Cisco Tetration Analytics & Tufin Orchestration Suite

Solution Brief

Solution Highlights

- **Visualize network security and connectivity in complex, hybrid environments**
- **Discover application connections automatically using network flow data**
- **Examine and enforce application compliance with security standards and industry regulations**
- **Accelerate application migration with zero-touch change automation**
- **Reduce the attack surface with streamlined application decommissioning**

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. Furthermore, 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.

Benefits

- **Enhance agility** with application-centric automation for network security policy changes
- **Reduce complexity** by managing enterprise security policies from a single pane of glass
- **Strengthen the security posture** by extending micro-segmentation across hybrid networks
- **Reduce time and effort invested in audit readiness** with continuous compliance
- **Gain visibility of applications' security and connectivity** across cloud and on-prem infrastructure
- **Ensure service uptime** with interactive topology map for connectivity analysis and troubleshooting
- **Increase control with a unified console** supporting all leading enterprise platforms – traditional networks and firewalls, SDN platforms and cloud platforms

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.

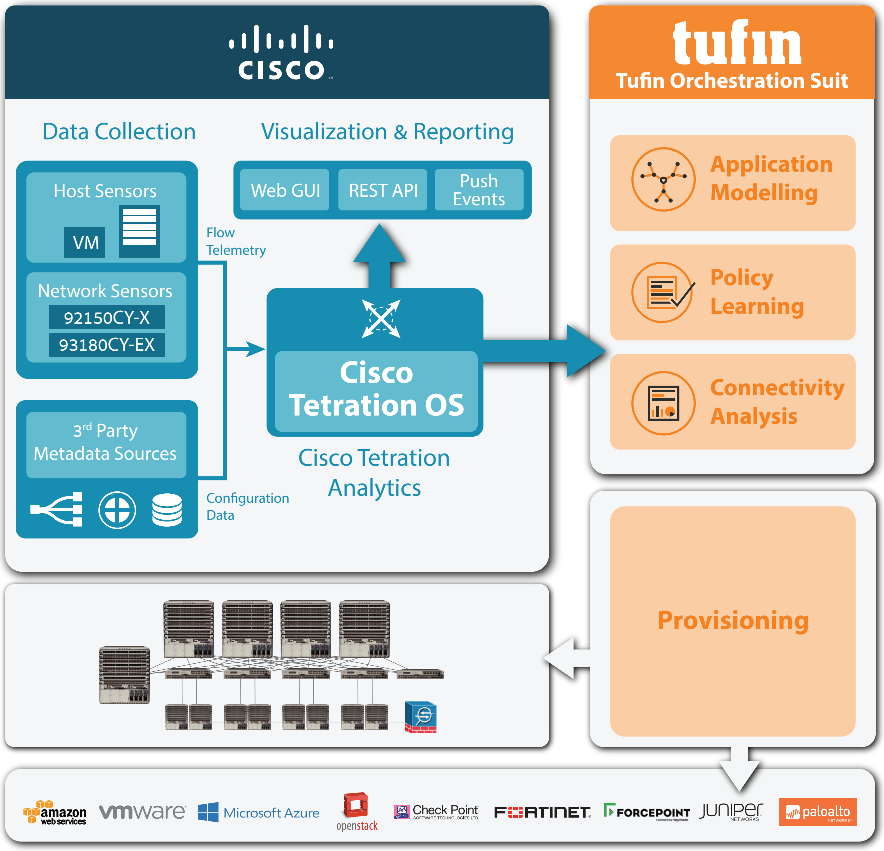
- **Inability to assess whether applications and traffic flows are in compliance:** Customers need a way to define and enforce a central security policy across the hybrid network to ensure compliance with industry regulations and with security standards

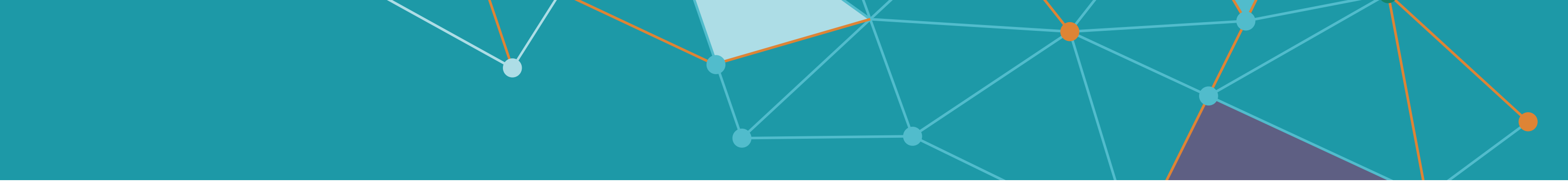
Cisco Tetration Analytics & Tufin Orchestration Suite Solution

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.

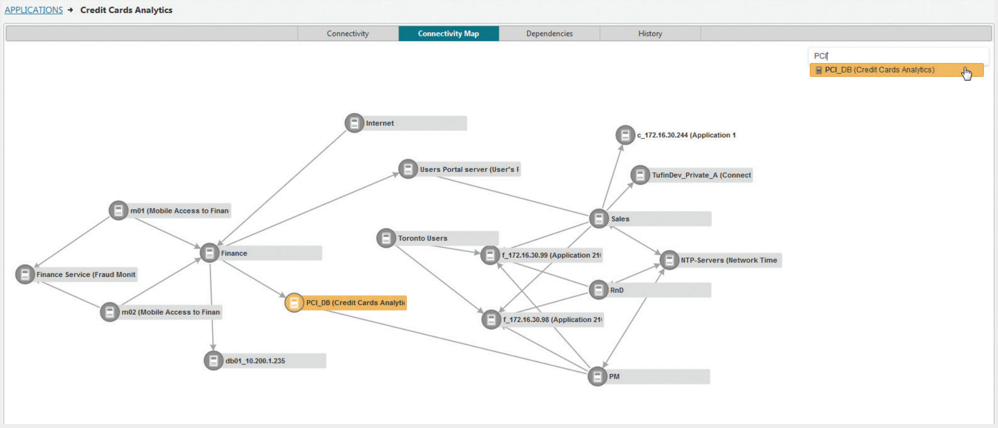
With the Cisco Tetration Analytics and Tufin Orchestration Suite solution, users can discover, monitor, modify, and validate application connectivity in the data center and the cloud in compliance with their security policy. Using the advanced behavioral analytics of the Cisco Tetration platform, users 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 and Visualization



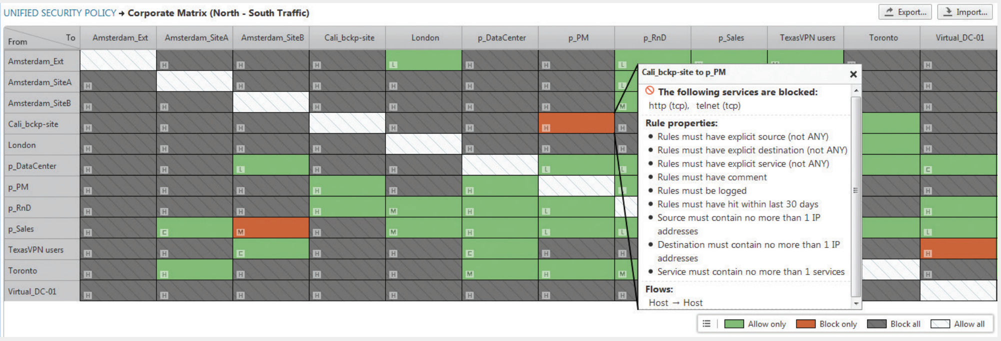
APPLICATIONS → Credit Cards Analytics

Connectivity
Connectivity Map
Dependencies
History
PCI
PCI_DB (Credit Cards Analytics)
Internet
c_172.16.30.244 (Application 1
Users Portal server (User's I
TufinDev_Private_A (Connect
m01 (Mobile Access to Finan
Sales
Toronto Users
Finance
f_172.16.30.99 (Application 21
NTP-Servers (Network Time
Finance Service (Fraud Monit
RnD
PCI_DB (Credit Cards Analytic
m02 (Mobile Access to Finan
f_172.16.30.98 (Application 21
db01_10.200.1.235
PM

Figure 1: Application Modeling in Tufin Orchestration Suite

Customers can use Tufin Orchestration Suite's SecureApp to Model and visualize 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: Application Compliance



UNIFIED SECURITY POLICY → Corporate Matrix (North - South Traffic)

From \ To	Amsterdam_Ext	Amsterdam_SiteA	Amsterdam_SiteB	Cali_bckp-site	London	p_DataCenter	p_PM	p_RnD	p_Sales	TexasVPN users	Toronto	Virtual_DC-01
Amsterdam_Ext		H	H	H	L	H	H	L				H
Amsterdam_SiteA	H		H	H	H	H	H	L				H
Amsterdam_SiteB	H	H		H	H	H	H	M				H
Cali_bckp-site	H	H	H		H	H	H	H				H
London	H	H	H	H		H	H	H				H
p_DataCenter	H	H	L	H	H		L	L				C
p_PM	H	H	H	H	H	H						H
p_RnD	H	H	H	H	M	H	L					H
p_Sales	H	C	M	H	M	H	L	L				L
TexasVPN users	H	H	C	H	H	C	H	H				H
Toronto	H	H	H	H	H	M	H	M				H
Virtual_DC-01	H	H	H	H	H	H	H	H				

Cali_bckp-site to p_PM

The following services are blocked:
http (tcp), telnet (tcp)

Rule properties:

- Rules must have explicit source (not ANY)
- Rules must have explicit destination (not ANY)
- Rules must have explicit service (not ANY)
- Rules must have comment
- Rules must be logged
- Rules must have hit within last 30 days
- Source must contain no more than 1 IP addresses
- Destination must contain no more than 1 IP addresses
- Service must contain no more than 1 services

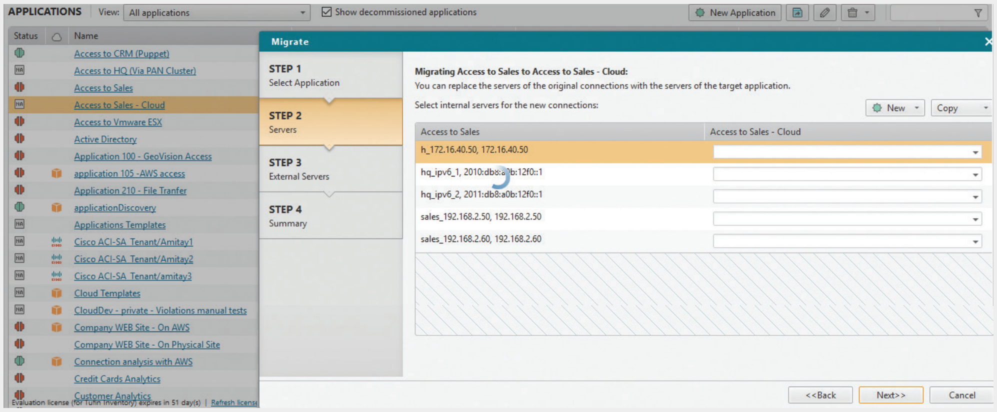
Flows:
Host → Host

🟩 Allow only 🟥 Block only ▨ Block all □ Allow all

Figure 2: Identify and control applications connection that violate security policy

Once applications are modeled based on Tetration flows analytics and imported into Tufin's SecureApp, customers can run compliance analysis to identify application connections that violate security standards and industry regulations. This allows customers to save time and efforts dedicated to audit preparations and to ensure security and compliance across the hybrid network.

Use Case 3: Application Migration and Service Delivery



APPLICATIONS View: All applications ☑ Show decommissioned applications

Access to CRM (Puppet)
Access to HQ (Via PAN Cluster)
Access to Sales
Access to Sales - Cloud
Access to Vmware ESX
Active Directory
Application 100 - GeoVision Access
application 105 -AWS access
Application 210 - File Tranfer
applicationDiscovery
Applications Templates
Cisco ACI-SA Tenant/Amitay1
Cisco ACI-SA Tenant/Amitay2
Cisco ACI-SA Tenant/amitay3
Cloud Templates
CloudDev - private - Violations manual tests
Company WEB Site - On AWS
Company WEB Site - On Physical Site
Connection analysis with AWS
Credit Cards Analytics
Customer Analytics

Evaluation license (for Tufin Inventory) expires in 51 day(s) | Refresh license

Migrate

STEP 1 Select Application
STEP 2 Servers
STEP 3 External Servers
STEP 4 Summary

Migrating Access to Sales to Access to Sales - Cloud:
You can replace the servers of the original connections with the servers of the target application.

Select internal servers for the new connections:

Access to Sales	Access to Sales - Cloud
h_172.16.40.50, 172.16.40.50	
hq_ipv6_1, 2010:db8:a0b:12f0::1	
hq_ipv6_2, 2011:db8:a0b:12f0::1	
sales_192.168.2.50, 192.168.2.50	
sales_192.168.2.60, 192.168.2.60	

Figure 3: Application migration automated workflow in Tufin SecureApp

Customers can use Cisco Tetration Analytics & Tufin Orchestration Suite for rapid and secured applications' migration to hybrid cloud platforms and micro-service architectures. Based on the imported application model Tufin automatically implements connectivity flows across vendors and platforms with built-in policy controls, to boost agility without compromising security.

Cisco Tetration Analytics & Tufin Orchestration Suite

Main Features & Benefits

The joint Cisco Tetration Analytics and Tufin Orchestration Suite solution provides many benefits:

- Discover, monitor, modify and validate application connectivity
- Discover applications in use
- 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. Once in-depth visibility is granted, vetting application compliance and measuring risk exposure are critical element for achieving audit readiness and prevent your next organization cyber breach. Going forward, organizations who leverage Tufin's & Cisco's synergy will dramatically increase their business agility without sacrificing security. The Cisco Tetration Analytics 2.0 platform together with Tufin Orchestration suite R17.1 GA are the missing components that enterprises need to propel their business transformation.

About Tufin

Tufin®, the leader in Network Security Policy Orchestration, allows enterprises to streamline the management of security policies across complex, heterogeneous environments. Serving over 1,900 customers, Tufin's network security automation enables enterprises to implement changes in minutes with proactive risk analysis and continuous policy compliance. Tufin assures business continuity with a robust security posture, rapid service delivery and regulatory compliance across physical, private, public and hybrid cloud environments. Find out more: www.tufin.com.