SOLUTION BRIEF

Fortinet and Logmanager Log Analysis Solution

Unified Firewall Log Insights for Faster Threat Detection, Investigation, and Response

Executive Summary

Fortinet and Logmanager have partnered to integrate Fortinet FortiGate Next-Generation Firewall (NGFW) logs into Logmanager's centralized log management and analytics multivendor platform to deliver context-rich security responses. This synergy results in more effective incident response and a deeper understanding of complex threat patterns.

The Challenge

Modern IT teams face rapidly growing volumes of security and operational data while being expected to detect and respond to incidents and threats faster than ever. Without centralized visibility and contextualized insights, critical events can be overlooked, investigations take longer, and the risk of business disruption increases.

At the same time, increasingly strict regulatory requirements demand reliable log retention, tamper-proof storage, and the ability to quickly produce audit-ready evidence, placing additional pressure on already constrained teams.

Joint Solution

Fortinet and Logmanager have partnered to address these challenges by combining the FortiGate NGFW advanced threat prevention capabilities with Logmanager's centralized log management and analytics multivendor platform. The integrated solution collects and consolidates Fortinet FortiGate NGFW logs into a single, normalized and enriched data stream, transforming raw security telemetry into actionable insight.

By integrating FortiGate NGFW data with information from across the entire IT infrastructure including servers, workstations, and other security layers, Logmanager provides a unified view that reveals the full scope of potential threats.

This context-rich visibility enables faster investigation, more efficient incident response, and improved operational awareness. At the same time, Logmanager ensures long-term, tamper-proof, compliance-ready storage, allowing organizations to meet regulatory requirements while maintaining a clear and reliable audit trail.

Solution Components

Fortinet FortiGate NGFWs protect data, assets, and users across today's hybrid environments. Built on patented Fortinet security processors, FortiGate NGFWs accelerate security and networking performance to effectively secure the growing volume of data-rich traffic and cloud-based applications. FortiGate NGFWs, backed by FortiGuard AI-Powered Security Services, help prevent cyberattacks and mitigate security risks with consistent, real-time protection and responses against even the newest and most sophisticated threats. Logmanager is a log management and analytics multivendor platform that radically simplifies responses to cyberthreats, legal compliance, and operational troubleshooting.

Solution Components

- Fortinet FortiGate Next-Generation Firewall
- Logmanager

Solution Benefits

- Streamlined log analysis through out-of-the-box or custom dashboards
- Fortinet FortiGate NGFW logs are normalized and enriched to become easily searchable within seconds using natural language
- Data is securely stored in tamper-proof storage for compliance and forensic purposes
- Unparalleled security protection with the Fortinet FortiGate NGFW and the Fortinet Security Fabric

FORTINET FABRIC-READY

Solution Integration

The integration between Fortinet FortiGate NGFW and Logmanager is designed for rapid deployment with minimal configuration. The process follows a streamlined “set and forget” principle, ensuring that organizations can gain visibility into their network traffic almost instantly.

Configuration and connectivity: Administrators can configure the FortiGate NGFW to forward logs to Logmanager via the intuitive web-based GUI or the Command Line Interface (CLI). By enabling the Syslog service and pointing it to the Logmanager IP address, the FortiGate NGFW begins streaming security and operational telemetry in real time. The solution supports standard logging formats, ensuring high-fidelity data transfer. Detailed, step-by-step configuration procedures for both GUI and CLI can be found in the Logmanager Documentation.

Automated ingestion and visualization: Once Logmanager receives the incoming stream, its built-in intelligence takes over. There is no need for manual mapping or complex parser development; Logmanager’s native FortiGate NGFW parsers automatically normalize and enrich the data. Pre-configured, out-of-the-box dashboards are immediately populated with live data, providing instant insights into security events, traffic patterns, and user activity without any additional setup required from the IT team.

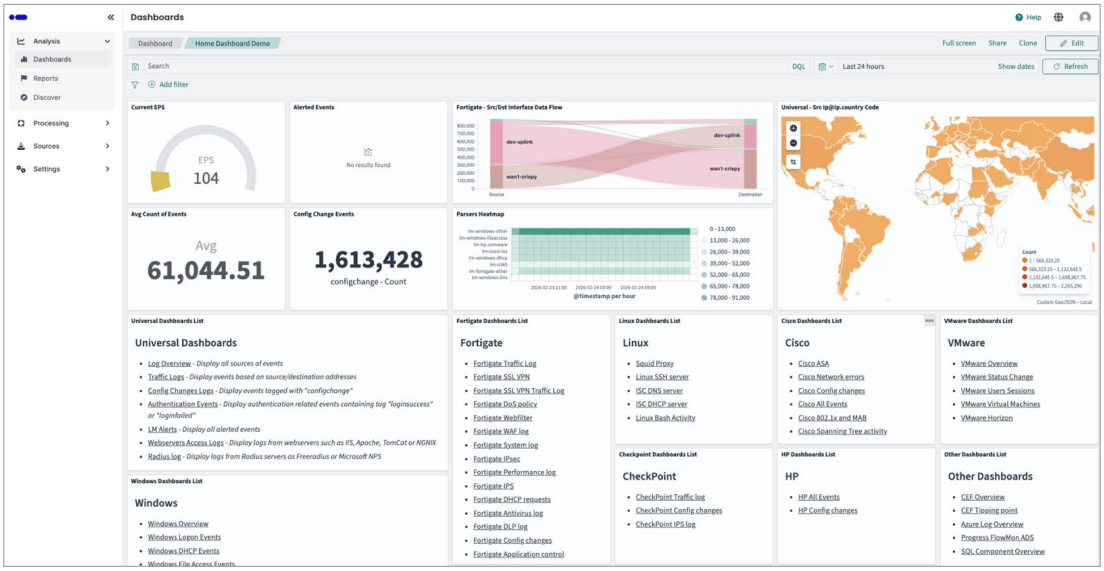


Figure 1: Logmanager built-in dashboards for Fortinet FortiGate NGFW

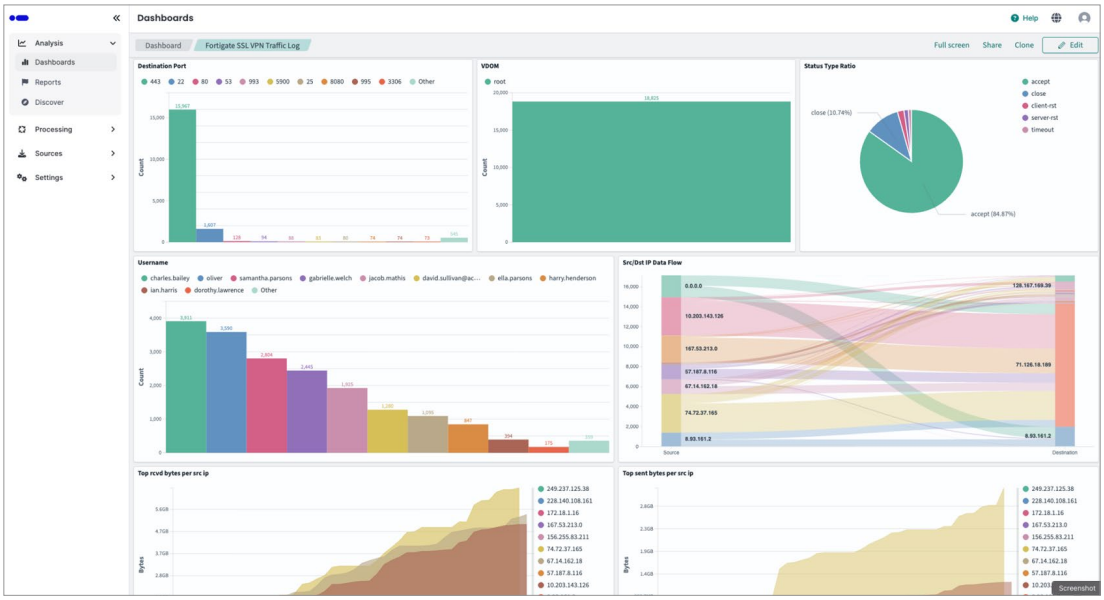


Figure 2: FortiGate NGFW SSL VPN traffic log dashboards

Joint Use Cases

Use case #1: FortiGate NGFW log analysis

Analyze FortiGate NGFW logs in the context of your assets, users, and the broader IT environment

Use case #2: Compliance-ready log retention

Retain FortiGate NGFW logs in Logmanager's tamper-proof storage to support audits, forensic investigations, and compliance with NIS2, ISO 27001, PCI DSS, DORA, and other regulatory requirements

About Logmanager

Logmanager is a log management platform enhanced with SIEM capabilities that radically simplifies responses to cyberthreats, legal compliance, and troubleshooting. By transforming diverse logs, events, metrics, and traces into actionable insights, it helps security and operations teams respond swiftly to any incident. Experience effortless self-management and customization, peerless functionality, and the flexibility to take control of your entire technology stack. Visit logmanager.com

About Fortinet

Founded in the San Francisco Bay Area in 2000, Fortinet continues to be a driving force in the evolution of cybersecurity and the convergence of networking and security. Securing people, devices, and data everywhere is our mission. To that end, our portfolio of over 50 enterprise-grade products is the largest integrated offering available, delivering proven cybersecurity everywhere you need it. More than 900,000 customers trust Fortinet solutions, which are among the most deployed, most patented, and most validated in the industry. For more information, visit fortinet.com

Copyright © 2026 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

May 2, 2026 9:19 AM / MKTG-3310-0-0-EN