FORWARD NETWORKS

USE CASE

Zero Trust Validation

Improving Visibility and Enforcement of Zero Trust Policies Across Agency Environments

Forward Networks has created the first network digital twin based on a mathematical model. The platform delivers visibility and actionable insight that scales the complexity and size of agencies' multi-vendor, multi-cloud environments.

Protecting federal IT systems is harder than ever. As threats continue to escalate and the transition to hybrid and multi-cloud environments accelerates, the boundaries are blurring and making it hard to visualize and monitor systems as a whole. Federal agencies – especially those with controlled unclassified information (CUI) workflows and sensitive mission data – need to cut through the noise of their complex and increasingly distributed architectures to rapidly visualize security postures and verify compliance with zero trust policies.

HOLISTIC MONITORING OF SYSTEMS PLAYS A CENTRAL ROLE IN ZERO TRUST GUIDANCE

As agencies lean into modern software-based services for remote work and more agile, mission-ready services, it becomes harder to understand if their systems meet the increasingly stringent cybersecurity controls. The resulting urgency has led to different zero trust models designed to guide agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA) Zero Trust Maturity Model, the National Institute of Standards and Technology (NIST) Zero Trust Architecture (SP800-207), the Defense Information Systems Agency (DISA) Zero Trust Reference Architecture, and NIST's National Cybersecurity Center of Excellence (NCCoE). What is central to these models is that agency networks – across cloud, on-premises, and virtual overlays – ensure the right configurations and connectivity are being enforced and that they continue to verify evolving network behaviors.

Zero trust requires a comprehensive understanding of agency inter-zone connectivity and the intended zero trust architectures to rapidly implement and enforce micro-segmentation and security policies. Boundaries blur, and configurations constantly shift with remote work and new application deployments, making it more difficult to uncover risks and verify whether agency security policies are performing as expected. Implicit trust is a thing of the past. Misconfigurations and/or intentional circumvention of security policies must be quickly identified and remediated before an incident occurs. IT teams are stretched to their limits. They need a new, more efficient approach to visualize and verify networks and protect agency missions without the load from manual data calls and inefficient processes.

A SINGLE SOURCE OF TRUTH FOR AGENCIES

Automated, always-on verification from Forward Networks allows agencies to mature their security posture in ways that were previously difficult to achieve. The solution offers an at-a-glance, mathematically proven, system-wide assessment of security zone connectivity and instant insight into connectivity at the individual device level and security postures at L2 – L4 and the application and user ID level (L7).

Forward Enterprise helps security teams mitigate vulnerabilities by identifying and validating all the possible traffic paths. The mathematical model from Forward Enterprise creates an always current, comprehensive digital twin of an agency's physical, virtual, and cloud networks, including all major network hardware vendors, end-points, and SDN deployments. With complete transparency over distributed agency estates and a single source of truth, Forward Networks helps security teams quickly visualize, verify, search, and predict network behaviors. Using this information, the team can create controls and continually verify policies are behaving as desired and without unintended side-effects to deploy and enforce zero trust faster.

Implement and Audit Zero Trust Across Entire Networks with Mathematical Certainty

Forward Networks provides intent-based verification and network assurance that many agencies are using to mature their zero trust architectures. Digital twins deliver the comprehensive view of network behaviors that IT leaders need to visualize every possible traffic path and uncover the potential for lateral movement after a breach. Network, cloud, and security teams now have a tool to instantly verify and continuously enforce zero trust across complex environments at the speed and efficiency required for federal agencies to meet escalating threats.

AGENCY BENEFITS OF FORWARD NETWORKS SOLUTIONS

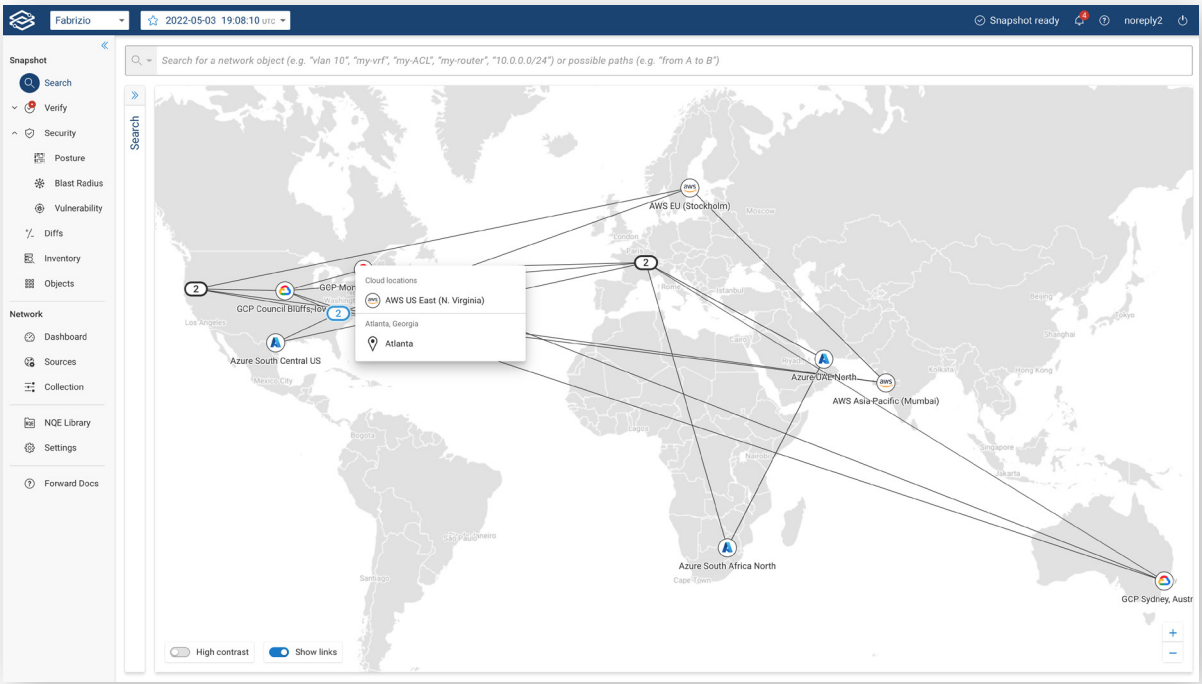
Agencies can use a network digital twin to gain a comprehensive view of physical, virtual, and cloud network behavior based on configuration and state information for all devices.
A Forward Networks digital twin supports effective zero trust policies in five key areas:

- Network visualization
- Always current security posture matrix that shows which zones have full or partial connectivity or are fully isolated at a glance
- Always on audits for policy verification and validation and compliance documentation
- Secure automated application deployment
- Blast radius and lateral movement identification

How Forward Networks Can Help Agencies Succeed with Zero Trust

NETWORK VISUALIZATION

Forward Enterprise's network digital twin allows agencies to gain unified visibility across blended systems and legacy IT as well as multi-cloud and cloud-native applications, providers, and security tools. For stretched IT teams working to apply zero trust policies across very different – often siloed – environments, this single source of truth gives managers the ability to efficiently defend sensitive CUI and mission data and improve performance without new certifications and expertise.



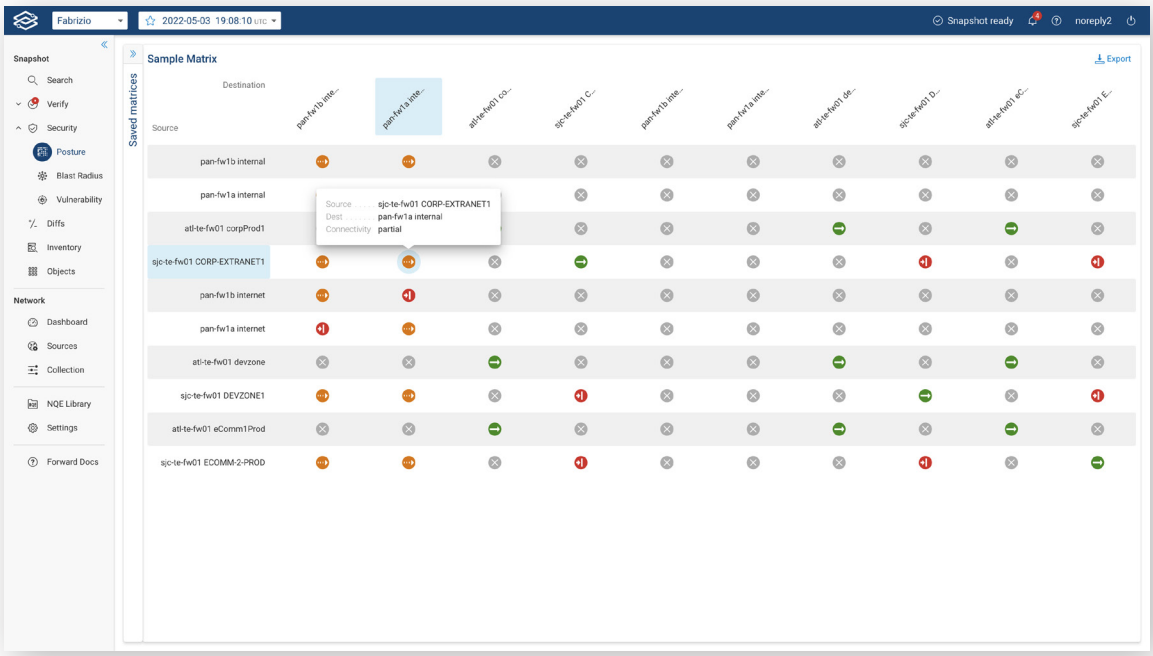
Forward Enterprise delivers a topological map for a vendor-agnostic, single source of truth across on-premises, multi-cloud (AWS, Azure, Google) estates. This view collapses complex interactions and connectivity into an easy-to-understand visualization for intuitive navigation with the ability to drill down to detailed device configuration and state information with a few clicks. Agencies can even visualize their high-side and low-side networks together with the ability to prove isolation between locations.

Using a mathematical model, every possible path a packet can travel through the network is discoverable and searchable within seconds to help operators find – and block – the unknown paths traffic can traverse. The platform delivers a complete flow analysis that combines infrastructure, security policy, and web application flow in a single stream, making it easy for users to view how a packet is processed at every hop.

This holistic view makes it easy to monitor connectivity as a whole and intuitively navigate through vast distributed IT for a deeper understanding of network behaviors and more centralized, efficient management of zero trust policies in federal environments.

ZONE-TO-ZONE CONNECTIVITY MATRIX AND OUTCOMES

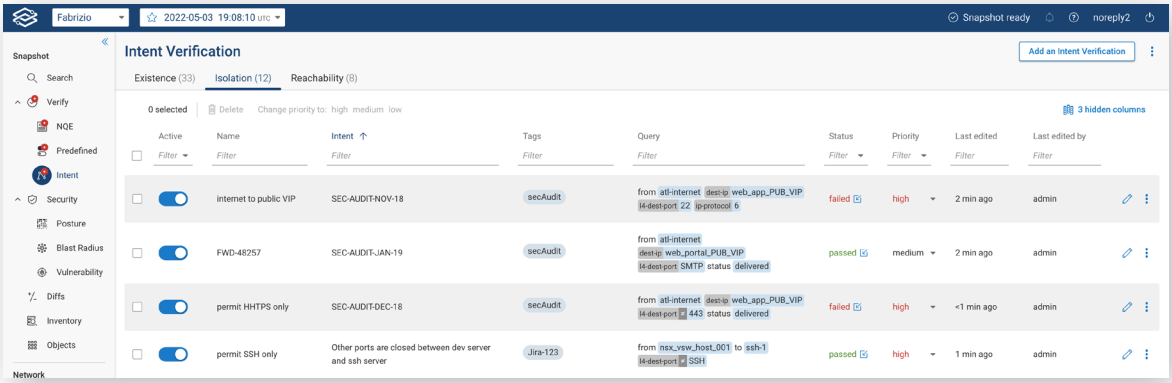
Enforcing zero trust, or least privileged access, to the myriad of security zones common to many federal environments can be time-intensive, especially for those agencies with classified workloads or high-side networks and different security clearances. Network and security teams need a fast way to understand and prove connectivity and isolation across very complex, hybridized environments.

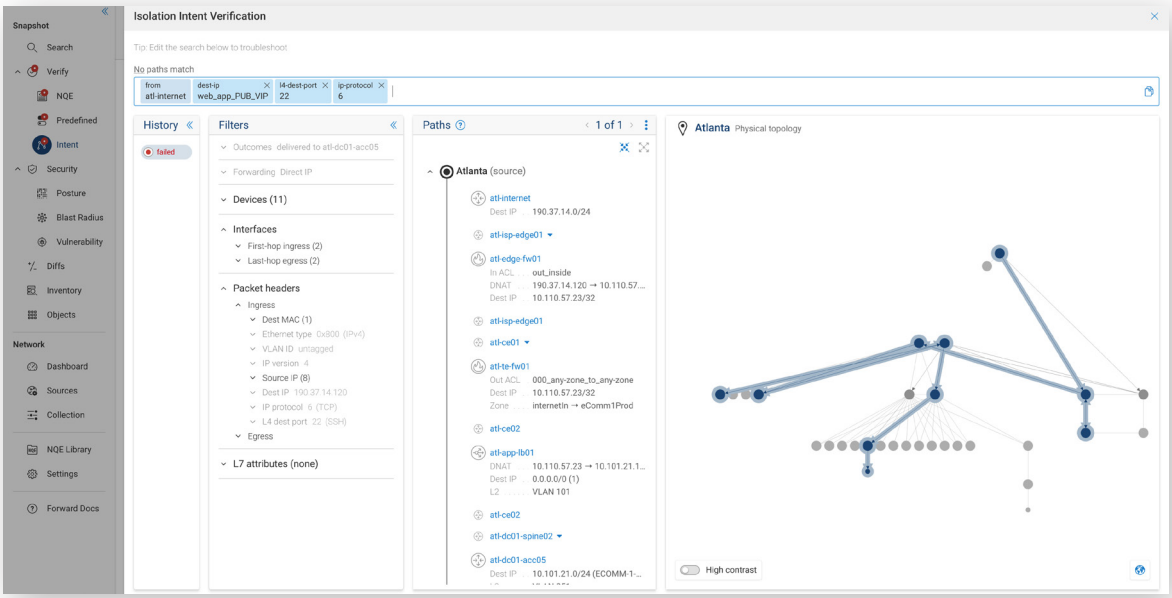


Micro-segmentation is the foundation of a zero trust architecture. Unfortunately, the policy matrix is rarely up-to-date or kept in a single place. Forward Enterprise fills this gap by delivering a visual zone-to-zone connectivity map delineating partial, full, or zero connectivity. It's now possible to prove at-a-glance that mission-critical information and internet data are isolated from each other, even when they cross the same physical links.

ALWAYS-ON AUDITS – POLICY VERIFICATION AND VALIDATION

Swiftly and efficiently validating compliance with zero trust policies and other mandates like DISA Security Technical Implementation Guide (STIG) requirements is not an easy task. Given the size and complexity of most federal environments, it's nearly impossible for IT teams to find configuration errors proactively as their architectures continually evolve. Forward Enterprise enables agencies to move from manual, time-consuming audits to regular, automated intent checks, purpose-built for specific mission requirements, that prove compliance or send real-time action alerts if security violations or misconfigurations are found.

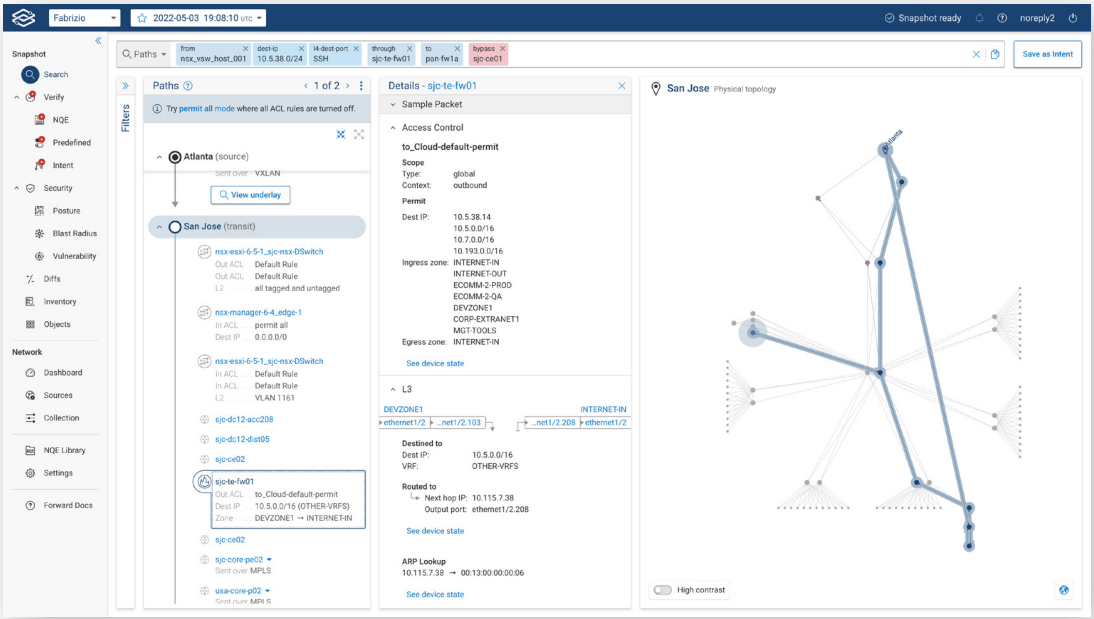




Forward Networks' custom intent checks act as always-on audits that prove security policies are behaving as intended without network and security teams manually gathering data to prove compliance. Using a digital twin to continuously validate security postures and catch and remediate security violations in real-time before bad actors can find and exploit vulnerabilities helps enforce zero trust as a permanent posture. An intent check can prove, for instance, that only a specific TCP port can reach applications from a specific destination while also accounting for NAT, ACLs, and load-balancing rules that occur along the path.

AUTOMATED SECURE APPLICATION DEPLOYMENT

Instant scalability of the cloud and faster application release cycles are helping federal agencies meet the increasing demand for agile IT services. However, faster application releases need to be proactively secured, so they don't cause unintended risks to the network.

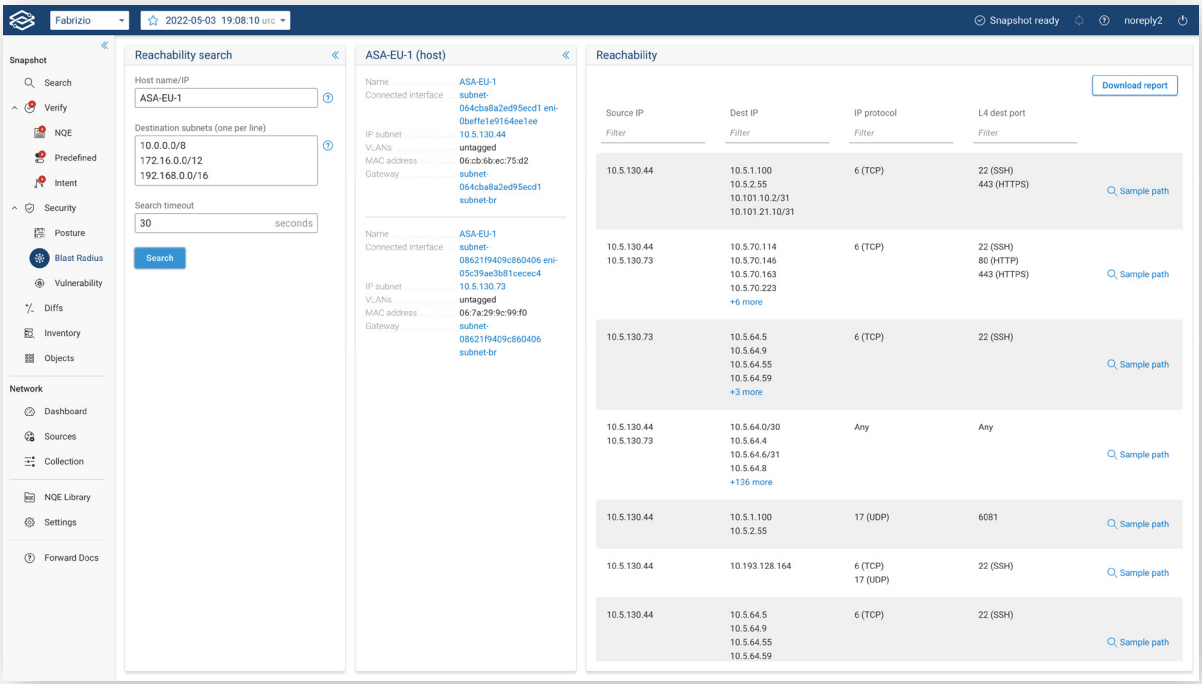


CERTIFYING NEW APPS

Without the visibility that Forward Networks provides, it is almost impossible to understand where changes to the network are creating new vulnerabilities. Developer, security, and network teams need a more efficient way of working together to proactively validate the impacts of updates.

BLAST RADIUS AND LATERAL MOVEMENT IDENTIFICATION

Federal agencies handling sensitive data to carry out their missions can now gain greater visibility in real-time to stop attackers from moving undetected through networks.



Once a compromised host has been identified, Forward Enterprise makes it easy to determine the scope of impact, including a bad actor's ability to move horizontally and vertically through the network. Using the blast radius button, security professionals can document every destination, protocol, and L4 port that could be impacted.

Achieving a Proactive Cybersecurity Stance

Forward Enterprise enables stretched agency IT teams to move from manual, time-consuming network processes to a single source of truth. With automated analysis that cuts through the noise and complexity of their vast estates, Forward Enterprise helps IT teams visualize, search, verify, predict, and compare network behaviors with game-changing speed and efficiency. Using a digital twin, agencies can move from a reactive security stance to a proactive one, saving time and resources and enabling agency network and security engineers to:

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. Forward Enterprise has added path search capabilities at L7, delerving Layer 7 application connectivity analysis, so administrators can construct more intelligent queries that reveal unwanted connectivity.

SEARCH the network as simply as a database with complete end-to-end path analyses. Search across the network for both on-premises and cloud infrastructure and identify configuration lines that impact traffic flow or violate security policy in milliseconds.

VERIFY that network security controls are working as intended using purpose-built intent checks. Continuously audit the network and receive actionable alerts for noncompliance with zero trust policies.

PREDICT the effect of proposed changes, so managers can deploy updates without the fear of unintended connectivity changes by using the network digital twin as a sandbox.

COMPARE network changes over time to understand impacts and prevent the recurrence of incidents. The network collector scans and saves snapshots of network configurations, topology, and device state that form a searchable, historical, point-in-time record of network behavior and compliance.

See for Yourself: Network Verification of Zero Trust with Forward Networks

Using Forward Enterprise, IT teams can take the holistic approach required to enforce zero trust policies. Check out this video for a quick demonstration of how Forward Networks makes it easy to verify the zero trust policy in your agency network.

And if you want to learn more about how Forward Networks can make zero trust verification and validation faster, simpler, and more effective for your agency, go to forwardnetworks.com/network-security and reach out to us at forwardnetworks.com/federal.

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 Santa Clara, California, and funded by top-tier investors, including Andreessen Horowitz, DFJ, A.Capital, SV Angel, and several luminaries in the networking and systems space.