SDSN(Software-Defined Secure Networks) 동작 원리

자동화된 위협 대응 및 비즈니스 연속성 보장

과제

기업은 네트워크를 위협하는 갈수록 고도화되는 공격에 맞서 끊임없이 진화해야 합니다. 그렇다고 보안에만 중점을 두다 보면 다른 중요한 작업들에 악영향을 줄 수 있으며, 결국 이로 인해 네트워크 보안과 비즈니스 연속성을 놓고 내부적으로 줄다리기가 벌어지게 됩니다.

솔루션

기업은 개방적인 멀티벤더 생태계 내에서 네트워크와 보안 요소들을 동등하게 활용하여 시너지를 일으킬 수 있는 접근방식을 채택해야 합니다. 아울러 중앙화된 정책, 분석, 관리를 통해 전통적인 네트워크를 보안 네트워크로 전환해야 합니다.

이점

- 보다 정확하고 효과적인 위협 탐지
- 네트워크 생태계 전반에 대한 글로벌 정책 관리 및 위협 분석
- 네트워크 내의 수많은 보안 실행 포인트를 통한 정교한 격리 기능
- 신속하고 자동화된 위협 대응

네트워크 구축 양상은 지난 십년 간 크게 달라졌습니다. 대부분의 기업이 클라우드로 급속히 이동하고 있으며, 사물인터넷(IoT)이나 블록체인(block chain) 같은 새로운 기술들이 빠르게 도입되고 있습니다. 이 모든 것들이 네트워크를 기반으로 합니다.

또한 신규 및 기존 인프라 보호를 위한 기업의 보안 비용이 급증하고 있습니다. 그럼에도 불구하고 보안 침해 사고는 전혀 줄어들 기미가 보이지 않습니다. 내부 기록과 고객 정보가 유출되어 최고 경매가에 팔려나가고, 이로 인해 기업은 평판에 돌이킬 수 없는 손상을 입게 됩니다. 그렇다면 이런 기업들은 네트워크 보안 접근방식에 있어서 매우 중요한 무언가를 놓치고 있는 것일까요?

과제

오늘날 차세대 방화벽, 샌드박스(sandboxing), CASB(cloud access security broker), SIEM(security event and information management), 엔드포인트 보안 등 매우 효과적인 보안 기술과 솔루션들이 시장에 나와 있습니다. 그러나 네트워크 전체의 보안 수준은 가장 취약한 링크의 보안 수준과 동일합니다. 따라서 모든 네트워크 요소들 간의 긴밀한 협업과 동기화가 이루어지지 않는다면, 기업은 보안 허점을 통해 공격에 취약하게 노출될 수 밖에 없습니다. 이것이 바로 인기 보안 제품에 막대한 비용을 투자하면서도 여전히 보안 현실이 기대 이하의 수준에 머무르는 이유입니다.

일반적인 인프라 및 보안 제품을 통한 기업 내 위협 전파

클라이언트, 엔드포인트, 액세스 스위치, 무선 액세스 포인트 등으로 이루어진 일반적인 엔터프라이즈 환경을 생각해 봅시다. 안티멀웨어 서비스와 연결된 차세대 방화벽이 North-South 위협 방어를 위해 네트워크 경계에서 사용됩니다. 클라이언트 상에서는 기기 타입이나 모델에 따라 엔드포인트 보안 소프트웨어를 사용할 수 있습니다. 하지만 IoT 환경의 네트워크 프린터나 최신 유형의 엔드포인트에서는 이러한 보호를 사용할 수 없습니다.

네트워크 보안 침해 과정

그림 1은 손상된 네트워크를 보여줍니다. 이러한 보안 침해는 일반적으로 다음과 같은 패턴을 따르게 됩니다.

1. 클라이언트가 Unknown 멀웨어 다운로드 시도.
2. 네트워크 경계 방화벽에서 해당 파일 스캐닝.
3. 방화벽이 분석을 위해 해당 파일을 안티멀웨어 서비스로 전송. 안티멀웨어 서비스가 방화벽에 해당 파일이 멀웨어임을 알림.
4. 방화벽이 해당 파일을 블록하여 다운로드 차단.
5. 그러나 클라이언트가 기업 네트워크 외부("non-enterprise" 환경)에서 감염되었거나 수동적인 방식으로 감염되었을 경우, 감염된 클라이언트는 네트워크 내에서 계속해서 접근가능한 다른 호스트들을 감염시키게 됨(위협 종류에 따라).

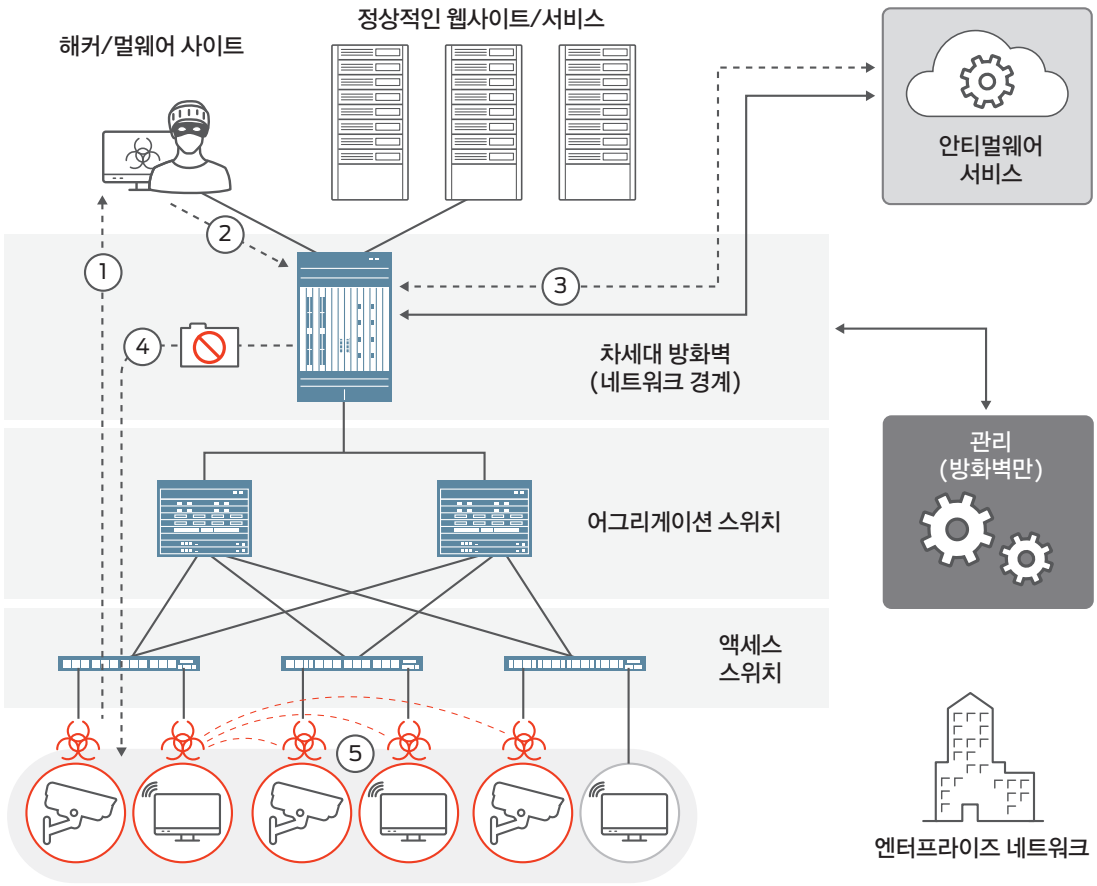

그림 1: 일반적인 인프라와 보안 제품들로 이루어진 엔터프라이즈 환경 내의 네트워크 보안 침해

따라서:

a. 단순히 클라이언트의 기업 네트워크 외부 연결을 차단하는 것만으로는 비효과적이며, 측면 이동(Lateral Movement)에 의한 위협 확산을 막을 수 없습니다.

b. 보안 솔루션이 네트워킹 요소들을 활용하고 서로 통신하지 못하면, 가시성이 저하되고 실행 포인트의 수도 제한됩니다.

c. 로깅 서버, 엔드포인트, 기타 네트워크 요소 등 다양한 정보 소스로부터 비정상적인 작업에 대한 리포트들을 취합하지 못한다는 것은 보안 전략 상의 중대한 약점입니다.

d. 기존 보안 전략은 방화벽에 중점을 두고 있기 때문에, 복잡한 방화벽 정책으로 인해 보안팀에 과부하가 일어나기 쉽습니다. 분산된 글로벌 기업의 경우, 이 문제가 더욱 심각해질 수 있습니다.

주니퍼 네트웍스 SDSN 솔루션

주니퍼 네트웍스 SDSN(Software-Defined Secure Network)은 새로운 차원의 기업 보안을 실현합니다. SDSN은 물리적 환경과 가상 환경을 모두 아우르는 전반적인 네트워크 보호에 필요한 엔드-투-엔드 네트워크 가시성을 제공합니다. 그리고 클라우드 경제성을 활용하여 위협을 신속하게 탐지하고 차단합니다. SDSN 플랫폼은 종합적인 제품 포트폴리오를 통해 정책, 탐지, 실행을 결합함으로써 보안을 중앙화하고 자동화합니다.

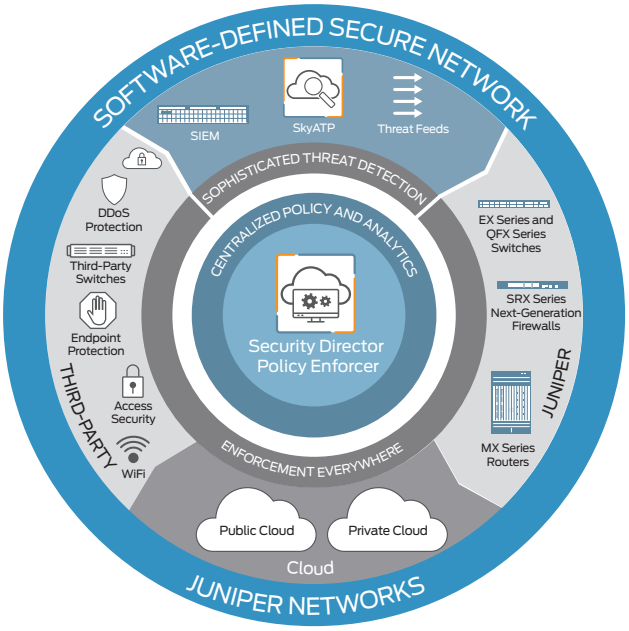

그림 2: SDSN 구성요소

SDSN 구성요소

SDSN(Software-Defined Secure Network)은 다음과 같은 요소들로 구성됩니다.

1. 정교한 위협 탐지 엔진:
   a. 주니퍼 네트웍스 Sky Advanced Threat Prevention 클라우드 기반 멀웨어 탐지 솔루션이 Known/Unknown 위협의 정확한 탐지를 위해 사용됩니다.
   b. 인하우스 로그 서버에서 얻은 정보는 물론 C&C(command and control) 서버, GeoIP, REST API를 통한 써드파티 디바이스 등 다양한 소스로부터 위협 피드 정보를 종합하여 알려진(Known) 위협을 탐지합니다.
   c. Sky ATP가 샌드박스(sandboxing), 머신러닝, 위협 디셉션(deception) 기술 등을 사용하여 Unknown 위협을 파악합니다
2. 중앙화된 관리, 정책, 분석:
   a. 주니퍼 네트웍스 Junos® Space Security Director가 확장가능하고 능동적인 보안 관리 애플리케이션 제공. 단일 관리창을 통한 보안 정책 관리 향상.
   b. Policy Enforcer(Security Director의 구성요소)가 중앙 인텔리전스 모듈로서 다음과 같은 기능 제공:
      - 차세대 방화벽 등 멀티벤더 환경의 네트워크 요소 및 보안 제품들과 통신하여 글로벌 보안 정책 실행 및 분석 제공
      - 다양한 소스로부터의 위협 인텔리전스 통합
3. 모든 곳에서 보안 실행:
   a. SDSN은 모든 네트워크 요소들을 실행 포인트로 활용.
   b. SDSN은 개방적인 멀티벤더 생태계를 통해 주니퍼 솔루션, 클라우드, 써드파티 생태계 전반에서 위협 탐지 및 보안 실행.
   c. SDSN은 신속하게 위협을 차단 또는 격리시키는 기능을 제공하여 North-South 또는 East-West 멀웨어 전파 차단.

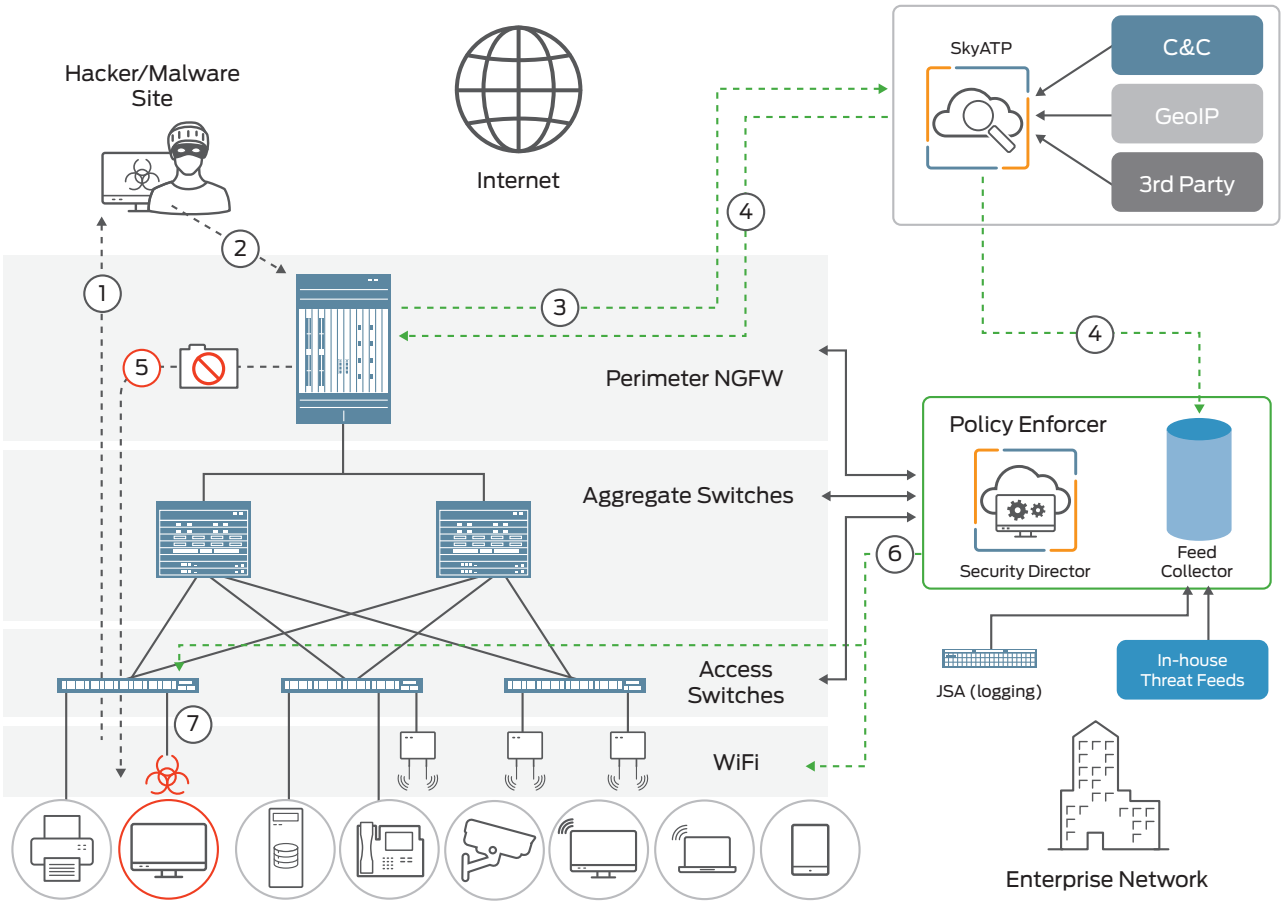

그림 3: SDSN을 통한 보안 네트워크 구축

SDSN을 통한 보안 네트워크 구축

네트워크 경계 방화벽으로 주니퍼 네트웍스 SRX 시리즈 서비스 게이트웨이를 사용하고 안티멀웨어 서비스를 위해 Sky Advanced Threat Prevention이 연결된 SDSN환경을 살펴 봅시다. Security Director Policy Enforcer는 중앙 인텔리전스 요소로서, 차세대 방화벽을 비롯한 다양한 네트워크 요소들과 통신하여 글로벌하게 보안 정책들을 실행합니다.

Policy Enforcer의 Feed Collector 모듈은 클라우드 및 내부의 물리적인 장비들로부터 수집된 위협 피드와 로깅(logging) 및 인하우스 위협 피드를 통합합니다. 클라이언트/엔드포인트는 액세스 스위치 또는 무선 액세스 포인트에 연결되고 엔드포인트 보안 소프트웨어로 보호됩니다. IoT 디바이스, 프린터, 최신 유형의 엔드포인트들은 이러한 보호를 받을 수 없으나, Policy Enforcer가 액세스 디바이스들과 통신하여 인텔리전스를 공유하고 필요한 곳에 보안을 실행할 수 있습니다.

SDSN은 일반적인 보안 침해 패턴을 근본적으로 무력화시킵니다. 주니퍼 보안 네트워크가 공격을 받을 경우, 다음과 같은 두 가지 시나리오로 대응이 가능합니다.

워크플로우 1: 멀웨어 다운로드

1. 클라이언트가 Unknown 멀웨어 다운로드 시도.
2. 네트워크 경계에서 SRX 시리즈 방화벽에서 해당 파일 스캐닝.
3. SRX 시리즈 방화벽이 해당 파일을 Sky ATP로 전송.
4. Sky ATP 해당 파일이 멀웨어임을 확인하고, 이를 SRX 시리즈 방화벽과 Policy Enforcer에 통보.
5. SRX 시리즈 방화벽이 해당 파일을 블록하여 다운로드 차단.
6. Policy Enforcer가 추가 조사가 가능할 때까지 해당 호스트를 특정 VLAN(스위치에서)에 격리. Policy Enforcer는 또한 클라이언트가 연결되어 있는 스위치 포트 또는 Wi-Fi 액세스 포인트를 비활성화시킬 수도 있음(옵션).
7. 공격 타겟이된 클라이언트는 이제 네트워크 내의 다른 호스트들을 감염시킬 수 없게 됨. East-West 및 North-South 멀웨어 전파가 차단됨. Policy Enforcer가 해당 클라이언트를 기억하여 이것이 다른 스위치나 Wi-Fi 액세스 포인트로 이동하더라도 위협을 식별하고 네트워크에서 차단.

워크플로우 2: 감염된 IoT 디바이스

1. 네트워크에 연결된 감염된 IoT 디바이스가 금지된 파일 다운로드를 시도하거나 또는 주요 인프라 상에서 공격을 개시.

2. JSA(Juniper Secure Analytics)가 무단 다운로드 시도를 로깅하고, 이를 Security Director Policy Enforcer에 보고.

3. Policy Enforcer가 ACL(access control list)/NAC(network access control) 규칙을 관련 스위치 포트 또는 Wi-Fi 액세스 포인트에 적용하여 해당 호스트를 격리하고, 신속하게 위협 대응 조치를 실행.

이와 같은 네트워크 상의 공격이 SDSN이 아닌 일반 네트워크에서 발생한다면, 문제의 IoT 디바이스는 계속해서 더 많은 정보에 액세스할 수 있을 것입니다. 전통적인 차세대 방화벽의 대응은 단순히 이 IoT 디바이스가 외부 조직과 통신하지 못하도록 하는데 그칩니다. 따라서 공격자가 회사 디바이스에 물리적으로 액세스하여 조직 내부에서 공격이 진행될 경우, 막대한 피해가 발생할 수 있습니다.

요약

주니퍼 네트웍스 SDSN(Software-Defined Secure Network)은 네트워크 요소와 보안 요소들을 결합시키고 중앙 관리 및 분석을 실행함으로써 네트워크 전반을 아우르는 보안(Pervasive Security)과 자동화된 위협 대응을 제공합니다. SDSN은 개방적인 멀티벤더 생태계를 지원하여 기업이 기존에 구축되어 있는 네트워크 및 보안 요소들을 사용할 수 있도록 해줍니다. 따라서 기존 투자를 보호하는 동시에 비즈니스 연속성을 보장합니다.

다음 단계

주니퍼 네트웍스 보안 솔루션에 대한 기타 정보는 www.juniper.net/kr/kr/products-services/security에서 확인하거나 주니퍼 네트웍스 담당자에게 문의 바랍니다.

주니퍼 네트웍스에 대하여

주니퍼 네트웍스는 네트워킹의 경제성을 혁신하는 제품, 솔루션, 서비스를 제공합니다. 주니퍼는 고객, 파트너들과 함께 민첩성, 성능, 가치를 제공하는 자동화되고 확장 가능하며 안전한 네트워크를 위한 혁신을 계속하고 있습니다. 자세한 정보는 주니퍼 네트웍스 웹사이트와 블로그, 트위터 및 페이스북을 통해 확인할 수 있습니다.

한국주니퍼네트웍스(주) 서울시 강남구 역삼 1동 736-1 캐피탈 타워 19층 TEL: 02)3483-3400 FAX: 02)3483-3488 www.juniper.net/kr/kr

본사
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

아태지역 및 EMEA 본부
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

주니퍼 네트웍스 솔루션에 대한 구매 문의는 한국주니퍼네트웍스 (전화 02-3483-3400, 이메일 salesinfo-korea@juniper.net)로 연락주십시오.

3510608-001-KR Mar 2017