



**USE CASE**

# Zone-to-Zone Connectivity Matrix



Because network teams and security engineers rely on a manually updated policy matrix and tribal knowledge for insight into interzone connectivity in the network, determining security policy intent and verifying compliance with data security and privacy regulations is an arduous and error-prone task.

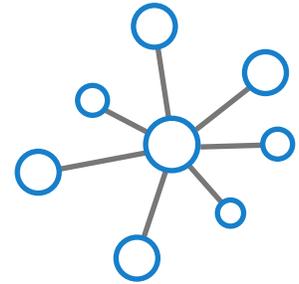
Without a current and comprehensive visual representation of network policies and configurations, it's exceptionally challenging for teams to know, with certainty, whether a specific area (firewall zone) in the network has intended connectivity to other zones. This lack of visibility undermines the very foundation of network security.

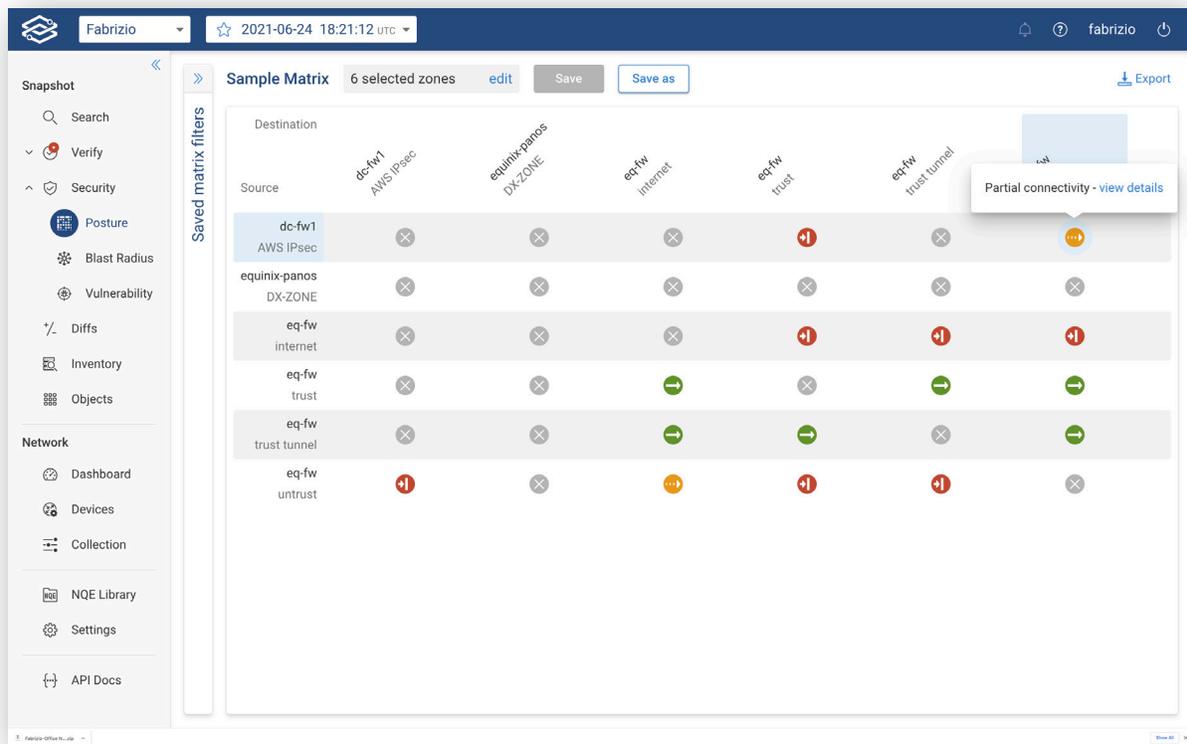
Implementing and enforcing zero trust policy and micro-segmentation in the network is nearly impossible for engineers. Networks are constantly growing and changing, and security zones are being added. This adds to complexity and leads to exponential increases in policy rule sets. Forward Enterprise provides at a glance representation of security zone connectivity, representing complex interactions in an easy-to-understand visualization.

# Providing an Always-Current Source of Truth for Zone-to-Zone Connectivity

Network teams and security engineers need access to a single source of truth for the network's behavior, so they can easily understand policy compliance at all times. The zone-to-zone connectivity matrix instantly indicates which zones in the network have open, partial, or no connectivity. They must also be able to validate network policies continuously and automatically every time there's a change in the environment—a frequent occurrence—to prove security policy compliance and validate the organization's zero trust architecture, if applicable. This helps to ensure an accurate picture of interzone connectivity is always maintained, and it also relieves teams of the need to update the policy matrix manually.

Forward Networks maps security policy and network behavior into an easy-to-use, graphical, zone-to-zone connectivity matrix to meet these needs.





The zone-to-zone connectivity matrix uses color-coded status indicators to represent flow outcomes, enabling teams to confirm compliance at a glance.

- **Green:** openly connected
- **Yellow:** partially connected
- **Red:** fully isolated

The screenshot displays a network management dashboard. On the left, a sidebar contains navigation options like Search, Verify, Security, Posture, Blast Radius, Vulnerability, Diffs, Inventory, Objects, Network, Dashboard, Devices, Collection, NQE Library, Settings, and API Docs. The main area shows a 'Saved matrix filters' section with 'FW-All' selected, and a 'FW-All 10 selected zones' matrix. The matrix lists various zones and their connectivity status. A 'Connectivity details' modal is open, showing a table of connectivity data between source and destination zones.

Source zone	Destination zone	Source IP	Dest IP	IP protocol	L4 dest port
PAN-FW-A2 shared-app	PAN-FW-A2 web-app	10.7.56.16/30 10.7.58.8/30 10.7.58.20/30 10.7.59.8/30 10.18.10.10	10.18.10.10	6 (TCP)	443 (HTTPS)
PAN-FW-A2 shared-app	PAN-FW-A2 web-app	10.7.56.16/30 10.7.58.8/30 10.7.58.20/30 10.7.59.8/30 10.18.10.10	10.17.1.10 10.17.2.14	Any	Any

Clicking on the icons shows how the connectivity occurs in the network — insight that a policy matrix on an Excel spreadsheet can't provide.

Using the Path Analysis, Network Query Engine, and the network-diff capabilities in the Forward Enterprise platform, network teams and security engineers can confirm that network segmentation is working as intended and pinpoint the cause of unintended connectivity quickly and easily. They can also build verification baselines from the matrix using Forward intent verification checks. Importantly, they can discover connectivity between zones that should not be occurring — and stop it.

# Enhance your Security Posture with a Network Digital Twin

Our mathematical model creates a complete and always-current digital twin of your physical, virtual, and cloud network estate, including config and state information for all devices. The digital twin provides a comprehensive view of all network behavior, with visibility into every possible path in your network. 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 view for on-premises, Cloud (AWS, Microsoft Azure, and Google Cloud Platform), and virtualized environments. Then, drill down to specific devices and traffic flows, including configuration and state data.



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



**VERIFY** that the security controls in the network are working as intended by using purpose-built (custom) intent checks. Continuously audit the network and receive actionable alerts for noncompliance with your security policies.



**PREDICT** the effect of proposed changes, so you 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 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.



# Gain Full Confidence in Your Zone-to-Zone Connectivity Posture

See for yourself how the zone-to-zone connectivity feature in the Forward Enterprise platform can help security operations professionals determine, at a glance, which zones in your network have full, partial, or no connectivity and whether network policies for security, including for zero trust, are working as expected. To see this feature and the power of a network digital twin, please request a demo.

## Getting Started With Forward Networks

Are you ready to deliver new capabilities through the network, reduce outages, enhance security, and save time?

[Request a personal demo >](#)



[www.forwardnetworks.com](http://www.forwardnetworks.com)