Verification and validation to **enhance zero trust**

Kevin Kuhls
Technical Solutions Architect,
Forward Networks

PROTECTING GOVERNMENT SYSTEMS in today's ever-evolving threat landscape requires agencies to maintain a deep understanding of their networks and the efficacy of their zero trust architecture. Threats can lurk anywhere, so it's critical to gather information both quickly and completely about all the endpoints on the network. However, it's also important for agencies to monitor the system as a whole and understand all possible traffic patterns.

That visibility can uncover risks that agencies would not have seen otherwise, and it can form the basis of a comprehensive cybersecurity strategy that continually verifies whether agency security policies are performing as expected.

Ensuring security compliance

Networking teams rely on standard configurations to maintain the security policy. These standard configurations dictate connectivity and traffic flows to ensure users can access appropriate resources while preventing unauthorized access. The idea of a standard configuration seems simple, but maintaining it is extremely difficult.

Validating configurations is clearly mission critical, but monitoring and validating network behavior are even more telling and help ensure that policies are not inadvertently being circumvented and that there is no unintended connectivity.

It's impossible for a human being to proactively identify errant configurations within dynamic network environments. Most errors are not caught until there is a problem. One way to address this issue is by using a digital twin of the network to continually verify and validate the security posture. Regular intent checks can detect misconfigurations and immediately provide operations engineers with actionable alerts to remediate the situation before there is an incident. Proactive monitoring can also provide evidence of compliance in the event of an audit or identify changes during a specific time that may have caused an issue.

Agencies should also be able to visualize their zone-to-zone security policy at a glance to ensure that network changes don't introduce new errors and that connectivity remains as expected. Advanced digital twins exactly replicate the network and can be used to predict the impact of network changes before they are pushed live so that engineers can execute changes confidently.

In the era of software-defined networking, some security risks are more difficult than ever to detect, and engineers need to be able to query the network in ways

Shutterstock/FCW Staff

> **A digital twin helps IT administrators find answers to difficult questions** about individual devices or look at the whole system to find mathematically proven answers in seconds.

that traditional tools do not allow. To deliver on the intent of zero trust, security engineers must be able to identify network-based vulnerabilities due to traffic being virtually routed around enforcement points.

What is a digital twin?

A digital twin is a behaviorally accurate software copy of an entire network and all the devices on it — including all possible traffic paths. It helps IT administrators find answers to difficult questions about individual devices or look at the whole system to find mathematically proven answers in seconds. In the past, it could take hours to do that, or agencies might not have been able to answer those questions at all.

Likewise, a digital twin can verify segmentation in cases where multiple networks are riding on the same infrastructure to prove that mission-critical information and internet data are isolated from each other when they cross the same physical links.

A digital twin is an always-on tool that helps engineers visualize, verify, search and predict network behavior. By acting as a single source of truth for the entire network, it helps engineering teams move from a reactive to a proactive posture. ■

Kevin Kuhls is technical solutions architect at Forward Networks.