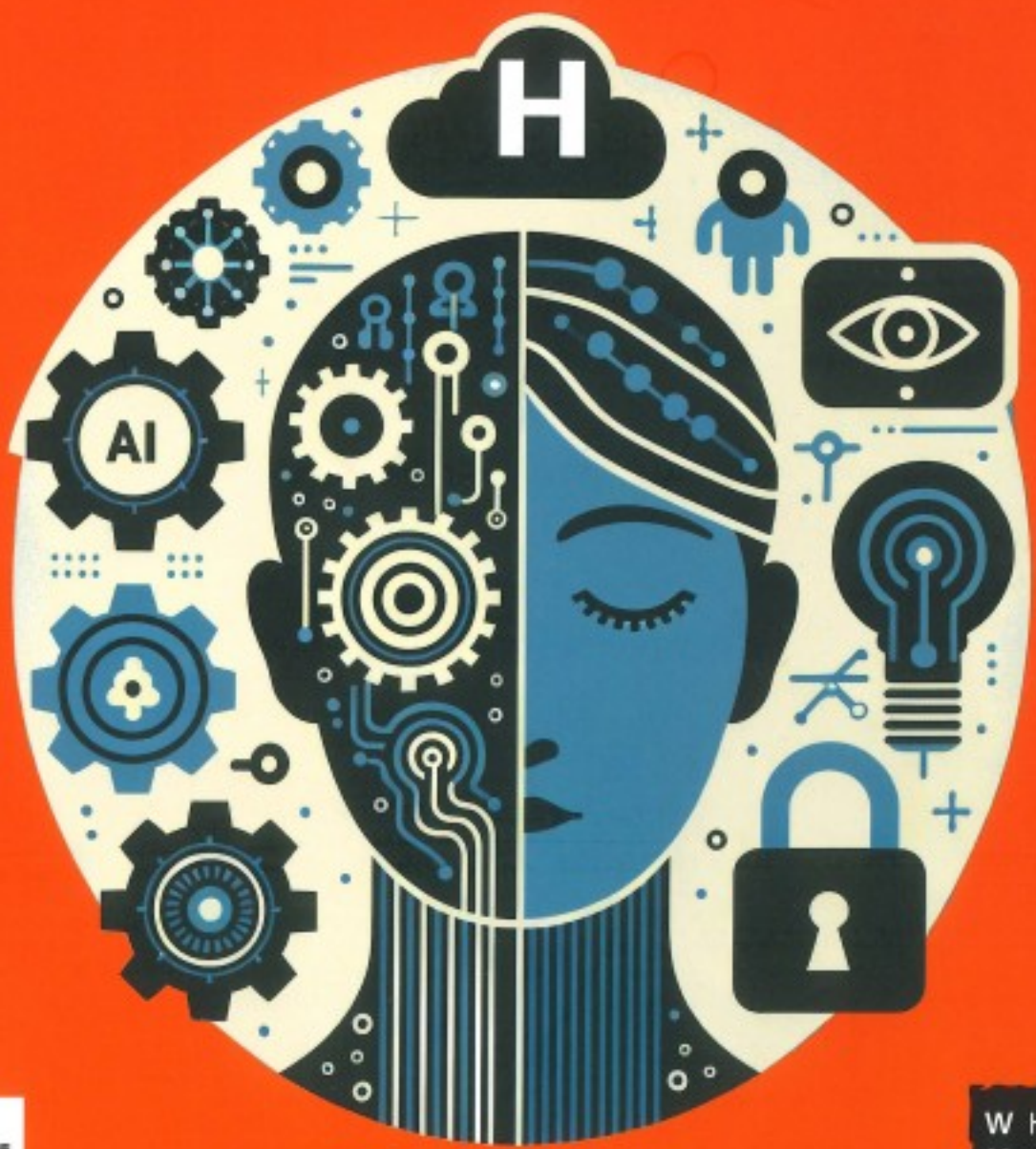
제로 트러스트
핵심 철학

사람 중심 보안

SECURITY GUIDE 2024 vol. 19



ISBN 979-11-88051-08-3

WHASAN MEDIA

네트워크 보안, 방화벽 정책관리

안전한 제로 트러스트 위해 차세대 네트워크 보안 필수

제로 트러스트를 강조하다보면 물리적 보안 경계를 지키는 네트워크 보안 솔루션은 필요 없는 것처럼 여겨진다.

이는 제로 트러스트에 대한 매우 심각한 오해 중 하나로, 제로 트러스트 원칙에서도 네트워크 보안은 필요하다. 사용자와 기기를 검증한 후 안전하게 연결하는 통신보안이 필요하며, 업무가 수행되는 중 허가받지 않은 외부 침입을 차단하는 기본 기능을 네트워크 보안에서 수행해야 하기 때문이다.

클라우드로 비즈니스가 이동한다 해도 온프레미스 데이터센터가 사라지는 것은 아니다. 클라우드 환경을 위한 네트워크 보안 솔루션이 필요하다. 클라우드 서비스 사업자(CSP)를 위한 대규모 고성능 네트워크 보안 솔루션 수요가 늘어난다. 네트워크 보안 시장은 그 어느 때보다 높은 매출 성장을 기대할 수 있다.

위협분석 전문성 탑재한 차세대 네트워크 보안

차세대 방화벽 등장 이후 방화벽, IPS, VPN을 구분하는 것이 의미 없어질 정도로 네트워크 보안 제품이 단일 플랫폼으로 통합되고 있다.

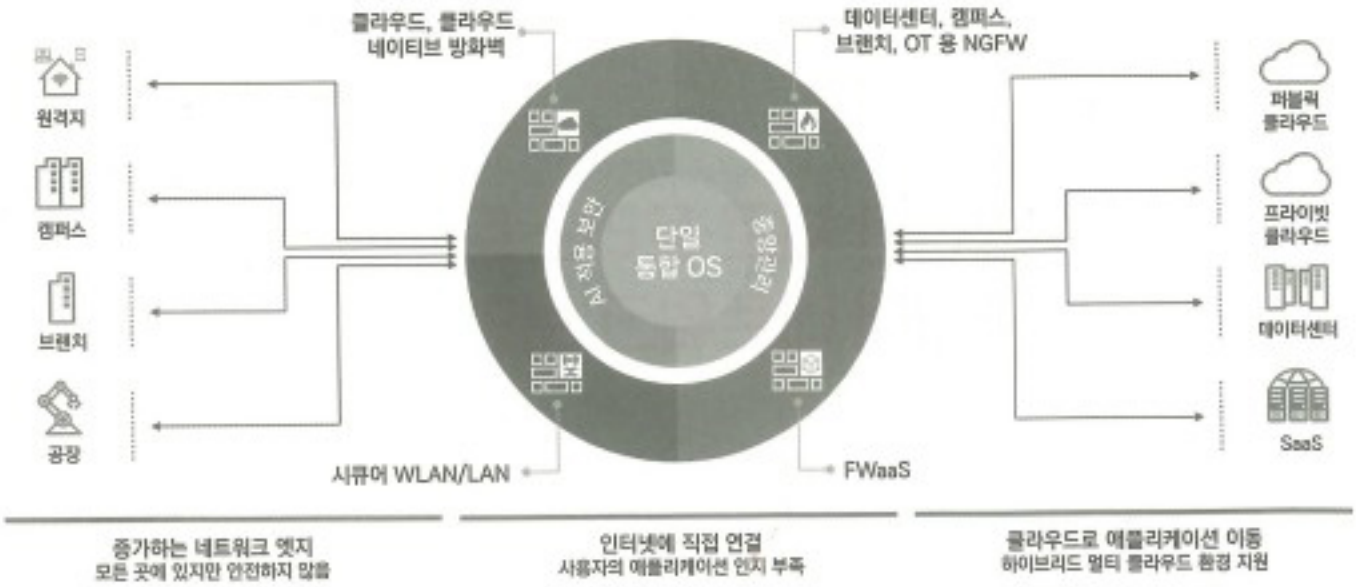
통합의 중심이 되는 차세대 방화벽은 ID 인지, 애플리케이션 제어 기능을 기본으로 탑재하며, IPS, VPN, 안티바이러스, URL 필터링 등 다양한 기능을 단일 어플라이언스에 통합해 네트워크 관문의 역할을 한다.

안랩은 네트워크 보안 시장 변화에 맞춘 완성도 높은 네트워크 보안 포트폴리오를 갖추고 있으며, 위협분석 조직과 인프라를 기반으로 국내 최적화된 위협 대응 능력을 지원한다.

자체 개발한 '어드밴스드 A 팀(Advanced A-TEAM)' 아키텍처를 채택해 패킷 처리 성능을 극대화했다. 이전 제품의 패킷 처리 속도 대비 몇 배 이상의 처리 속도를 보장하며, 멀티 코어 최적 활용 기술과 소프트웨어 가속 처리 기술을 지원한다.

차세대 방화벽 '트러스가드(TrusGuard)'는 안랩 엔드포인트 보안 솔루션과 연동해 엔드포인트부터 네트워크까지 중단 없는 보안을 제공한다. 원격접속 사용자 보안을 위해 SSL VPN 접속 시 보안 점검 검수를 수행하고 디바이스 상태를 확인한 후 접속을

〈그림 1〉 하이브리드 메시 방화벽 개념



(자료: 포티넷)

허용한다.

IPS 솔루션 '안랩 AIPS'는 알려진 공격뿐 아니라 다양한 취약점 공격까지 대응할 수 있는 진화한 보안 기능을 제공한다. 국내 네트워크에 최적화된 안랩의 6000여개 네트워크 공격 대응 시그니처를 제공하며, 암호화 트래픽의 가시성을 제공한다.

고성능 보장하는 네트워크 보안

국내 네트워크 보안 시장의 강자인 시큐아이는 클라우드, OT 환경에도 최적화된 솔루션과 서비스를 제공하면서 경쟁력을 입증하고 있다.

차세대 방화벽 '블루맥스 NGF(BLUEMAX NGF)', IPS '블루맥스 IPS', 무선 침입방지 시스템 '블루맥스 WIPS', 통합관리 시스템 '블루맥스 TAMS', 디도스 방어 '시큐아이 MFD', 네트워크 취약점 방어 '스캔 용 블루맥스 클라이언트' 등으로 구성된 네트워크 보안 포트폴리오를 갖고 있다.

클라우드 환경을 위한 차세대 방화벽 '블루맥스 NGF VE'도 지원해 다양한 가상화 클라우드 플랫폼 환경에서도 내외부 위협을 효과적으로 차단한다. Rest API 연동으로 보안 오케스트레이션을 지원해 보안조직의 탐지·대응을 효율화한다.

'블루맥스 NGF'는 PQC 알고리즘, 머신러닝이 추가돼 차세대 보안 요구에 최적의 대안을 제시한다. 더불어 SD-WAN 기능도 탑재해 시큐어 액세스 서비스 엣지(SASE) 플랫폼으로 진화하기 위한 기반을 마련했다. 더불어 통합 보안 플랫폼 '에스스퀘어오픈(S2OPEN)'과 연계해 클라우드 보안과 매니지드 서비스까지 지원하고 있다.

뛰어난 성능의 차세대 방화벽으로 인정받는 엑스게이트(AXGATE)의 차세대 방화벽은 논리적 가상화 기술을 적용해 방화벽 한 대로 여러 대의 방화벽과 VPN을 사용하는 것과 같은 독립적인 보안 서비스를 제공한다.

저가의 인터넷 회선을 묶어 고대역폭 VPN 채널을 제공하는 '디큐브 본딩(dCube Bonding)' 기술로

비용 효율적인 고성능 보안을 보장한다.

지능적인 로드밸런싱 기술을 적용해 네트워크 성능을 극대화하며, 멀티코어에 최적화된 설계로 안정적인 성능을 구현하며, 존 기반 정책으로 보안 정책 효율성을 높인다.

가상머신의 엑스게이트 OS를 포팅해 클라우드 망 내에서도 차세대 방화벽 기능을 이용할 수 있게 한다

글로벌 서비스 사업자부터 SOHO까지 지원

국내 네트워크 보안 시장에서 포티넷이 1, 2위를 다투는 강력한 경쟁력을 보이고 있다. 비용 효율적이고 관리가 편하며 다른 솔루션과 통합이 유연한 포티넷 차세대 방화벽 '포티게이트(FortiGate)'는 소규모 사무소부터 글로벌 서비스 사업자, 운영기술(OT) 환경까지 지원하는 다양한 제품군을 갖추고 있다.

포티게이트는 맞춤형 ASIC 아키텍처를 통해 업계 최고의 성능과 안정성, 트래픽 복호화 기능을 제공한다. 경쟁사 동급 방화벽보다 36배 우수한 성능, 사이버 레이팅 평가 보안 효율성 99.88% 획득 등의 검증된 기술을 기록하고 있다.

포티게이트는 포티매니저(FortiManager)를 통해 하이브리드 메시 방화벽을 구성할 수 있다. 포티매니저는 포티게이트, 시큐어 SD-WAN, 시큐어 WLAN/LAN, 유니버설 ZTNA 등 엔터프라이즈 네트워크를 모두 포괄하는 포티넷의 중앙 집중식 관리 솔루션이다.

단일 벤더 SASE 솔루션 '포티SASE'와 통합돼 하이브리드 네트워크 전반에서 일관된 보안, 관리, 분석을 제공한다.

'차세대 방화벽'이라는 용어를 처음 만들고 시장을 개척해 온 팔로알토 네트웍스는 방화벽에 인라인 머신러닝 기능을 탑재해 지능형 우회 공격까지 효과적으로 차단한다. 시그니처에 없는 공격도 10초 이내에 시그니처로 만들어 배포함으로써 실시간에 가까운 선제방어가 가능하다.

고성능 어플라이언스 'PA 시리즈'부터 클라우드 NGFW, 클라우드·가상환경을 위한 'VM 시리즈', 클라우드 네이티브를 위한 'CN 시리즈'까지 다양한 포트폴리오를 갖추고 있다.

이를 통해 엔터프라이즈 네트워크는 물론이고 클라우드, IoT, 커넥티드 디바이스 전반에서 머신러닝 기반 가시성을 보장하며, AIOps를 구현할 수 있게 하고 높은 ROI를 실현한다.

방화벽의 대명사라고 할 수 있는 체크포인트는 방화벽 성능을 선형적으로 높이는 '퀀텀(Quantum)' 솔루션으로 투자를 보호하면서 고성능 보안 요구에 대응할 수 있게 한다. 퀀텀은 사용자, 클라우드 앱, 클라우드 자산, 데이터, 게이트웨이, 퍼블릭·프라이빗 클라우드까지 통합 관리해 보안운영센터(SOC) 업무를 줄인다.

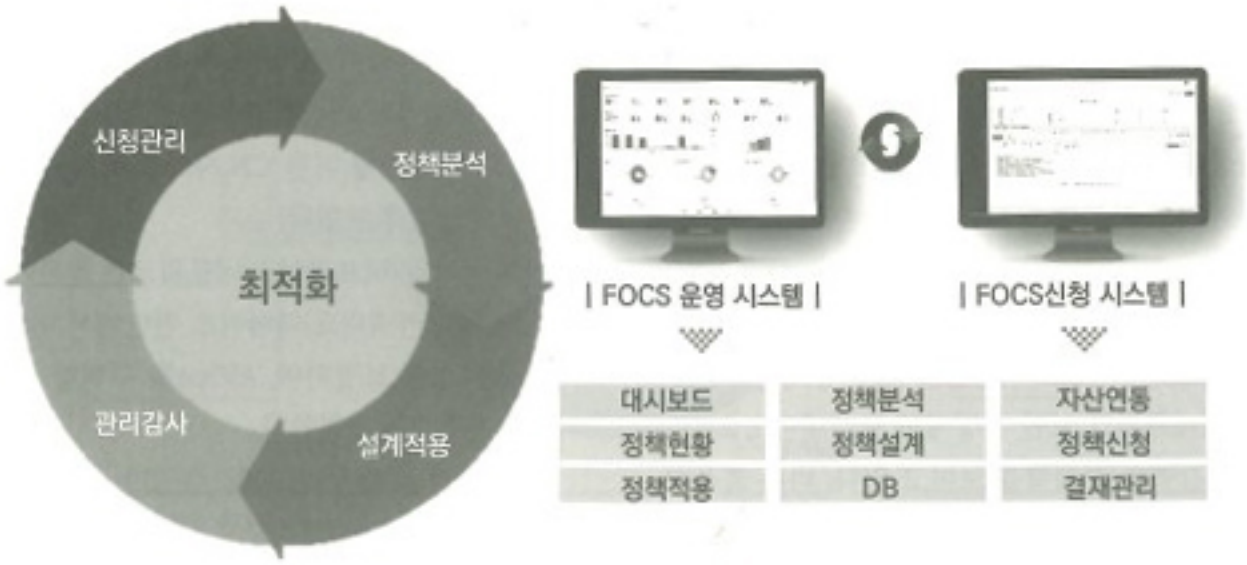
글로벌 위협 인텔리전스와 뛰어난 샌드박스 기능으로 위협의 선제방어부터 감염 후 피해 확산까지 막을 수 있다. 제로데이 공격 방어를 위해 콘텐츠 무해화(CDR) 기능을 적용, 악성코드 없는 안전한 파일만 사용자에게 전달한다.

자동화된 방화벽 정책관리 필수

방화벽의 활용도가 무한 확장되면서 방화벽 관리 문제가 크게 불거지게 됐다. 특히 방화벽 정책 문제로 비즈니스가 중단되는 사고까지 발생하면서 방화벽 정책관리 자동화 솔루션이 필수가 됐다.

방화벽 정책관리 솔루션은 다양한 이종 방화벽을 연동해야 하는데, 비표준 기반으로 설계된 오래된 방화벽이나 일부 국산 방화벽은 연동이 쉽지 않다. 그래서 방화벽 정책관리 솔루션 시장에서는 토종 솔루션이 점유율을 높이고 있다.

<그림 2> 벨로크 FOCS 정책 최적화 프로세스



유넷시스템즈가 제공하는 '에니몬에프엠(AnymonFM)'은 특허받은 정책분석 기술 '피밸리데이터(Pvaildator)' 검증모듈을 사용해 방화벽 정책 이관 시에도 중단이나 장애 없이 최적화된 정책을 유지할 수 있게 한다.

방화벽 추가 혹은 업그레이드 시 정책 이관이 자유롭지 않아 비즈니스 중단 우려로부터 자유롭지 못했는데, 에니몬에프엠의 피밸리데이터를 이용하면 원본과 이관된 방화벽의 정책과 객체 정보를 비교하고 안전하게 운영할 수 있다. 더불어 AI를 적용해 중복정책을 최적화한다.

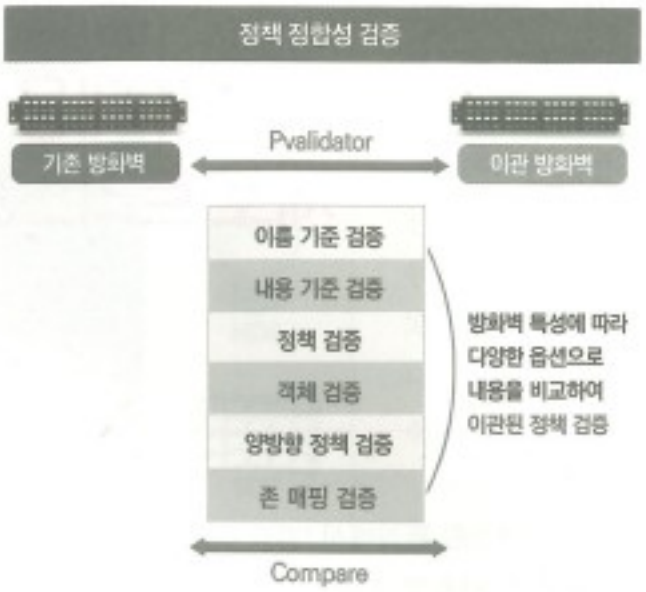
벨로크의 '팍스(FOCS)'는 금융·공공기관 등에 공급되면서 기술력과 안정성을 인정받고 있다. 팍스는 보안관리 동향을 고려해 고객이 필요로 하는 방화벽 정책을 통합 관리한다. 방화벽 관리자 업무 부담을 줄이면서 대규모 방화벽을 효율적으로 관리할 수 있게 한다.

에스에스앤씨가 국내에 공급하는 'FPMS'는 국내 여러 글로벌 제조사에서 안정적으로 운영하고 있는 솔루션으로, 방화벽 운영 효율성을 높인다. 방화벽 정책에서 컴플라이언스 등을 확인해 보안성을 강화하며, 퍼블릭 클라우드와 이기종 방화벽 지원 기능을 제공한다.

통합보안관리 시스템(OASIS)와 함께 사용하면 보다 원활한 정책관리가 가능하다. OASIS는 운영 중인 모든 보안 솔루션의 효율적인 보안관리, 결재를 자동화한다. 이 시스템은 향후 보안 포털의 기반이 될 수 있다.

자동화된 정책 분석·정합성 기술로 방화벽 정책 최적화

유넷시스템즈의 방화벽 정책 관리 자동화 솔루션 '애니몬에프엠(AnymonFM)'은 이기종 방화벽 정책 분석과 최적화를 통한 통합관리를 제공하며, 신규정책 입력 시에 정책결재와 푸시를 자동으로 해준다. 특허받은 정책 분석 기술을 탑재했으며, 2팩터인증(2FA) 기능을 통해 원격·재택근무 시에도 안전하게 솔루션에 접근할 수 있다.



자체 개발 정책 검증 모듈로 정책 이관·검증 최적화

방화벽 정책 관리는 네트워크 보안을 유지하고 규정을 준수하며, 효율적인 트래픽 관리를 위해 필수적인 솔루션이다. ISMS-P 인증심사 시에도 '최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립 이행하고 정책적용 현황을 관리해야 한다'라고 명시하고 있다.

방화벽 정책 관리를 제대로 하지 못하면 치명적인 보안 사고를 겪을 수 있지만, 관리자의 수작업으로는 복잡한 정책 관리를 제대로 수행하지 못한다. 방화벽 관리자는 단순 반복적인 신규 정책을 적용하는 것 만으로도 일과의 대부분을 사용하고 있으며, 정책 중복, 충돌, 만료된 정책 관리, 침해대응 등 중요한 업무에는 거의 시간을 할애하지 못한다.

최신 정책 업데이트, 새로운 방화벽 교체 등으로 인한 방화벽 정책 이관 문제도 심각하다. 방화벽 정책 이관 시 누락이나 변경 없이 방화벽 정책이 안전하게 이관됐다는 사실을 확인하기 쉽지 않다.

애니몬에프엠은 자체 개발한 정책 정합성 검증 기술 '피밸리데이터(Pvaildator)'를 이용해 원래 정책과 이관된 정책, 객체정보 비교할 수 있게 한다. 정책이나 객체 비교 시 이름 기준 또는 내용 기준으로 옵션화해 검증할 수 있으며, 인터페이스나 존의 명칭이 다를 경우에도 매핑정보를 이용해 검증할 수 있다.

유넷은 정책 정합성 검증 기능을 별도 모듈화해 공급, 활용 사례를 다양하게 만들 계획이다. 방화벽 제조사와 협력해 고객 방화벽 업그레이드와 교체 시 활용하며, 기존 솔루션 영업도 지역이나 산업군 특화 채널사 등을 활용해 마케팅을 강화할 계획이다.

정책 푸시 디바이스팩으로 활용 사례 다각화

애니몬에프엠은 기존 기술을 고도화하면서 정책 관리 업무를 개선했다. 정책신청 푸시 모듈을 방화벽 제조사와 제품별 디바이스팩 형태로 바꿔 기존 운영환경을 변경하지 않고 디바이스팩 추가 장착만으로 이기종 방화벽에 대한 추가 연동할 수 있게 했다. 또한 디바이스별로 프로세스가 동작하기 때문에 시스템 안정성 향상은 물론 부하분산, 동시 처리 성능 향상 등 솔루션의 성능을 높여 운영효율화를 기할 수 있다는 장점이 있다.

또한 AI 기술을 방화벽 정책 관리에 접목해 데이터 분석, 머신러닝 학습 기능을 활용할 수 있게 하며, 중복정책 최적화 추천 등의 기능을 이용할 수 있다.

유넷시스템즈 02-2088-3030 www.unet.kr