KX 넥스지 Since 2001

NeXForce ACRON
차세대 방화벽

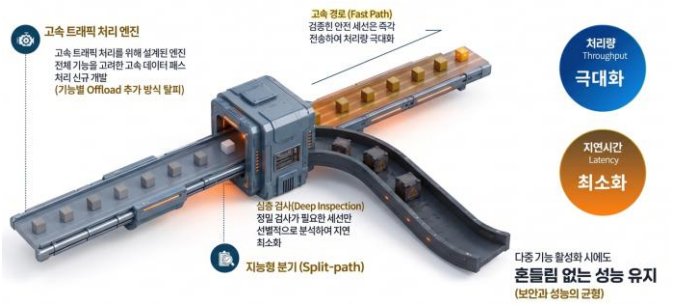
보안의 새로운 기준

- 하나의 플랫폼, 모든 보안 -

보안 최적화 OS 기반 고성능 엔진과 유연한 모듈 구조로,
현재의 안정성은 물론 AI·양자보안 등 미래 기술을
선도하는 차세대 All-in-One 플랫폼입니다.

지능형 분기(Split-path) 기술 적용

- 대규모 트래픽 환경의 고성능 트래픽 처리 기술 적용.
- 다중 보안 기능 사용 환경에도 흔들림 없는 보안과 성능 제공.

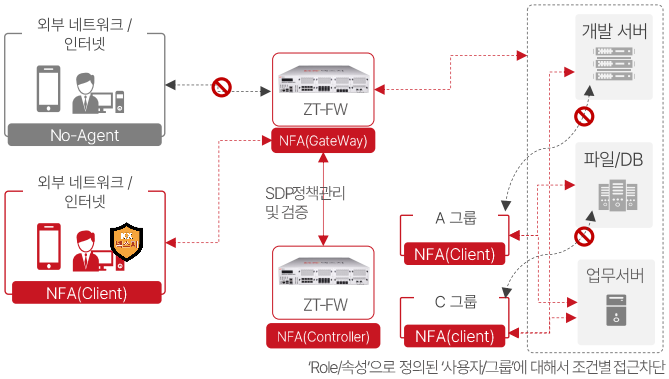


AI 보안 위협탐지

- 암호화된 트래픽의 흐름과 행위 특성 분석기술로 이상 징후 식별
- 과도한 보안 로그와 이벤트 LLM 기반 운영 자동화 제공

제로트러스트 인증(SDP)

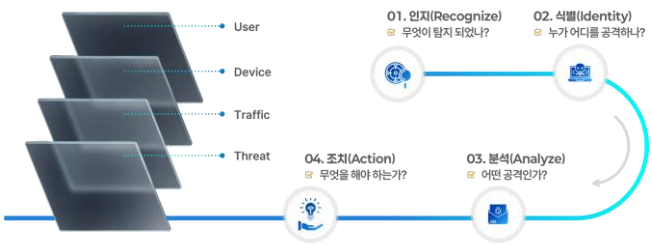
- Identity 중심의 엄격한 인증 및 조건별 접근 차단
- ZT모델 표준준수(NIST SP 800-207 등), 국가망 보안체계(N2SF) 기반의 ZT환경 제공



'Role/속성'으로 정의된 '사용자/그룹'에 대해서 조건별 접근차단

다층 분석 구조(Multi-layer Context)

- 단순한 이벤트 나열을 넘어 사용자, 디바이스, 애플리케이션, 트래픽을 관통하는 입체적 연결 관점 IntelliView 제공



Software Function

NGFW

1	사용자·디바이스·애플리케이션 기반 통합 정책 제어 (SaaS 포함)
2	다양한 사용자 인증 및 식별 (Captive Portal, AD SSO 연동)
3	애플리케이션·사용자·웹 카테고리 기반 맞춤형 QoS 제공
4	사용자 정의 애플리케이션 패턴(Custom Pattern) 지원

사용자 인증

1	AD, LDAP, RADIUS 등 다양한 외부 인증 서버 및 DBMS 연동 지원
2	IPv4/IPv6 환경을 모두 지원하는 유연한 Captive Portal 인증 정책
3	OTP 기반 다단계 인증(MFA) 프로파일 구성 및 상세한 인증 로그 모니터링

Firewall

1	IPv4/IPv6 기반 방화벽 정책, 블랙리스트 정책(예외 지원)
2	도메인(URL 객체) 및 국가(GeoIP) 기반 정밀 접근 제어
3	L2 계층 방어(MAC 필터) 및 논리적 보안 정책 그룹 설정
4	시간 및 스케줄 기반 유연한 보안 정책 관리
5	다양한 네트워크 주소 변환 (S-NAT, D-NAT, Double NAT 지원)
6	대규모 트래픽 처리를 위한 LSNAT (SNAT/DNAT 풀) 부하분산
7	정책 시뮬레이션을 통한 정책 유효성 및 안전성 검사 지원
8	미사용 객체·정책 및 중복 정책 검색 기능을 통한 정책 운영 최적화 지원
9	정책 Hit 카운트 및 세션 매칭 현황 실시간 모니터링
10	정책 설정 화면과 로그 조회/분석 원클릭 연계 기능
11	대규모 보안 정책 관리를 위한 Import/Export 기능 지원

Virtual Domain

1	다중 Virtual Domain(네임스페이스 기반 멀티테넌트아키텍처)
2	VD(가상 도메인)별 독립적인 보안 정책 수립 및 시스템 자원 할당

ZTNA / SDP

1	컨트롤러, 게이트웨이, 에이전트(Windows, Android) 통합 구성 지원
2	사용자 신원 및 단말 무결성 검증 기반의 동적 최소 권한 접근 제어
3	SPA 기반 인프라 자원 은폐(Stealth Mode) 및 동적 암호화 보안 채널 형성 지원

N2SF

1	제로 트러스트 아키텍처 기반의 완벽한 내부 논리적 망분리 구현
2	데이터 등급 분류 기반 보안 존(Zone) 구성 및 차등적 접근 통제
3	보안 존(Zone) 간 이동 트래픽 격리 및 정밀 제어 (L7 검사, 콘텐츠 통제)
4	존(Zone) 별 정책 위반 실시간 탐지·알림 및 컴플라이언스 증적 리포팅

Device 제어

1	사용자 및 단말 식별자(Device Identity) 기반 Zero Trust 접근 제어
2	단말 위험도(Risk Score) 실시간 평가 및 비인가·위협 단말 자동 차단
3	필수 보안 컴플라이언스(백신/패치/암호화 등) 검사를 통한 단말 무결성 확보
4	SSL VPN Client와의 완벽한 통합을 통한 끊김 없는 보안 환경 제공

DLP

1	파일 유형 및 세부 콘텐츠 정밀 분석을 통한 내부 중요 데이터 외부 유출 통제
2	민감한 개인정보 및 기업 핵심 키워드에 대한 정밀 패턴 탐지 및 차단

SSL Inspection

1	최신 암호화 프로토콜(TLS 1.2/1.3, HTTP/2) 및 다중 트래픽(HTTPS, SMTPS 등) 복호화
2	복호화 트래픽의 IPS, Web Filter, Anti-Virus 연동을 통한 사각지대 없는 심층 통합 검사
3	시스템 부하 방지를 위한 용량 제어(임계값 설정) 및 SNI 기반 유연한 복호화 예외 처리
4	프로파일별 다중 CA 인증서 관리 및 HTTP/2 경로(Path) 레벨의 정밀한 필터링

IPS

1	최신 위협 대응을 위한 자동화된 시그니처 DB 업데이트 및 멀티패턴 탐지 엔진
2	프로파일 기반 맞춤형 방어 및 PCRE(정규식) 활용 사용자 정의 시그니처 지원

Anti DDoS

1	L3/L4 네트워크 계층부터 L7 응용 계층(행위 기반 웹 공격, DRDoS 등)까지 전방위 방어
2	보호 대상(Domain) 단위의 세밀한 프로파일 기반 임계값(Threshold) 설정
3	실시간 공격자 탐지·차단, 패킷 덤프(Dump) 및 예외 호스트 관리 기능 제공

Anti-Virus & Anti-SPAM

1	고성능 Anti-Virus 엔진 기반의 실시간 메일 프로토콜 및 첨부파일 악성코드 검사/제거
2	실시간 블랙리스트(RBL), 스팸 점수 및 PCRE 키워드 기반 정밀 스팸 필터링 판정

Web Filter

1	방통위 유해 DB 및 글로벌 URL 평판 DB를 연동한 강력한 카테고리별 웹 필터링
2	도메인, IP 주소 및 정규식(PCRE) 패턴 기반, URL 확장 검사(쿼리 검사) 기반 차단
3	웹 보안 현황 심층 분석 및 URL 매치 시뮬레이션 제공 (맞춤형 경고 페이지 지원)

IPsec VPN

1	IKEv1/IKEv2, PKI 기반 강력한 인증 및 다양한 국내외 표준 암호화·무결성 알고리즘 지원
2	자체 커널 모듈(HW 가속) 기반의 고성능 데이터플레인 처리 및 다중 터널링(GRE, L2TP 등) 지원
3	DPD 검사, DR 연결 및 자체 회선 장애 감지를 통한 무중단 VPN Failover 및 로드밸런싱
4	다양한 네트워크 환경(L3, Bridge, Bonding 등) 완벽 지원 및 직관적인 터널 상태 모니터링

SSL VPN

1	ONE-PASS URL(QR코드) 간편 인증 및 MFA 기반(ID / PWD, 인증서, OTP) 강력한 접근 제어
2	IPv6 네트워크 완벽 지원 및 트래픽 최적화를 위한 Full/Split 터널링 제공
3	PC, 모바일, 임베디드 등 다양한 디바이스 지원 및 클라이언트 자동 업데이트
4	사용자 그룹별 세밀한 임대 IP 할당 및 맞춤형 보안 접근 권한 통제

SD-WAN

1	애플리케이션 및 정책(IPv4/IPv6) 기반의 지능형 트래픽 경로 자동 제어
2	실시간 회선 품질 모니터링을 통한 오버레이 터널 Failover 및 동적 부하분산
3	관리 편의성을 극대화한 프로파일 기반의 간편한 SD-WAN 환경 설정

양자보안

1	글로벌(NIST) 및 국내(KpqC) 표준 양자내성암호(PQC) 알고리즘 적용 VPN
2	QRNG(양자난수생성기) 연동을 통한 예측 불가능한 최고 수준의 보안 암호키 생성

네트워크

1	IPv4/IPv6 기반의 다양한 동적 라우팅 (OSPF, BGP 등) 및 멀티캐스트 지원
2	LACP(Bonding), VLAN, STP 등 안정적인 무중단 L2/L3 스위칭 환경 제공
3	DHCP/DHCPv6, DNS, DDNS 등 유연한 인프라 구성을 위한 필수 네트워크 서비스
4	IP, 애플리케이션, 인터페이스 기반의 세밀한 네트워크 대역폭 품질 보장(QoS)
5	NAT64, NAT46, 터널링(6to4) 등 이기종 망을 위한 완벽한 IPv6 트랜지션 지원

HA

1	Active-Active / Active-Standby 및 L4 Cluster 기반 무중단 세션·설정 동기화 지원
2	VIP/세션 Sync Group 단위 선택적(세분화) Failover 지원

모니터링

1	전방위 통합 모니터링 대시보드 (네트워크, VPN, 위협, 사용자 현황 등)
2	DB 기반 대용량 로그 관리 및 다층(Multi-Layer) 위협 분석
3	사용자·애플리케이션별 트래픽 및 세션 심층 분석
4	임계치 기반 실시간 경고(이메일/SMS/팝업) 및 맞춤형 보고서 제공

관리 기능

1	다단계 관리자 권한 프로파일 및 보안 인증 통제 (LDAP, OTP 등 연동)
2	무결성 검증, 펌웨어 롤백(Downgrade), 백업/복구를 통한 시스템 안정성 보장
3	Setup Wizard, GUI 패킷 캡처, 시스템 일괄 진단 등 직관적 운영 편의성
4	Open API (REST) 지원을 통한 외부 보안 솔루션과의 유연한 연동

AI 보안

1	LLM 기반 자연어 위협 분석 및 이상 징후 자동 선별을 지원하는 AI 보안 어시스턴트
2	AI 엔진 기반 암호화 트래픽 심층 분석 및 제로데이·비정상 통신(C2) 선제적 차단

Hardware Specification

사양 항목		ACRON 200	ACRON 400	ACRON 800	ACRON 1000	ACRON 2000	ACRON 4000	ACRON 5000	ACRON 6000
Core		2	2	4	4	8	8	24	32
Memory		1GB	1GB	4GB	4GB	16GB	16GB	64GB	64GB
Storage		32GB	32GB	32GB	32GB	128GB	256GB	256GB	256GB
		-	-	512GB	512GB	1TB	1TB	2TB	2TB
NIC	1GC	7(1 PoE)	16(8 switch)	6	8	8	4(max 12)	8(max 64)	8(max 64)
	1GF	-	-	-	0(max 2)	4(max 12)	4(max 12)	8(max 64)	8(max 64)
	10GF	-	-	-	0(max 2)	0(max 8)	2(max 6)	4(max 32)	4(max 32)
	40GF	-	-	-	-	-	0(max 2)	0(max 16)	0(max 16)
	100GF	-	-	-	-	-	-	0(max 16)	0(max 16)
Power		Single	Single	Single	Single	Redundant	Redundant	Redundant	Redundant
Throughput		2 Gbps	2.5 Gbps	6 Gbps	12 Gbps	40 Gbps	60 Gbps	180 Gbps	300 Gbps

❖ 사양과 외관은 제품 개선을 위해 변경될 수 있습니다.