FORWARD NETWORKS

USE CASE

Reduce Mean Time to Innocence with Hop by Hop Visibility

For many companies, once traffic hits the cloud, it's nearly impossible to trace its path — that's no longer the case. Faster MTTI means fewer issues and happier employees and customers.

Most enterprises today have multiple cloud migration projects underway or in the planning stages. By moving more on-premises applications and data to third-party cloud platforms and accelerating digital transformation, these organizations look to support remote or hybrid workforce collaboration, serve customers more effectively, increase business agility and resilience, reduce costs, and more.

While the potential benefits of cloud migrations are significant, these complex IT projects are tough to execute and optimize. They're made even more challenging and costly due to the lack of visibility that network and security teams have across the organization's cloud estate, which typically includes multiple cloud platforms running and hundreds or even thousands of apps.

So, when a performance issue arises between the on-premises environment and the cloud, or between clouds, it can take teams a long time to prove network innocence before they can even start to resolve the issue with their cloud providers. Whether addressing a performance issue or an outright outage, time is money, and fast resolution is imperative for business continuity and a positive customer experience.

Your network and security teams' struggle to understand what's happening across your cloud estate is due largely to a lack of appropriate tools. The tools they use to validate connectivity and security for on-premises networking are completely different from those used for the cloud — and between clouds. Cloud topology is also represented much differently from on-premises topology. [See Figure 1]

	aws REGIONS & ZONES	Azure REGIONS	Google Cloud REGIONS & ZONES
Compute Services	Elastic Compute Cloud (EC_2)	Virtual Machines	Compute Engine
App Hosting	Amazon Elastic Beanstalk	Azure Cloud Services	Google App Engine
Serverless Computing	AWS Lambda	Azure Functions	Google Cloud Functions
Container Support	Elastic Container Service	Azure Container Serivces	Container Engine
Scaling Options	Autoscaling	Aszure Autoscale	Autoscaler
Object Storage	Amazon Simple Storage (S_3)	Azure Blob Storage	Cloud Storage
Block Storage	Amazon Elastic Block Storage	Azure Managed Storage	Persistent Disk
Content Delivery Network (CDN)	Amazon CloudFont	Azure CDN	Cloud CDN
SQL Database Options	Amazon RDS	Azure SQL Database	Cloud SQL
NaSQL Database Options	Amazon DynamicDB	Azure DocumentDB	Cloud Datastore
Virtual Network	Amazon VPC	Azure Virtual Network	Cloud Virtual Network
Private Connectivity	AWS Direct Connect	Azure Express Route	Cloud Interconnect
DNS Service	Amazon Route 53	Azure Traffic Manager	Cloud DNS
Log Monitoring	Amazon CloudTrail	Azure Operational Insights	Cloud Logging
Performance Monitoring	Amazon CloudWatch	Azure Application Insights	Stackdriver Monitoring
Administration & Security	AWS Identity & Access Management	Azure Active Directory	Cloud Identity & Access Management
Compliace	AWS CloudHSM	Azure Trust Center	Google Cloud Platform Security
Analytics	Amazon Kinesis	Azure Stream Analytics	Cloud Dataflow
Automation	AWS Opsworks	Azure Automation	Compute Engine Management
Management Services & Options	Amazon CloudInformation	Azure Resource Manager	Cloud Deployment Manager
Notifications	Amazon Simple Notification Service	Azure Notification Hub	None
Load Balancing	Elastic Load Balancing	Load Balancing for Azure	Cloud Load Balancing

Figure 1: Cloud providers do not share nomenclature

Complicating matters further: Cloud providers use their own nomenclature, methodology, visualization, and toolset. And when virtual machines are thrown into the mix, visibility effectively drops off a cliff. Provider tools can visualize traffic up to a virtual device, such as a Palo Alto Networks L7 firewall, but once the packets enter the firewall, there's no information on how they were manipulated by the device and where they subsequently went.

The Forward Enterprise platform from Forward Networks helps your teams overcome these challenges by providing a clear visualization of your cloud estate alongside your on-premises environment in a single normalized view. That view includes your entire cloud inventory — every instance and object associated with every provider — and how those objects relate to and interact with each other and where they're located, including geographically. At a glance, you can see what's happening now and over time in your cloud environment.

Anytime you want to explore more information about a specific element within your network, like a cloud platform, firewall, or transit gateway, you can just click on that element in Forward Enterprise. For example, clicking on a platform in your environment from a major cloud provider, like Amazon Web Services (AWS), Google Cloud Platform (GCP), or Microsoft Azure, could show that you have four virtual private cloud instances (VPCs), one transit VPC, and several subnets related to that platform. [See Figure 2]

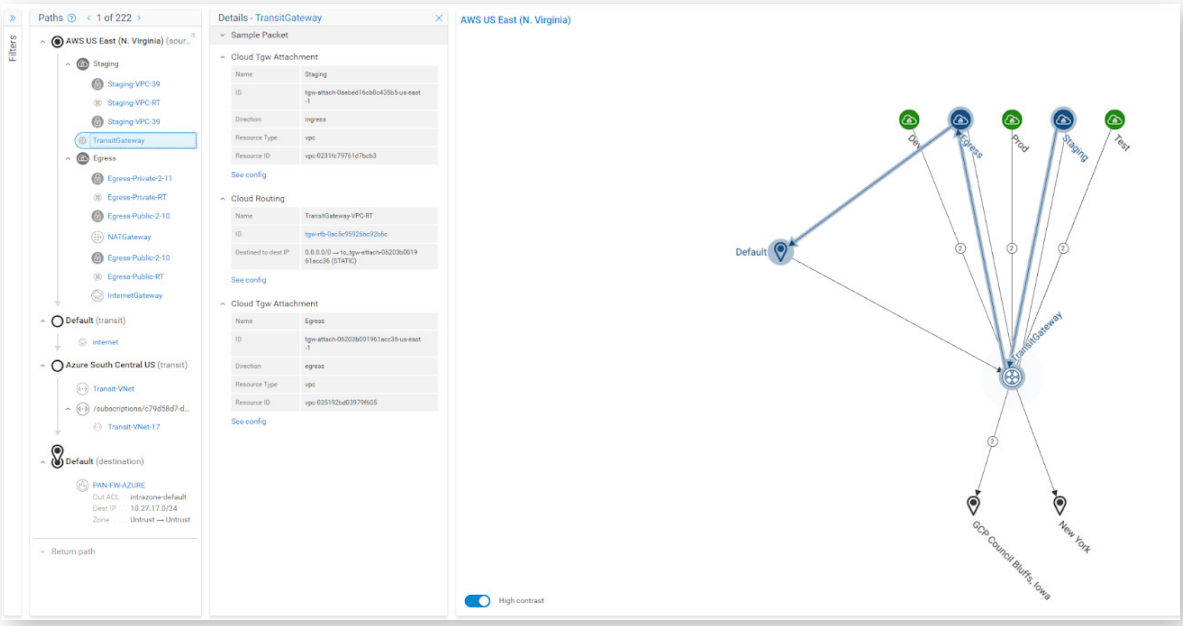

Figure 2: Detailed Information about multi-cloud resources is always available

The Forward Enterprise platform offers hop-by-hop visibility, from access points through multi-cloud, allowing your teams to get granular when troubleshooting cloud performance issues. They can determine exactly how, and how effectively, traffic is moving between your on-premises environment and any instance in your cloud environment, as well as between points within your multi-cloud environment.

Your teams can quickly identify problems and issue tickets to appropriate teams to investigate and resolve problems. They can also confirm that redundancy and availability are meeting expectations. And they can verify the security posture between zones, both on-premises and in the cloud.

A Single Source of Truth for Your On-Premises, Hybrid, and Multi-Cloud Estate

Forward Networks' 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 network elements and your hybrid or multi-cloud environment. The digital twin provides a comprehensive view of all network behavior with visibility into every possible path a packet can take. It brings mathematical certainty to network security validations by enabling security operations teams to:

VISUALIZE network layer 2 – 4 topology and all possible traffic paths within a single pane of glass including on-premises, cloud (AWS, GCP, and Microsoft Azure), and virtualized environments. Then, drill down to specific devices and traffic flows, including configuration and state data. View the global network in a single view or drill down to a single device.

SEARCH the entire estate 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 also enables you to locate devices and access detailed information on their location, configuration, and state in milliseconds.

VERIFY that the security policies are extended to the cloud using purpose-built (custom) intent checks. Continuously audit the network and receive actionable alerts for non-compliance with your security policies. Know that applications are compliant before provisioning them.

COMPARE network changes over time to understand their impact on the network and prevent incidents from reoccurring. The network collector frequently scans the network, taking and saving network configurations, topology, and device state snapshots. 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 security policy.

See for yourself how the Forward Enterprise platform can help your network and security teams monitor and verify all your clouds through a single pane of glass and explore any object in your cloud environment to ensure everything is working exactly as it should be. To see this feature and the power of a network digital twin in action, please request a demo.

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.