ARISTA

Solution Brief

Arista CloudVision and Forward Networks Brief

Using Arista CloudVision and Forward Enterprise for Automated Network and Security Verification.

Overview

Network automation has numerous benefits for organizations adopting a DevOps model for managing their infrastructure, including speed, agility, and a consistent change control process. However, with improvements in speed, there comes an added risk of configuration errors rapidly propagating through the network. To safeguard against potential mistakes, network and security verification become an essential part of the network DevOps lifecycle. This paper outlines an approach to pre-change and post-change network and security verification using Forward Enterprise and CloudVision to continuously validate that the network is compliant with security and availability policies.

Key Benefits of integration

- Seamless integration into manual and automated change workflows
- Pre-change and post-change verification of network and security posture
- Continuous validation of network and security service availability

Introduction

Automation allows developers to rapidly adapt their applications to meet the ever-changing business needs. This creates tremendous pressure on the network engineering and operations teams that are asked to ensure the network supports constant updates without compromising security and availability. With the high velocity of change, it becomes critical to apply verification technologies both before and after applying changes to the network, to ensure that errors are not introduced into the network as part of the change control process. Having these verification tests in place allows operators to accelerate their network evolution by providing assurances that any changes being made are not negatively impacting service availability. By integrating Arista CloudVision® with Forward Enterprise, network operators can leverage the monitoring, change control, and configuration management of CloudVision, while using Forward Enterprise to execute pre-change and post-change network and security verifications.

FORWARD NETWORKS

Arista CloudVision

Arista CloudVision is a network-wide approach for workload orchestration, workflow automation, and real-time telemetry as a turnkey solution for Cloud Networking.

CloudVision's network-wide perspective delivers a more efficient approach for several operational and network telemetry use-cases:

- Centralized representation of distributed network state, allowing for a single point of integration and network-wide visibility and analytics
- Turn-key automation for initial and ongoing zero-touch provisioning, configuration management and network-wide change management, including automated upgrades, network rollback, and network snapshots.
- Compliance dashboard for security, audit, and patch management
- Real-time state streaming for network telemetry and analytics
- State repository, analytics engines, and telemetry apps to provide an unprecedented level of granularity in real-time monitoring and historic network state for forensic troubleshooting

Forward Enterprise

The Forward Enterprise platform provides network intelligence that makes networks more predictable, agile and secure. Forward Enterprise generates a vendor-neutral software abstraction (digital twin) that models the entire multi-vendor network infrastructure including switches, routers, firewalls, and load balancers, both on-premises and in the cloud.

With available REST APIs, it easily integrates into new and existing network management workflows.

Forward Enterprise enables network, security, cloud engineers, and operators to:

- **Search**: search network behavior, configuration, and state network-wide with an intuitive and powerful interface. Find any device in the network, including its connections and all forwarding behavior for fast root-cause isolation and incident remediation. Perform complete end-to-end path analyses across the network for both on-prem and multi-cloud infrastructure (support for AWS, Azure, and Google Cloud Platform).
- **Verify**: verify that the network is configured and behaving exactly as intended across on-prem, cloud, and virtual overlay networks. Set, verify, and customize policies for the entire network. Continuously audit the network and receive timely, actionable non-compliance.
- **Security**: enhance the network's security posture with automated security posture connectivity analysis, blast radius of compromised hosts, enhanced automated vulnerability analysis, and cloud security verification
- **Behavior Diffs**: side-by-side comparison in one quick view of configuration file and state changes for any device, between any points in time. Identify what policy rules and behavior checks have changed between snapshots. Quickly see new device connections, topology changes, and interface updates. Learn how routes are altered due to changes with the ability to filter results by VRF, next-hop address, IP destination, and more.
- **Network Query Engine (NQE)**: query the network like a database. Define and perform custom verification checks.
- **Predict**: understand the outcome of network configuration changes for ACL and NAT environments. Proactively identify potential connectivity and security policy violations.
- **Dashboard**: see key network insights with visualizations that are easily consumable and exportable.

CloudVision and Forward Enterprise Integrated Workflow

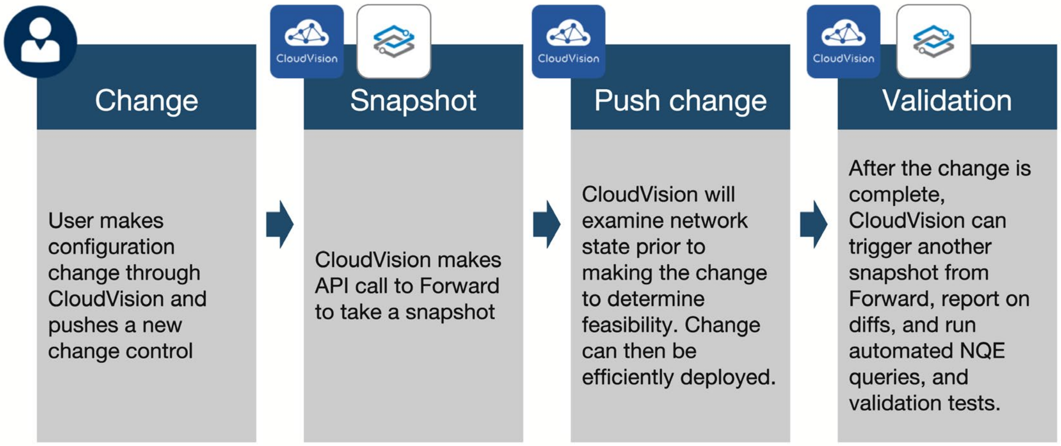
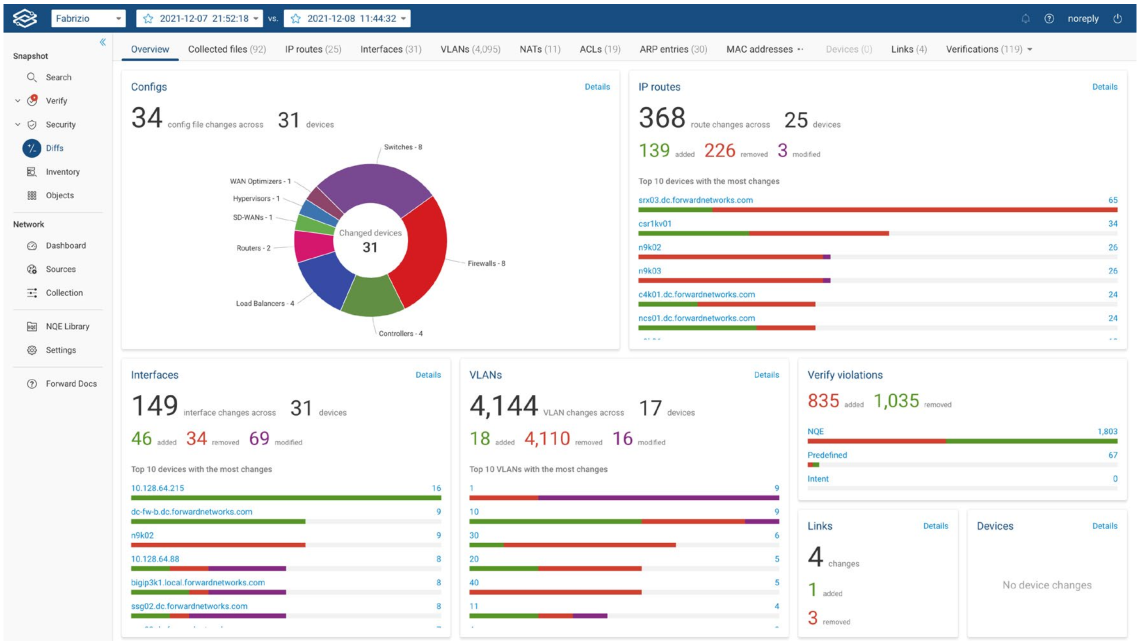

CloudVision
Change
User makes configuration change through CloudVision and pushes a new change control
Snapshot
CloudVision makes API call to Forward to take a snapshot
Push change
CloudVision will examine network state prior to making the change to determine feasibility. Change can then be efficiently deployed.
Validation
After the change is complete, CloudVision can trigger another snapshot from Forward, report on diffs, and run automated NQE queries, and validation tests.

Figure 1: CloudVision and Forward Integrated Workflow

With this CloudVision and Forward Enterprise integration, users get a turn-key network verification platform that fits into any operational workflow. Operators can prevent mistakes from propagating the entire network by using CloudVision to

- Provide a single pane of glass to manage device software and configuration.
- propose a change for one or more devices and analyze it to ensure it is feasible
- Request a new pre-change network snapshot from the Forward Enterprise platform using an API call
- Deploy the configuration change to the network
- Provide real-time monitoring of the network and track the configuration changes over time
- After the change is complete, send another API call to Forward Enterprise triggering another network snapshot and create a comprehensive report of the differences in the network between the pre-change and post-change. The Forward report includes configuration file and state, policy rules, behavior checks, device connections, interface, routes. Additionally, it will run automated Network Query Engine queries and validation tests.



Configs

34 config file changes across 31 devices

IP routes

368 route changes across 25 devices

139 added 226 removed 3 modified

Top 10 devices with the most changes

srx03.dc.forwardnetworks.com	65
csr1kv01	34
n9k02	26
n9k03	26
c4k01.dc.forwardnetworks.com	24
ncs01.dc.forwardnetworks.com	24

Interfaces

149 interface changes across 31 devices

46 added 34 removed 69 modified

Top 10 devices with the most changes

10.128.64.215	16
dc-fw-b.dc.forwardnetworks.com	9
n9k02	9
10.128.64.88	8
bigip3k1.local.forwardnetworks.com	8
ssg02.dc.forwardnetworks.com	8

VLANs

4,144 VLAN changes across 17 devices

18 added 4,110 removed 16 modified

Top 10 VLANs with the most changes

1	9
10	9
30	6
20	5
40	5
11	4

Verify violations

835 added 1,035 removed

NQE	1,803
Predefined	67
Intent	0

Links

4 changes

1 added

3 removed

Devices

No device changes

Figure 2: Forward Enterprise pre- and post-change report

Forward Enterprise is key to continuously ensure that the network is compliant with security and availability policies.

Call to Action

Please note that this is a beta version of the solution which is still undergoing further enhancements.

For more information, reach out to your Arista or Forward Networks representative.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989