



DoyleResearch

Accelerating Network Verification
with Intent Based Networking

Sponsored by Forward Networks

Executive Summary

In the new digital enterprise, IT organizations must adapt their infrastructure to rapidly changing application demands. They must deploy and manage complex hybrid cloud platforms, secure the enterprise against advanced cyber threats and deliver end-to-end quality of user experience for mission critical applications. The complexity of the enterprise network makes it a leading challenge for IT to deliver the agility, reliability and security required by most organizations.

Large enterprise networks consist of multiple network elements (e.g. switches, routers, firewalls, application delivery controllers, etc.) from multiple vendors – each with their own management interfaces. With this complexity, there has never been a way to quickly visualize the network on an end-to-end basis to verify intended policies or diagnose errors. It remains a tedious task for experienced network professionals to identify and resolve networking issues (e.g. downtime, slowdowns, application performance degradation).

IT professionals need new tools to rapidly analyze, diagnose and verify the network matches their intended network and security policies for critical applications. Traditional network management tools are difficult to use and too labor intensive to keep up with requirements from digital transformation. The ability to streamline network operations is becoming increasingly important to IT success.

Intent-based networking (IBN) products are now available to intelligently automate many networking tasks, including verification and compliance reviews. IBN can provide the end-to-end view of network policies and behavior needed to verify device configurations and connectivity. IBN has the ability to intelligently reason about network behavior to automate many remediation and testing processes.

Forward Networks' IBN solution helps IT shift from a reactive to proactive response to network issues, proving policies are in place rather than waiting or reacting to failures. The automated intelligence that IBN can offer is also helping to replicate the rare expertise of the critical IT engineers in diagnosing outages, documenting network requirements and verifying fixes. This operational model improves network agility to support rapidly changing application requirements, improves security and reduces downtime.

New Network Challenges

Enterprise networks are typically comprised of multiple types of networking technology, including ethernet switches, routers, firewalls and application delivery controllers. Operation and administration are still typically done via command line interfaces with each network element having its own unique management console. The advent of SDN has provided some operational improvements, but for most IT shops the network is a limiting factor in terms of operational agility.

Ensuring that existing network implementations are properly aligned with applications and security policies end-to-end remains one of the most challenging aspects of enterprise network management. If there is an error in a single device configuration, then administrators must look for the “needle in a haystack” for problem resolution. IT organizations need to move from a reactive state, dealing with outages and trouble tickets after they happen, to a pro-active IT process where organizations can verify a priori that their network designs and implementations are correct.

Network Assurance and Verification Solution Requirements

Advances in network software (i.e., Intent Based Networks) are now making network automation of new verification and analysis tasks possible. Network assurance and verification solutions can automate the complex tasks of reviewing network designs to ensure policies are fully implemented as intended and fault-tolerant at all times. Network software should be applicable for both existing (brownfield) network and new (greenfield) network designs. It should be non-intrusive and non-disruptive to existing networks.

The new software should be easy to learn and use. The user interface should be intuitive – for example, an interactive visual topology of the entire network. The software needs to support a wide variety of network devices (switches, routers, firewalls, etc.) from a range of leading suppliers. As SDN protocols become more popular, IBN must integrate well with the leading SDN products including Cisco’s ACI and VMware’s NSX.

The Value of Automating Network Verification

IBN enables IT operators to move from manual to automated network verification processes. IBN allows the configuration, monitoring and troubleshooting of thousands of disparate network elements with real-time verification of the health and policy alignment of ongoing deployments. Implementation of IBN enables IT to improve application availability, increase security and reduce operational costs.

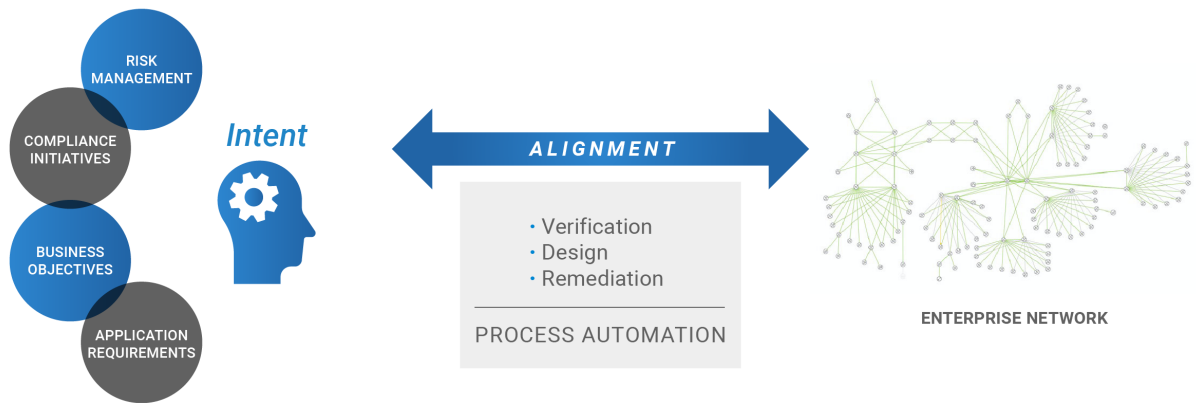
Network IT teams can now troubleshoot faster and proactively eliminate problems prior to a breach or outage. Leading IT organizations who have deployed IBN software report the following benefits:

- Reduced time to trouble ticket resolution
- Reduced time spent on audit related fixes and updates
- Fewer, shorter change windows for network updates

IBN enables rapid verification of network designs to help avoid outages, facilitate compliance processes and accelerate change windows and upgrades. IBN platforms can verify security policies, such as confirming traffic flow isolation. IT and security teams can leverage IBN to accelerate the root-cause analysis around anomalous traffic flows.

IBN can facilitate hybrid cloud and virtual (SDN) network deployments. In a hybrid cloud, end-to-end paths and policies can be analyzed from on-premises network nodes all the way through public cloud endpoints. Network policies can be defined and analyzed across virtual overlay segments as easily as physical networks. Operators can view the overlay or underlay network paths to get immediate correlation between the two layers. See Figure 1.

Figure 1
Benefits of Intent-Based Networks



Forward Networks Delivers Intent Based Networking and Network Verification

Forward Networks is a venture funded company based in Palo Alto, CA. Its mission is to simplify network operations, increase network visibility and verify network implementations. Forward Enterprise enables IT professionals to analyze network behavior and quickly isolate configuration errors and policy violations.

Forward Enterprise is a network assurance and intent-based verification platform. It collects device configuration data from every network device, including state information that governs the active behavior of the device. Forward Enterprise can then analyze the behavior of the entire network end-to-end, and report on potential vulnerabilities, policy violations or risk exposure. It compares policy requirements to the actual implementation of the network to detect and isolate errors. Customers are able to proactively ensure error-free networks, reduce outages and mitigate issues, while accelerating testing and deployment processes.

Forward's network assurance solution is based on a behaviorally-accurate software model of the network. The mathematical model is built from a thorough understanding of the behavior of each network device (switch, router, application controller or firewall), how it's configured, and its state. From this model, Forward Enterprise maps every possible end-to-end behavior that the network supports or allows, as well as definitively ruling out specific undesired behaviors.

Forward enables organizations to describe their intended behaviors as sets of rules or policies that are continually checked to detect anomalies and avert future issues or compliance breaches. Users can quickly analyze and remediate issues, while automating verification tests on proposed changes to shorten change windows, reduce roll-backs and accelerate network deployments. See Figure 2.

Figure 2
Forward Networks Platform



Case Study: Large Online Payment Processor

A large online payment processor has deployed Forward Enterprise, for analysis, network assurance, and policy verification across its entire global payment network. The solution provides them with the ability to query the existing network to determine broad behavior patterns in near real-time and to verify compliance and security requirements.

The application team uses Forward Enterprise to gather information on the network, specifically to query whether existing network designs are able to support specific

application network and security policies - thus providing the required connectivity and access requirements for new deployments. This accelerated network analysis and policy verification process has reduced the number of trouble tickets and manual inquiries dramatically resulting in significant cost savings. Forward Networks was able to handle the scale and scope of the network (over 5,000 devices), as well as accurately analyze and troubleshoot their extensive security policies across their global network.

Recommendations for IT Leaders

IT organizations are tasked with delivering quality of user experience for mission critical applications, rapidly onboarding new applications and deploying hybrid cloud architectures. They need to streamline network operations to support the rapidly changing digital environments and to secure their networks against increasingly sophisticated attacks. Verifying network designs and configurations manually is tedious and time intensive, making it an excellent candidate for IT automation.

Improvements in network software offer improved automation, security, and analytics to the network. IBN software enables automation of networking tasks for verification and rapid remediation of connectivity issues. It supports multi-vendor, multi-element (e.g. switches, routers, firewalls) deployments for both greenfield and existing networks.

IBN software enables IT organizations to move from a reactive mode to proactively being able to validate changes, analyze network performance on an end-to-end basis, and rapidly identify network problems. It also helps IT teams to translate intent into network configurations, automates time consuming manual processes and reduces human error.

Forward Networks offers IBN software to facilitate network verification which simplifies cloud deployments and virtual networking. IBN automates the analysis and remediation of network errors, as well as analyzing configuration updates, to align with administrators' high-level intent. Forward's customers report significant reduction in time and resources to resolve trouble tickets caused by configuration errors or unexpected changes in the operational state of network devices.

Meet the Author

Lee Doyle is Principal Analyst at Doyle Research, providing client focused targeted analysis on the Evolution of Intelligent Networks. He has over 25 years' experience analyzing the IT, network, and telecom markets. Lee has written extensively on such topics as SDN, NFV, enterprise adoption of networking technologies, and IT-Telecom convergence. Before founding Doyle Research, Lee was Group VP for Network, Telecom, and Security research at IDC. Lee contributes to such industry periodicals as Network World, Fierce, and Tech Target. Lee holds a B.A. in Economics from Williams College.