Solution Overview

Cisco Tetration Analytics and Tufin Orchestration Suite Solution

Solution Highlights
- Visualize security policy using network flow data.
- Discover application connectivity in complex, hybrid environments.
- Measure application compliance with security policy.
- Maintain service uptime while rapidly responding to business change.
Introduction

Modern data centers are dynamic, with virtualization technologies, container adoption, and workload mobility promoting rapid application deployment and constantly shifting communication patterns between application components. Applications move across data centers and on different infrastructures. In addition, customers want a highly available network with no scheduled downtime. This dynamic application environment presents a new set of challenges.

Customers have limited visibility into an application’s components and their communication patterns, the application interdependencies, and the application’s dependency on the infrastructure. Also, they have no visibility into the application flows and the overall application behavior. Application components running on different infrastructures present challenges in enforcing a scalable security model: in determining who can talk to whom, and on what ports, and using what protocols, etc. As a result, it is hard to identify deviations when workloads fail to adhere to policies. The increasing east-west traffic patterns exacerbate the situation by obscuring visibility and hindering forensics.

By combining unsupervised machine learning, behavior analysis, and intelligent algorithms, the Cisco Tetration Analytics™ platform brings a new level of network and security analysis to the data center. Using this application insight, Tufin Orchestration Suite enables customers to discover applications, identify existing security policy based on network flows, and assess application compliance with security policy.

Customers can help ensure that applications comply with security policy while maintaining service uptime and business continuity to keep pace with today’s rapidly changing business needs.

Why Existing Approaches Cannot Meet These Challenges

Existing approaches to data collection, analysis, and correlation fail to provide the data center scale needed to address today’s visibility, security, and forensics requirements.

- Inability to collect consistent telemetry information to support data center scale: Most enterprises use outdated tools to collect data.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 such as system logs (syslogs), Cisco® NetFlow, sampled flow (sFlow), etc.; and network blind spots (typically encountered in traffic between virtual machines and across VLANs) that obscure visibility and hinder forensics.
- Inability to analyze data in real time: Most tools that exist today cannot analyze in real time the volume of data that flows through modern data centers and so cannot address the operational issues comprehensively. Most tools aim to support a single use case (for example, application performance). Also, these tools do not provide long-term data retention capabilities for effective forensics and tend to aggregate observations over a period of time. Hence, customers end up with separate tools for different use cases without any correlation between them.
- Complexity of those systems that have the technology to address the challenges: Customers need advanced data scientist resources to implement algorithms to support many use cases. This approach is expensive, cumbersome, and complicated to maintain.
Cisco Tetration Analytics and Tufin Orchestration Suite Solution

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

With the Cisco Tetration Analytics and Tufin Orchestration Suite solution, users can discover, monitor, modify, and validate application connectivity in the data center and the cloud in compliance with their security policy. Using the advanced behavioral analytics of the Cisco Tetration platform, users of Orchestration Suite gain greater insight into application and endpoint connectivity, enabling them to discover applications in use. Users can also help ensure that applications comply with security policy while maintaining service uptime and business continuity to keep pace with today’s rapidly changing business needs.

By combining the Cisco Tetration Analytics platform with Tufin Orchestration Suite, users achieve greater business agility without sacrificing security when implementing new applications or modifying existing ones.

Use Case 1: Application Modeling

Customers can use Tufin SecureApp to model application connectivity across heterogeneous, complex network environments. With the Cisco Tetration Analytics platform, customers can use the abundant flow information to discover application connectivity that may have been previously unavailable through firewall configuration files and model these connections in SecureApp (Figure 1).

Use Case 2: Policy Learning

Using the flows produced by the Cisco Tetration Analytics platform, users of Tufin Orchestration Suite can define, optimize, and monitor their security policy vs. actual behavior. Using Orchestration Suite, Cisco Tetration Analytics customers can:

• Learn and populate the Tufin Unified Security Policy (USP) from the network flows.
• Enforce the policy on the enterprise network after the policy is established.
• Evaluate flows against the pre-established policies to identify discrepancies and optimize them.

Use Case 3: Connectivity Analysis

Maintaining business connectivity, especially in large and complex environments. Tufin’s interactive topology map allows users to visualize and understand how flows are implemented across their heterogeneous corporate networks. Combined with the Tetration Analytics, this analysis now also shows the actual network behavior on top of the intended behavior – this provides unprecedented visibility and accelerated mean-time-to-resolution when it is most needed.
Main Features and Benefits

The joint Cisco and Tufin solution provides many benefits:

- Discover, monitor, modify, and validate application connectivity.
- Discover applications in use.
- Discover rough applications.
- Learn the effective security policy from applications flows.
- Monitor compliance with security policy.
- Optimize security policies.
- Achieve business agility without sacrificing security.
- Maintain service uptime and business continuity.

Conclusion

Business factors and trends such as software-defined networking (SDN), DevOps, and containers mandate visibility across the entire data center. Real-time application behavior insight powered by machine learning and algorithms enables pervasive visibility into both applications and infrastructure. The Cisco Tetration Analytics platform is the missing component that enterprises need to propel their business transformation.

For More Information

www.cisco.com/go/tetration