DATA SHEET

Technical Data Sheet

Overview

Forward Networks industry-leading verification platform, Forward Enterprise, analyzes and verifies network behaviors and security posture, to proactively surface configuration errors and policy intent violations. The platform can compare the intent of the network designers to actual end-to-end behavior in order to expose any inconsistencies. Network IT teams can now obtain quick access to relevant network data to troubleshoot rapidly and eliminate problems prior to a security breach or a network outage.

Forward Enterprise shifts the focus from a purely reactive approach to troubleshooting to a proactive approach of network assurance and verification. Get away from tedious, manual device-specific processes, to automated end-to-end verification in minutes. Other key benefits include the ability to certify that proposed changes are compliant with existing policies quickly before going live, and increasing the overall responsiveness of the IT team to change requests and network updates.

In addition to traditional on-premises networks, Forward Enterprise provides unmatched flow visibility and behavior verification for private, hybrid and public multi-cloud environments.

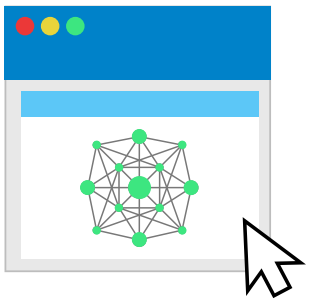
Why Forward Networks:

VERIFICATION IS KEY:

Intent Based Networking (IBN) is one of the most interesting and significant trends in IT in recent years. IBN automates the configuration of networks to align with administrators' high-level intent, as well as the analysis and remediation of network issues. Nearly all successful IBN deployments today are focused on the verification process. The ROI benefits are immediately tangible because verification helps reduce tedious network implementation processes and provides a boost to business agility. Verification is now fully capable of shifting the network IT model from a reactive to a proactive approach where an automated analysis of the current network implementation can virtually eliminate human errors and mis-configurations. Verification automates the key IT processes such as:

- Root cause analysis and reduce MTTR for trouble tickets
- Compliance and Audit related tasks
- Change window validation and post change verification

MATHEMATICAL MODEL:



To reason about network behavior, a system needs an accurate working model of the complete network, incorporating how each device responds to every possible packet. It is referred to as a mathematical or behavioral model of the network because each network device is modeled as a transformations function on a set of potential packets. The transformations are essentially algebraic or logical operations that, when analyzed end-to-end, can verify the complete network design against required policies or behaviors. A mathematical model, as opposed to monitoring or testing live traffic, can perform exhaustive and definitive analysis of network implementations and behavior, including proving network isolation or security rules compliance.

Every application that Forward Enterprise provides is built on the mathematical model. The model forms a deep analytical engine of the Forward platform. Forward Enterprise is the first highly scalable, multi-vendor network verification solution available today. The sophistication and scale of its mathematical model allows for completely new analytical and verification features compared to existing network management, monitoring or analysis solutions. The automation of key IT processes for remediation, analysis and change verification makes it an ideal solution to complement any network automation project and to return an immediate ROI to large enterprise organizations by reducing manual IT efforts and reducing the risk of network outages.

Architecture

Forward Enterprise collects device configuration and state information from every networking device that includes switches, routers, firewalls, load balancers, cloud instances etc. Forward Network then emulates the behavior of the entire network by creating a digital twin of the network that discovers potential configuration anomalies, risk exposures, policy violations among the many other things.

DEPLOYMENT OPTIONS:

- Forward Enterprise can be deployed on-premises or as a SaaS solution in the Forward cloud.
- Network requirements: SSH must be configured and working on the network devices from which the Forward Collector will collect data.
- The OS instance on which the Forward Collector is installed must have IP and SSH port reachability to the network devices, either directly, or via a jump server.

On-premises deployment requirements:

- Forward Enterprise is deployed as a Virtual Machine (VM-OVA format) for KVM and ESXi environments. The deployment requires the following resources (for up to 1000 network elements):
  - Cores: 16
  - RAM: 128 GB of reserved memory. Performance may improve with more memory availability, but only when individual snapshots are large.
  - Disk: 250 GB of disk. The amount of disk consumed will depend on the number of historical snapshots to be stored, as well as the size of each one.

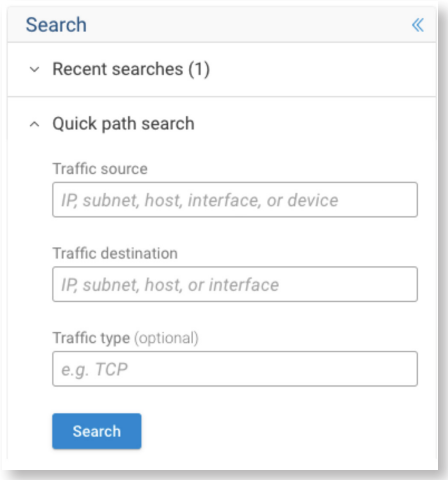
Note: For more than 1000 elements, requirement varies

SaaS deployment requirements:

- A machine (virtual or physical) with at least two dedicated cores and 4GB of RAM.
- Supported Operating Systems: Ubuntu Linux (14.04 and 16.04), Apple Mac OS X (10.12 or later versions), and Windows 7 (or later versions). The machine must be able to access the https://fwd.app web page via HTTPS.
- The user must have admin privileges on the machine.
- The latest versions of supported browsers: Chrome, Edge (Chromium-based versions only) or Firefox and Safari (Mac only) are required to access the Forward Enterprise UI.

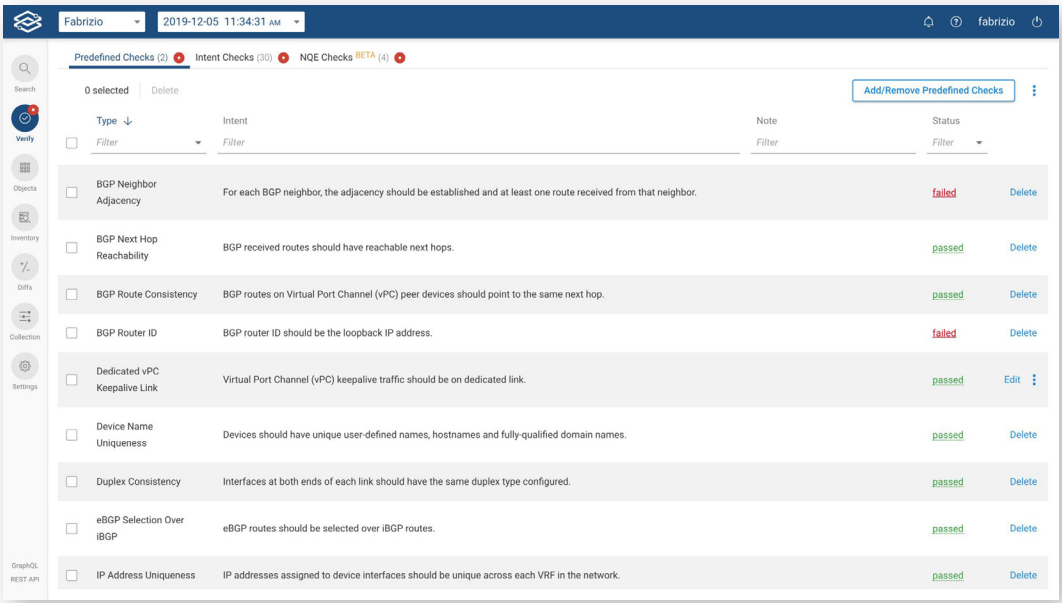
Key Applications:

FORWARD SEARCH



- A powerful search engine for your network.
  - Search feature is fast and easy It finds all possible network information from the always-up-to-date digital twin of your network across tens of thousands of devices within seconds.
  - The search engine comes handy in finding key information such as IP address (host or subnet or range), MAC address, VLANs, VRFs, Security zones, Multicast groups etc.
  - It also allows searching free form text of a particular configuration or text file. Certain patterns such as wild card search, fuzzy words, phrased queries etc. are among the key methods available to the search engine.
- Topology that gives clear understanding of network map and documentation
  - The enhanced topology view gives users an ability to understand how each section of the network is connected to each other. It supports both on-prem and cloud network topology.
  - Upon collecting the state and configuration of all the devices, Forward Enterprise creates the digital map through a powerful feature called link inferences.
  - Users have the ability to maintain the diagram in a way they like by rearranging the device layout.
- Path Search to visually represent end-to-end network behavior
  - Enhanced end-to-end communication behavior analysis that helps users gain important insight about their traffic flows.
  - It helps understand things such as alternate paths, hop by hop analysis, sample packet etc.
  - Path Search advanced capabilities can help understand communication from a source to destinations, correlation between network's underlay and overlay etc.

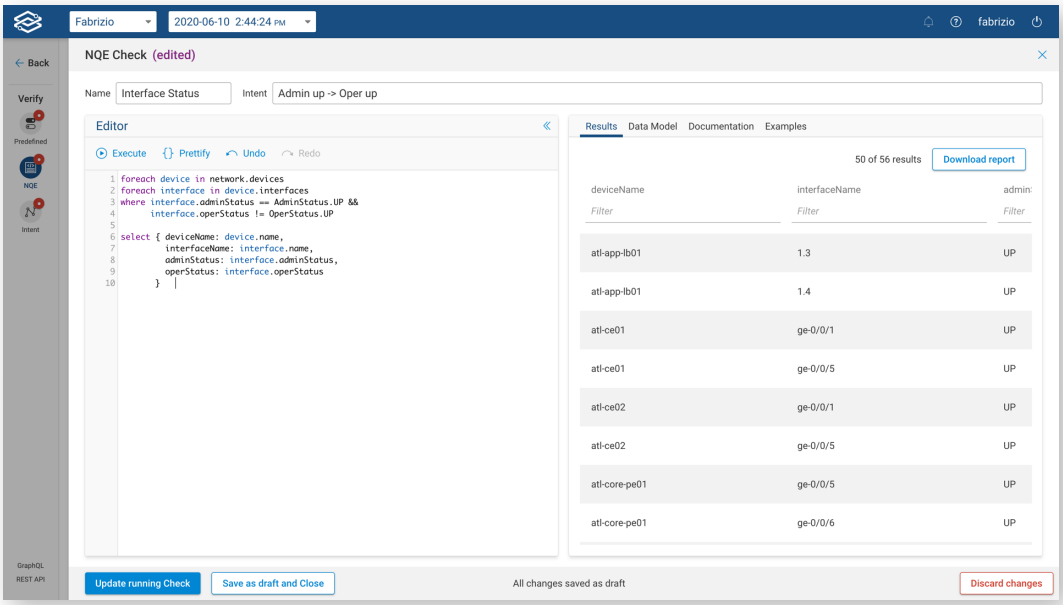
FORWARD VERIFY



- Intent based network verification made simple through Forward Verify
    - Predefined checks - Forward Enterprise comes with a list of predefined verification checks from L1 to L4 to verify network hygiene.
    - Intent checks - Users can create their own intent based verification checks through defined path search for existing path, or isolated path or reachability to a specific host/ destination.
    - Network Query Engine (NQE) checks - Users can create queries that will return normalized structured state and configuration data across different vendors.

In addition to the above verification types, Forward Verify comes with a capability of integrating the intents to workflow systems such as ServiceNow.

NETWORK QUERY ENGINE



- A robust mechanism to retrieve any information from the network

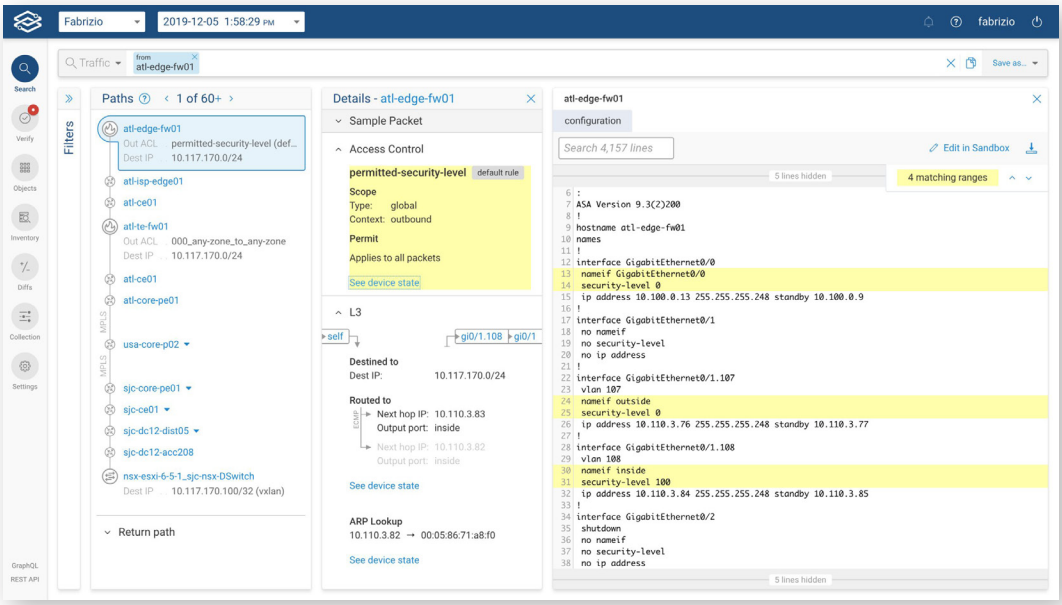
  - Network Query Engine is unmatched to any other in the industry which can be leveraged for many purposes such as finding the relevant information quickly, validating intents by writing simple condition checks etc.

  - Network teams often need to collect and parse devices output to gather some insights from the Network, implement specific verification and sanity checks or as part of their network documentation. These scripts collect state and/or configuration from every device in the network and then need to partially parse the gathered text files (typically text is the only “API” on these devices) to implement the checks or build documentation. Building and maintaining tools that collect and parse device output across the broad range of devices, OSes, and features found in enterprise networks poses a significant burden for Network Teams.

  - With the introduction of Network Query Engine (NQE), Forward Networks removes this burden by providing access to normalized structured data about the network, enabling the network teams to focus on the higher-level aspects of their use cases, which is actually making their networks more resilient, agile and robust without spending time writing collectors and parsers.

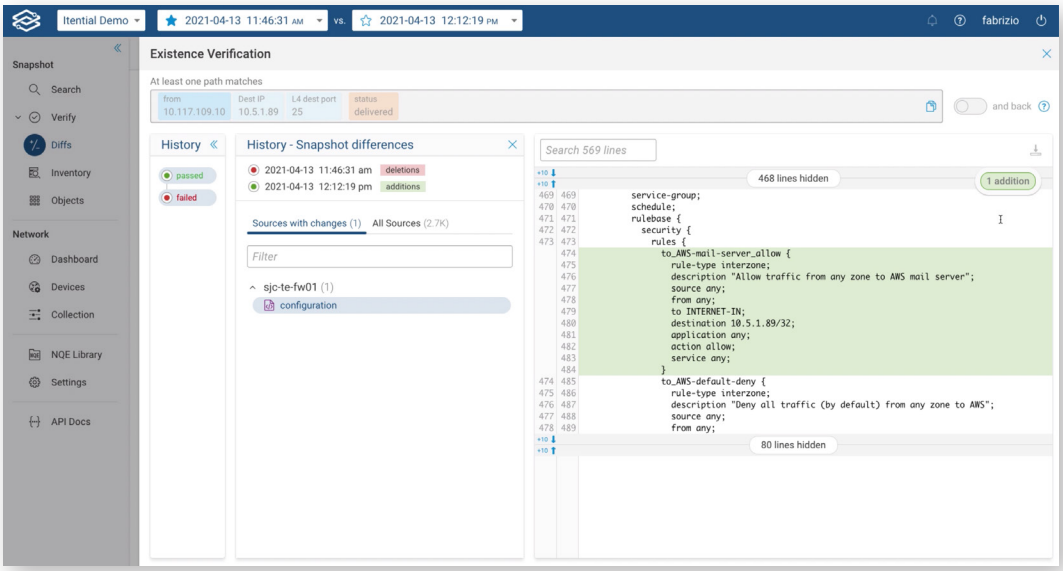
  - Forward Enterprise comes with a pre-populated list of queries stored as Intents for the smooth operation of Day 2 Networking.

FORWARD PREDICT



- Be proactive by understanding an impact of a change beforehand.
  - Forward Enterprise's predict capabilities will allow users to do sandboxing of certain network changes to understand the impact on the overall network behavior.
  - This feature can be very helpful in implementing quick changes and performing end to end impact analysis with limited time which makes users confident in the production deployment.

BEHAVIORAL DIFFS



- Validates all the changes in design and behavior
  - Behavioral diffs enables network operators to gain visibility into changes that have occurred in the network between two configurable points in time.
  - The analysis reduces the Change Management Window time and faster the updates in the network. It also helps in diagnosing and troubleshooting the issues that are related to the new changes implemented in the network.
  - It surfaces what has changed at different layers in network stacks beyond simply highlighting the text-file diffs.

FORWARD SECURITY

Security Posture Analysis

- Network zones are secured based on the policies implemented between them for allowing or restricting communications. The security posture analysis provides inter-zone connectivity details throughout the network.
- This single pane of glass view can help security engineers understand if there are any loopholes in the policy that are overlooked. The graphical matrix can tell whether given zones are fully connected, partially connected or fully isolated from each other.
- Forward Enterprise analyzes connectivity between various zones configured on devices and defines the connectivity that clearly indicates if the it exists fully or partially or does not exist due to policy or routing.
- On Day-1 of deployment, Forward Enterprise will present a sample security matrix that shows the connectivity status between zones. Users will have the ability to define their own matrix.

Blast Radius Analysis

- Blast radius analysis identifies and isolates the reachability of a compromised host from a security attack with just a one click.
- It does provide analysis of which L4 ports can be reached over what protocols so that the security engineer can understand the scale of exposure.

Device Vulnerability Analysis

- The device vulnerability analysis uses information provided by NIST National Vulnerability Database to identify the devices that are vulnerable.
- It displays the information in an actionable format so that the operation team can utilize their time fixing the vulnerabilities more efficiently.
- Furthermore, the analysis is provided in a vendor agnostic fashion which ensures the heterogeneous networks are covered for this capability.

Supported Vendors and Devices

Forward Enterprise supports over 456 device types and more than 1479 OS versions across 19 different vendors, including:

Cloud support (client virtual devices hosted in cloud platforms):

ABOUT FORWARD NETWORKS

Forward Networks' mission is to de-risk and accelerate network operations, by increasing efficiency, reducing outages and verifying network intent. Built on a series of breakthrough algorithms, the Forward Platform provides enhanced network visibility, policy verification and change modeling for legacy, SDN or hybrid environments.

Forward Networks is headquartered in Palo Alto, California, and funded by top-tier investors, including Andreessen Horowitz, DFJ, A.Capital, SV Angel, and several luminaries in the networking and systems space.

FORWARD NETWORKS