Cisco Tetration Analytics and Infoblox Joint Solution

Highlights

• Advanced forensics enables you to search billions of flows in less than a second.
• A single Cisco Tetration Analytics™ appliance can monitor up to 1 million unique events per second and support 5000 unique endpoints.
• The open Cisco Tetration Analytics API fosters a broad ecosystem of partners.
• The combined Cisco® and Infoblox solution provides a zero-trust operational model, fivefold reduction in attack surface, and 200 percent faster application-behavior insights.

Introduction

Modern data centers are highly dynamic. With the use of virtualization technologies, container adoption, and workload mobility, applications are deployed rapidly, and communication patterns between application components are constantly shifting. Applications also move across data centers and across different infrastructures. And customers want a highly available network, with no scheduled or unscheduled downtime. This dynamic application environment presents a new set of challenges.

Customers may have no awareness of an application’s various components, communication patterns, and dependencies. They also may have no visibility into the application flows and the overall application behavior. Application components running in different infrastructures present challenges in enforcing a scalable security model: who can talk to whom, and on what ports, and using what protocols, etc. As a result, deviations are difficult to detect when workloads fail to adhere to policies. And increasing east-west traffic patterns exacerbate the problem by obscuring visibility and hindering forensics.

The Cisco Tetration Analytics™ and Infoblox joint solution enables enterprises to perform enhanced correlation of Domain Name System (DNS) query data with Cisco Tetration Analytics application flow data and provide enriched application insights to data center operators. The solution also helps customers perform efficient IP allocation for application and capacity planning, and it enhances security through anomaly detection and quarantine mechanisms.
Why existing approaches cannot meet these challenges

Existing approaches to data collection, analysis, and correlation do not meet the data center scale requirements needed for visibility, security, and forensics.

- Inability to collect consistent telemetry data needed to support data center scale: Most enterprises use outdated tools to collect data. Problems include lack of scalable telemetry data collection, inconsistent telemetry data coming from disparate data sources (syslog, Cisco® NetFlow, sampled flow [sFlow], and other tools), and network blind spots (typically encountered in traffic between virtual machines and across VLANs) that obscure visibility and forensics.
- Inability to analyze data in real time: Most tools that exist today cannot in real time analyze the volume of data that modern data centers receive, nor can they address operational issues comprehensively. Most tools try to support a single use case (for example, application performance). Also, these tools do not have the long-term data retention capabilities needed for effective forensics, and they tend to aggregate observations over a period of time. Hence customers end up with siloed tools for specific tasks without any correlation between them.
- Complexity associated with systems that have the technology to address the challenges:

Customers need advanced data scientists to implement algorithms to support these complex systems. These systems are expensive, cumbersome, and complicated to maintain.

Cisco Tetration Analytics and Infoblox solution

The Cisco Tetration Analytics platform uses advanced big data technologies such as unsupervised machine learning, behavioral analysis, and algorithmic approaches to provide a ready-to-use solution to address these challenges and critical data center operational use cases. The Cisco platform is designed for massive scalability and can process millions of flows per second to provide valuable application insights. The platform supports several important use cases, including application dependency mapping, whitelist policy generation and simulation, rule-based forensics and querying to identify anomalous flows, and easy troubleshooting.

Infoblox provides the industry-leading platform for secure DNS, Domain Host Configuration Protocol (DHCP), and IP address management (IPAM)—collectively referred to as DDI. By delivering actionable network intelligence through a centrally managed interface, Infoblox helps secure core network services, automate discovery and provisioning, and control a diverse architecture with powerful views and management features.

![Figure 1. Cisco Tetration Analytics and Infoblox combined solution](image-url)
The Infoblox platform comes ready to immediately integrate with existing workflow automation and security orchestration solutions to help ensure that intelligence can be shared with the existing networking and security infrastructure. For example, Infoblox can share discovered end-host and network parameters with other platforms. Infoblox also works with selected partners to share underlying data and insights through its representational state transfer (REST) and streaming APIs.

The Cisco Tetration Analytics and Infoblox platforms take complementary approaches to providing actionable intelligence to enterprises. The combination of Cisco Tetration Analytics and Infoblox’s analytics and discovered data provides a comprehensive context that allows enterprises to make better operational decisions and provide greater security.

Figure 1 provides an overview of the combined solution.

Solution use cases
This section presents two use cases for the Cisco Tetration Analytics and Infoblox solution.

Use-case 1: Enhance Cisco Tetration Analytics application insight with Infoblox DNS query records
Infoblox provides protocol-independent DNS query data, which is a good indicator of network traffic within the data center, across private and public clouds, and across the public Internet. Every day, users issue millions of queries to well-known external webpages, and each of these results in hundreds of subconnections and queries to traffic counters, adserving sites, etc. Enterprise administrators can view insights generated by Infoblox, generate reports based on these queries, and set up these queries to traverse the data for detailed analysis. The Cisco Tetration Analytics platform can use the insights generated by Infoblox and the cached DNS query data to better correlate and present the application dependencies to promote better decision making based on more comprehensive data sets. Infoblox uses a streaming API to provide this DNS query data to the Cisco Tetration Analytics platform.

Use-Case 2: Use Cisco Tetration Analytics data to enhance compliance and security for Infoblox customers
Data about data center application endpoints and devices must be consolidated for Infoblox IPAM. Combining Cisco Tetration Analytics analysis data with the data available in the Infoblox Actionable Network Intelligence platform (for example, application type, port, data center rack, and location) provides a more comprehensive context. The resulting insights generated by Infoblox help enhance security and improve application capacity planning and IP allocation for more efficient operations. Cisco Tetration Analytics sends anomalies and outlier data to Infoblox through the Cisco Tetration Analytics API for proper quarantine actions.

For example, if Infoblox detects an infected client, that may be the first indicator of a compromised system. By combining intelligence with the detailed flow data over time, available through the Cisco Tetration Analytics platform, Infoblox can provide a comprehensive view of the threat’s propagation through the enterprise network.

Conclusion
Business factors and technology trends including software-defined networking (SDN), DevOps, and containers mandate data center–wide visibility. Real-time application behavior insights are powered by machine learning and algorithms that enable pervasive visibility into applications and infrastructure. The combination of data derived from the Cisco Tetration Analytics and Infoblox platforms increases the accuracy of the analytics and provides the missing ingredient that enterprises need for their business transformation.

For more information
For additional information, see:
- https://www.cisco.com/go/aci
- https://www.cisco.com/go/dcecosystem
- https://www.cisco.com/go/infoblox