FORWARD NETWORKS

USE CASE

Blast Radius Identification and Isolation

Most organizations today realize that it's not a matter of if, but when, they'll be the target of a disruptive, costly, and potentially, ruinous, cyberattack. And when it does happen, they want their security teams to contain and remediate the threat quickly. To do that, security operations professionals need to identify the compromised host, know what other devices are connected to that compromised host, and understand the traffic patterns between all of those objects.

However, security teams can't move fast if they need to sift through spreadsheets, perform data calls, and engage in other time-consuming processes to answer critical questions such as: What are all the possible paths attackers can take from the compromised host? What ports can they access? What objects are along these paths, and what do those devices touch? Is it possible for the attackers to move laterally in the network to reach critical systems or exfiltrate data to the internet?

Security teams need access to actionable information about everything in the network—what things are, where they are, how they interact, and all relevant details about their configuration and state. Ideally, they will also have at their fingertips the ability to not only isolate devices and cut off paths after an attack, but also prevent hosts from being vulnerable to attackers in the first place.

Understand Network Exposure to Cyber Threats With Mathematical Certainty

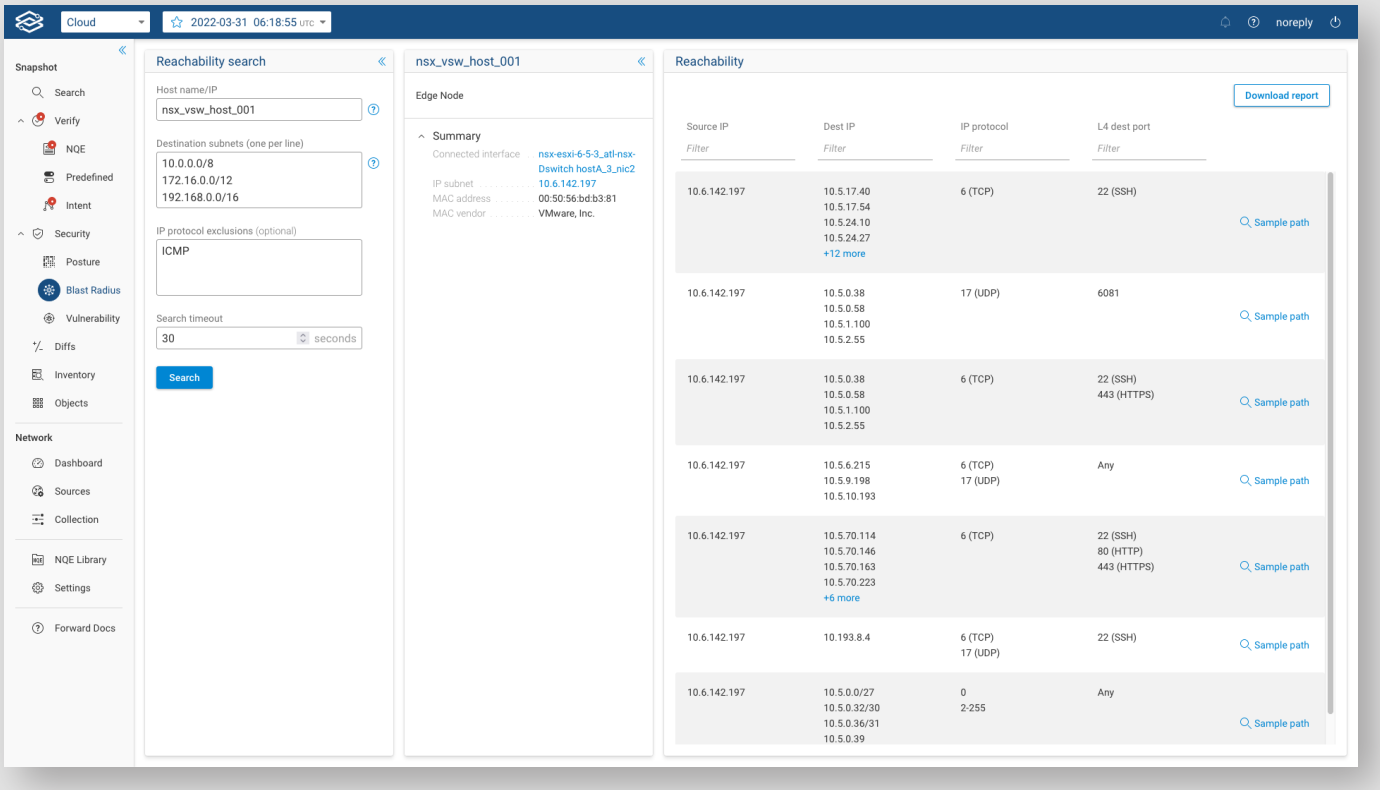
Forward Networks is the industry leader in network assurance and intent-based verification. Our platform is designed to regularly collect detailed L2 – L4 state and configuration information on the network, the exact information needed to understand the scope of an incident.

We developed our blast radius feature for identification and isolation in response to our customers' request that we engineer the Forward Enterprise platform to help them quickly understand their exposure in the event they have a compromised host in their network environment. We can now provide their security teams with the same searchable and actionable information about their network topology that we provide to their operations engineers through an interface that's quick and easy to navigate, highly visual, and capable of delivering immediate, detailed results.

Immediately Identify Compromised Hosts and Other Devices With Blast Radius

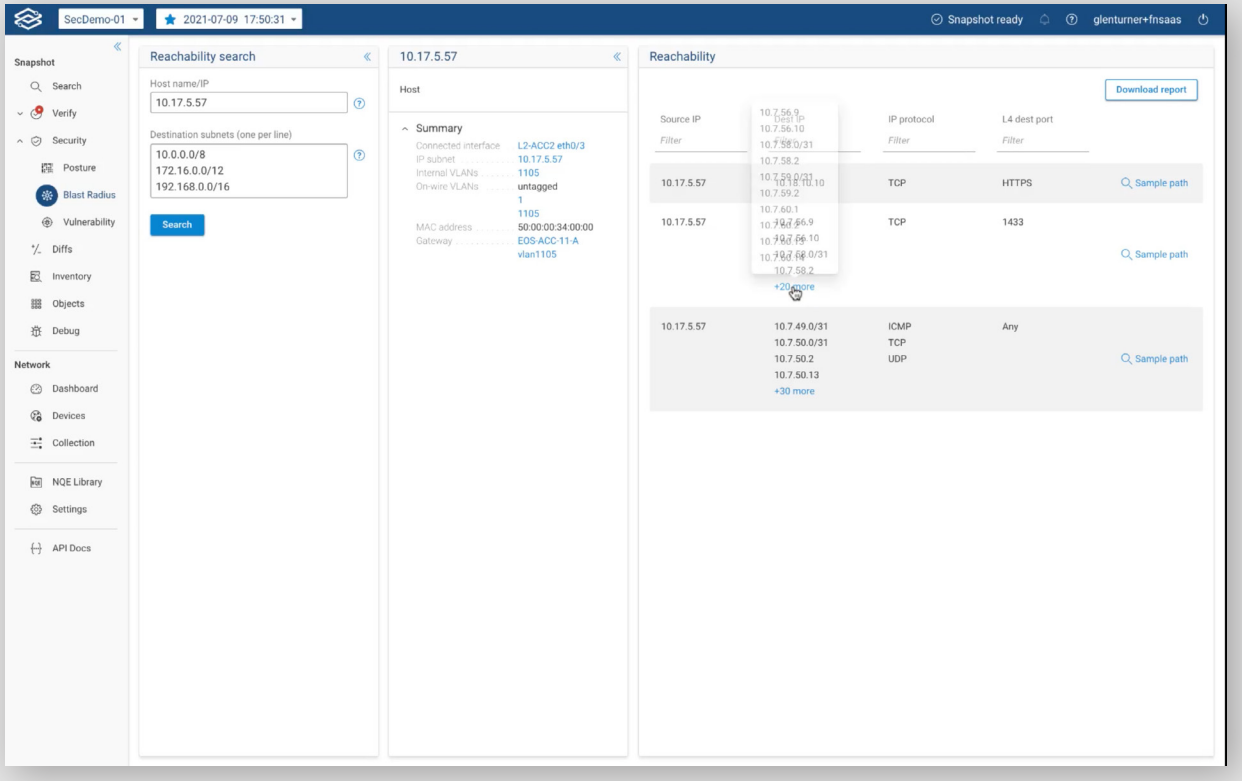
Think of the Forward Enterprise blast radius feature as an “easy button” for your security operations professionals, who need to move as fast as possible to contain and remediate cyber threats in your network. In one click, they can get detailed information about a compromised host, all the other devices connected to that compromised host, and traffic patterns.

Once the exposure is identified, isolating the devices is a much simpler and faster process. Following is an example of how security operations professionals would use the blast radius feature to locate the host device and document every destination, protocol, and L4 port it could possibly reach in seconds:



STEP 1

Select the Blast Radius feature under the security tab and input the hostname of the compromised device and any destination IP addresses that may be of interest. Then click on the blast radius button.



STEP 2

View a comprehensive topology and all possible flows from the host to the destination subnets including protocol and L4 destination port. In a single click, you can download a report that documents the blast radius.

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 complete 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 snapshots of network configurations, topology, and device state. 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 blast radius feature in the Forward Enterprise platform can help security operations professionals immediately identify compromised hosts and other potentially compromised devices and contain threats to your enterprise network — fast. 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 ›

FORWARD NETWORKS

www.forwardnetworks.com