며 다음과 같이 구축할 수 있습니다.

- 전용 Cisco ASA Firewall 및 Cisco FirePOWER 네트워크 보안 어플라이언스에 통합된 네트워크 기반 솔루션
- PC, Mac, 모바일 디바이스, 가상 환경의 엔드포인트 솔루션
- 개인 정보 보호 요건이 까다로운 환경에 적합한 온프레미스 프라이빗 클라우드 가상 어플라이언스
- Cisco Cloud Web Security Appliance 또는 Cisco Web & Email Security Appliance에 통합된 기능

네트워크용 AMP는 모든 FirePOWER 센서에 사용할 수 있는 기능입니다. 이러한 설계 및 구축 고려 사항은 FirePOWER 서비스 모듈 및 FirePOWER 어플라이언스와 정확하게 동일합니다.

AMP for Endpoints는 Windows PC, Mac, 가상 환경, 모바일 디바이스에 설치할 수 있는 기능입니다. AMP for Endpoints에서는 악의적인 콘텐츠에 대해 파일을 모니터링할 뿐만 아니라 시스템에 제공되는 알 수 없는 파일에서 발생하는 작업도 감시할 수 있습니다. 그러면 해당 파일이 악의적인 것으로 판단되는 경우 시스템에서 확산되거나 손상을 주지 않도록 파일을 차단할 수 있습니다.

콘텐츠 보안 제어

Cisco 콘텐츠 보안 제품에서는 물리적 어플라이언스, 가상 어플라이언스, 클라우드 제품을 포함하여 보안 게이트웨이 구축 옵션의 모든 측면을 다룹니다. 고객의 환경 요구 사항에 따라 이메일 및 웹 보안 제품 모두에서 이러한 옵션을 다룹니다. Email Security 및 Web Security 제품 모두 투명한 인라인 디바이스가 아닙니다. 둘 다 게이트웨이를 통과하는 페이로드를 가져오기 위해 어느 정도의 리디렉션 또는 라우팅이 있어야 합니다.

Email Security 구축 옵션

ESA는 SMTP MTA(Mail Transfer Agent) 기능을 수행합니다. Exchange, Lotus Notes 또는 기타 서드파티의 데이터 저장소처럼 이메일 사서함 서버를 위한 것은 아닙니다. ESA와 주고받는 SMTP 라우팅은 이메일 메시지의 도메인 부분을 기반으로 MX 레코드를 사용하거나 하나의 레코드 또는 여러 IP 주소를 기반으로 정의된 SMTP 경로를 사용하여 DNS를 통해 수행됩니다.

- ESA 하드웨어 어플라이언스는 3가지 모델(C170, C380, C680)로 제공되며, 각각 소규모, 중간 규모, 대규모 네트워크에 적합합니다. 소프트웨어 기능은 모든 어플라이언스 규모에서 동일합니다.
- ESAV(ESA Virtual) 어플라이언스는 VMware ESXi 하이퍼바이저에서 지원되며 다음과 같이 다양한 규모로 제공됩니다.
    - 평가 전용 Cisco ESAV C000v
    - 최대 1000개의 사서함을 위한 Cisco ESAV C100v
    - 최대 5000개의 사서함을 위한 Cisco ESAV C300v
    - 대기업 또는 통신 사업자를 위한 Cisco ESAV C600v
- Cisco CES(Cloud Email Security)에서는 온프레미스에 구축한 물리적 또는 가상 ESA 어플라이언스에 대한 대안으로 Cisco 데이터 센터에서 호스팅하는 서비스와 동일한 레벨의 보호 기능을 제공합니다. 하이브리드 구축도 가능합니다.
- ESA에 대한 권장 사례는 엔터프라이즈 네트워크에 들어오는 첫 번째 SMTP 홉이자 나가는 마지막 홉이 되는 것입니다.
- ESA 어플라이언스는 일반적으로 간소화를 위해 메일 및 관리 트래픽 모두 하나의 인터페이스와 IP 주소를 사용하여 구축해야 합니다.
- ESA 구축 옵션에 대한 전체적인 논의는 이 문서의 범위를 벗어납니다. 자세한 내용은 www.cisco.com/go/designzone에서 인터넷 에지용 Cisco Design Zone을 참고하십시오.

Web Security 구축 옵션

- WSA 하드웨어 어플라이언스는 3가지 모델(S170, S380, S680)로 제공되며, 각각 소규모, 중간 규모, 대규모 네트워크에 적합합니다. 소프트웨어 기능은 모든 어플라이언스 규모에서 동일합니다.
- WSAV(WSA Virtual) 어플라이언스는 KVM 또는 VMware ESXi 하이퍼바이저에서 지원되며 다음과 같이 다양한 규모로 제공됩니다.
    - 최대 1000명의 웹 사용자를 위한 Cisco ESAV C000v
    - 최대 3000명의 웹 사용자를 위한 Cisco ESAV C100v
    - 최대 6000명의 웹 사용자를 위한 Cisco ESAV C300v
- Cisco CWS는 전체를 클라우드 기반 솔루션으로 구축하거나 구내 WSA 어플라이언스와 함께 통합할 수 있습니다. Cisco CWS 프리미엄에서는 지능형 위협 탐지를 강화하기 위해 AMP 및 CTA를 통합합니다.
- WSA 어플라이언스는 투명 리디렉션 및 명시적 프록시 컨피그레이션을 포함하여 다양한 옵션을 사용하여 구축할 수 있습니다. WSA 구축 옵션에 대한 전체적인 논의는 이 문서의 범위를 벗어납니다. 자세한 내용은 www.cisco.com/go/designzone에서 인터넷 에지용 Cisco Design Zone을 참고하십시오.

TrustSec 및 Identity Services Engine

Cisco TrustSec의 CVD, ISE, 엔드포인트 보호 서비스를 포함한 자세한 내용은 www.cisco.com/go/trustsec에서 확인할 수 있습니다.

결론

이 문서에서는 최신 지능형 위협으로부터 네트워크를 방어하는 것과 관련된 몇 가지 당면 과제에 대해 논의하고 Cisco Cyber Threat Defense 솔루션의 설계 지침을 제공합니다. 이 솔루션은 기존의 네트워크 경계에서 뿐만 아니라 네트워크 내부에서 활동하는 위협을 탐지하고 대응하는 데 필요한 상황 인식을 개선하고 시간을 단축하는 데 주력합니다. 이를 위해 네트워크 인프라에서 향상된 가시성과 제어 권한을 제공하고, Cisco의 앞선 보안 기술을 통합 설계에 포함할 수 있도록 합니다. 결과적으로 위협을 새로운 방식으로 탐지 및 차단하고 교정할 수 있는 방어자의 기술을 실제로 개선했습니다.

참조

일반 보안 정보

NIST(National Institute of Standards & Technology) IR 7298 개정판 2: *Glossary of Key Information Security Terms*
http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

NIST SP 800-61 개정판 2: *Computer Security Incident Handling Guide*
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Lockheed Martin Corporation, *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*
http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Cisco Systems, *Cisco 2015 연례 보안 보고서*
http://www.cisco.com/go/security