**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 Palo Alto Networks Next-Generation Firewall 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 your 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 advanced notice about common issues that can lead to bigger problems. These issues might include hidden configuration drift, forgotten ongoing maintenance tasks, or a combination of 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 Palo Alto Networks Next-Generation Firewalls 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.

# Seven types of use cases

For Palo Alto Networks Next-Generation Firewalls customers, moving beyond the reactive mindset when things go awry is within reach. In this section, we outline seven scenarios that you might encounter, with specific real-world examples. Each explores how Infrastructure Assurance can help ensure that your security infrastructure is working as intended.

## Use case 1: Stateful health checking

Infrastructure Assurance continuously assesses the health of Palo Alto Networks NGFW 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:

- Debug mode enabled
- Next hop inaccessible
- Policy-Based Forwarding rule is down
- SSL decryption—sessions near capacity, SSL decryption memory usage is high, tracking of SSL global counters and notification if the device has opted to drop packets or leave traffic encrypted
- Maximum number of routes nearing limit
- Packet drop counters increasing significantly—TCP flow non-sync packets, flow policy-deny, NAT'ed packets
- Capacity of dynamic address groups approaching device limit



Once issues are detected, Infrastructure Assurance provides actionable information to help IT operations teams address it. This includes a description of the issue, remediation steps, and links to articles on Palo Alto Networks' support portal.

## 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. Through regular testing, Infrastructure Assurance's automation features ensure that communication with these external services is available at all times.

| | **Syslog services** | |
| **Threat prevention policies** | Auditing, complience, incident response, troubleshooting | **NTP and DNS servers** |
| Dynamic content update- WildFire, URL filtering, application package, antivirus content package, etc. | **paloalto** NETWORKS | Clock synchronization, name resolution |
| **Active Directory** | | **Panorama, external dynamic list** |
| Identity awareness | **RADIUS and LDAP servers** | Firewall policies- internal or external |
| | Authentification, authorization | |

Critical services that a firewall requires include clock synchronization with an NTP server, access to DNS for name resolution, and forwarding syslog to an external server for auditing, compliance, troubleshooting, or incident response.

Firewalls may need continuous access to Active Directory for identity awareness to make forwarding decisions. They also need access to RADIUS or LDAP servers for user authentication and authorization.

To equip firewalls with the latest preventative intelligence, firewalls frequently get updates from WildFire, the URL filtering cloud, and other tools. Timely updates are key to protecting your networks before threats become widespread. Infrastructure Assurance continuously checks that packages are kept up to date by always maintaining an active connection. It also ensures best practices are followed. This includes, for example, always making sure that the action is set to "download-and-install" and that the frequency for WildFire is set to one minute.

Firewalls also need up-to-date policies from Panorama. Your firewalls are likely importing objects (such as IP addresses, URLs, and domains) from an external web server to protect against malicious hosts. The list of objects is known as an external dynamic list (EDL). Infrastructure Assurance goes beyond just checking for reachability to the web server hosting the EDL. It also ensures that the EDL is not empty and that it has not reached its capacity.

## Use case 3: Misconfigurations

Device misconfiguration is another major cause of unplanned downtime. Configuration errors can create security gaps in your network, making it vulnerable to cyberattacks. BlueCat Infrastructure Assurance continuously detects misconfigurations by verifying against a gold standard for your network. It even notifies you if a scheduled commit from Panorama failed. Misconfiguration issues that BlueCat Infrastructure Assurance might alert you to include:

- Default route in static route table not available
- Static routing table has changed
- DNS, Panorama, NTP, or RADIUS configuration does not match requirement
- SNMP community string or SNMP trap community string configuration does not match requirement
- Time zone configuration does not match requirement
- Panorama—commit not scheduled or scheduled commit failed
- Authentication profile(s) misconfigured
- EDL(s) configured is/are not used in policy

## Use case 4: High availability readiness

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. This includes configuration state and ensuring adherence to best practices. Examples of high availability readiness issues that Infrastructure Assurance might detect and provide alerts for include:

- High availability interface not receiving traffic
- High availability pair member in suspended state for too long
- Cluster has preemption enabled
- Cluster configuration not synchronized
- High availability configurations not meeting best practices

## Use case 5: Auto-detect security risks and ensure compliance

Enterprises are hypervigilant about how they secure their security infrastructure. Device hardening is necessary to reduce the attack surface. BlueCat Infrastructure Assurance has hundreds of automation elements to identify security risks and compliance violations. Regardless of your regulatory compliance requirements, we likely have the security control validations in place to help you prepare for your audit.

For example, here are snapshots from a Payment Card Industry Data Security Standard (PCI DSS) compliance report:

## PCI DSS 4 - Encrypt Transmitted Data

**Time range:** 01/09/2023 08:32 - 01/09/2024 08:32    **Issues:** Resolved & Unresolved, Archived & Not Archived

Legend:
- SNMPv2c/v1 used
- SSH version 1 is enabled
- Weak cipher used with SSL profiles
- Weak security protocol used with SSL profiles
- Default certificate used
- Telnet is enabled on the device

Devices: CP-R80.40-GW1-1, BluecoatProxySG, F5-10.11.90.202, PAN-FW1-10.0, PAN-FW2-10.0, FortiGate-V6_4_8-FW01, FortiGate-V6_4_9-FW02, Fortinet V5, BIGIP17-LB01, PAN-FW-peer-10, BIGIP17-LB02

## PCI DSS 5 - Maintain Anti-Virus

**Time range:** 01/09/2023 08:32 - 01/09/2024 08:32    **Issues:** Resolved & Unresolved, Archived & Not Archived

Legend:
- EDL(s) configured is empty
- EDL(s) configured not reachable

Devices: PAN-FW7-10.0, PAN-FW1-10.0

## PCI DSS 6 - Software Updates

**Time range:** 01/09/2023 08:33 - 01/09/2024 08:33    **Issues:** Resolved & Unresolved, Archived & Not Archived

Legend:
- Content update schedule is not following best practices
- Update schedule set to download only
- OS/Software version does not match requirement

Devices: PAN-FW2-10.0, PAN-FW1-10.0, PAN-FW-peer-10, CP-R80.20-GW1-2, BlueCat_Address_Manager

## PCI DSS 7/8 - Admin Access to Data

**Time range:** 01/09/2023 08:33 - 01/09/2024 08:33    **Issues:** Resolved & Unresolved, Archived & Not Archived

Legend:
- Ensure cplogs is set to on
- Login Banner not configured
- Permit only the necessary IP addresses to be used to manage the device
- Repeated failed login attempts by a user
- Admin Lockout Time is not within the recommended range
- Failed login attempts
- Local administrators configured with no password profile
- Security Rule with Source and Destination Zones set to Any
- Service setting of ANY configured on security policy
- Configured SSH timeout too high
- Configured Web Management (GUI) timeout too high
- Max Failed login attempts setting

Devices: CP-R80.20-GW1-2, CP-R80.40-GW1-1, CP-R81-VSX1-2, PAN-FW2-10.0, PAN-FW-peer-10, Panorama-10.x-1, Panorama-9.0.2-203, Panorama-8.1.0-204

**PCI DSS 11 - Vulnerabilities**

Time range: 01/09/2023 08:34 - 01/09/2024 08:34    Issues: Resolved & Unresolved, Archived & Not Archived

Panorama-8.1.0-204
Panorama-9.0.2-203
illab-panorama02
PAN-FW7-10.0
PAN-FW1-10.0
PAN-FW-peer-10
Panorama-10.x-2
Panorama-10.x-1
FortiGate-V6_4.8-FW01
illab-panorama01
Fortinet-V5
FortiGate-V6_4_8-FW07

0    9    18    27    36

- Authenticated administrator can delete arbitrary system file
- Authenticated user command injection vulnerability
- Authentication Bypass in PAN-OS Management Web Interface (CVE-2022-0030)
- Authentication Bypass in SAML Authentication
- Buffer overflow in authd authentication response
- Buffer overflow in management server payload parser
- Buffer overflow in the management server
- Buffer overflow when Captive Portal or Multi-Factor Authentication (MFA) is enabled
- Cross-Site Scripting
- Denial of Service in PAN-OS Management Web Interface
- DOM-Based cross site scripting vulnerability in management web interface
- GlobalProtect Clientless VPN session hijacking
- GlobalProtect Portal PHP session fixation vulnerability
- Improper SAML SSO authorization of shared local users
- Memory Corruption Vulnerability in GlobalProtect Portal and Gateway Interfaces
- Missing XML Validation in PAN-OS Web Interface
- Nginx integer overflow may lead to information leak
- Nginx software upgraded to resolve multiple vulnerabilities
- OpenSSH software upgraded to resolve multiple vulnerabilities
- OS command injection in management server
- OS command injection or arbitrary file deletion vulnerability
- OS command injection vulnerability in FIPS-CC mode certificate verification
- OS command injection vulnerability in management interface certificate generator
- OS injection vulnerability in PAN-OS management server
- Panorama authentication bypass vulnerability
- Panorama context switch session cookie disclosure

## Use case 6: Automate easily forgotten maintenance tasks

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, device authentication for GlobalProtect VPN, IPSec site-to-site VPN, EDL validation, User-ID agent and TS agent access. 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 take action. Infrastructure Assurance also checks for valid licenses to ensure software license compliance whether it is for vendor support, hardware, software, or access to threat intelligence. Automating these maintenance activities can truly help maintain the health and performance of your firewalls.

## Use case 7: Automated troubleshooting

When an issue is detected, Infrastructure Assurance will automatically apply device-specific domain knowledge to the problem. It will analyze the problem to accelerate root cause analysis.

Let's look at a simple example: A firewall is unable to reach its EDL server. Before doing the actual troubleshooting, Infrastructure Assurance gathers the information it needs to perform effective troubleshooting, just like a human would. In this example, effective troubleshooting means understanding if a proxy is in the picture, what the service route gateway is, etc.

RESOLVED                ID: 19420

EDL(s) configured not reachable

Created: Oct 19 2023 18:12                    Updated: Oct 19 2023 21:35

AUTO-DETECT        AUTO-TRIAGE

**External Dynamic List not reachable**

External Dynamic List

testing-second_list                                              ⌄

                                                          ‹ 1 out of 1 ›
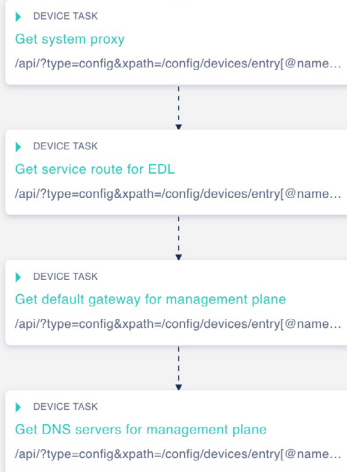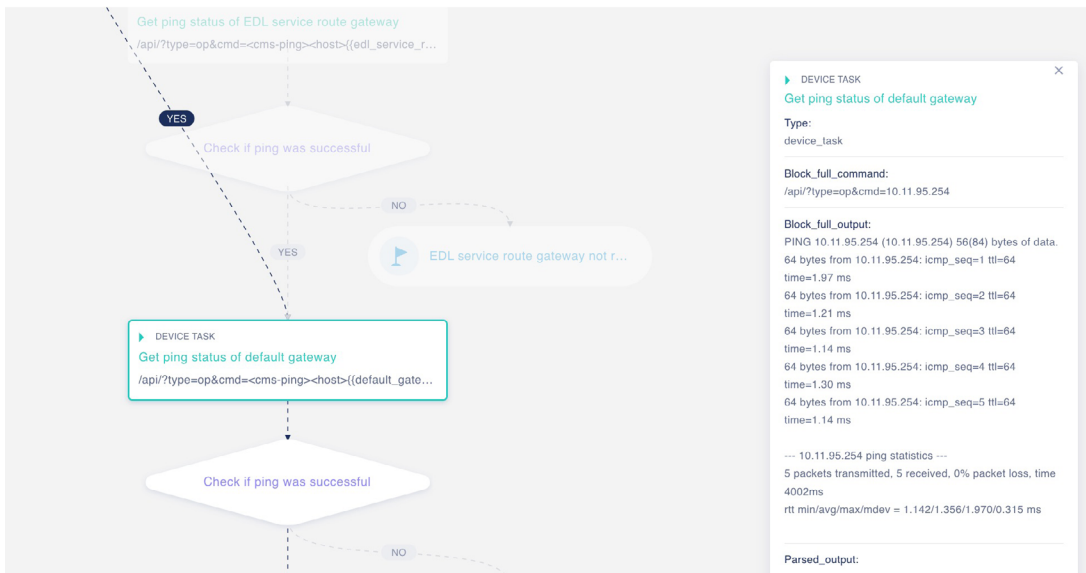
Issue Diagnosis

The DNS server defined in the system is not able to resolve configured URL into EDL testing-second_list.

Remediation Steps

Check if the DNS server is correct and/or change the DNS server to use an alternative DNS.

▶ DEVICE TASK
Get system proxy
/api/?type=config&xpath=/config/devices/entry[@name...

▶ DEVICE TASK
Get service route for EDL
/api/?type=config&xpath=/config/devices/entry[@name...

▶ DEVICE TASK
Get default gateway for management plane
/api/?type=config&xpath=/config/devices/entry[@name...

▶ DEVICE TASK
Get DNS servers for management plane
/api/?type=config&xpath=/config/devices/entry[@name...

To reach the EDL server, the first step is to make sure that the firewall can reach its EDL service route gateway. To do that, we issue a ping command from the firewall. You can see the output of the ping command being executed. In this case, the firewall can reach its service route gateway.

Get ping status of EDL service route gateway
/api/?type=op&cmd=<cms-ping><host>{{edl_service_r...

YES

Check if ping was successful

YES

NO

EDL service route gateway not r...

▶ DEVICE TASK
Get ping status of default gateway
/api/?type=op&cmd=<cms-ping><host>{{default_gate...

Check if ping was successful

NO

▶ DEVICE TASK                                             ✕
Get ping status of default gateway

Type:
device_task

Block_full_command:
/api/?type=op&cmd=10.11.95.254

Block_full_output:
PING 10.11.95.254 (10.11.95.254) 56(84) bytes of data.
64 bytes from 10.11.95.254: icmp_seq=1 ttl=64 time=1.97 ms
64 bytes from 10.11.95.254: icmp_seq=2 ttl=64 time=1.21 ms
64 bytes from 10.11.95.254: icmp_seq=3 ttl=64 time=1.14 ms
64 bytes from 10.11.95.254: icmp_seq=4 ttl=64 time=1.30 ms
64 bytes from 10.11.95.254: icmp_seq=5 ttl=64 time=1.14 ms

--- 10.11.95.254 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 1.142/1.356/1.970/0.315 ms

Parsed_output:

Knowing that the firewall can reach the outside world, the next step is to get the external IP address of the EDL server. To do that, we need to resolve the IP address of the EDL server. We factor if a proxy is applicable in the environment. In this example, it is not. We simply fetch the URL of the EDL server and resolve the IP address.
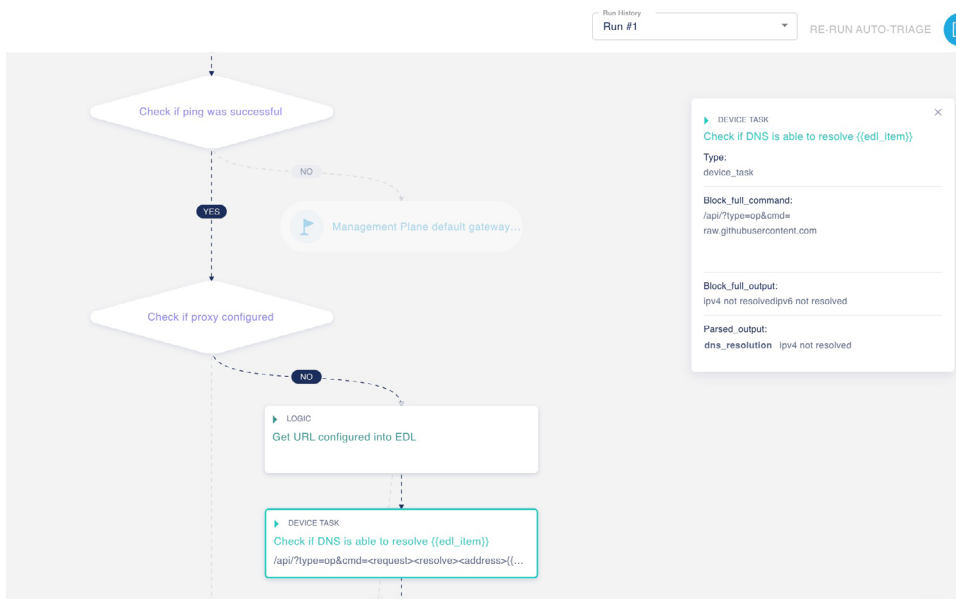
To ensure that we can resolve the IP address, we make sure that we can reach the DNS server by issuing a ping command. If we can reach the DNS server, we can safely conclude that the root cause of the problem is due to DNS resolution.
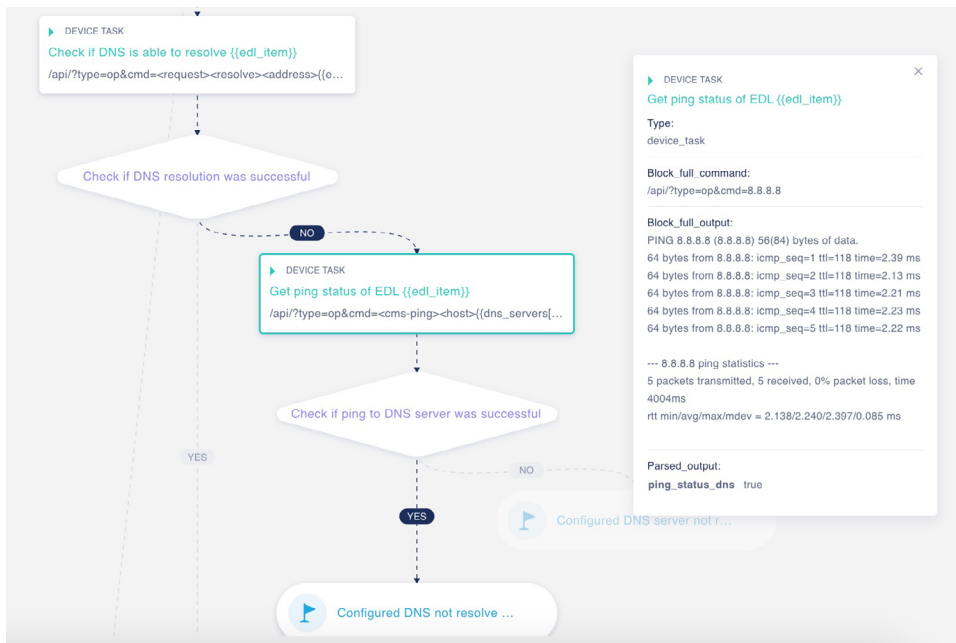


In this example, we are able to reach the DNS server but cannot resolve the IP address. Therefore, we can conclude that the root cause of the problem is due to DNS resolution.

It is not always possible for Infrastructure Assurance to determine the root cause of a problem. The goal is to capture the problem the moment it occurs. Doing so provides a better chance of collecting information about events and conditions that led to the problem so you don't need to re-create the failure. This is particularly useful for intermittent problems. Re-creating a problem can be difficult; worse, it is often not feasible.

# Key differentiators

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

1. The automation elements in this solution 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 provides a mechanism to bring 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 BlueCat Infrastructure Assurance as a solution for hidden issue detection and recommended remediation. They include:

- Achieve zero 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.

**Next steps**

Discover how BlueCat Infrastructure Assurance can reduce service tickets and avoid outages.

Request a live demo