aa teknoloji

Palo Alto Networks ML-Powered NGFW

Next-generation firewall driven by machine learning; analyzes all traffic using App-ID, User-ID, and Content-ID. Supports Zero Trust architecture by stopping zero-day threats with Advanced WildFire.

Network Security Challenges

Cyberattacks that constantly change form and unmanaged new devices added to the network expand the attack surface of organizations. Traditional security products drain operational resources by forcing manual interventions, leaving the infrastructure exposed to threats.
Attackers utilize encrypted traffic to bypass security devices. Phishing and the exploitation of stolen credentials represent the largest blind spots, making up 90% of security breaches in 2021.
The inadequacy of traditional signature and fingerprint-based systems makes it impossible to detect unknown threats and SaaS applications.

⚠ Who can benefit?

- Teams unable to see threats within encrypted traffic (TLS 1.3 and HTTPS/2)
- Those seeking protection against identity theft and evasive phishing attacks
- Those looking to prevent unauthorized SaaS applications (Shadow IT) and data leaks
- Those aiming to detect and secure unmanaged IoT devices across the network

Core Principles

Zero Trust
Full verification independent of location

Visibility
Application, content, and identity detection

SaaS Control
Data protection with next-generation CASB

Prevention
ML-powered zero-day prevention

Technical Specifications

Traffic and Identity Control
- Full application-based visibility with App-ID
- Compatibility with User-ID and Cloud Identity Engine
- Automation with Dynamic User Groups (DUG)
- Decryption for TLS 1.3 and HTTPS/2

Advanced Threat Prevention
- Zero-day analysis with Advanced WildFire
- Advanced URL Filtering and Web Protection
- Machine learning-powered inline IPS
- C2 traffic blocking with DNS Security

SaaS and Cloud Security
- SaaS application management with Next-Gen CASB
- Real-time SaaS data protection
- Prisma Access SASE integration
- Hardware, VM, and Container form factors

Centralized Management and Visibility
- Device management from a single screen with Panorama
- NIST-compliant protection with Enterprise IoT
- Centralized logging via Cortex Data Lake
- 3rd party automation with extensive API support

How Does NGFW Work?

The ML-Powered Next-Generation Firewall inspects traffic via App-ID, User-ID, and Content-ID instead of ports. It blocks zero-day threats in a single pass with its single-pass architecture and confidently enforces Zero Trust policies.

Workflow

1. Traffic Classification
- App-ID directly detects all applications.
- User-ID maps users with network traffic.
- SSL/TLS traffic is decrypted when necessary.
- All IoT devices are identified without signatures.

→

2. Content and Threat Analysis
- Unknown files are forwarded to WildFire for analysis.
- Malicious software is instantly blocked with Inline ML.
- Complex DNS attacks are blocked with DNS Security.
- URL Filtering identifies evasive phishing sites.

→

3. Decision and Optimization
- Zero Trust-based security policies are executed.
- Processing is done without latency via Single-Pass architecture.
- Risky SaaS applications are blocked with Next-Gen CASB.
- Cortex Data Lake performs log correlation.

Centralized Management & Global Intelligence

The Panorama management infrastructure unifies policies across all branches, data centers, and cloud devices. With Shared Threat Intelligence, the protective shield of a newly detected threat is distributed to the entire global ecosystem within seconds.

Advantages

Single-Pass Architecture
Abandons traditional layered analysis. Provides predictable performance by performing application, user, and content analysis in a single pass.

Comprehensive IoT Security
Detects all unmanaged IoT devices on the network using ML. Strengthens Zero Trust architecture with context-aware segmentation.

Next-Generation CASB
Grants access to corporate SaaS accounts while blocking risky applications (Shadow IT) with real-time data protection.

Zero Trust Enforcement
Verifies users across every location with the Cloud Identity Engine. Mitigates risks through application and identity-based restrictions.

aa teknoloji

AA Teknoloji is an AI-powered media technologies platform developed for modern newsrooms. Our integrated solutions, ranging from news workflow systems to digital archive solutions, real-time broadcasting infrastructure to multi-channel content management, accelerate the digital transformation processes of media organizations and offer scalable broadcasting operations.

For more information, visit aateknoloji.tr or follow the @aateknoloji LinkedIn account.