LogRhythm

Joint Solution Brief

LogRhythm and SonicWall Firewall

LogRhythm and SonicWall combine to accelerate threat prevention, detection, and response across the entire IT infrastructure

Benefits

- Gain complete visibility into the network
- Leverage real-time, actionable threat intelligence
- Accelerate threat identification and response

Solution Overview

LogRhythm and SonicWall integrate to synergistically elevate enterprise-wide threat detection and response capabilities by offering forensic visibility and advanced behavioral analytics. SonicWall firewalls constantly monitor and filter incoming and outgoing traffic. Packets are scrutinized to ensure that only authorized traffic enters, and advanced threats are prevented. Integration with LogRhythm SIEM builds upon these capabilities, helping security teams centralize detection of threats and reduce response time. LogRhythm SIEM collects and analyzes SonicWall logs to help security teams quickly understand the scope of an attack via a centralized dashboard. Attack containment and remediation is accelerated by LogRhythm's automated workflows that trigger action by SonicWall OS. For example, as logs are ingested, LogRhythm SmartResponse™ for SonicWall OS can automatically log out all users from all their open sessions.

Log Collection

Securing an organization's network and operations begins with high-fidelity and trustworthy log and network traffic data. LogRhythm uses a single schema, Machine Data Intelligence (MDI) Fabric, to normalize structured and unstructured data. Our security teams review these sources and ensure that relevant security data is normalized with other consumable security data. The results are trusted logs and alerts that allow for precision rule creation and comprehensive remediation efforts in an attack.

SONICWALL

About LogRhythm and SonicWall

LogRhythm and SonicWall work together to help organizations increase network visibility and protect against modern cyberattacks. The combined solution empowers security teams to identify behavioral anomalies, internal and external threats, and to prioritize their responses based on accurate enterprise security intelligence. LogRhythm and SonicWall empower security teams to navigate a changing threat landscape with confidence.

How It Works

LogRhythm SIEM collects from every device, application, and sensor in an environment while our MDI Fabric classifies and contextually structures every log message. Logs are ingested by the LogRhythm SIEM platform where they are parsed and normalized to the LogRhythm schema. Normalized data is then sent to LogRhythm's analytics engine and storage tier for analysis, storage, and reporting via consolidated dashboards containing all security events.

When used with SonicWall, LogRhythm pulls event logs from SonicWall Firewalls. The logs are then parsed and normalized to the LogRhythm schema before they are sent to the LogRhythm SIEM for analysis, storage, and reporting via a centralized dashboard of all security events.

How Automated Workflows Work

To streamline security response workflows, organizations can use LogRhythm SmartResponse™, which is part of LogRhythm's security orchestration, automation, and response (SOAR) solution. LogRhythm SmartResponse accelerates response to suspicious or unauthorized authentication requests to minimize damage, eliminating manual intervention by security analysts. This advanced capability is delivered to end users through the LogRhythm SmartResponse for SonicWall integration.

The LogRhythm SmartResponse for SonicWall contains multiple actions that can be configured to execute automatically in response to an alarm or manually through analyst workflow. Each action can also be configured to require approval before execution. For example, if the security team finds suspicious activities associated with specific users, the team can log the users out by IP. This empowers security teams to investigate the activity and prevent any unauthorized access or malicious activity from continuing.

Action	Description	Use Case
Create SonicWall Configuration file	Execute this response and rerun it before using other available actions whenever you change the fixed-value parameter	Functionality that must be run first, before other SmartResponse functions can execute
Get Connection Status	Retrieves Firewall connection status report	Display connection status
Get IP Addresses	Fetches IP dddresses	Display list of IP addresses
Get NIC Status	Retrieves information about the network interface	Display network interface information
Get Report IP Route	Fetches Route report for specific IP	Display IP route for specific IP
Get Storage Info Status	Fetches information about the storage and capacity utilization of the system	Fetch storage information
Get Security Status	Retrieves report about the status of the security of the system	Fetch system security status
Get System Status	Retrieves information about operational status	Fetch information about system operations
Get Zone Info	Retrieves zone configuration	Display zone configuration
Log Everyone Out	Close out all sessions for all users	Log all users out of all open sessions
Get User Status	Retrieve status of all users	Display status of all users
Get User Status by Name	Retrieve user status of user specified by name	Fetch status of user specified by name
Log Users out by IP	Close all sessions for a user with specific IP	Log users out by specified IP
Resolve the FDQN Address	Queries FDQN to retrieve the associated IP address	Fetch list of domains and their corresponding IP addresses
Unlock User	Unlock specific user account	Unlock user account
Virtual Assist Deny	Create a new virtual assist deny request	Deny virtual assistance
Set Config Mode	Preempt the other user, set self to config mode.	Enter config mode to manage settings
Set Non-Config Mode	Release config mode, set self to non-config mode	Return to standard operating state from config mode