Cisco IT Brief

Cisco Tetration Analytics: Initial Implementation

What

Cisco IT, in collaboration with Cisco Insieme Business Unit (INSBU), recently completed the initial implementation of the Cisco® Tetration Analytics™ solution. The platform delivers behavior-based application insight with deep forensics, providing real-time visibility into traffic across all Cisco data centers and a better understanding of dependencies among applications. This implementation is part of a broader initiative to move our data centers to a Cisco Application Centric Infrastructure (Cisco ACI™) design. Cisco ACI allows us to use a common operating model across physical and virtual data center environments that is both application-aware and policy-based. Cisco Tetration Analytics is intended to help simplify and accelerate the ACI migration process and enable adoption of the ACI whitelist security model.

The Cisco Tetration Analytics architecture includes software ("host") sensors deployed on endpoints, such as virtual machines and bare metal servers, and hardware ("network") sensors embedded in Cisco Nexus 9000 Series network switches. The sensors gather telemetry data related to network flows from endpoints, interpacket variations that can be observed within traffic flows, and context details derived outside of packet details. Context details include information about who initiated a flow, and what processes and user IDs are associated with the flow. The sensors do not have visibility into the actual payload.

The Cisco Tetration Analytics engine in the platform analyzes telemetry data gathered from host and network sensors using advanced machine-learning techniques to identify application dependencies. The data collected from the sensors can also can be integrated with third-party metadata sources, such as an IP address management database, prior to analysis. Tetration Analytics administrators then create application views that depict application dependencies. Network, application, and security teams can access application network profiles and validate network flows through an easy-to-use web GUI interface.

Results

Cisco IT has deployed three functional clusters of the Tetration Analytics platform on premises, along with 10,000 sensors on Linux hosts to collect network flows for the analytics. In addition, we have tested this new approach to application migration with several use cases, including one for Hadoop, and have experienced positive outcomes.

"Our adoption of ACI is application-centric. And for the first time, we will be taking a multitenancy approach for our entire IT portfolio," says Anitha Parimi, Principal Engineer and IT Architect at Cisco. "We need visibility to understand what servers will make up an endpoint group, and how we should group different endpoints to create an application network profile. Without Tetration Analytics, there is no way that we could do this."

Next Steps

Cisco IT is now working to add a fourth cluster and develop other capabilities for the Tetration Analytics solution, such as a customizable notification system that can push out alerts about policy violations and other issues. Windows Agent also will be available soon. API access to raw data will be available in the next software release, as well. In the future, we plan to deploy Tetration Analytics host sensors on endpoints in the cloud (containers). We expect that, over time, the combination of Cisco Tetration Analytics and Cisco ACI will provide us with more capabilities for hardening network and data center security and for analyzing and improving application performance.

For More Information

How Cisco Tetration Analytics Helps Enable Cisco IT Migrate Applications to ACI

Cisco Tetration Analytics