Get Smart with AIOps for Next-Generation Firewalls

A guide to strengthening security and avoiding network disruptions with machine learning-driven insights

paloalto® NETWORKS | STRATA BY PALO ALTO NETWORKS

SITC SECUREIT CONSULT

Table of Contents

Network Security Operations at the Crossroads 3

What Happened to the "R" In ROI? 3

Security Gaps 3

Business Disruptions 3

Planning Uncertainty 4

What Is AIOps for NGFW? 4

Continuous Detection Enables Proactive Network Operations 5

Alerts Help Network Teams Proactively Remediate Issues 6

Scenario 1: Firewall Misconfigurations Create Vulnerabilities 7

Scenario 2: Overloaded Firewalls Cause Network Disruptions 8

Scenario 3: Stolen Credentials Can Lead to Data Exfiltration 9

AIOps for NGFW Delivers Business Value 10

Strengthen Security Posture 10

Avoid Business Disruptions 10

Plan with Confidence 10

How We Can Help 11

Network Security Operations at the Crossroads

Network security operations today are under intense scrutiny by IT leaders and corporate executives. Organizations are investing heavily in highly sophisticated tools such as next-generation firewalls (NGFWs) to protect their critical information and keep their operations running smoothly. Often, those investments aren't paying off as well as they should—and executives are asking why.

For one thing, today's hybrid network architectures are complex, with applications and data spread across multiple public and private clouds and users dispersed to remote locations such as branches and home offices. As a result, the security perimeter has effectively disappeared, requiring network architects to embed security throughout the network using multiple firewalls and Zero Trust principles. Security teams struggle to optimize these complex and dynamic architectures, which can degrade the organization's security posture and cause network slowdowns and even outages.

One critical weakness of existing solutions is that they can't provide the insights that security teams need to respond proactively. As a result, they're always playing catch up, reacting to the latest unknown threat, phishing technique, or exfiltration exploit. When the inevitable network outage occurs, security teams spend considerable time looking for the root cause while under intense pressure to bring the business back online.

The bottom line is network security operations today are laborious and reactive, requiring substantial capital investment and operational expense with poor return on investment (ROI).

What Happened to the "R" in ROI?

As discussed earlier, organizations are having problems getting a reasonable return on their security investments. Let's take a closer look at the limitations of current solutions and how they drain away ROI.

Security Gaps

As networks have grown in size and complexity, organizations add new firewalls and upgrade existing firewalls in a piecemeal way. These mash-ups of disparate security solutions create gaps in security that are nearly impossible to find with existing tools. Cyberattackers can use these gaps as "safe houses," that is, places in the network where malicious agents can avoid detection. The result is a vulnerable network with significant risk of breaches and exfiltration of valuable information.

Business Disruptions

IT groups are constantly in a reactive mode, playing catch up. When the network begins to affect user productivity, the pressure to locate and remediate the problem grows exponentially with time. Unfortunately, troubleshooting complex security systems is challenging and time-consuming. IT groups today simply lack the informed insights and best practices they need to manage the network proactively.

Planning Uncertainty

Today's fast-moving markets require that businesses be continually planning how to adapt to dynamic circumstances. However, security architects today have no way to accurately predict the impact of proposed firewall deployments and often must rely on gut feel. This uncertainty acts as a headwind that hinders planning and causes IT managers to constantly second-guess themselves. Meanwhile, planning uncertainty can provide openings to competitors who have the ability to look ahead accurately and plan with confidence.

Network security managers face an important choice. If they remain on the same path and operate in the future as they have in the past, they can expect the same results. Alternatively, security managers can turn to an emerging technology that holds great promise for improving network security operations—artificial intelligence for IT operations, or AIOps for NGFW.

What Is AIOps for NGFW?

Artificial intelligence (AI) is arguably the most talked-about technology today, already in use in diverse applications from online shopping and automated translations to smartphones and industrial robots. The power of AI lies in its ability to mimic the problem-solving and decision-making capabilities of the human mind. Therefore, it's no wonder that scientists and developers are turning to AI to address the problems of network operations.

AIOps (artificial intelligence for IT operations) combines big data and machine learning to automate IT operations processes. Adoption of this groundbreaking technology has been steadily increasing—a recent survey found that 64% of companies are already using AIOps.[1] The driving factors for this trend are the growing complexity of the network and the skills shortage in IT departments.

Now Palo Alto Networks is bringing that technology to the firewall with the introduction of AIOps for NGFW. The secret sauce of AIOps for NGFW is machine learning (ML), a subset of AI. ML algorithms train on existing data sets and then adjust themselves (learn) through experience. ML algorithms are particularly good at finding patterns in mountains of data that would overwhelm humans. In AIOps for NGFW, ML algorithms take in log data and other telemetry, contextualize the information using historical data, and generate actionable insights.

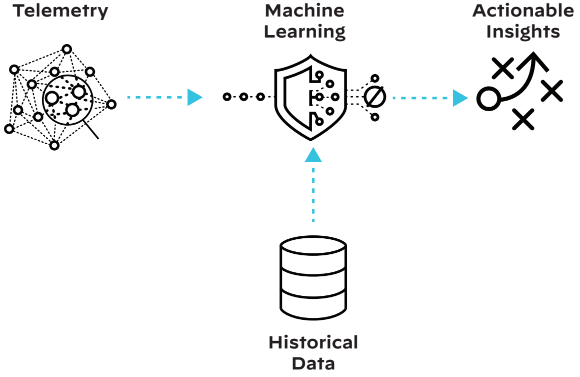


Figure 1: How AIOps for NGFW works

[1] James Connolly, "AIOps Adoption Gains Steam in Enterprises," RTInsights, November 3, 2021, https://www.rtinsights.com/aiops-adoption-gains-steam-in-enterprises/.

Continuous Detection Enables Proactive Network Operations

The legacy approach to IT operations is reactive—when something goes wrong, you fix it—and highly labor-intensive. AIOps for NGFW fundamentally changes the way IT teams work with continuous detection and proactive remediations. AIOps for NGFW automates many manual tasks to make operations more efficient and lessen the drain on IT staff. By leveraging the power of ML, AIOps for NGFW delivers a wide range of insights and recommendations that enable security teams to continuously improve their security posture and prevent business disruptions:

- Firewall hygiene assessments and guided best practices recommendations help security teams quickly eliminate firewall misconfigurations.
- Predictions, anomaly detection, and informative and timely alerts enable security teams to proactively remediate issues before they cause disruptions and identify root causes more quickly.
- Clear, accurate reports and simplified ticket creation streamline the administrative side of firewall management, freeing security experts to spend more time on strategic initiatives.

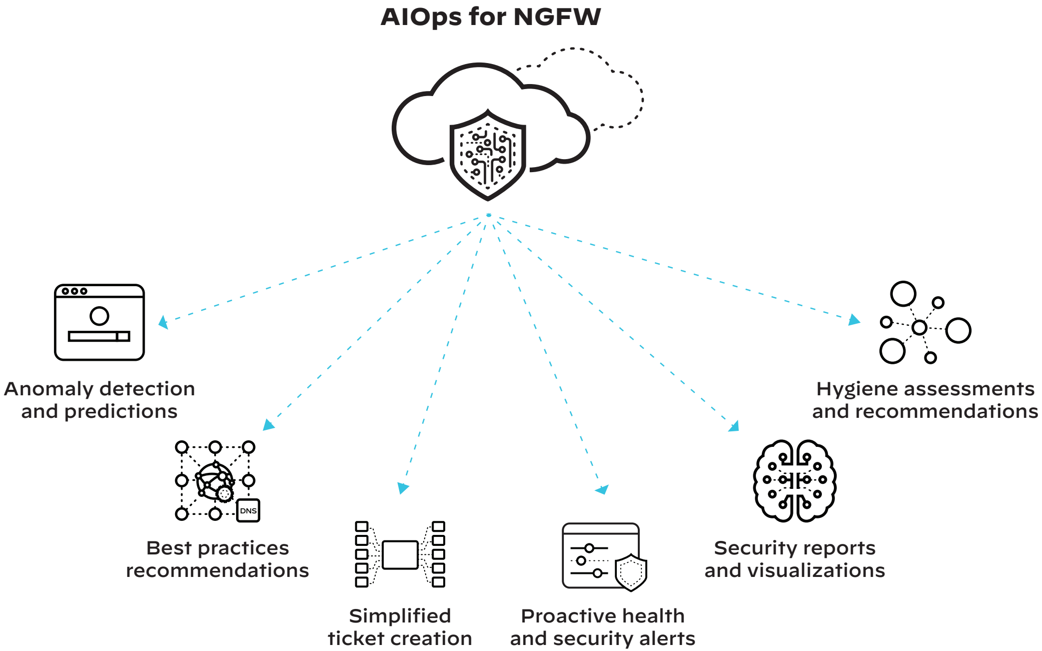

AIOps for NGFW
Anomaly detection and predictions
Best practices recommendations
DNS
Simplified ticket creation
Proactive health and security alerts
Security reports and visualizations
Hygiene assessments and recommendations

Figure 2: AIOps for NGFW delivers a range of actionable insights

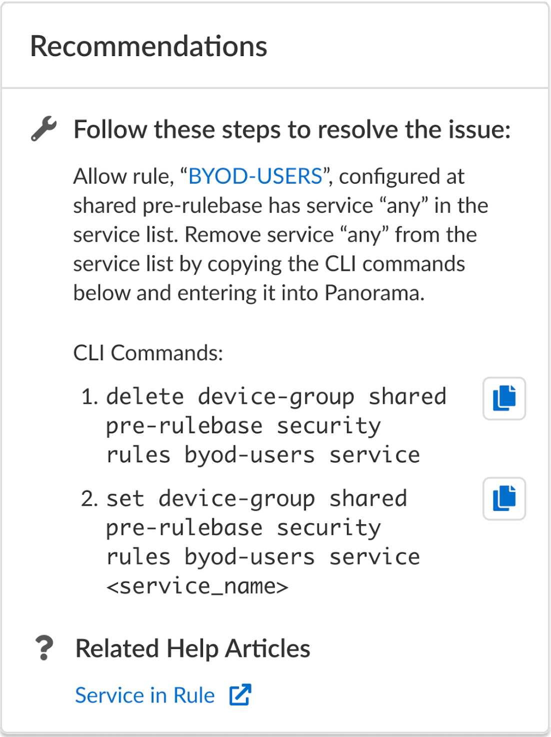
Alerts Help Network Teams Proactively Remediate Issues

Alerts are a vital weapon in the fight against cyberthreats, but they can also drag down productivity and even affect staff retention due to so-called “alert fatigue.” In addition, manual alert remediation can eat up hours of IT staff time that could be better spent on skills development and strategic initiatives.

AIOps for NGFW reduces time to remediation in several ways. ML algorithms use past behavior to better detect strange user behavior and predict metrics that may rise to a critical level in the next seven days. Once the alert is generated, AIOps for NGFW speeds remediation by offering specific recommendations and automatically opening tickets in ServiceNow.

AIOps also reduces the rate of false positives. The alerts in AIOps are generated when a specific metric:

- Crosses a threshold
- Changes state
- Trends toward critical severity in the next seven days
- Indicates unusual user behavior compared to historical data



Recommendations

Follow these steps to resolve the issue:

Allow rule, “BYOD-USERS”, configured at shared pre-rulebase has service “any” in the service list. Remove service “any” from the service list by copying the CLI commands below and entering it into Panorama.

CLI Commands:

1. `delete device-group shared pre-rulebase security rules byod-users service`
2. `set device-group shared pre-rulebase security rules byod-users service <service_name>`

Related Help Articles

Service in Rule

Figure 3: Typical recommendation generated by AIOps for NGFW

Scenario 1: Firewall Misconfigurations Create Vulnerabilities

In this scenario, the network security manager forgets to enable decryption, leading to a misconfigured firewall. When the unsuspecting user requests access to a compromised website, the request is granted and the malware infects the user's machine.

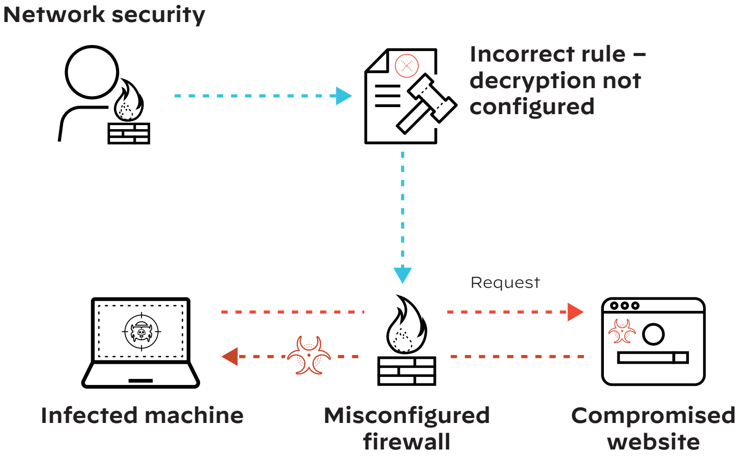


Figure 4: Malware protection before AIOps for NGFW

Solution: AIOps for NGFW Corrects Misconfigurations

AIOps for NGFW detects decryption policy error and alerts the network security team, providing remediation steps to help them quickly and accurately correct the rule. Now the firewall is properly configured to deny access to the compromised website and protect the user's machine from malware downloads.

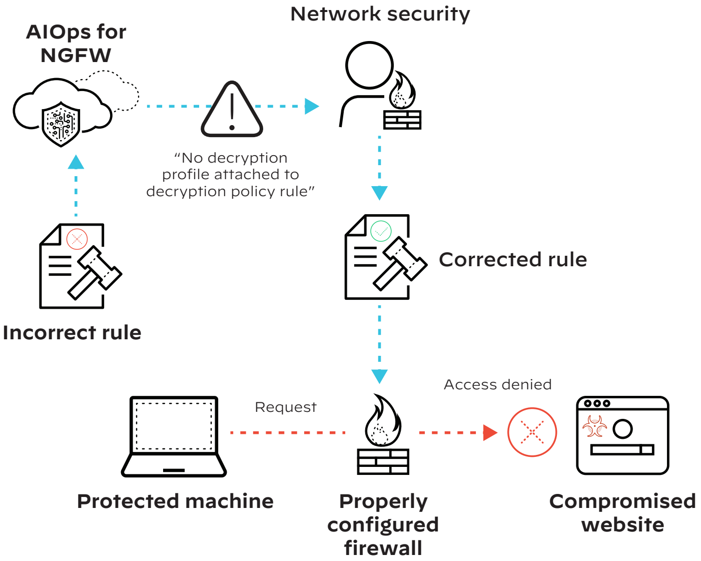


Figure 5: AIOps for NGFW proactively guides remediation and prevents malware infection

Scenario 2: Overloaded Firewalls Cause Network Disruptions

In this scenario, a sudden increase in network traffic exceeds the capacity of a critical firewall, leading to performance problems that disrupt the network and hinder productivity. The existing monitoring solution alerts the network security team but provides no information about the root cause. Security managers are now in a highly reactive mode under significant pressure to resolve the issue quickly with not enough information.

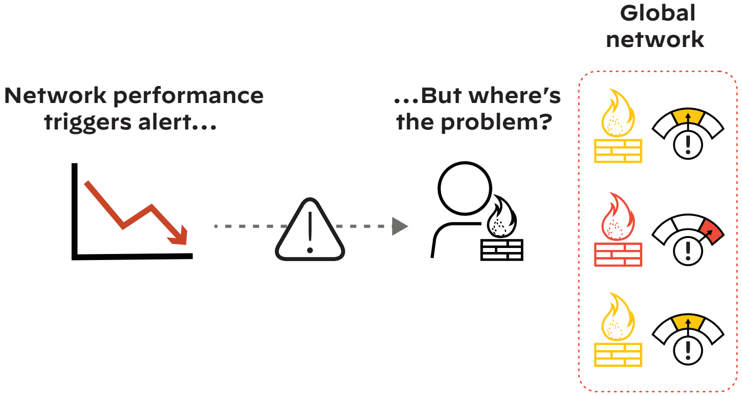

Network performance triggers alert...
...But where's the problem?
Global network

Figure 6: Reactive security staff lacks information to remediate

Solution: AIOps for NGFW Enables Proactive Remediation

AIOps for NGFW analyzes the trend to increased network traffic, forecasts possible disruptions, and alerts the network security team. The alert contains specific predictions of firewall utilization, contributing events, and recommended remediation. Now security managers can work proactively to prevent the disruption, for example, by increasing firewall capacity at the potential point of failure.

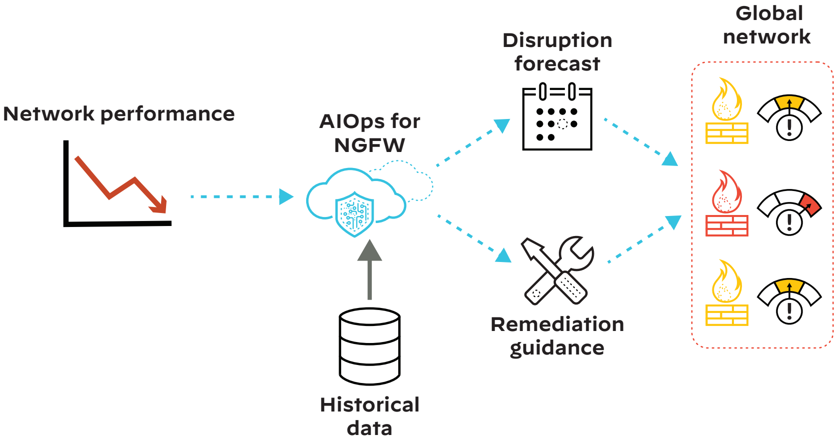


Figure 7: AIOps for NGFW enables proactive security to prevent disruptions

Scenario 3: Stolen Credentials Can Lead to Data Exfiltration

Credential phishing prevention (CPP) prevents users from submitting their corporate credentials to a phishing site that is disguised as a legitimate corporate website. In this scenario, the network security admin forgets to add CPP to the URL filtering profile. An unsuspecting employee accesses a site that looks like a corporate site but in fact is a phishing site that steals the employee's credentials. Now the hacker has a legitimate set of credentials to access confidential information and exfiltrate data.

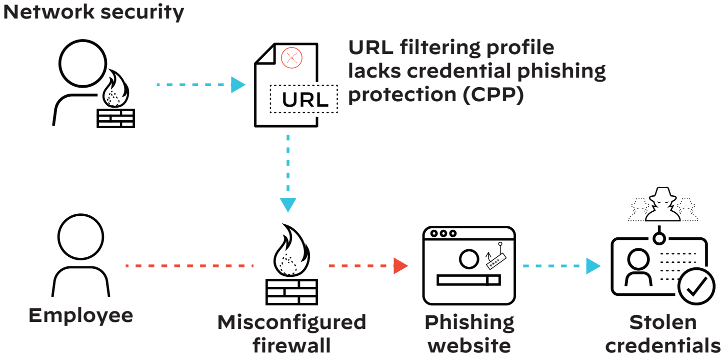
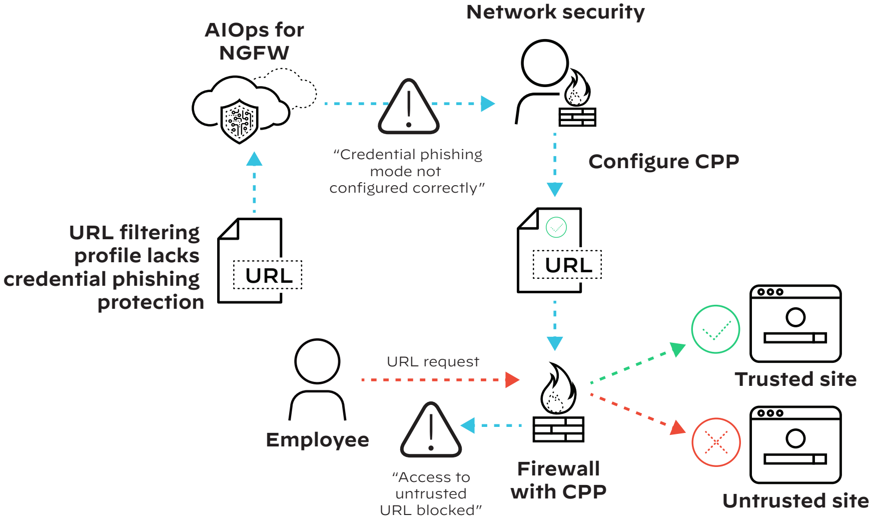


Figure 8: Without credential phishing prevention, hackers can steal credentials and exfiltrate data

Solution: AIOps for NGFW Alerts Network Manager

Once again, AIOps for NGFW detects the omission of CPP from the URL profile and immediately alerts the network security admin, who can then easily correct the mistake. Now the firewall can detect attempts to access an untrusted site and blocks the employee's access. Alternatively, the firewall can be configured to alert the employee to the danger of proceeding to the site but leaves the decision up to the user.



AIOps for NGFW
Network security
"Credential phishing mode not configured correctly"
Configure CPP
URL filtering profile lacks credential phishing protection
URL
URL
URL request
Trusted site
Employee
"Access to untrusted URL blocked"
Firewall with CPP
Untrusted site

Figure 9: AIOps for NGFW alerts network manager to correct configuration mistake and avoid credential theft

AIOps for NGFW Delivers Business Value

In summary, AIOps for NGFW addresses the three primary operational issues described earlier, making it possible for network teams to deliver a higher level of ROI.

Strengthen Security Posture

Using AIOps for NGFW, organizations can continuously optimize firewall configurations for even the most dynamic environments using ML-driven best practices and policy recommendations. For example, AIOps for NGFW can generate an alert when a required process such as credential phishing prevention is not turned on in a newly generated rule. This early warning allows firewall administrators to correct the rule and avoid a potentially dangerous misconfiguration.

Avoid Business Disruptions

AIOps for NGFW empowers network security operations teams to become proactive with ML-powered anomaly detection and actionable insights into the health and performance of the entire deployment. Now network security teams can confidently predict failures before they occur. For example, AIOps for NGFW can provide an early warning by identifying a specific firewall that may reach capacity at a particular point in the near future. Armed with that forecast, the network security team can deploy another firewall in time to avoid the disruption.

Plan with Confidence

As organizations look to the future, they need to have a clear understanding of the past. AIOps for NGFW provides insights into the current operating characteristics of the network, which makes it easier to predict how changes and additions will affect network operations. Now network architects can plan for infrastructure expansions and architectural modifications with confidence that these changes will deliver the desired benefits.

How We Can Help

Palo Alto Networks is revolutionizing network security with AIOps for NGFW, the first domain-centric implementation of this ground-breaking technology. Unlike other security vendors, our AIOps for NGFW solution provides *continuous* recommendations, essential for maximizing your security posture. AIOps for NGFW from Palo Alto Networks intelligently interprets telemetry data and provides actionable recommendations to prevent firewall disruptions—in other words, we help your team move from reactive troubleshooting to proactive network management that maximizes your ROI.

AIOps for NGFW is the future of network security operations—and the future is now.

Start Preventing Firewall Disruptions Today

Get ML-powered insights for your best security posture and optimal firewall health. Read the Solution Brief, then try AIOPs for NGFW for free.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com