FORWARD NETWORKS

USE CASE

Improve Network Operations and Security by Preventing Config Drift

What is Config Drift?

Network administrators use a “Golden Config” or configuration policy to ensure the network’s overall health, performance, and security. If this configuration is maintained, risk is minimized, and business continuity is protected. Unfortunately for most enterprises, gradual changes cause the network to “drift” away from the prescribed configuration, introducing risks to security and performance over time.

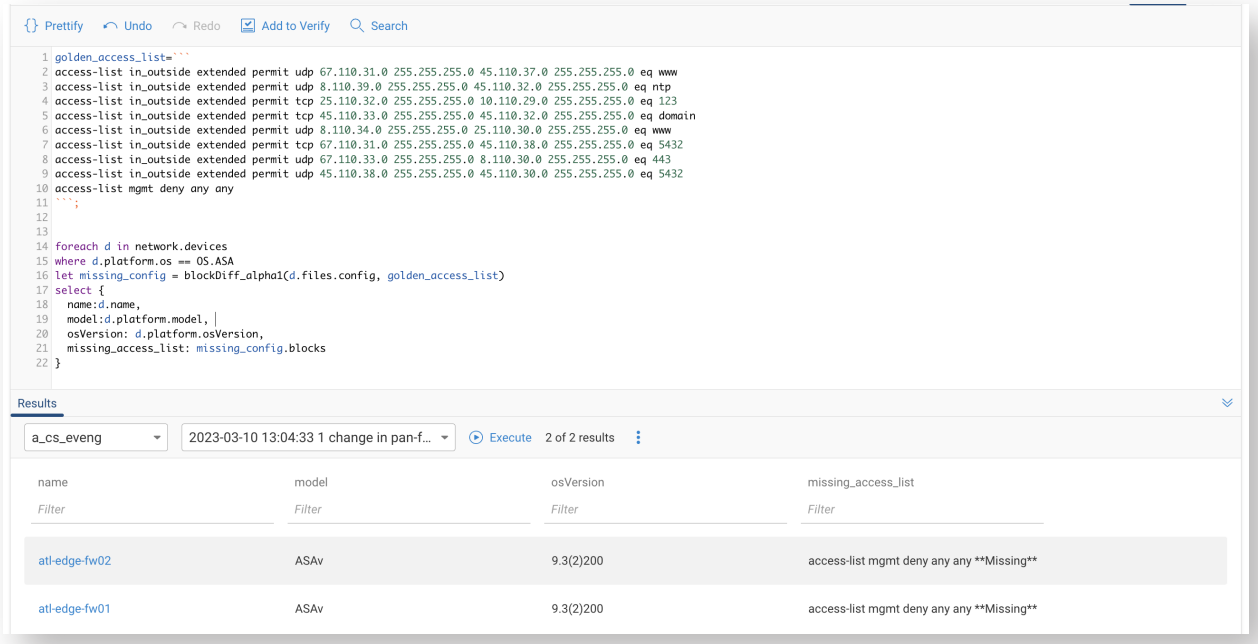
Enterprise networks are dynamic environments comprised of tens of thousands of devices from dozens of vendors that are constantly being updated or changed. Typically these changes are made by engineers seeking to solve a specific problem; they are done ad hoc and are often not recorded. Although highly skilled engineers make these updates to address a pressing issue, each represents an opportunity for errors that take the network out of compliance, potentially introducing serious vulnerabilities.

Preventing config drift is critical to network operations and security operations teams responsible for keeping the network safe and reliable. Config drift is frequently the cause of security breaches. The ability to verify changes adhere to the in-policy config is critical to ensuring performance, security, and even successful audits. But how do you do that when there are literally billions of lines of config in every network? IDC states that config drift identification and prevention “cannot be achieved by even the most conscientious of SOC analysts.” (Worldwide Tier 2 SOC Analytics and Cloud-Native XDR Market Shares, 2021: Rethinking the Cybersecurity SOC Software Stack).

Using our Digital Twin to Eliminate Config Drift with Mathematical Certainty

Software support is the only effective way to detect and remediate non-compliant configuration before it causes an incident. Our digital twin uses read-only access to collect configuration and state data from all traditional networking devices like switches, routers, firewalls, load balancers, SD-WAN, and software-defined elements like NSX and HCI. That data is then indexed and becomes searchable. Forward Networks is the industry leader in network assurance and intent-based verification. Our platform is designed to regularly collect detailed L2 – L4 and L7 state and configuration information from the network.

Using the Network Query Engine (NQE), engineers can proactively check for non-compliant configurations using custom searches or one of the hundreds of pre-built verification checks.



Network Query Engine highlights missing configurations

For an engineer using Forward Enterprise, this is what a reactive compliance audit looks like:

STEP 1: Use the Network Query Engine (NQE) to search the entire network just like a database. Devices can be searched by type, specific configuration, IP address, MAC address, and more with NQE. There are hundreds of pre-built verification checks loaded into the platform. Additionally, engineers can craft custom searches.

STEP 2: Identify the noncompliant configuration. Because NQE parses data and returns it in an intuitive, normalized data model, finding the cause of an issue is often possible in seconds vs. minutes and days using older methods.

After identifying the cause and resolving the issue, two easy steps turn a one-time troubleshooting mission into a proactive, always-on audit:

STEP 3: Using the query you just ran, create a verification check to ensure your desired network behavior and configurations are always in place.

STEP 4: Should an intent check fail, Forward Enterprise API integrations can send notifications and verifications to operations teams via Slack, Microsoft Teams, Cisco Webex, and email. API integrations with applications such as ServiceNow automatically generate tickets to remediate issues. Detailed information is shared between Forward Enterprise Platform and ServiceNow to ensure everyone is working from the same source of truth and to facilitate faster resolutions.

Preventing config drift in the modern enterprise requires teamwork, tenacity, and transparency. The Forward Networks platform enables all of the above by increasing visibility into the network, enabling continuous monitoring for issues, and breaking down silos across teams — from network operations to security operations to DevOps. Teams are empowered to access network information, do their own data calls, and move swiftly to pinpoint and address compliance issues in the network. And because the network snapshots that Forward Networks provides are read-only, there's no risk of users disrupting the network or introducing new security or compliance risks as they work to resolve existing ones.

A Single-Source-of-Truth for Network Configuration

Creating the "Golden Config" or stated policy requires significant time, thought, and resources. One hurdle to protecting the configuration is ensuring it's communicated clearly and correctly, leaving no room for misinterpretation. Using institutional knowledge, email, and outdated documents to communicate policy is a recipe for failure. Companies need a clearly defined, always-current, and easy-to-access single source of truth.

Forward Enterprise provides this by integrating with databases like NetBox, which store the correct approved configurations. By integrating with NetBox, the Forward Enterprise digital twin can regularly audit network configurations to detect deviation from the approved configurations (e.g., ACLs, NTP, Syslog, DNS).

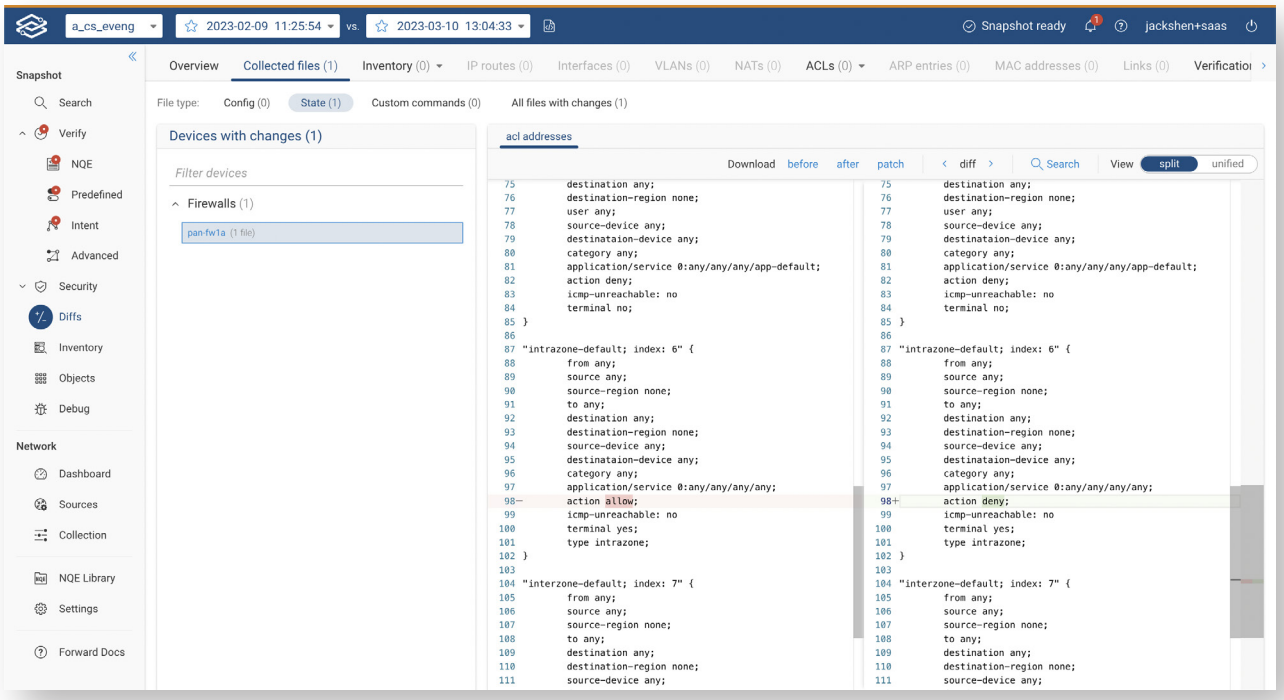
Automating ACL Compliance Checks Saves $800,000

In a network with 40,000 devices that each receive an ACL update once a month, Forward Enterprise can reduce costs by $800,000 by saving engineering time. Assuming each device requires 1 minute to review, Forward Enterprise eliminates 8,000 hours of work.

Compare Network Changes Daily, Use the Diffs Feature to Effortlessly Detect Non-Compliance

The only constant in a network is change, but how do you keep track of that change and ensure that it's not creating risk? The Forward Enterprise digital twin takes network observability to the next level by collecting and storing snapshots of network configurations once a day (or on your preferred schedule).

The diffs feature in Forward Enterprise compares the two most recent snapshots and highlights configuration changes with granular detail as to what change was made. Doing this regularly provides a historical network configuration analysis and can be used as proof of compliance during an audit.



Forward Enterprise Diffs feature highlights changes between snapshots

Keeping BDDS appliances in policy

There are approximately 4,000 Bluecat BDDS appliances deployed at the Bank. Each device has a unique configuration (e.g., security, NTP, Syslog, TACAS+). These devices control DNS, DHCP, and IPAM, so they must work properly.

Unfortunately, prior to Forward Networks, detailed monitoring the configuration of these devices over time has been nearly impossible due to the number of devices and complexity. Although there was consensus that tracking changes in the configuration was vital, there hasn't been a reliable method to do so.

Using the diffs analysis, the bank now collects configuration on all BDDS appliances every night and compares them to the previous day's snapshot. Detected changes are sent to the appropriate team to review. Should they discover a mistake, they can immediately correct it.

As an added benefit, the snapshots become a backup in the event it's necessary to "roll back" the network, saving time, money, and stress.

Protect your configuration and ensure policy adherence with a Network Digital Twin

Our mathematical model creates a complete and always-current digital twin of your physical, virtual, and multi-cloud network estate, including config and state information for all devices. The digital twin provides a complete view of all network behavior, with visibility into every possible path in your network.

VISUALIZE network layer 2 – 4 topology and all possible traffic paths within a single-pane view for on-premises, cloud (AWS, Microsoft Azure, and Google Cloud Platform), and virtualized environments. Then, drill down to specific devices and traffic flows, including configuration and state data.

SEARCH the network as simply as a database. Our browser-like search feature performs complete end-to-end path analyses across the network for both on-premises and cloud infrastructure. This enables you to locate devices and access detailed information on their location, configuration, and state in milliseconds.

VERIFY that the network is in-policy and working as intended using purpose-built (custom) or existing intent checks. Continuously audit the network and receive actionable alerts for config drift.

COMPARE network changes over time to understand their impact and prevent incidents from reoccurring. The network collector frequently scans the network taking and saving snapshots of network configurations, topology, and device state. These “snapshots” become a searchable historical record of network behavior and compliance at any point in time. And the behavior diffs feature makes it easy to quickly find and compare snapshots

to identify changes that may violate your network policy.

See for yourself how the verification feature in the Forward Enterprise platform can help operations professionals protect their network configurations. Please request a demo to see this feature and the power of a network digital twin.

ABOUT FORWARD NETWORKS

Forward Networks is revolutionizing the way large networks are managed. Forward's advanced software delivers a "digital twin" of the network, enabling network operators to verify intent, predict network behavior, and simplify network management. The platform supports devices from all major networking vendors and cloud operators, including AWS, Azure, and Google Cloud Platform.

Forward Networks was founded in 2013 by four Stanford Ph.D. graduates and is headquartered in Santa Clara, California. Investors include Goldman Sachs, Andreessen Horowitz, Threshold Ventures, and A. Capital.