LiveAction

From Reactive to Proactive: 8 Critical Features for Firewall Monitoring Tools

Firewall monitoring is critical for maintaining a secure, high-performing network. The best tools do more than just track metrics—they proactively detect issues, provide actionable remediation steps, and ensure adherence to best practices. While **network performance monitoring (NPM) tools** are essential for infrastructure oversight, they often fall short when it comes to managing security infrastructure, particularly firewalls.

Below are **eight reasons why traditional NPM tools may not be enough for firewall monitoring - and what capabilities you should look for instead.**

1. TOO MANY UNDETECTED FIREWALL ISSUES

No CISO wants to hear about an outage from a frustrated executive. Yet, many firewall issues go undetected despite having multiple monitoring tools in place.

A key limitation? Traditional NPM tools rely on **SNMP polling**, which is effective for routers and switches but lacks full visibility into firewalls. For example, **a BGP peer down event can disrupt internet connectivity**, yet some firewalls, like Check Point secure gateways, lack predefined SNMP object identifiers for BGP states—leaving such critical incidents unnoticed.

What to Look for:

- Deep firewall-specific monitoring beyond SNMP
- Proactive detection of service-impacting events

2. UNIQUE FIREWALL REDUNDANCY REQUIREMENTS

Unlike switches and routers that use **VRRP or GLBP** for redundancy, firewalls rely on **High Availability (HA) clustering.** If configurations aren't properly synchronized across active, standby, and backup firewalls, **outages can occur** due to missing static routes or misaligned policy-based routing.

Additionally, HA firewalls in standby mode often **appear inactive** to traditional NPM tools, leading to **false positives** that create unnecessary noise for IT teams.

What to Look for:

- Awareness of **HA status** to eliminate false alerts
- Detection of **configuration mismatches** in clusters

3. MONITORING BEYOND THE FIREWALL DEVICE

Firewalls depend on various **internal and external services** to function correctly. For instance, they need:

- Continuous access to **Active Directory** for identity-based policies
- Dynamic updates from **external threat intelligence feeds**
- Connectivity to **external dynamic lists** of IPs, domains, and URLs

Traditional monitoring tools rarely track these dependencies, leaving blind spots that can lead to security gaps.

What to Look for:

- End-to-end monitoring of firewall **dependencies and integrations**
- Alerts when firewalls lose connectivity to **critical services**

4. FROM REACTIVE TO PROACTIVE MONITORING

Many traditional monitoring tools are **reactive** - they only alert you once a problem has already impacted services. Yet, studies like **Uptime's 2021 annual survey** suggest that ***76% of outages could be avoided*** if IT teams had **advanced warning** about hidden configuration drifts, forgotten maintenance, or vendor best practice deviations.

For instance, if a firewall's **accelerated path processing** is disabled, early detection can prevent performance degradation before users notice any impact.

What to Look for:

- Proactive detection of **hidden risks**
- Alerts for **best practice violations**

5. ACTIONABLE REMEDIATION, NOT JUST ALERTS

Security teams are often stretched thin, especially with the ongoing **cybersecurity talent shortage.** Many NPM tools simply generate alerts—**without suggesting next steps.**

A modern firewall monitoring solution should **guide IT teams through remediation,** reducing downtime and improving operational efficiency.

What to Look for:

- **Step-by-step remediation guidance**
- **Automated knowledge sharing** to upskill IT teams

6. BEST PRACTICES FOR PROACTIVE NETWORK MONITORING

Misconfigurations are one of the leading causes of security incidents. Ensuring firewalls follow **vendor and industry best practices** is a key step toward **preventing network outages and security gaps.**

What to Look for:

- Continuous **best practice validation**
- **Automated compliance checks** against vendor recommendations

7. BEYOND MONITORING: THE POWER OF AUTOMATION

With the cybersecurity skills gap widening, security engineers are often overwhelmed. One way to close this gap is through network automation—offloading repetitive tasks like:

- Ongoing firewall maintenance
- Regulatory compliance checks
- Vulnerability assessments

By automating these tasks, security teams can focus on higher-priority initiatives rather than manual, time-consuming operations.

What to Look for:

- **Automated policy enforcement**
- **Compliance automation** to reduce manual workloads

8. AUTOMATED TROUBLESHOOTING FOR FASTER RECOVERY

When a firewall issue occurs, manual troubleshooting can be slow and complex. A truly advanced monitoring tool should do more than detect an issue—it should also:

- Apply device-specific domain knowledge
- Perform automated root cause analysis
- Collect real-time diagnostic data for faster resolution

What to Look for:

- **Automated triage and diagnostics**
- **Self-healing capabilities** for common issues

LOOK BEYOND TRADITIONAL NETWORK PERFORMANCE MONITORING, WITH AN EYE TOWARD NETWORK OBSERVABILITY AND INTELLIGENCE

Monitoring is crucial, but modern security demands **more than just visibility**. As threats become more sophisticated, organizations must shift from **reactive** monitoring to **proactive, automated security operations.**

Next Steps:

- **Explore firewall automation** to bridge visibility gaps in your Network Observability & Intelligence solution
- **Leverage proactive monitoring** to prevent outages
- **Adopt automation-driven remediation** to close security gaps faster

LiveAction delivers **security infrastructure** automation with **unprecedented visibility**—transforming firewall monitoring into a predictive, actionable, and automated process.

Ready to take the next step?
Try our security automation capabilities today!

\ FREE TRIAL

\ CONTACT SALES

LiveAction

901 Campisi Way, Suite 222
Campbell, CA 95008
(888) 881-1116

LiveAction offers industry-leading network performance monitoring solutions designed to meet the unique needs of the banking sector. Our solutions provide deep visibility, real-time analytics, and comprehensive security integration, ensuring robust network performance and compliance.

For more information, visit **www.liveaction.com**.