Challenge

Undetected issues with firewalls can expose your network to security breaches or lead to an outage. Existing monitoring tools are reactive, only notifying users of an issue after it occurs, and do not provide actionable next steps.

Solution

BlueCat Infrastructure Assurance proactively alerts Fortinet FortiGate users to issues and provides remediation steps that IT operations teams can use to resolve problems before they cause significant damage.

Benefits

- Proactively identify issues to avoid outages
- Optimize the performance of security infrastructure
- Reduce mean time to resolution
- Work more effectively

Request a live demo

Automating best practices and operational device issue detection in your security infrastructure

Without automation, IT operations teams would spend countless hours gathering diagnostics and device data to keep firewalls up and running. IT teams that manage firewalls often have limited resources, resulting in an even greater need for automated diagnostics and issue detection. The typical security engineer spends a notable portion of their time identifying and remediating known errors.

IT operations teams can avoid costly outages if they receive advance notice about common issues that can lead to bigger problems. These issues might include hidden configuration drift, forgotten ongoing maintenance tasks, or a lack of adherence to vendor, industry, and/or high availability best practices.

This solution brief presents how BlueCat Infrastructure Assurance automates detection of operational device issues, which are often hidden, in your security infrastructure. This brief provides specific examples from a variety of use cases for Fortinet FortiGate customers to simplify Day 2 operations, adhere to best practices, and ensure maximum reliability. It also covers key differentiators from other solutions and key solution benefits.

Solution overview

Infrastructure Assurance avoids network disruption with automation. Think of it as a virtual expert that can expand team skills and is on duty 24/7.

Infrastructure Assurance provides deep visibility into your security infrastructure to flag early warning signs of issues. With our domain expertise codified into Infrastructure Assurance, the platform knows what to look for, analyzing your firewalls to ensure they are healthy.

Should it find something, the platform proactively alerts IT operations teams that there might be a service failure—or any level of degradation of service—coming. Our auto-triage capability will investigate a problem without any human intervention. It gathers additional contextual diagnostic information, analyzes, and performs common troubleshooting tasks and root cause analysis.

Then, Infrastructure Assurance provides a list of recommended remediation steps that IT operations teams can use as a guide to help address the problem. IT operations teams gain firewall-specific knowledge from issue descriptions and recommended remediations built from the real-world experience of certified security experts.

Effectively, we've automated best practices to help you improve the efficiency of your security operations, reduce mean time to resolution, and prevent costly disruptions.

Five types of use cases

For Fortinet FortiGate customers, moving beyond the reactive mindset when things go awry is within reach. In this section, we outline five scenarios that you might encounter, with specific real-world examples of detected issues. Each explores how Infrastructure Assurance can help ensure that your security infrastructure is working as intended.

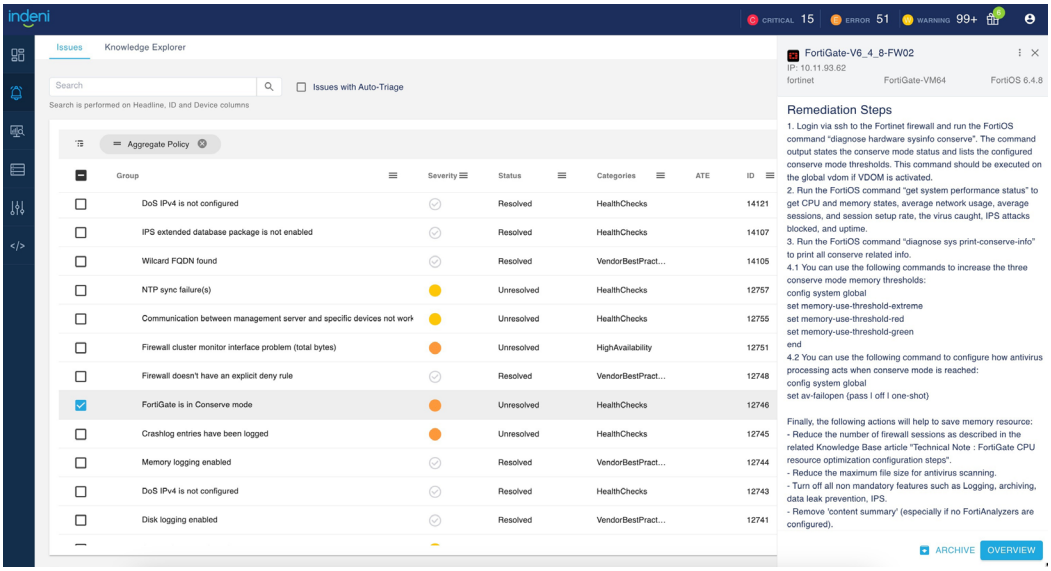
Once issues are detected, Infrastructure Assurance provides actionable information to help IT operations teams address them. They can troubleshoot issues by following the remediation steps authored by certified Fortinet Network Security Experts.

Use case 1: Stateful health checking

Infrastructure Assurance continuously assesses the health of Fortinet FortiGate by comparing expected device configurations against the current status. The goal is to find lurking issues and address them before they impact services.

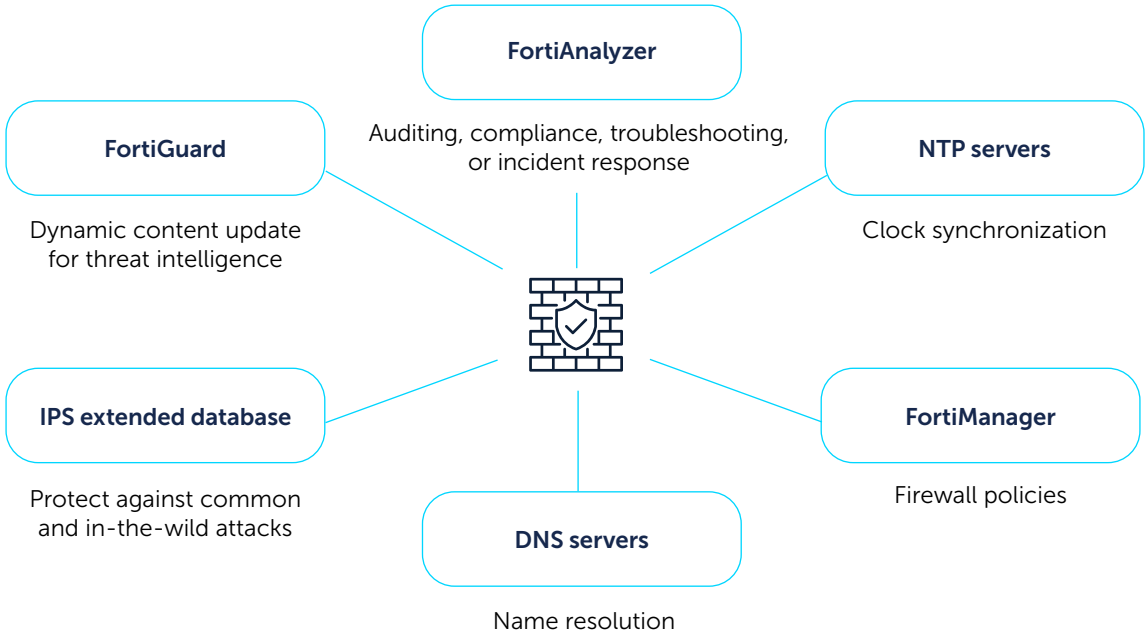
Sample common issues detected, based on real experience, include:

- Firewall enters conserve mode, with an analysis of memory consumption by process
- Crashlog entries have been logged
- Log disk utilization is high
- Firewall not connected to FortiAnalyzer
- Top active file descriptors, socket memory, and memory processes
- Session clash
- Kernel sessions are deleted due to lack of memory or resources
- Sessions have been dropped due to maximum limit
- High number of ephemeral sessions, which can be an indication of denial-of-service attacks
- Memory logging is enabled
- Session clash counter increase



Use case 2: External critical services

Firewalls have near real-time dependency on many external services. It is important to monitor the connection to these critical services. Infrastructure Assurance's automation features ensure, through regular testing, that communication with these external services is always available.



Critical services that a firewall requires include:

- Clock synchronization with an NTP server
- Access to DNS for name resolution
- Access to FortiManager for firewall policies
- Forwarding syslog to FortiAnalyzer for auditing, compliance, troubleshooting, or incident response

To equip firewalls with the latest preventative threat intelligence, firewalls frequently get dynamic content updates from FortiGuard. Timely updates are key to protecting your networks before threats become widespread. Infrastructure Assurance ensures frequent updates of intrusion prevention system (IPS) signatures and antivirus databases to minimize exposure to zero-day attacks.

Use case 3: Ensure high availability

To prevent a single point of failure on your network, you made the investment to deploy redundant infrastructure to ensure always-on services. Unfortunately, despite the investment, failovers do not always go smoothly. Infrastructure Assurance constantly detects high availability unreadiness from cross-device inconsistencies in security policies, forwarding tables, and other configurations and states.

Examples of high availability readiness issues that Infrastructure Assurance might detect and provide alerts for include:

- One or more firewalls in a firewall cluster experiences problems
- Firewall cluster configuration synchronization issues, including checks for sync status, debug zone, and configuration file checksum
- Cluster heartbeat interface problems by tracking link status and bandwidth utilization
- Status of critical high availability monitor links
- The number of operational heartbeat links are less than the two recommended high availability links (no redundancy)
- High availability heartbeat interfaces do not have different priorities

Use case 4: Misconfigurations and best practices validation

Device misconfiguration is a major cause of unplanned downtime. Configuration errors can create security

gaps in your network, making it vulnerable to cyberattacks. Infrastructure Assurance continuously detects misconfigurations by verifying against a gold standard for your network. It continuously assesses devices for alignment with configuration recommendations from Fortinet and seasoned practitioners.

Issues that Infrastructure Assurance might detect and provide notifications for include:

- Static routing table has changed
- DNS or NTP servers configured do not match requirement
- IPv4 Denial of Service policy L3 or L4 is not configured
- Firewall does not have an explicit deny rule to log unauthorized traffic (violation traffic)
- Wildcard FQDNs are used in firewall rules
- Disk logging enabled, potentially causing performance degradation
- Fortinet uninterruptible upgrade is disabled
- NTP sync status critical for logging analysis and troubleshooting

Use case 5: Proactive maintenance notifications

Maintaining availability requires ongoing maintenance. Tasks like device configuration backup are important to ensure your security infrastructure is safe from failure and disruption. Infrastructure Assurance automates device configuration backup and proactively notifies you if the backup is unsuccessful.

One of the most easily forgotten maintenance tasks is certificate renewal. Your firewalls use certificates for a variety of purposes. Valid certificates are needed for inbound SSL inspection, user authentication, and IPSec site-to-site VPN. Not having a valid certificate will likely impact services. Infrastructure Assurance provides warnings in advance if certificates are about to expire, giving you ample time to act.

Infrastructure Assurance also checks for valid licenses to ensure software license compliance. An expired license can potentially cause a service outage to security profiles such as web filters. Automating these maintenance activities can truly help maintain the health and performance of your firewalls.

Key differentiators

There are four major differences between Infrastructure Assurance and other network monitoring and management solutions.

1. Our automation elements are developed by our community of experts. By bringing expertise from our community, security vendors, and Fortune 1,000 customers, we can gather the most relevant and important device knowledge. Crowdsourcing brings together ideas and expertise that would not otherwise be available.
2. When deploying Infrastructure Assurance in a security environment, customers immediately receive notifications about misconfigurations, errors, security risks, vulnerabilities, and lack of adherence to best practices. Because Infrastructure Assurance knows what to look for, the platform can continually and preemptively identify issues to avoid bigger problems. Other network monitoring solutions lack specific, codified domain expertise.
3. When it detects the symptoms of various potential problems, Infrastructure Assurance automates the troubleshooting process to determine root causes. Other network monitoring and management solutions provide alerts but stop there. It's left to IT operations teams to conduct troubleshooting and root cause analysis themselves. Automated detection and analysis of issues can prevent them from recurring and reduce downtime.
4. Once root causes have been determined, Infrastructure Assurance goes further than other monitoring solutions by providing a list of actionable remediation steps that IT operations teams can take. IT operations teams gain specific knowledge from the issue descriptions and recommended remediations

compiled from the real-world experience of experts. These specific, actionable insights also reduce troubleshooting time.

Solution benefits

IT operations teams enjoy several benefits when using Infrastructure Assurance as a solution for hidden issue detection and recommended remediation. They include:

- **Avoid downtime.** Proactively identify misconfigurations, high availability inconsistencies, forgotten maintenance tasks, and other best practices to avoid outages.
- **Optimize the performance of your security infrastructure.** Automation streamlines IT operations, allowing IT teams to deliver optimal security services to your organization.
- **Reduce mean time to resolution.** Accelerate troubleshooting by conducting automated root cause analysis, without human intervention.
- **Work more efficiently.** Infrastructure Assurance surfaces useful and actionable information that will immediately facilitate your IT operations team's work.

Corporate Headquarters
4100 Yonge St. 3rd Floor, Toronto, ON, M2P 2B5
1-416-646-8400 | 1-866-895-6931

Next steps

Discover how Infrastructure Assurance can proactively alert you to issues to help avoid network outages.

Request a live demo