

WHITE PAPER

Resolving Key Post Merger IT Integration Challenges with a Digital Twin



How Does IT Impact M&A Success?

According to [Bain & Company, 2023 M&A activity](#) will be on par with or exceed the level of activity in 2022. Even in the face of an uncertain economic outlook, savvy executives will continue to use M&A activity to bolster their companies. As the report stated, companies that made at least one merger or acquisition during the 2008-2009 downturn earned 120 basis points more in total shareholder returns than companies that were inactive in M&A. Downturns also present a substantial opportunity for industry re-defining deals.

IT is the underpinning of successful mergers. When IT integration is incomplete, workers suffer from a lack of access to information and reduced collaboration. There's no shortage of consulting firms offering extensive services to integrate IT organizations and ensure business continuity. They exist because IT integration is complex; if done incorrectly, it can strain the merger's success. Common problems include:

- 1. Loss of productivity:** Improperly integrated IT systems can lead to significant downtime and loss of productivity. This can result in lost revenue and dissatisfied customers.
- 2. Increased costs:** IT integration can be a significant expense, but the costs of not managing it can be even higher. Inefficient processes, duplicated efforts, and other issues can drive up costs and hurt the bottom line. Most networks are riddled with unidentified assets, some of which may need to be replaced.
- 3. Security risks:** If IT systems are not properly integrated, it can expose security vulnerabilities that cybercriminals can exploit. This can result in data breaches, theft of intellectual property, and other security incidents that can harm the company's reputation and bottom line.
- 4. Legal and regulatory issues:** Mergers can raise legal and regulatory issues, particularly if the companies operate in different countries or industries. Failure to properly manage IT integration can result in regulatory violations, lawsuits, and fines.

Overall, the costs of not managing IT integration during a merger can be significant in terms of financial costs and other negative impacts on the company's operations and reputation.

What are the toughest IT challenges during a merger?

Smooth integration of IT systems is the foundation of a successful merger. As the backbone of the business, the network is responsible for employee productivity, customer satisfaction, and for many companies, revenue generation. Unfortunately, it's a highly complex undertaking with many barriers to success.

NETWORK COMPLEXITY

On-premises enterprise networks have grown organically over the decades; they can comprise tens of thousands of devices from dozens of vendors running billions of lines of code. [According to a 451 Group Pathfinder Report \(See It, Fix It, Manage It\)](#), cloud complexity is also growing. 59% of enterprises said they are moving toward an integrated multi-cloud IT architecture, while another 20% are moving entirely to the cloud.

Even if the task at hand is integrating a relatively small network into an enterprise environment, it's still a gargantuan task. Almost every enterprise has documented its on-premises and cloud architecture, but only at a high level. Very few have current documentation of their global topology down to a single device or instance. According to a [report on cybersecurity in mergers and acquisitions](#), over half (53%) of technology leaders say they find unaccounted-for devices after completing the integration of a new acquisition.

Unless you accurately understand the devices on the networks and how those devices are configured, it is impossible to understand the ramifications of connecting them.

SECURITY RISKS

According to the above-referenced study, 62% of respondents believe their company faces significant cybersecurity risk when acquiring new companies. The IT team protects the company's digital assets, manages risk, and ensures regulatory compliance. During an M&A event, this requires assessing the vulnerabilities and ensuring the newly acquired network adheres to the parent company's security policies.

How can a network digital twin streamline and de-risk IT integration during a merger?

The lack of accurate data is the common thread that ties all network-related M&A challenges together. Forward Enterprise, the most sophisticated network digital twin available, provides engineers with the current and detailed information they need to quickly and safely merge networks.

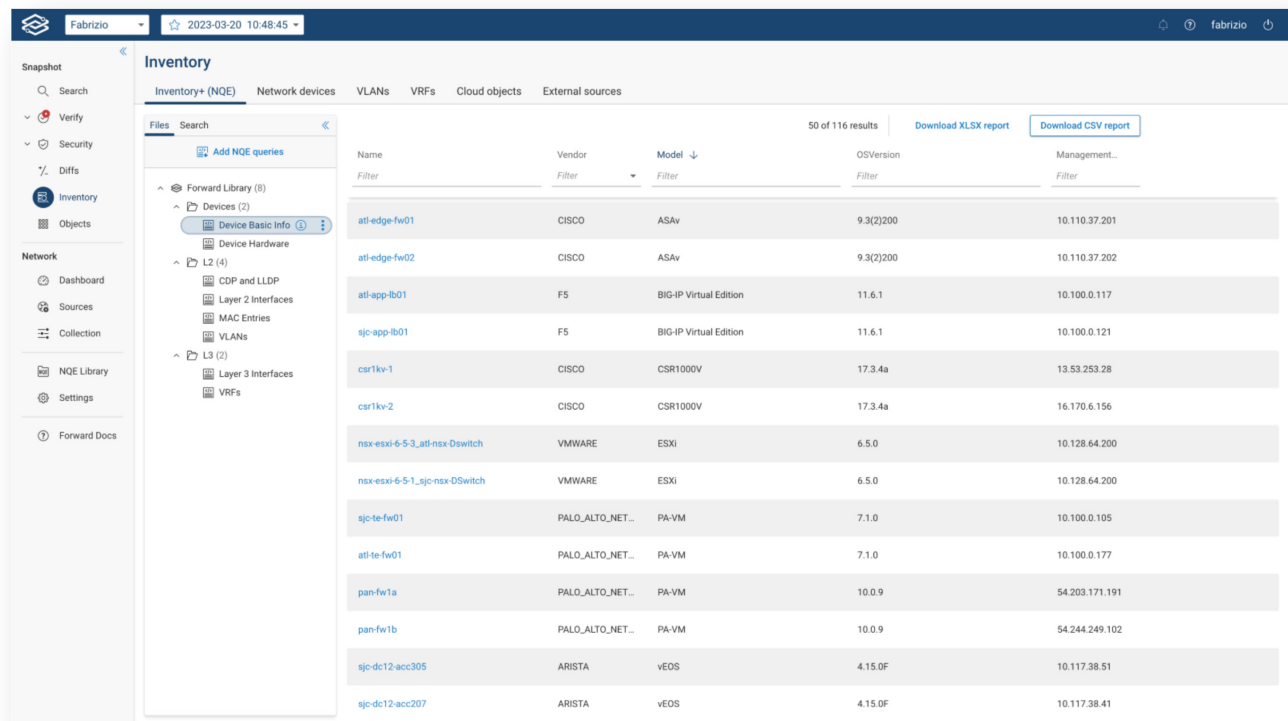
The Forward Enterprise collector gathers detailed information about all L2-L4 and some L7 devices on the network and cloud instances using read-only network access and commercially available cloud APIs. This information is parsed and normalized to make it accessible and actionable for even the team's most junior member. The data is used to build visual network topology models, reason all possible paths in the network, create an accurate inventory, and assess vulnerabilities. Furthermore, the platform offers verification checks that enable engineers to ensure the network is compliant and behaving as expected. This detailed data eliminates guesswork during the integration process.

STEP 1: Understanding network inventory

Before contemplating joining networks, knowing what devices are in use and their configuration is critical. Unfortunately, most IT departments don't have a dynamic network inventory; instead, they work from high-level architecture diagrams or out-of-date spreadsheets.

Companies using Forward Enterprise can easily address this challenge using the Network Query Engine (NQE) dynamic inventory tool (see figure 1). NQE's dynamic inventory enables users to see the network's granular details (e.g., configurations, state, interfaces, power supply serial number, module firmware rev, etc.). One of the many benefits of NQE is that data collected from multiple vendor devices is normalized so that anyone can interpret it – no need for vendor-specific expertise.

The data collected by Forward effectively creates “Google for your network”; a simple search can locate an IP address, circuit ID, or piece of equipment in seconds.



The screenshot shows the NQE dynamic inventory tool interface. The main content area displays a table of network devices. The table has the following columns: Name, Vendor, Model, OS Version, and Management IP. The table contains 16 rows of device information. The interface also includes a search bar, a sidebar with navigation options, and buttons for downloading reports.

Name	Vendor	Model	OS Version	Management IP
atl-edge-fw01	CISCO	ASAv	9.3(2)200	10.110.37.201
atl-edge-fw02	CISCO	ASAv	9.3(2)200	10.110.37.202
atl-app-ib01	F5	BIG-IP Virtual Edition	11.6.1	10.100.0.117
sjc-app-ib01	F5	BIG-IP Virtual Edition	11.6.1	10.100.0.121
csr1kv-1	CISCO	CSR1000V	17.3.4a	13.53.253.28
csr1kv-2	CISCO	CSR1000V	17.3.4a	16.170.6.156
nsx-esxi-6-5-3_atl-nsx-Dswitch	VMWARE	ESXI	6.5.0	10.128.64.200
nsx-esxi-6-5-1_sjc-nsx-Dswitch	VMWARE	ESXI	6.5.0	10.128.64.200
sjc-te-fw01	PALO_ALTO_NET...	PA-VM	7.1.0	10.100.0.105
atl-te-fw01	PALO_ALTO_NET...	PA-VM	7.1.0	10.100.0.177
pan-fw1a	PALO_ALTO_NET...	PA-VM	10.0.9	54.203.171.191
pan-fw1b	PALO_ALTO_NET...	PA-VM	10.0.9	54.244.249.102
sjc-dc12-acc305	ARISTA	vEOS	4.15.0F	10.117.38.51
sjc-dc12-acc207	ARISTA	vEOS	4.15.0F	10.117.38.41

Figure 1: NQE dynamic inventory

STEP 2: Understanding network topology

Enterprise topology is rarely understood at a granular level. Most NetOps teams have current architecture diagrams and have a high-level understanding of physical and logical network topology. Details often reside in the organizational wisdom (AKA inside the heads of people who've been with the organization for some time).

The notion of interconnecting networks with only high-level topological knowledge is disconcerting. Out of an abundance of caution, the networks are often maintained separately rather than integrated as a security mechanism. This can lead to inefficiency and higher operating costs.

Forward Enterprise provides a visualization of your organization's entire (L2-L4) hybrid, multi-cloud estate in a single normalized view (see figures 2-4). We collect config and state data from all your on-premises devices, such as routers, switches, load balancers, firewalls, SD-WAN, and virtualization platforms (e.g., VMware NSX and Cisco ACI). And we use publicly available APIs to gather similar read-only information for your various cloud accounts to create a network digital twin.

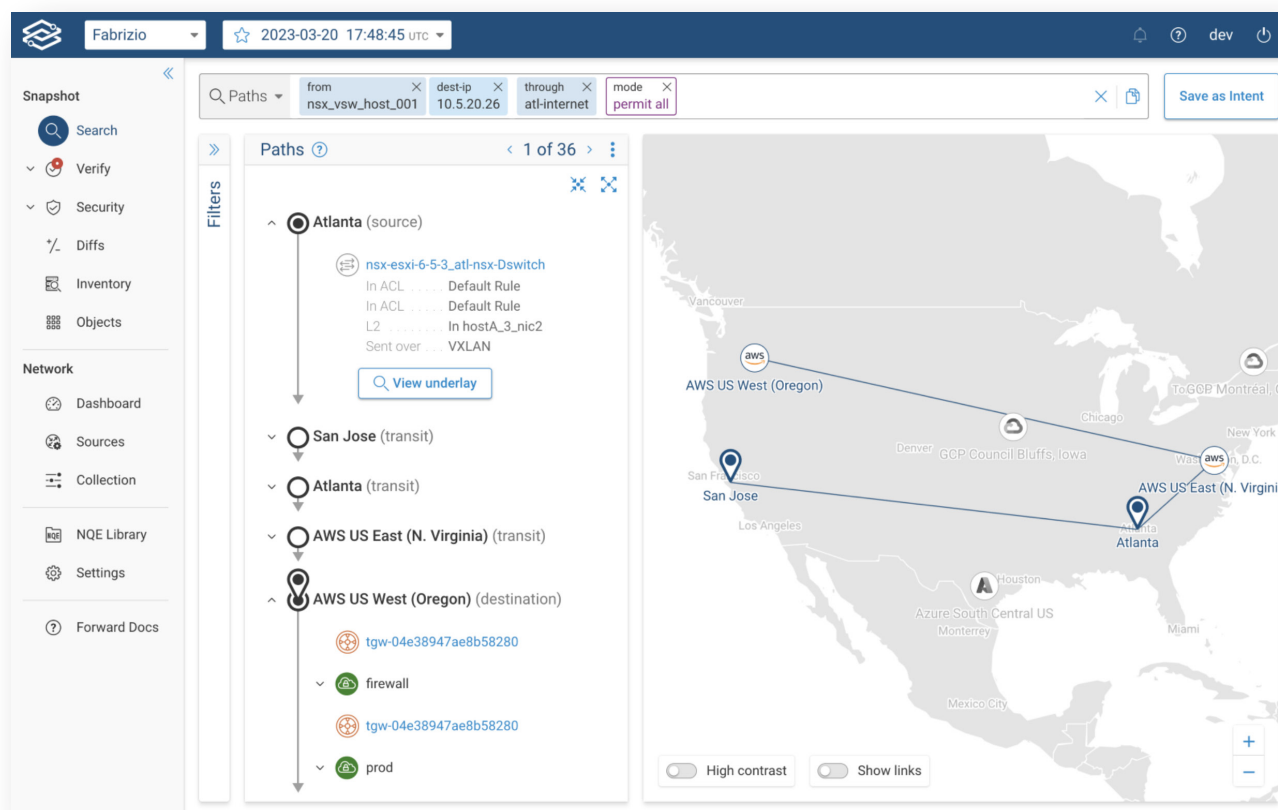


Figure 2: Location based topology

STEP 3: Understand all possible paths in the network

Connectivity is the cornerstone of network reliability and security. Using [an advanced mathematical model](#), Forward Enterprise can compute all possible paths in the network within a single-pane view for on-premises, Cloud (AWS, Microsoft Azure, and Google Cloud Platform), and virtualized environments. This detailed information helps NetOps engineers ensure the network will behave as expected.

Forward Enterprise is the only digital twin that can deliver insights into end-to-end paths that traverse multiple legacy networks, i.e., in situations where two networks have overlapping subnets and require NAT translation (see figure 3).

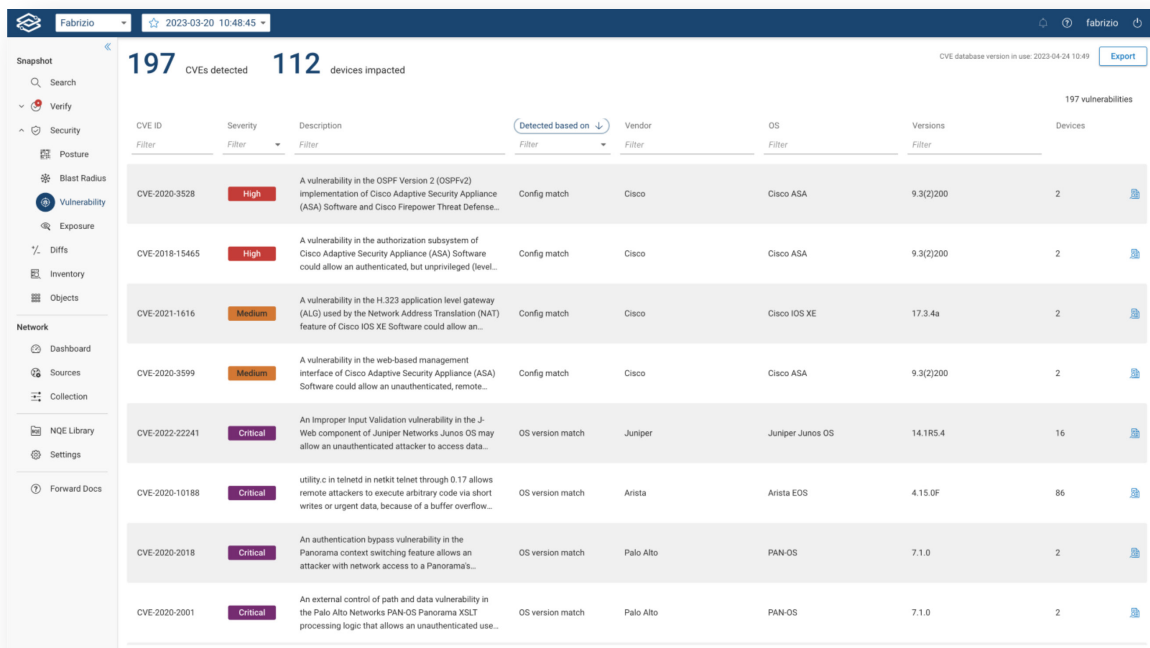
STEP 4: Validate security policies

Maintaining regulatory and security compliance is critical to NetOps and SecOps teams alike. During a merger or acquisition, they are asked to integrate networks that they cannot prove comply with their security policies or mandated regulations.

Forward Enterprise can mitigate the risk during this process by enabling your team to verify that the new organization's network behavior conforms with corporate policy. Using pre-built or custom intent checks, Forward Enterprise can evaluate the configurations of the new network and identify any non-compliant configurations. This information can be transferred into ServiceNow for immediate resolution.

STEP 5: Check for vulnerabilities

It's essential to verify that there are no critical vulnerabilities on devices in the new network before integration. Forward Enterprise integrates with the NIST database and vendor databases to identify Common Vulnerabilities and Exposures (CVEs) and compare them against the devices, operating systems, CVE specific configurations, and features in use. This will identify any issues in the new network and provide a prioritized remediation plan. This check runs continuously across the entire network, so SecOps and NetOps teams will always know their risks (see figure 5).



CVE ID	Severity	Description	Detected based on	Vendor	OS	Versions	Devices
CVE-2020-3528	High	A vulnerability in the OSPF Version 2 (OSPFv2) implementation of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense...	Config match	Cisco	Cisco ASA	9.3(2)200	2
CVE-2018-15465	High	A vulnerability in the authorization subsystem of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, but unprivileged level...	Config match	Cisco	Cisco ASA	9.3(2)200	2
CVE-2021-1616	Medium	A vulnerability in the H.323 application level gateway (ALG) used by the Network Address Translation (NAT) feature of Cisco IOS XE Software could allow an...	Config match	Cisco	Cisco IOS XE	17.3.4a	2
CVE-2020-3599	Medium	A vulnerability in the web-based management interface of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote...	Config match	Cisco	Cisco ASA	9.3(2)200	2
CVE-2022-22241	Critical	An Improper Input Validation vulnerability in the J-Web component of Juniper Networks Junos OS may allow an unauthenticated attacker to access data...	OS version match	Juniper	Juniper Junos OS	14.1R5.4	16
CVE-2020-10188	Critical	utility c in telnetd in netkit telnetd through 0.17 allows remote attackers to execute arbitrary code via short writes or urgent data, because of a buffer overflow...	OS version match	Arista	Arista EOS	4.15.0F	86
CVE-2020-2018	Critical	An authentication bypass vulnerability in the Panorama context switching feature allows an attacker with network access to a Panorama's...	OS version match	Palo Alto	PAN-OS	7.1.0	2
CVE-2020-2001	Critical	An external control of path and data vulnerability in the Palo Alto Networks PAN-OS Panorama XSLT processing logic that allows an unauthenticated use...	OS version match	Palo Alto	PAN-OS	7.1.0	2

Figure 5: Prioritized CVE report

Additionally, integration with vulnerability scanning tools like [Rapid7](#) and Tenable will identify within seconds which end-hosts impacted by critical vulnerabilities can be accessed from the internet or from any user-defined exposure point like a contractor’s VPN and which compromised end-hosts can access internal critical infrastructure, adding another layer of assurance that the new network is not introducing risk (see figures 6 and 7).

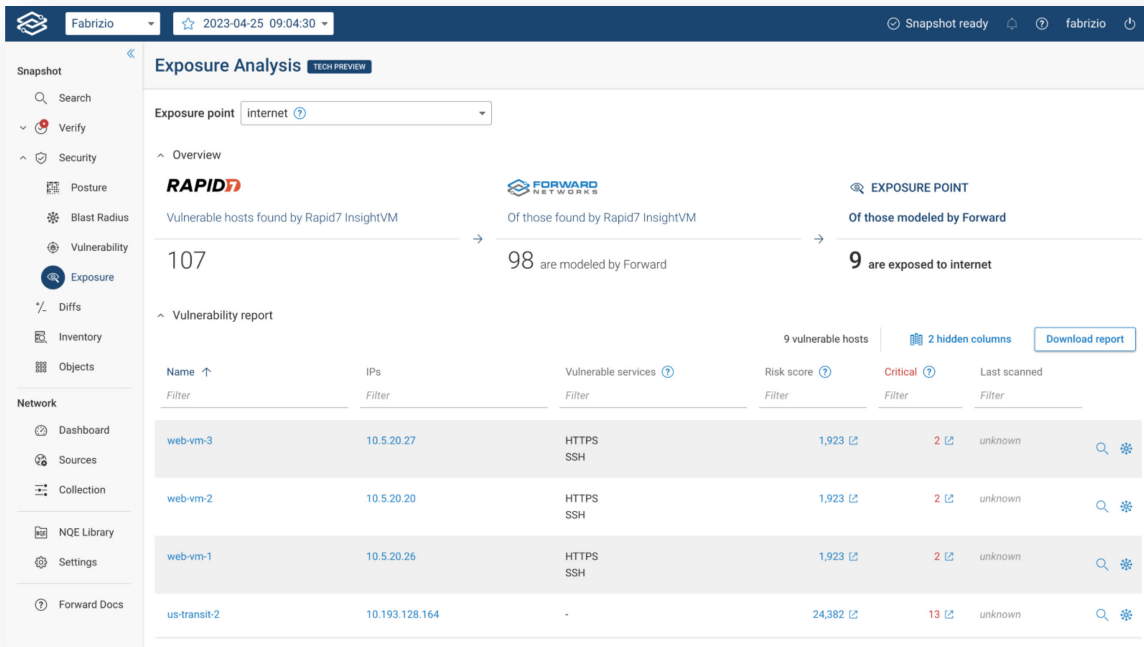


Figure 6: Rapid 7 integration

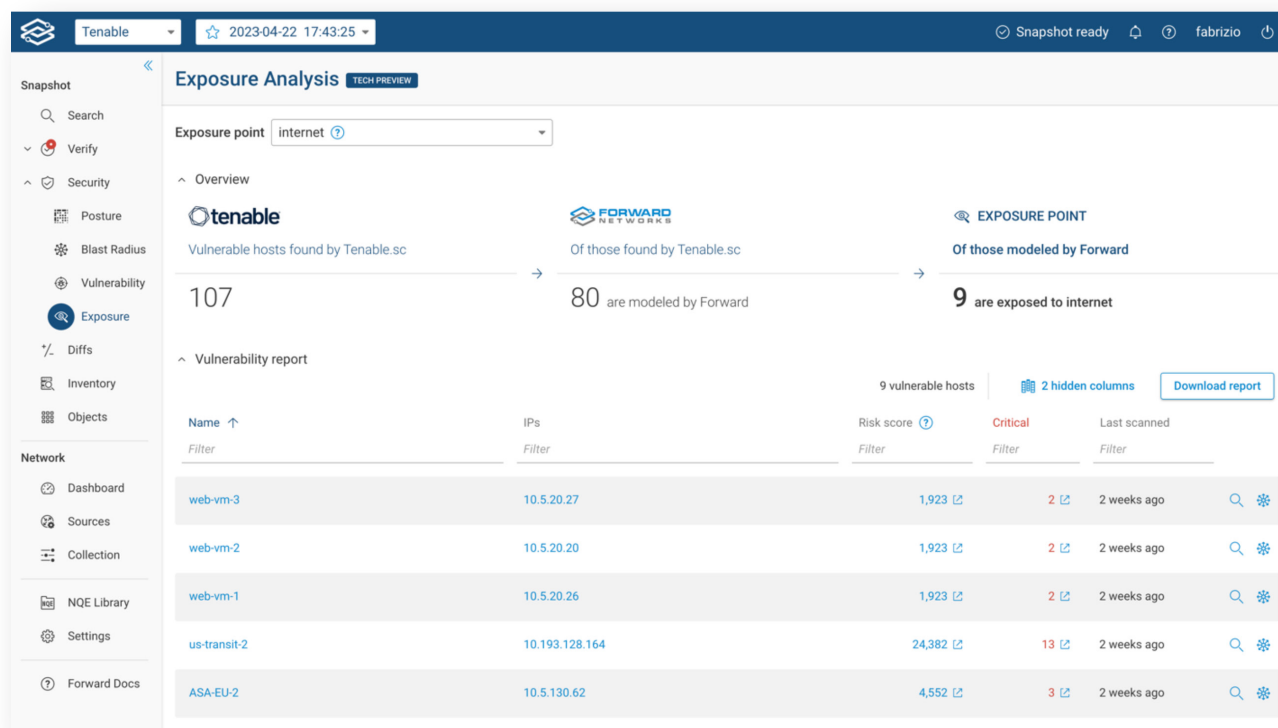


Figure 7: Tenable integration

STEP 6: Verify zone-to-zone security posture

Network segmentation is the backbone of a security policy. Before merging networks, engineering teams should evaluate the security posture of the new network and ensure that connectivity is as they desire. Doing this manually is time-consuming and labor-intensive.

Using the Forward Enterprise platform, they can get a current view of the complex zone-to-zone interactions occurring in the on-prem or multi-cloud network presented in one easy-to-understand visualization. It only takes a glance to see which zones have full, partial, or zero connectivity with color-coded status indicators to represent flow outcomes so that teams can confirm compliance at a glance (see figure 8).

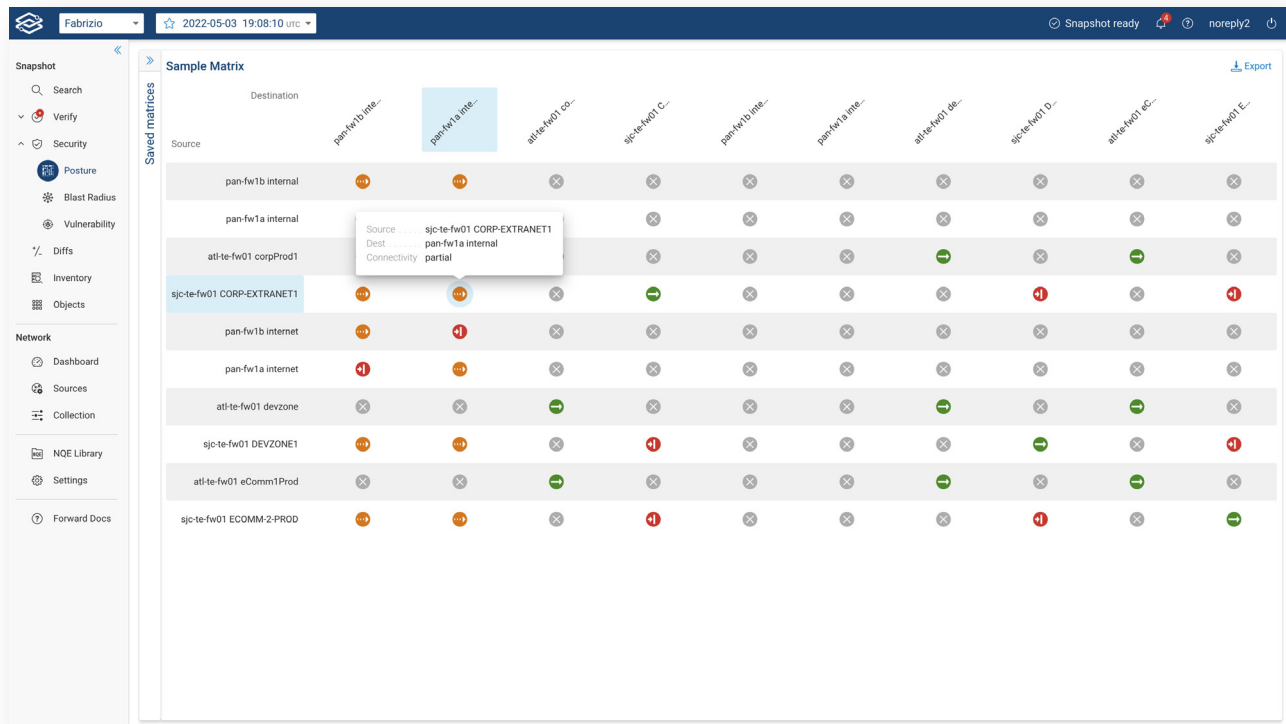


Figure 8: Zone-to-zone security posture

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
- **ORANGE:** partially connected
- **GREY:** no routing
- **RED:** fully isolated

A digital twin takes the guesswork out of merging networks

As the backbone of the business, IT is a critical dependency for a successful merger. Bringing two networks together is a complex process involving several teams of people. Trying to manually complete the steps laid out above would be a risky, time-consuming, and error-prone process. A digital twin can create a single source of truth that unifies the teams and provides a mathematically correct depiction of both the “home” network and the newly acquired company.

Once the process of documenting, visualizing, and verifying the security of the network is started, the platform regularly collects data – ensuring everyone is working from up-to-date information. It’s the only way to visualize your entire global network, including public clouds, in a single screen with the ability to drill down to specific device or instance configurations. This level of detailed data enables the digital twin to discover vulnerabilities and verify security posture to limit risk.

A merger would never happen without due diligence on the financial side; empowering IT teams with the same level of detailed data is critical to ensure their success.

To learn more, [request a demo](#).

ABOUT FORWARD NETWORKS

Forward Networks is revolutionizing the way large networks are managed. Forward’s advanced software delivers a “digital twin” of the network, enabling network operators to verify intent, predict network behavior, and simplify network management. The platform supports devices from all major networking vendors and cloud operators, including AWS, Azure, and Google Cloud Platform.

Forward Networks was founded in 2013 by four Stanford Ph.D. graduates and is headquartered in Santa Clara, California. Investors include Goldman Sachs, Andreessen Horowitz, Threshold Ventures, and A. Capital.

