

# 제로 트러스트, 오해와 이해

Security Guide 2023 (v.18)

Z E R O T R U S T



WHASAN MEDIA

05

침해 시도 차단\_④ 네트워크 보안

2부

제로 트러스트 이행 방안

## 방화벽 사고 99% 관리자 실수... 자동화된 정책관리 필수

방화벽은 사전에 정의된 정책을 기반으로 트래픽을 허용 혹은 차단한다. 미리 정해진 정책에 따라 통제하기 때문에 단순하다고 생각할 수 있지만 결코 그렇지 않다. 방화벽은 네트워크 관문에 설치되기 때문에 잠깐의 장애에도 비즈니스 중단 등의 피해를 입을 수 있다. 방화벽 정책 한 줄 잘못 설정해 몇 시간 동안 서비스가 중단되는 사고가 빈번하게 일어나고 있으며, 무단으로 외부인이 침투할 수 있는 통로를 만들기도 한다.

비즈니스가 복잡해지면서 방화벽 정책 신청이 수없이 쏟아지는데 모든 신청을 다 수용할 수 없으며, 잘못된 정책 설정으로 서비스 장애가 일어날 수 있기 때문에 보안·관리조직은 직원들이 모두 퇴근한 후 티켓을 처리한다. 이중 방화벽마다 정책 설정 방법과 환경이 달라 담당자의 업무는 더 늘어나며, 너무 많은 정책 신청으로 필요 없어진 정책이나 중복된 정책, 잘못 설정된 정책을 확인하지 못한다.

이렇게 관리되지 못한 방화벽 정책은 다양한 문제를 일으킨다. 우선 현업 담당자들의 불만이 쏟아진다. 급하게 처리해야 하는 업무를 방화벽에 막혀 처리할 수 없다고 불만을 토로한다.

재택근무가 급하게 확산됐을 때 직원들에게 VPN을 배포하고 방화벽에서 설정을 변경해야 했으며, 다시 사무실로 돌아왔을 때 또다시 변경해야 한다. 이 일이 즉각

적으로 이뤄지지 않으면 운영에 큰 지장이 생긴다.

정책을 잘 살펴볼 시간이 없는 보안 담당자가 신청한 티켓을 모두 처리했을 때 과도한 허용으로 보안위협이 증가할 수 있으며, 컴플라이언스 위반으로 제재를 받을 수 있다. 신규 정책이 기존 정책과 충돌하기도 하고, 중복된 정책이 너무 많아서 방화벽 속도를 느리게 할 수 있다. 한시적으로만 허용된 정책이 제거되지 않고 남아서 보안홀이 되기도 한다.

실제로 한 금융사는 블랙IP를 잘못 입력해 서비스가 중단되기도 했으며, 후자의 한 항공사는 하루 동안 항공권 예약과 발급이 중단되는 초유의 사건을 겪기도 했다. 가트너는 방화벽 사고의 99%가 잘못된 설정, 관리자 실수로 인해 발생한다고 분석하기도 했다.

### ID 기반 정책관리로 관리자 재택근무 지원

방화벽의 종류가 늘어나면서 방화벽 정책관리는 더 심각한 문제가 되고 있다. 그래서 방화벽 정책 자동 관리 솔루션의 수요가 급증하고 있다.

방화벽 정책관리 솔루션은 정책관리에 대한 규제 준수 의무가 있는 공공·금융기관을 중심으로 시작됐으나 최근에는 클라우드 확장으로 더 복잡해지는 정책관리 문제를 해결하기 위한 엔터프라이즈의 수요도 크게 늘고 있다.

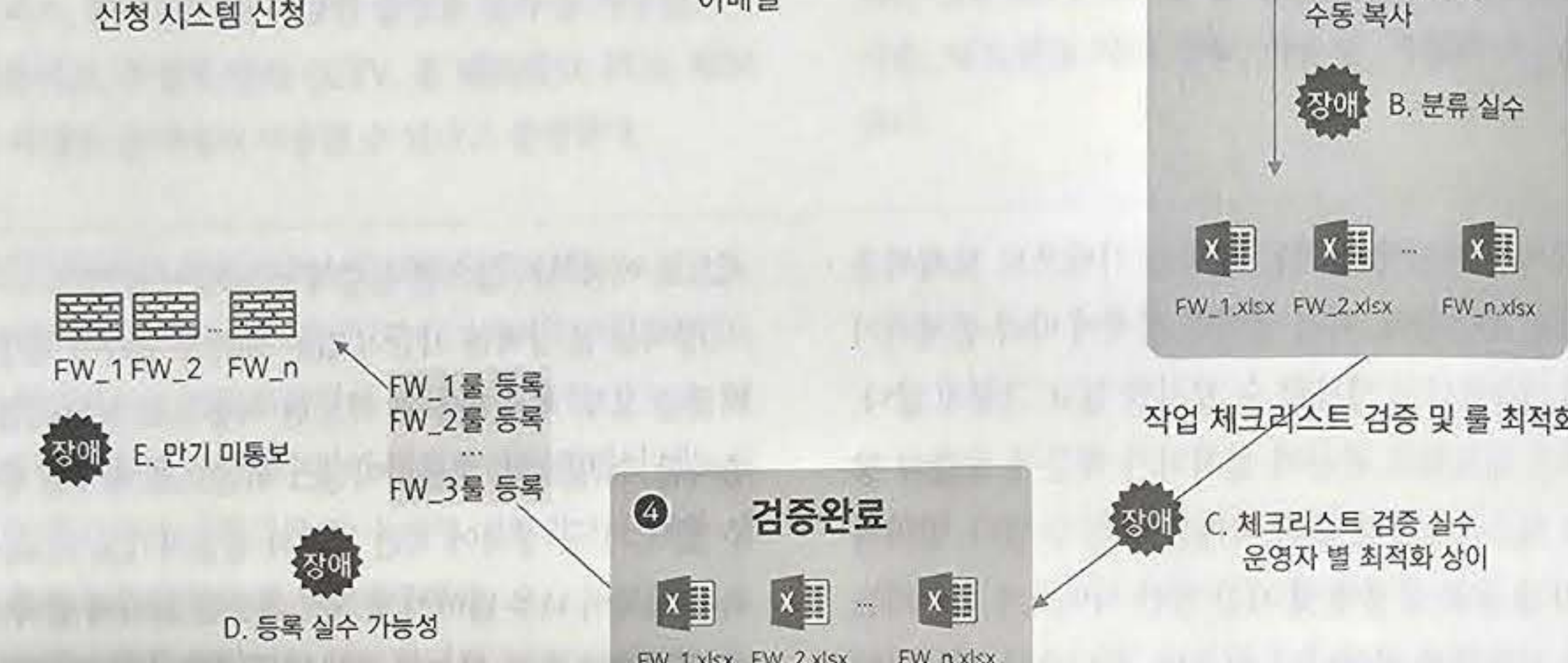
방화벽·네트워크 정책관리 201

05

침해 시도 차단\_④ 네트워크 보안

방화벽 정책 수동관리 시 발생하는 문제

방화벽 신청 시스템 → 메일 통보 → 정책 수동 처리 → 방화벽 수동 접속 및 적용



(자료: 에스에스엔씨)

에스에스엔씨는 방화벽 운영 업무를 자동화하는 'FPMS'를 공급하면서 시장의 성장을 주도하고 있다. FPMS는 방화벽 정책관리를 자동화해 실수와 장애를 없애고 현업의 업무 지연을 막는다.

FPMS는 이미 설정된 방화벽 정책을 분석해 중복되거나 충돌되는지 확인하고 불필요하거나 장애를 일으킬 정책을 제거한다. 티켓이 생성되면 기존 정책과 중복·충돌 여부를 확인한 후 사전에 설계된 보안 기준에 따라 정책 허용 여부를 결정한다.

신청하는 방화벽 정책에 대한 최적화 알고리즘에 따라 최적화하며, 신청 정보와 방화벽 정책이 일치하는지 여부를 분석한다. 모든 과정은 자동으로 이뤄지며, API를 자동으로 적용해 이기종 방화벽, 클라우드에도 원활

하게 적용 가능하다.

ID 기반 정책관리를 지원해 사무실-집을 오가면서 업무하는 하이브리드 환경에서도 정책 변경 없이 업무할 수 있게 하며, 지점으로 신규 인력이 전입할 때 사용하는 목적지 그룹으로 신청할 수 있어 조직변경으로 인한 인력 변동에도 방화벽 정책 변경 업무를 크게 줄일 수 있다.

FPMS는 타사 대비 방화벽 업무 자동화 BMT 평가점수가 월등히 높으며, 특히 하이브리드 업무 환경에서는 4배 가까이 높은 점수를 받았다.

삼성에 공급된 FPMS는 800대의 방화벽, 12만건의 신청서를 단 5시간 만에 처리했다. 국내의 11개 데이터 센터의 클라우드 방화벽에도 적용해 정책 자동화 관리

202 SECURITY GUIDE 2023 v.18

2부

제로 트러스트 이행 방안

를 지원했다.

농협은행은 FPMS 도입으로 방화벽 정책 검증 시간을 88% 줄이고 업무량을 57% 감소시켜 보안팀의 업무를 효율화하는 성과를 거뒀다. 불필요한 정책을 제거해 방화벽 성능을 최적화해 운영 품질을 높이는 효과도 가져왔다.

### 기존 운영환경 변경 없이 이중 방화벽 연동

유넷시스템의 '애니몬에프엠(AnymonFM)'도 호평을 받으면서 점유율을 높이고 있다. 애니몬FM은 정책신청과 적용을 제조사·제품별로 모듈화 해 기존 운영환경 변경 없이 이중 방화벽 연동이 가능하게 했다. 또한 부하 분산과 동시처리 성능 향상 등 운영 효율성을 높일 수 있다. 차세대 방화벽 L7 기능을 지원하며, NAT 기능으로 고객사별 특성에 따른 방화벽 세부 관리절차, 다양한 운영환경 지원이 가능하다.

2팩트인증(2FA)을 적용해 방화벽 담당자의 재택근무 시에도 사내 방화벽에 안전하게 접근해 관리할 수 있게 했으며, 정책신청 프로세스를 개선해 사용 편의성을 높였다.

벨로크의 'FOCS(Firewall policy Orchestration Center System)'는 실제 업무환경에 최적화된 방화벽 정책 관리 자동화를 지원한다. 특히발은 대용량 시스로그 처리방범론, 트래픽 답러닝 학습 기능을 탑재해 정확한 경로 분석과 경로 설계 적용 기능을 적용했으며, 정합성 높은 분석 데이터를 기반으로 시스템 내 각 기능에 활용할 수 있게 한다.

방화벽 경유지 분석을 통한 정책의 설계 가이드를 제공해 정책의 설계, 적용, 자동적용 기능의 신뢰성을 높이고 정책관리 시 기반데이터로 활용해 정책을 최적화할 수 있게 한다.

또한 실 트래픽 수집과 학습을 통한 정확한 경유지 토폴로지 맵을 제공한다. 실 트래픽 기반 기술과 방화벽 인

터페이스(ZONE)라우팅 정보를 더해 정확한 방화벽 경유지 분석결과를 토폴로지 맵으로 구현해 방화벽 운영 현황을 시각화한다.

상세 TCP 플래그 분석 데이터를 제공, 방화벽 설비 관리뿐만 아니라 출발지에서 목적지까지 네트워크 경로상의 모든 경유지 방화벽의 상세로그를 제공해 네트워크 환경관리에도 많은 이점을 줄 수 있다.

### 네트워크 보안 정책 관리로 확장

글로벌 시장에서 방화벽 정책관리는 NSPM(Network Security Policy Manager)으로 확장되고 있다. NSPM 시장을 이끌고 있는 파이어몬은 방화벽뿐 아니라 다양한 네트워크 장비, 퍼블릭 클라우드내 VPC, VNET, SD-WAN, SASE까지 지원한다. 서비스나우, 지라 등 SaaS 형태의 ITSM과 연동해 티켓관리 자동화 효과를 더욱 높이며, 국내의 다양한 네트워크 솔루션과 연계해 네트워크 전반의 운영 효율성을 높인다.

방화벽 정책관리 솔루션은 최초 도입 시 이중 방화벽과 잘 연동되다가 방화벽 버전을 몇 번 업그레이드하면 작동하지 않거나 장애가 발생하는 등의 문제가 생긴다. 벤더별, 버전별로 각각 달라지는 환경을 정책관리 솔루션 벤더 혹은 고객사 담당자가 직접 연동 문제를 해결해야 하며, 시간이 지남수록 이 문제가 점점 심각해져 정책관리 솔루션 도입 의미가 없어진다. 파이어몬은 방화벽 벤더와 긴밀히 협력하면서 업그레이드 버전도 최적화해 지원하기 때문에 운영상의 효율성을 높일 수 있다.

방화벽·네트워크 정책관리 203

방화벽 정책 관리

유넷시스템 '애니몬 FM'

## 신규 기능 확충·알고리즘 최적화로 효율성 높여

유넷시스템의 애니몬 FM은 이기종 방화벽의 정책의 분석은 물론 최적화를 통한 통합 관리를 제공하며 신규 정책 입력 시 정책결과와 무시를 자동으로 해주는 '방화벽 정책 통합 관리 자동화 솔루션'이다. 유넷시스템은 다수 고객사에서 쌓아왔던 노하우와 기술력을 결집해 지난해 솔루션 고도화에 집중, 신규 기능 대거 확충은 물론 기존 기능들도 최적화된 알고리즘을 통해 더 솔루션과 차별화를 꾀했다.

### 솔루션 고도화 통한 차별화 노력

방화벽 정책 관리 솔루션의 핵심 기능 중 하나는 '정책 신청과 적용(무시)' 부분이다. 이를 위해 유넷은 하나의 무시 모듈 형태로 돼 있던 것을 방화벽 제조사와 제품별 디바이스팩 형태로 변화시켰다. 이렇게 개선된 디바이스팩 형태의 무시 모듈을 활용하면 기존 운영 환경을 변경하지 않고 디바이스팩 추가 장착만으로 이기종 방화벽에 대한 추가 연동이 가능해진다.

또 디바이스별로 프로세스가 동작하기 때문에 시스템 안정성 향상은 물론 부하 분산, 동시 처리 성능 향상 등 솔루션 성능을 높여 운영 효율화를 기할 수 있다는 장점이 있다.

정책신청 프로세스도 개선해 사용자 편의성을 강화했다. 사용자가 직관적으로 쉽게 이해할 수 있도록 메뉴를 구성했으며, 각 프로세스별 필수 기능은 물론 고객사별로 원하는 기능을 취사선택할 수 있도록 옵션 기능을 추가로 제공한다.

방화벽 정책 관리 솔루션 사업에서 중요한 기능으로 요구되고 있는 차세대 방화벽 L7 기능과 NAT 기능도 지원해 고객사 특성에 따라 차이가 많은 방화벽의 세부 관리 절차 및 다양한 운영 상황도 문제없다.

### 재택 방화벽 정책 관리도 효율적

유넷시스템은 보안성을 대폭 강화한 2팩트 인증을 적용해 계속되는 코로나 시기에도 차별화된 기능을 제공했다. ID/PW를 이용한 1차 인증과 보안인증 토큰을 이용한 2차 인증을 추가로 진행해 방화벽 담당자가 재택근무 시에도 사내 방화벽에 안전하게 접근하고 효율적으로 정책 관리를 할 수 있다.

최근 방화벽 정책 관리 솔루션에 대한 인지도가 지속 높아지고 있지만, 고객들은 솔루션을 도입해 활용하겠다는 인식이 낮은 것이 현실이다. 그러나 방화벽 정책 최적화를 제대로 하지 못한다면 사내 보안 위협을 증가시키는 중요한 요인을 놓칠 수 있다. 대부분의 방화벽 담당자들이 신규 정책을 적용하기에도 부족한 일과를 보내고 있어 중복 정책/미사용 정책/기간 만료 정책을 삭제하지 못하고 있으며, 이처럼 관리되지 못하는 정책 누적이 보안 위협으로 이어지고 있기 때문이다.

따라서 방화벽 정책 최적화는 보안 담당자 입장에서 반드시 점검해야 하는 기본사항임은 물론 ISMS-P 인증심사 시에도 '최신 정책 업데이트, 롤백 변경, 이벤트 모니터링 등 운영 절차를 수립해 이행하고 정책 적용 현황을 관리해야 한다'고 명시해 반드시 체크하도록 하고 있다.

유넷시스템 02-2088-3030 www.unet.kr