SOLUTION BRIEF

# Fortinet and Indeni Security Solution

## Broad, integrated solution for security infrastructure automation

### Executive Summary

**Without automation, IT operations teams would spend countless hours gathering diagnostics and device data to keep firewalls up and running. The Fortinet-Indeni partnership enables security infrastructure automation of Fortinet best practices that deliver predictive, prioritized, and actionable insights and help to prevent costly disruptions.**

### Challenge

IT teams that manage firewalls are often limited in staff, which makes the case for the need for automation. The typical network administrator spends 70% of his or her time identifying and remediating known errors. 80% of outages (*source*) can be avoided if IT operations teams receive an advanced notice with respect to common issues stemming from hidden configuration skew, forgotten ongoing maintenance, or a combination of lack of adherence to vendor, industry, and high-availability (HA) best practices.

To address these challenges, Indeni and Fortinet have established a technology partnership to protect Enterprise networks from external cyber threats. With this joint solution, Indeni's security infrastructure automation platform and Fortinet FortiGate enterprise firewall products enable IT teams to simplify day 2 operations and ensure maximum reliability.

### Joint Solution

When deploying Fortinet FortiGate firewalls, organizations have a need to ensure that correct configurations get deployed and synchronized consistently across multiple infrastructure devices. They should also be able to gather relevant data and insights to be able to assess and optimize the performance of security and infrastructure devices. With the Fortinet and Indeni partnership, engineering and operations teams enjoy best of breed as the Fortinet FortiGate secures and accelerates the network and user experience, and Indeni continuously assesses and notifies on misconfigurations and degradations in performance before it can result in service downtime.

Indeni automatically detects issues relating to Fortinet FortiGate firewalls and offers a way to remediate them. IT operations teams can gain Fortinet-specific knowledge from the descriptions and recommended remediations built from real-world experience of certified Network Security Experts. Together, the joint solution enables automating FortiGate nextgeneration firewall (NGFW) best practices to prevent costly disruptions from occurring, thus keeping the enterprise networks safe at all times.

#### Four automation practices by the joint solution

##### Ensure High Availability

Constant detection of HA unreadiness from cross-device inconsistencies in security policies, forwarding tables, and other configuration and state:

- Alert if one or more firewalls in a firewall cluster experiences problems
- Identify firewall cluster configuration synchronization issues including checks for sync status, debug zone, and configuration file checksum
- Identify cluster heartbeat interface problems by tracking link status and total bytes
- Alert if the number of operational heartbeat links are less than two (no redundancy)
- Alert if HA heartbeat interfaces do not have different priorities

### Solution Components

- Indeni Security Infrastructure Automation
- Fortinet Security Fabric—Next-Generation Firewall

### Joint Solution Benefits

- Identify latent issues and receive detailed remediation steps to reduce downtime
- Increase alert accuracy through the correlation of configuration, logs, and device statistics, resulting in fewer and shorter interruptions
- Preemptively identify misconfigurations, forgotten maintenance tasks, high availability, and other best practices to avoid bigger problems
- Leverage remediation best practices crowdsourced from industry experts and Fortune 100 customers to gather the most relevant and important device health checks

FORTINET Fabric-Ready

**Stateful Health Checking**

Continuously assess device health by comparing expectations of device configuration against reality of current status. Sample issues:

- Crashlog entries have been logged
- Fortinet uninterruptible upgrade is disabled
- High CPU or memory usage on the subordinate device
- Log disk utilization is high

**Validate Best Practices**

Continuously assess devices for alignment with configuration recommendations from Fortinet and seasoned practitioners. Alert if following conditions detected:

- Firewall does not have an explicit deny rule to log unauthorized traffic (violation traffic)
- Wildcard FQDNs are used
- Disk logging enabled
- Default static route is not configured
- Firewall not connected to FortiAnalyzer

**Proactive Maintenance Notification**

Cross off often forgotten maintenance tasks such as identifying:

- Upcoming license expiration nearing
- SSL certificate expiration nearing
- Log service expiration nearing


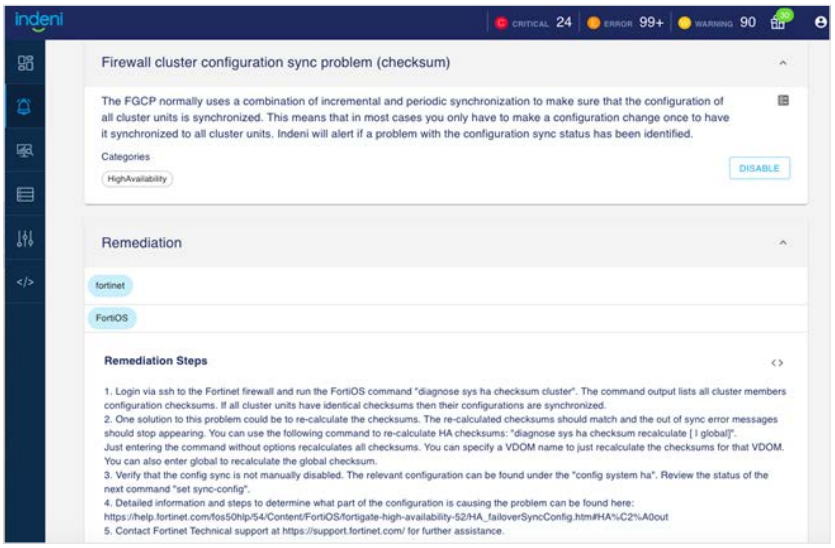


Figure 1: Remediation steps for the firewall cluster configuration sync problem.

## Indeni Security Infrastructure Automation

Indeni provides security infrastructure automation with an unprecedented level of visibility. Indeni continuously detects issues and validates that devices meet standards before or after a configuration change. Issues that are no longer present are automatically resolved. With AutoTriage, best practice issue investigation is launched the moment an issue is detected. The investigative steps can be as simple as gathering additional contextual diagnostics information, or as in-depth as analyzing and performing common troubleshooting tasks. We deliver production-ready automation elements, continuously curated from vetted, community-sourced experience, to auto-remediate difficult tasks.

## FortiGate Enterprise Firewall

FortiGate NGFWs enable security-driven networking and consolidate industry-leading security capabilities such as intrusion prevention system (IPS), web filtering, secure sockets layer (SSL) inspection, and automated threat protection. Fortinet NGFWs meet the performance needs of highly scalable, hybrid IT architectures, enabling organizations to reduce complexity and manage security risks.

As an integral part of the Fortinet Security Fabric, FortiGate NGFWs can communicate within the comprehensive Fortinet security portfolio as well as third-party security solutions in a multivendor environment. To increase the speed of operations and response, they share threat intelligence and improve security posture and automated workflow.

## Use Cases

1. Automate the process to ensure a firewall cluster failover is seamless
2. Automate ongoing maintenance tasks such as device configuration backup and proactive maintenance notification
3. Validate best practices for alignment with configuration recommendations from Fortinet and seasoned practitioners
4. Consistent measurement of device configuration skew against locally defined organizational standards

## About Indeni

Indeni provides security infrastructure automation with unprecedented visibility that's up and running in minutes. We've automated the world's best practices to deliver predictive, prioritized, and actionable insights that help you prevent costly disruptions. We dramatically reduce chaos and risk to improve agility, giving you the confidence to accelerate mission-critical projects that drive new business. Learn more at indeni.com.

FORTINET

www.fortinet.com



June 26, 2020 1:49 AM

705332-0-0-EN

D:\Fortinet\Solution Briefs\Grey Solution Brief\Indeni\sb-FA-fortinet-and-indeni-security-solution-6232020\sb-FAfortinet-and-indeni-security-solution-6232020