The eight most common use cases for the Forward Platform

Forward Networks has created a revolutionary platform for analyzing network behavior and quickly isolating potential misconfigurations. The platform can compare the intent of the network designers and all application and compliance requirements to the actual behavior currently in place. The benefits of the Forward Networks solution are so broadly applicable to network administration and IT operations that it’s helpful to highlight several of the top use case scenarios that our customers in order to better learn about the product.

In this white paper, we describe eight of the most common use cases including documenting network behavior, automating root-cause analysis, accelerating network change windows, creating compliance checks, to diagnosing complex network faults. Several of these use cases dealing with verification of network policy and intent are key aspects of intent-based networking, a next-generation vision for automating network analysis and remediation.

Use Case #1
Network Documentation and Topology Diagrams

Using Forward Networks, it’s easy to maintain an always-up-to-date set of network documentation, topology diagrams and configuration files, e.g. a configuration management database (CMDB) (see Figure 1). Network admins universally have a problem maintaining a usable form of network documentation for them to analyze, maintain or update their networks. The problem is a result of having more than one “single source of truth” about the network.

In banking, for example, the source of truth for all account information is the live transactional accounts database. Although live transactions are updating by the microsecond, it is the only source of truth for accurate account details and amounts. There is no back-up ledger or paper trail. A second source of truth would be too slow and eventually worthless, as well as too expensive to try and maintain.

In networking, we have large networks whose behavior is orders of magnitude more complicated than a bank accounts ledger. The distributed device configurations and network state are too complex for a network engineer to work with. A second source of network documentation and truth must be maintained. Naturally, as the pace of network change becomes more frequent, the network documentation is never current. Whether you are using
spreadsheets, Visio diagrams or other network documentation tools, it is either tedious to maintain and keep current, or they become useless for diagnosing issues in real time.

Forward Enterprise solves this problem by integrating current network configurations and state into a documentation, topology diagramming and audit tool. Forward Enterprise becomes your always-up-to-date, human readable, single source of truth for all things networking. On top of this, we also enable an analytics and search engine to quickly isolate potential problems or network violations, adding the intelligence of a network expert to the network diagrams and documentation.

Figure 1. Portion of a large network topology diagram created by Forward Networks
By providing the IP addresses of your network devices, Forward Enterprise collects device configurations and state from each device. We quickly understand how devices are connected, subnets defined, routing tables are created, and how network paths are determined. We then can create an up-to-date network topology diagram. We can also quickly search and analyze configuration files on a particular device in order to drill down on specific issues (see Figure 2).

Figure 2. Drilling down into a topology diagram allows users to see all details on individual devices and connections.
Want to see an inventory list of all your devices? It’s quickly accessible from the inventory tab. From here you can see all the device details, connections, and latest configuration information (see Figure 3).

For the first time, network engineers have a centralized, searchable repository of all network information that can be used for training, diagnostics, maintenance or audit purposes. A usable single source of truth at your fingertips, with a powerful user-interface to quickly identify the information that you need.

Figure 3. Easily generate an inventory list of all devices, VLANs, etc., and centralizes configuration details.
Use Case #2
Maintaining Consistency in Basic Network Configurations

Forward Enterprise helps organizations automate the elimination of most common network configuration errors. Such configuration parameters can cause unexpected incompatibilities between devices and connections, and are particularly difficult to diagnose and troubleshoot.

Examples of such device configurations are duplex type, link speed, maximum transmission unit (MTU), as well as IP address uniqueness, consistent VLAN definitions and elimination of forwarding loops. Many of these can result in intermittent problems or in more serious network downtimes, and isolating the root cause can be like looking for a needle in a haystack across a large network.

With Forward Enterprise, we create a behaviorally accurate software model of your current network. This model can be easily analyzed to identify silent configuration issues and potential points of network failure or incompatibility. We call this process verification, which is verifying the accuracy and risk-free nature of the network implementation against intended policies.

All of the basic network configuration errors just mentioned are covered in a series of pre-defined checks that the Forward Enterprise includes and evaluates (see Figure 4). By comparing current network configurations and state with these policies, we can immediately identify any misconfigurations. If device links are consistent on both sides of the connection. If VLAN definitions are consistent. If duplicate IP addresses exist, or if there is a possibility of forwarding loops in the network topology.

Figure 4. General network policy requirements can be regularly checked to quickly identify issues and avoid network problems, with saving IT admins tens of hours in troubleshooting.
Use Case #3

Accelerate Network Diagnostics with End to End Path-Based Analysis

Figure 5. Forward Enterprise shows allowed paths through the network that match the policy or search query. We can explore paths device by device to quickly identify root-cause issues.

Perhaps the most widely used feature of Forward Enterprise is the ability to analyze network and security policies as a series of end-to-end paths, rather than troubleshooting network devices individually, hop-by-hop. In the real world, network policies are really the definitions of which traffic should flow along which path, including which traffic should be blocked, the priorities for various applications and quality of service, as well as isolation of subnets and virtual overlays.

If most real-world policies are defined by full path behavior, the problem for network admins is that network configurations and testing is done on a box-by-box basis. The configurations and state of a particular device does not have the visibility or information of the flow packets are going to take through the entire network, so they provide little insight into policy-related behavior. The traditional tools that network specialists have used to test traffic patterns are crude at best, such as ping and traceroute. But to identify why a ping test may be failing reverts back to looking at each device individually with little insight as to the root cause.

Let’s look at an example how we can better understand network behavior and compare it to our intended policies with this approach. In Figure 5, we have initiated a query in the top bar with colored blocks that connects a source and destination address using an MPLS network. The system responds with a set of 256 viable paths (in this example) that meet all query conditions.
through the network, of which one is selected. The selected path shows each of the devices in
the flow, using a vendor neutral language, so we can quickly understand how configurations
affect this specific path and policy.
All network services at Layer 2, 3 and 4 are included in the analysis, including hosts, firewalls
and load balancers. At any selected device, we can quickly bring up the specific configuration
details that are implementing the shown network service, such as L3 routing or a firewalls ACL
rules to further examine any anomalies (see Figure 6).

![Fabric details example](image)

**Figure 6.** Quickly display the configuration details for a particular service on a particular device selected from the
traffic flow under consideration, in this case L4 ACL rules on a edge firewall.

In the above Figure 5 example, with more than a dozen devices in the traffic flow, over multiple
protocols and services, with both underlay and overlay networks involved, diagnosing policy or
performance issues between these endpoints could take hours to several days. Forward
Enterprise can frequently cut that analysis time by 90% or more with the ability to quickly
understand and display the possible behaviors that this network currently supports and where
they may deviate from intended policies.
Use Case #4

Accelerate, Reduce Risk and Adverse Impacts of Change Windows

In a network change window, network devices are updated with new policy or application requirements or upgraded to a new software version. Depending on the nature and extent of the change, this can introduce a great deal of instability and risk into the network. This is due to a general lack of time to thoroughly test network changes under all conditions at scale, and a limited amount of adequate testing tools available in lab networks. In fast paced DevOps environments, where software and builds can be developed and pushed out in a single day, even more pressure is placed on network teams to support agility and rapid deployment processes, without the same degree of network automation.

Until now, there has never been a way to efficiently validate a complex policy change implementation before it goes live for Monday morning. Forward Enterprise changes that with our intent-based verification platform. Forward Enterprise replicates complex networks accurately in software, providing a platform to fully evaluate the impact of changes before they are pushed live. And it does it by going beyond limited test scenarios that are possible in the lab to include complex policy rules and evaluates for all possible conditions.

Verification doesn't rely on specific tests, but is a comprehensive evaluation of the end-to-end network behavior, identifying scenarios that could cause potential issues, and quickly flagging the specific configurations, all before your changes go live.

In Figure 7, we show a number of network intents or policies that must hold true for all deployments. For large enterprise networks, these could easily reach into hundreds of rules or more. Prior to pushing any change to the live network, Forward Enterprise shows specifically which rules could now possibly be violated. In this Figure 7 case, incoming internet traffic is allowed to reach application servers on ports other than 443 for secure HTTP, as shown in the bottom alert. Since this violates our intended policy, we would remediate this failure before pushing network changes live or diagnose the issue with guidance if it was detected in the live network.

At the pace of today’s network changes and requirements for business and application agility, network IT teams just don’t have the time or tools to perform this level of analysis. Or if they do, change windows can take weeks after high-level peer reviews of proposed changes and detailed but usually insufficient lab testing. With Forward Enterprise, customers are seeing change windows and associated analysis and testing times reduced by 60-90%.
### Use Case #5

#### Troubleshooting based on Historical Diffs

![Figure 7](image-url) A series of custom policy policies that matches a specific customer’s network requirements. These policy rules are easily created from topology diagram and search filters.

Troubleshooting network issues, as we have discussed earlier, is complicated by the fact that it is so difficult to find the single source of truth for network design, configuration and state details outside the live network (which is rarely accessible or useful for analysis anyway). Any offline documentation, like a Visio diagram, is rarely up-to-date and likely doesn’t represent the snapshot in time that may be of interest in isolating a network problem. So, how do you find out what is really going on, or go back to what may have been going on, when things may have worked correctly? When changes have to be made fast, documentation and historical state details can be lost, or at least go undocumented. How do you easily roll back to a known “good state” if things do start to go wrong as a result of a network change?

Forward Enterprise works by collecting frequent snapshots of the entire network implementation: configurations and state information, and organizing the details into a
behaviorally-accurate software model of the network. From these archived snapshots, we not only can go back and evaluate network behavior at any point in time, say to when things weren’t broken, but also highlight the configuration diffs between any prior state and the current state. We immediately see if at a prior point in time the behavior was the same, or quickly isolate what changed that could have resulted in the change in network policy.

Network issues can now be resolved in a fraction of the time. And for compliance and reporting purposes, you always have an accurate historical record of then-current policies, as well as way to evaluate potential behavior if rolled-back to a prior state. Many times, the policy violation will be highlighted immediately if it triggers a violation of one our pre-defined checks or custom rules as part of our Forward verification process.

Starting from the example we laid out in Figure 7, for example, in Figure 8 we show how we can pull down a list of saved network snapshots to compare with. If we have reason to believe that a particular policy violation was not an issue at a prior state, we can revert back in our software model, replay the tests, and compare diffs to highlight the problematic changes.

![Figure 8](image)

**Figure 8.** Users can run policy checks against any prior network state to identify when an issue arose, and quickly highlight the changed configuration between historical snapshots that could have led to the issue.

*Use Case #6*
Democratizing Network Information, Enabling Application Team Self-Service

Nearly every organization has a certain amount of finger-pointing between application teams and network teams. When performance or access issues arise, application teams are quick to blame the network, largely because they typically have no visibility into network implementations or ways to diagnose communication issues. Too frequently the onus is on the network team to waste time to prove innocence or verify that it’s really an application issue.

The underlying problem is less with communication and trust issues between teams, but that nobody, not even the network team, has an efficient way to quickly verify network behavior compared to the defined or desired policies. Large networks are also too brittle and complex to allow anyone outside the network team to inspect or analyze network behavior, or understand it. This leads to too many trouble tickets, many of which are misdirected, and delays in remediating valid issues.

Forward Enterprise is the ideal platform to reduce the Mean Time to Innocence (MTI) for the network team with an efficient way for non-networking teams to query network behavior and policy implementations themselves. We have heard this called Democratizing network information, or for the first time busting down organizational silos and easily sharing details of the network across the organization.

Forward Enterprise also makes it easy to verify if any specific policy is currently in place, or to define new queries for any new scenario that may be required, even without networking expertise. Finally, if the Forward Platform dashboard is not ideal for socializing network information, API calls to Forward Enterprise can display the required details in any enterprise system or external application to better access the required network details.

For example, it would be simple (and safe) to give access to application development teams to the dashboard shown earlier in Figure 7, to verify that all of their policy requirements are being met. Other views could verify connectivity between end points or servers under required conditions on the topology diagram as well. If new policies are required for a new application, those policy queries could be easily built and tested against current network design by the application team before requesting evaluation and modifications by the network team.
Use Case #7

Evaluate New Network Requirements with Custom Policy Verifications

Perhaps not so much a separate use case as a key feature, Forward Enterprise allows organizations to easily build customized policy rules that are continuously verified in the network design. This was alluded to at the end of the prior use case. These policy checks are built from the simple building blocks and the interactive topology diagram in the form of queries that are verified in the network. If the network implementation no longer supports the policy under all possible conditions, the violation is flagged, and the offending devices or configurations are highlighted for analysis and resolution.

The process begins when a new application or compliance objective introduces a new requirement on the network. Examples of policy rules might be that there are no possible paths allowed to a database server except from the set of application servers, or it might be that there are at least four possible redundant paths between two critical end-points for quality and availability. The rule is built in the intuitive user interface, and subsequently verified against all future network updates and device configurations. Examples of custom policy checks that could be developed are shown in Figure 7.

For a large network, it’s possible to ensure hundreds of sophisticated policy requirements are enforced at all times without tedious manual testing. If a network update happens to conflict with a years-old policy requirement that was not deemed to be related when reviewed by network experts, it will be immediately flagged in Forward Enterprise and the conflicting configurations can be quickly resolved.

As a result, organizations can avoid nearly all unanticipated network outages caused by policy violations, and proceed through network change windows with confidence and considerably less testing and manual oversight. This feature is a critical component of other use cases described earlier, particularly #4 and #6 where organizations are looking to de-risk and accelerate their change processes, as well as allowing application development teams or other non-IT organizations to validate the current network design and policy implementations with new requirements.
Use Case #8
Modeling and Verifying Possible Network Updates

Again, we have a primary capability that's important to highlight that is closely related to the earlier use case of verifying network changes before they are rolled out into the live network. In Forward Enterprise, we call this feature Predict. Predict gives you the ability to evaluate potential changes in a software model of your network to ensure that you are not introducing any risk or policy violations.

Figure 9. Once soft changes are made in our safe sandbox, Forward Enterprise can verify that the new configurations don't violate any existing policies or network intent prior to moving them to the live network.

The possible changes are validated against all of our pre-defined policy rules, as well as the customized policies for our particular network. The edits to configuration files are made in a safe sandbox, so you can evaluate the impact of any changes before pushing them live. A great example of this scenario is adding or deleting firewall rules. Changing firewall rules can impact seemingly unrelated applications and services in ways that may not have been documented or are easily forgotten. Many organizations never delete firewall rules that were supporting decommissioned applications and servers for fear they could break some other service in ways they cannot check or test. As a result, firewall rules tend to grow unbounded.

With Forward Enterprise, you can predict and verify any changes, giving you control back over your network, with perfect insight into the implementation and resulting network policies. For example, let's say that we are making edits to the firewall configuration details shown in Figure
6. We make two edits to remove ACL rules for HTTP and SSH. How do we know that doesn’t affect another application or violate another policy?

As shown in Figure 9, we can select “Analyze changes”, and rerun our policy checks against the new configurations. We will immediately be notified if the changes introduced any other issues and why.

**Summary**

Forward Networks has delivered the first behaviorally-accurate software model of large enterprise networks. Our platform provides a revolutionary approach to analyzing and troubleshooting complex network issues, as well as allowing functional validation of network designs rather than traditionally sporadic testing under limited conditions. Network verification is a key component of intent-based networking and the next-generation of IT automation.

As with any fundamentally new approach or capability to an area as diverse as network operations, Forward Networks enables an almost unlimited number of compelling use cases and process improvements, many of which are going to be specific to individual organizations as their experience and network processes evolve. In this paper, we have enumerated several of the most basic use case scenarios that early customers have benefited from and built off of.

With the safety and simplicity of the Forward Enterprise, organizations can easily get started and achieve a tangible ROI immediately from pre-installed policy checks and finding their network topology diagrams and documentation always up to date. Over time, more sophisticated policy checks can easily be built, and information from verification runs can be shared across the organization. For more information and to get started, find us at [www.forwardnetworks.com](http://www.forwardnetworks.com).

---

**Forward Networks, Inc.**
555 California Ave., Suite 200
Palo Alto, CA 94306
United States

© 2018 Forward Networks, Inc. All Rights Reserved. Specifications subject to change without notice.