Case Study

차세대 방화벽과 EPP로 구현하는 제로 트러스트 보안

안랩은 당사가 계속해서 고도화해고 있는 통합 보안 전략을 바탕으로 엔드포인트 보안 플랫폼(EPP)와 차세대 방화벽을 연동한 '제로 트러스트' 보안을 제공한다. 특히, 안랩이 올 상반기 출시한 새로운 차세대 방화벽 AhnLab XTG는 기존 AhnLab TrusGuard 대비 강력한 성능과 ZTNA(Zero Trust Network Access) 등 차세대 보안을 위한 기능들을 제공한다.

AhnLab EPP와 AhnLab XTG를 연동하여 엔드포인트 – 네트워크 연계 제로 트러스트 보안을 구현하는 사례들을 소개한다.

AhnLab EPP: 안랩 통합 보안 전략의 핵심

AhnLab EPP는 기존 포인트 보안 솔루션 중심의 단순한 보안 관리를 넘어 유기적인 엔드포인트 보안 관리 및 운영을 통해 더 강력하고 효율적인 위협 대응을 역량을 제공한다. 여러 엔드포인트 보안 솔루션들을 단일 에이전트, 단일 관리 콘솔을 기반으로 관리해 복잡다단한 엔드포인트 환경을 효율적으로 보호할 수 있다.

AhnLab EPP는 가장 잘 알려져 있는 안티바이러스 솔루션 AhnLab V3를 포함해 EPP Privacy Management(EPrM), EPP Patch Management(EPM), EPP Security Assessment(ESA), EPP Device Control(EDC), 그리고 EDR까지 6개의 엔드포인트 보안 솔루션으로 구성되어 있다. 각각의 솔루션이 안티바이러스, 개인정보 보호, 패치 관리, 취약점 점검 & 조치, 디바이스 제어, 위협 탐지 및 대응 등 보안에 필요한 기능들을 수행하고, 이를 단일 에이전트와 단일 콘솔을 기반으로 관리할 수 있어 고객 입장에서 보안성과 효율성을 제고할 수 있다.

[그림 1] AhnLab EPP 구성도

AhnLab EPP를 통해 다수의 엔드포인트 보안 솔루션 간 규칙 및 대응 조치를 유기적으로 연계해 설정함으로써 보안 위협에 더욱 강력한 대응이 가능해진다. 보안 담당자의 필요에 따라 다양한 보안 정책을 적용할 수 있어 고객 주도적이며 능동적인 보안 운영이 가능하다.

AhnLab XTG: 제로 트러스트를 위한 차세대 네트워크 방화벽

안랩은 2025년 상반기, 새로운 차세대 방화벽 AhnLab XTG를 출시했다. AhnLab XTG는 강력한 성능과 함께 ZTNA, SD-WAN 등 최신 네트워크 보안 활용 사례들을 지원하는 진일보한 솔루션이다. 사용자 인터페이스(UI)도 고객 친화적으로 구성하여 탁월한 사용성을 제공한다.

이 밖에, IPS(Intrusion Prevention System), 애플리케이션 제어, VPN, C&C 탐지 및 차단, 안티바이러스, 안티스팸, DLP(Data Loss Prevention) 등의 기능들을 제공한다. 로우엔드 모델부터 데이터센터급 모델까지 다양한 제품 라인업을 갖추고 있어 기업이 네트워크 환경에 맞춰 효율적으로 적용할 수 있다.

다음은 AhnLab XTG의 주요 기능 중 본 문서에서 소개할 운영 사례와 관련된 주요 기능들을 정리한 것이다.

1. 애플리케이션 제어

AhnLab XTG는 차세대 보안 기술인 애플리케이션 제어(Application Control) 기능을 탑재해 P2P, 웹하드, 메신저, SNS 등 수 천 개의 애플리케이션에 대해 실시간 분석 및 차단•허용•행위 제어가 가능하다. 또한, 식별이 불가능한 알려지지 않은(Unknown) 애플리케이션 인지를 통해 허용된 애플리케이션에 대한 통신만 가능하게 하여 보안성을 강화한다.

2. 사용자 & 디바이스 기반 제어

AhnLab XTG는 IP 주소를 기반으로 사용자를 식별하는 방식과 함께 사용자 ID 기반의 사용자 구분 및 행위 제어 기능을 제공해 효율적인 내부 보안 관리와 신속한 보안 위협 대응이 가능하도록 한다. 또한, 디바이스 상태 정보를 인지하여 OS 버전, 보안 패치 여부, 필수 SW 설치 유무, 취약점 점검 결과 등에 따라 네트워크 접근을 제어할 수 있다.

3. ZTNA

AhnLab XTG의 ZTNA는 제로 트러스트의 기본 원칙인 '항시 검증/최소 권한 접근'을 기반으로 안전한 네트워크 접근을 보장한다. 사용자와 기기의 신원과 보안 상태를 지속적으로 확인하여 검증된 사용자만 애플리케이션 및 네트워크 리소스에 접근하도록 한다. 애플리케이션 단위의 세분화된 보안 정책을 적용할 수 있어 보다 안전한 원격 접속이 가능하다.

EPP & XTG 연동 사례 1: SSL VPN을 활용한 디바이스 제어

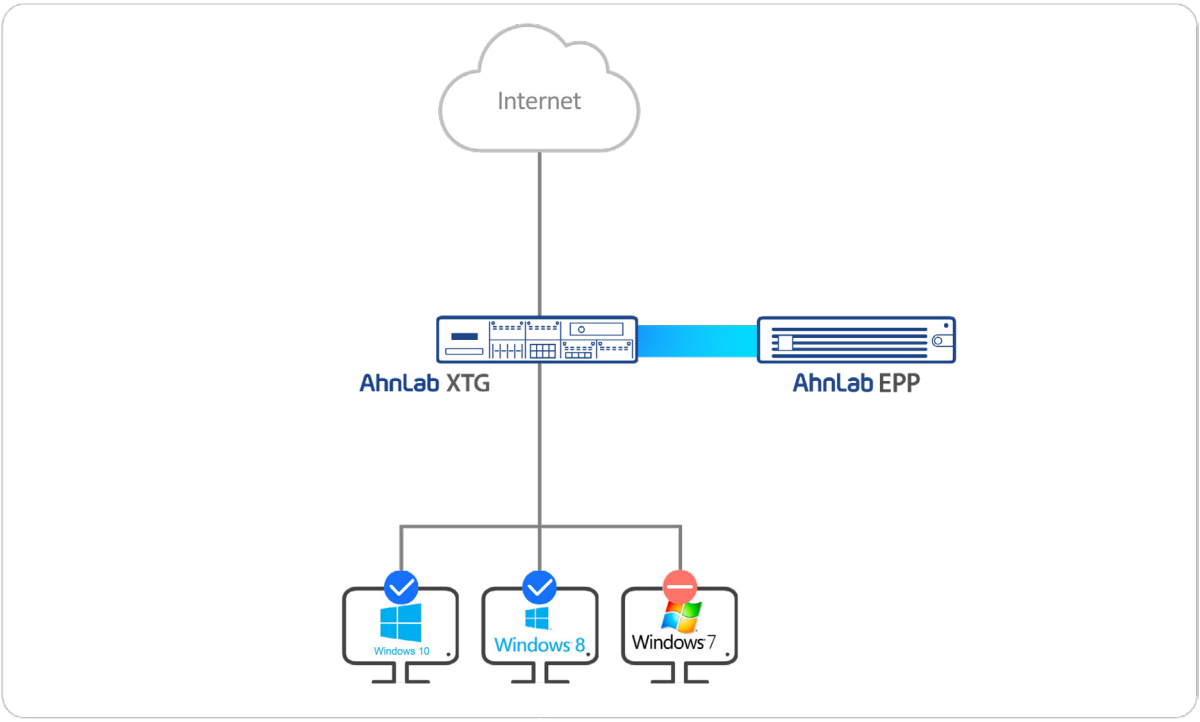
디바이스 기반 제어 연동 사례의 핵심은 EPP 서버에서 에이전트가 설치된 사내망 PC를 관리하고, XTG가 EPP 서버로부터 PC들에 대한 다양한 정보 수집하여 관리자가 설정한 디바이스 제어 기준에 따라 트래픽 허용/차단 등 다양한 방화벽 기능을 적용하는 것이다. 이 때, XTG의 에이전트는 별도로 설치할 필요가 없어(Agentless) 사용자 입장에서 보다 효율적으로 엔드포인트 - 네트워크 연계 보안을 운영할 수 있다.

EPP와 XTG의 디바이스 기반 제어 운영 사례는 크게 ▲OS 버전 기준 제어 ▲V3 설치 여부 기준 제어가 있다.

1. OS 버전 기준 제어

기업에서 아직까지 Windows 7을 사용하는 단말이 있다고 가정해보자. Windows 7은 마이크로소프트(Microsoft)에서 지원을 종료한 버전으로 보안 이슈가 발생했을 때 패치가 어렵다. 이제 대부분 Windows 10 혹은 11 이전이 완료되었지만, 부득이한 사정으로 혹은 파악이 되지 않은 채로 Windows 7을 계속 사용하는 경우도 있다.

먼저, EPP에서 Windows 7을 사용 중인 단말을 확인하면 XTG 연동을 통해 Windows 7을 사용하는 PC에 대하여 내부 네트워크 접근은 허용하되 인터넷 접속을 차단하고 안티스팸 기능을 적용한다. 그리고, Windows 10 미만 버전을 사용하는 PC는 유해사이트와 C&C 연결을 차단할 수 있다. 만약 Windows 8이나 8.1을 사용하는 PC가 있다면 SSL Proxy(프록시)와 DLP 기능을 적용하는 것도 가능하다.



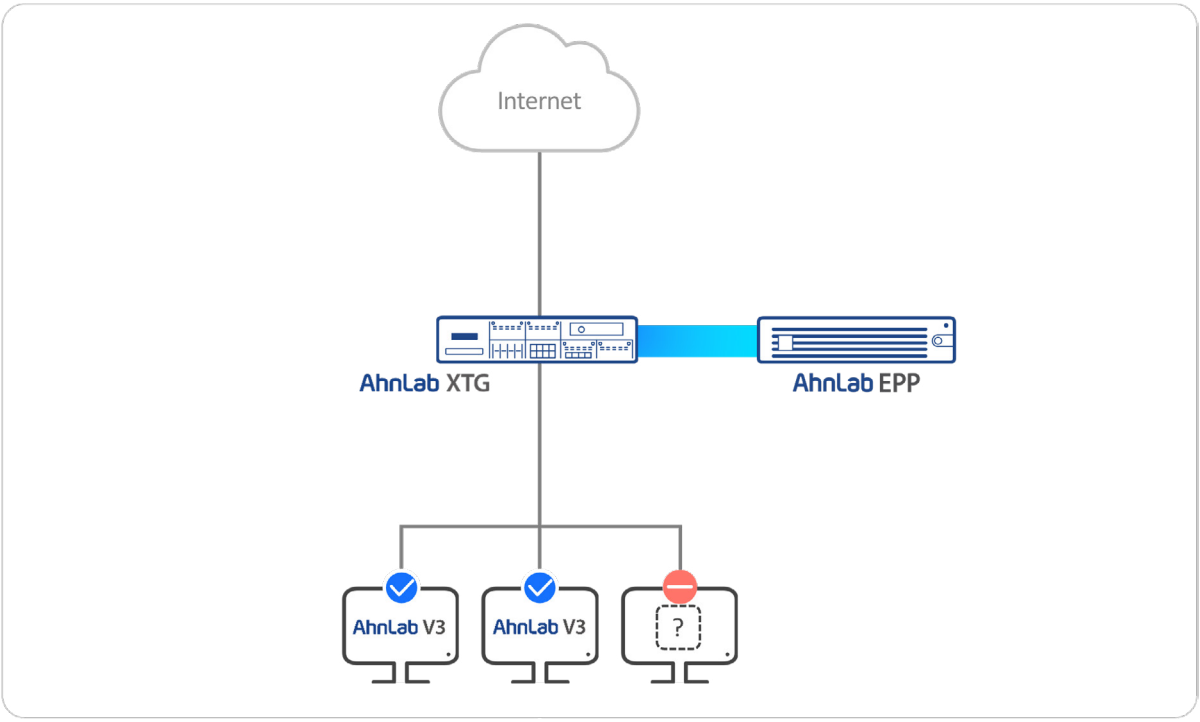
[그림 2] OS 버전 기준 제어

이 밖에, Windows 7을 사용하는 PC는 카카오톡의 메신저 기능만 허용하고 파일 업/다운로드는 차단하거나, Windows 10 미만 버전에 대해 원격 접속을 방지하고 Windows 8 PC의 경우 대역폭을 1Mbps, 세션 수를 1만개로 제한하는 것도 가능하다. 이처럼, 엔드포인트에서 확인된 OS 관련 보안 정보를 XTG의 애플리케이션 및 디바이스 제어 기능과 연동하여 탁월한 보안 효과를 누릴 수 있다.

2. V3 설치 여부 기준 제어

V3 설치 여부를 기준으로 단말을 제어하는 것은 본 운영 사례의 가장 기본이라 할 수 있다. 기업에서 보안 담당자가 관리하는 임직원의 PC가 다수가 아니라면 수동으로도 관리가 가능하다. 하지만, 그 수가 천 단위 혹은 만 단위가 되면 기본적인 백신 프로그램이 설치되지 않은 PC들이 종종 발견된다.

EPP는 정책 적용을 통해 V3 설치를 강제할 수 있다. 하지만, 해당 정책이 적용되어 있지 않은 경우에 여러가지 이유로 백신이 설치되지 않은 PC가 존재한다. 이 때 V3 설치 여부를 파악하고 설치되어 있지 않은 단말에 대해서는 XTG와 연동해 네트워크 차단 혹은 부분적 허용 등을 적용할 수 있다.

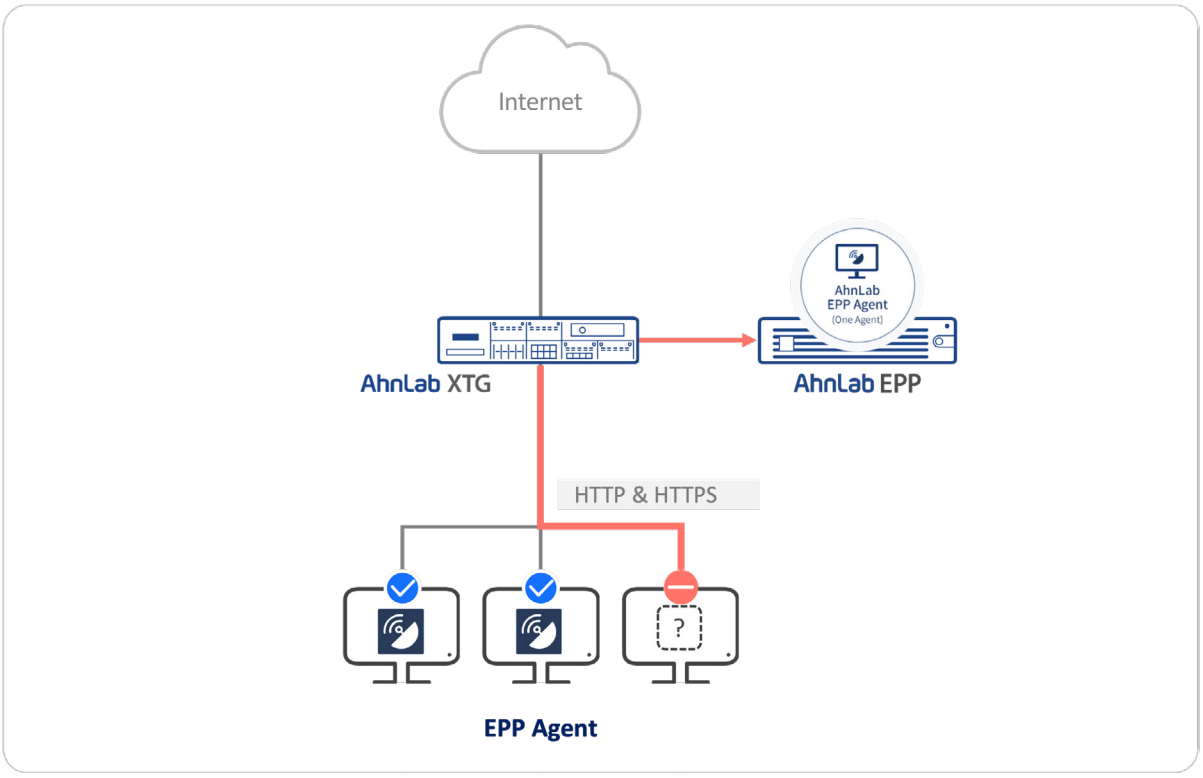


[그림 3] V3 설치 여부 기준 제어

세부적인 적용 방안은 위 두 가지 사례와 유사하다. V3 설치 PC에 대해서만 특정 외부 사이트로의 접근을 허용할 수 있고, 메신저 서비스의 경우에도 V3 미설치 PC는 접근을 차단하고 설치 PC는 카카오톡 파일 업/다운로드를 허용할 수 있다. 또, V3 미설치 PC는 침입방지시스템(IPS), 웹필터, 안티스팸, 유해사이트 차단 등 보안 위협 대응 기능을 모두 적용하는 등 V3 설치 여부에 따라 다양한 정책 적용이 가능하다.

EPP & XTG 연동사례 2: EPP 에이전트 리다이렉트

EPP 에이전트 리다이렉트 기능은 EPP 에이전트가 설치되지 않은 PC가 인터넷 통신을 할 경우, 에이전트 설치를 유도하여 보안성을 확보할 수 있도록 한다. 동작 원리를 살펴보면, EPP 에이전트 미설치 PC가 인터넷 통신을 시도하면 XTG에서 해당 트래픽을 EPP 서버로 리다이렉트하고, EPP 서버에서 에이전트 설치 유도 페이지를 안내한다. 이후, EPP 에이전트가 설치된 PC만 네트워크를 사용하도록 할 수 있다.



[그림 4] EPP 에이전트 리다이렉트

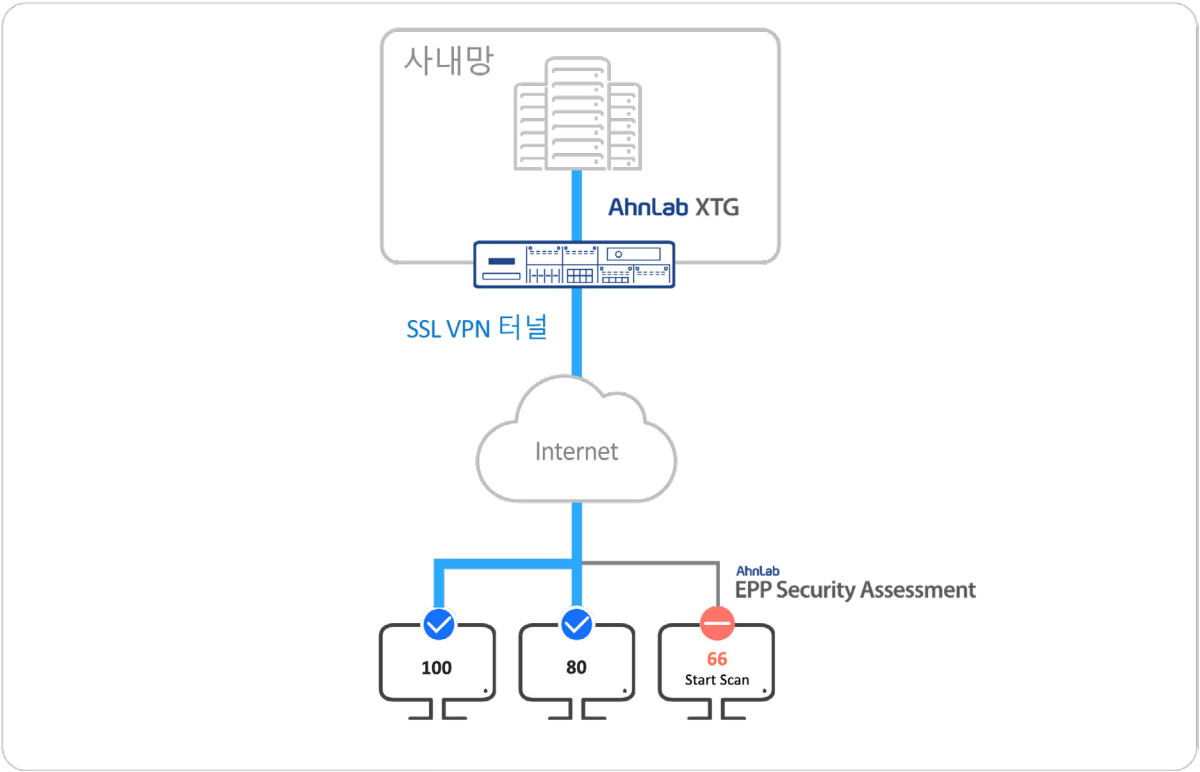
사용자 입장에서 보면, EPP 신규 도입을 계획하거나 사용 중인 상황에서 HTTPS 웹 접속에 대해서도 EPP 에이전트 리다이렉트 기능을 원하는 경우 효과적이다. XTG는 HTTP와 HTTPS 모두에 대해 해당 기능을 제공하기 때문이다. 또, 네트워크가 NAT(Network Address Translation) 환경이라 EPP 에이전트 리다이렉트가 불가능한 경우에도, XTG를 NAT 장비로 사용하면 문제가 해결된다.

EPP & XTG 연동사례 3: ZTNA – ESA 연동

최근, 지사-본사, 협력사-본사, 원격 근무 등 조직의 연결 지점이 늘어나고 있다. 조직들은 다양한 연결 사례를 지원하는 보안 체계 수립이 필요해졌고 실제 많은 기업들이 고민하고 있는 부분이기도 하다.

AhnLab XTG는 안전한 사내망 접속을 위해 ZTNA를 적용한다. 다만, ZTNA를 활용하더라도 외부 단말이 악성코드에 감염되거나 해커에 의해 장악되어 있다면 문제가 될 수 있다. 따라서, 내부 시스템에 접근하는 원격 단말 자체의 보안을 점검하는 것도 굉장히 중요하다.

안랩은 EPP 구성 솔루션인 ESA와 XTG의 ZTNA를 연동하여 안전한 단말에 대해서만 원격 접속을 허용하도록 한다. 동작 원리를 간단히 살펴보면, XTG의 ZTNA 클라이언트가 단말의 보안 점검 점수를 확인하여, 관리자가 설정한 점수를 충족할 경우에만 ZTNA 로그인이 가능하도록 제어한다. 이를테면, 보안 점검 점수 90점을 넘는 경우에만 접속이 가능하도록 하는 정책을 적용하는 것이다. 또, ESA 점검 점수를 분 단위로 판단하여 실시간성까지 보장한다.



[그림 5] ZTNA – ESA 연동

고객 입장에서는 '안전한 단말과 제로 트러스트 접근'을 결합해 안정적인 비즈니스 환경을 조성할 수 있게 된다. 재택 근무자 혹은 외부 협력사의 사내망 접속 단말에 대한 보안 적용과 관리가 불가능할 때, 혹은 다른 여러 원격 접속 상황에서 최소한의 단말 보안에 대한 점검 후 사내망 접속을 허용하고자 하는 경우 효과를 볼 수 있다.

결론

최근의 보안 지형은 ▲위협 고도화 ▲보안 복잡성 심화 두 가지로 요약할 수 있다. 풀어보면, 공격 방식이 고도화되는 가운데 기업들은 많은 솔루션들을 도입하고 또 많은 것들을 분석해야 하는 보안 복잡성을 마주하고 있다는 뜻이다.

이 두 가지 도전과제를 효과적으로 해결할 수 있는 전략이 바로 통합 보안이다. 이번 글에서 살펴본 엔드포인트 – 네트워크 연계 보안 운영 사례와 같이 조직들이 통합 보안 전략을 올바르게 적용한다면 보다 강력하면서도 효율적인 제로 트러스트 보안 체계를 구축해 안정적인 비즈니스 환경을 조성할 수 있다.

올바른 제로 트러스트 보안 전략을 고심하고 있는 많은 기업들이 통합 기반 보안 체계를 구축하여 장기적인 비즈니스 경쟁력을 제고해 나가길 바란다.

- AhnLab XTG 제품정보페이지 바로가기
- AhnLab EPP 제품정보페이지 바로가기

AhnLab

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901