Cisco Tetration Analytics & Tufin Orchestration Suite

Solution Brief

Solution Highlights

- Enforce enterprise-wide unified security policy
- Assure application security and compliance
- Define, optimize, and monitor security policy and make policy recommendations
- Monitor actual network behavior as compared to intended network behavior
- Ensure that discovered policies are in-line with security policy and firewall rules
- Automate security policy changes based on application definitions
- Migrate applications to hybrid cloud platforms and micro-service architectures

Introduction

New Challenges

Modern data centers are a dynamic combination of public and private clouds virtualized networks, and on-prem infrastructures. Workload mobility, the adoption of containers, and constantly shifting communication patterns between application components, are increasing the complexity of managing these heterogeneous, hybrid cloud networks. In addition, organizations are supporting a diverse set of applications that move across data centers and infrastructures, and internal users are demanding rapid application change deployment. The challenge is exacerbated by the fact that customers expect a seamless experience from a highly available network with no downtime. This dynamic application environment presents a whole new set of challenges for IT and security professionals.

Limited Visibility

Organizations have limited visibility into application components, communication patterns, interdependencies, and Infrastructure dependencies, and have no visibility into application flows and the overall application behavior. Application components running on different infrastructures present hurdles for enforcing network segmentation, microsegmentation, and a scalable security model, such as determining who can talk to whom, on what ports, and using what protocols. As a result, it is hard to identify deviations when workloads fail to adhere to policies. The increasing East-West traffic patterns intensify the situation by further obscuring visibility and hindering forensics.

Cisco Tetration Analytics™ & Tufin Orchestration Suite™

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. Tufin Orchestration Suite™ integrates with Cisco Teteration Analytics and uses this application insight to discover and model business applications, identify existing security policy based on network flows, and assess application compliance in relation to security policy. Together, Tufin Orchestration Suite and Cisco Tetration Analytics guarantee applications comply with security policy, maintain service uptime, and ensure the business continuity needed to keep pace with today's rapidly changing business needs.

Benefits

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

Cisco Tetration Analytics & Tufin Orchestration Suite

Why Existing Approaches Cannot Meet These Challenges

Existing approaches to data collection, analysis, and correlation fail to provide the scale needed in the data center to address today's visibility, security, and forensics requirements because of the:

- **Inability to collect consistent telemetry information to support data center scale:** Most enterprises use outdated tools to collect data, leading to problems that include a lack of scalable telemetry data collection 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 in existence today are unable to analyze in real-time the volume of data that flows through modern data centers and cannot address operational issues comprehensively. Existing tools only support a single use case, such as application performance, do not provide long-term data retention capabilities for effective forensics, and instead aggregate observations. This lack of real-time analysis leaves organizations with disparate tools that lack correlation.

- **Complexity of systems to address challenges:** To provide the needed information to support their many use cases, organizations require advanced data science resources to develop and implement complex algorithms. This approach is expensive, cumbersome, and complicated to maintain.

- **Inability to assess whether applications and traffic flows are in compliance:** Without a way to define and enforce a central security policy across the hybrid network, organizations cannot ensure compliance with industry regulations and security standards.

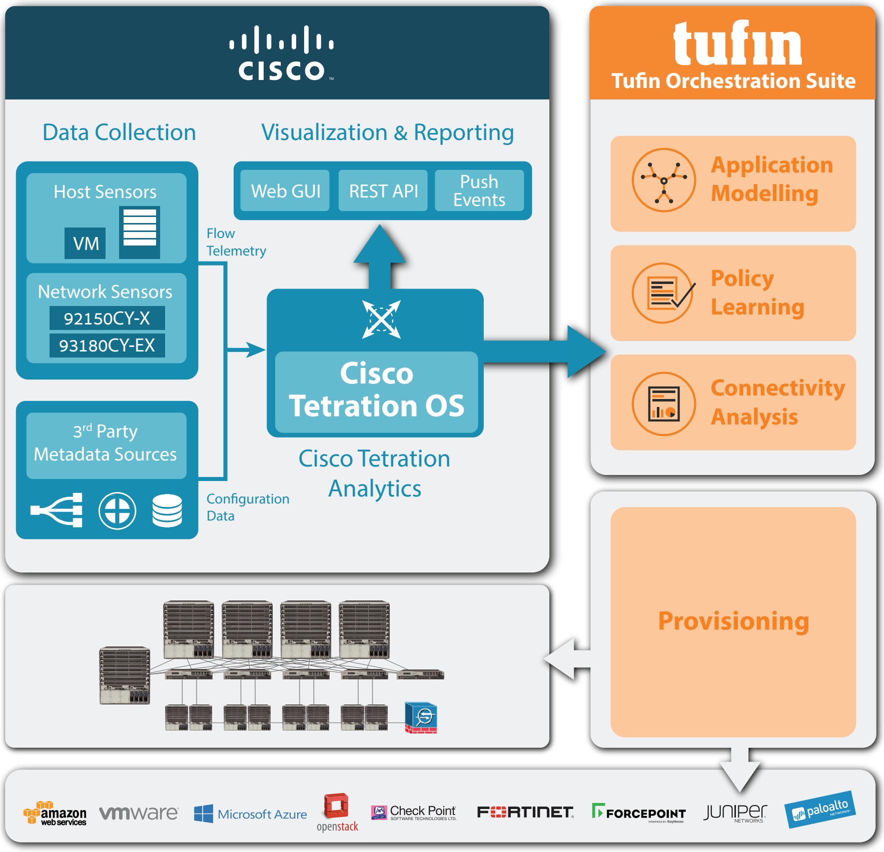
Cisco Tetration Analytics™ & Tufin Orchestration Suite™

The Cisco Tetration Analytics platform uses advanced big data and analytics for unsupervised machine learning and behavioral analysis, and employs an algorithimic approach to provide a ready-to-use solution to address critical data center use cases.

Cisco Tetration is built for massive scalability and can process millions of flows per second to provide valuable application insights. The platform supports 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.

When combined, the Cisco Tetration Analytics and Tufin Orchestration Suite solution makes it possible to segment applications, automate policy enforcement and provide users with the ability to 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 Analytics platform, users of Tufin Orchestration Suite gain greater insight into application and endpoint connectivity, discover applications already in use, and implement new applications or modify existing applications without sacrificing security. 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 and achieve greater business agility.



Use Case 1: Application Modeling and Visualization

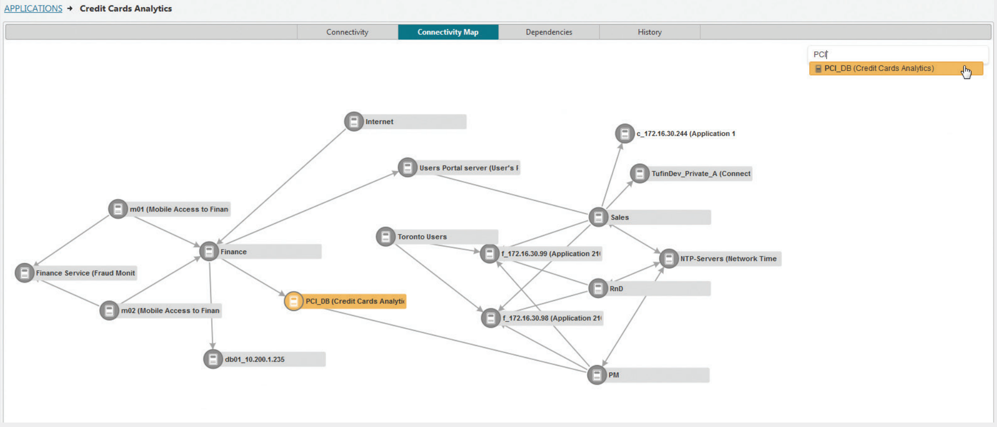
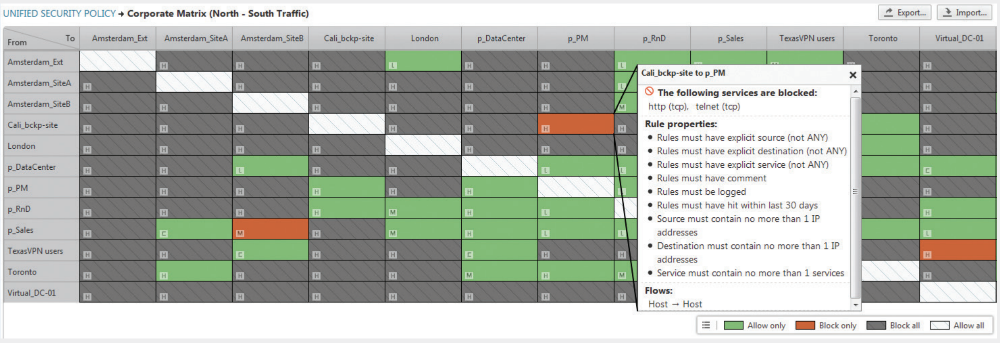

APPLICATIONS → Credit Cards Analytics
Connectivity
Connectivity Map
Dependencies
History
PCI
PCI_DB (Credit Cards Analytics)
Internet
Users Portal server (User's I
m01 (Mobile Access to Finan
Finance
Finance Service (Fraud Monit
m02 (Mobile Access to Finan
PCI_DB (Credit Cards Analytic
db01_10.200.1.235
Toronto Users
f_172.16.30.99 (Application 21
f_172.16.30.98 (Application 21
c_172.16.30.244 (Application 1
TufinDev_Private_A (Connect
Sales
NTP-Servers (Network Time
RnD
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 of information to discover application connectivity that may have been previously unavailable through firewall configuration files and model these. (Figure 1)

Use Case 2: Application Compliance


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

Export... Import...

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	□	L			▨	▨ 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

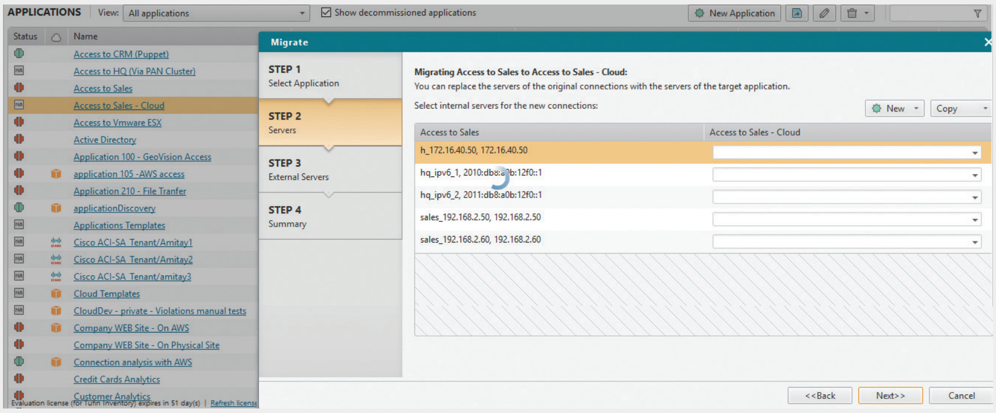
Flows:
Host → Host

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

Figure 2: Identify and control application connections that violate security policy

Once applications are modeled in Tetration Analytics and imported into Tufin SecureApp, customers can run compliance analysis to identify application connections that violate security standards and industry regulations. This allows customers to save time and effort on audit preparations and ensure security and compliance across the hybrid network. (Figure 2)

Use Case 3: Application Migration and Service Delivery


APPLICATIONS View: All applications ☑ Show decommissioned applications New Application

Status | Name

- 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: New Copy

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	

<<Back Next>> Cancel

Figure 3: Application migration automated workflow in Tufin SecureApp

Customers use Cisco Tetration Analytics & Tufin Orchestration Suite for rapid and secured application migration to hybrid cloud platforms and microservice architectures. Based on the imported application model, Tufin Orchestration Suite automatically implements connectivity flows across vendors and platforms with built-in policy controls to boost agility without compromising security. (Figure 3)

Cisco Tetration Analytics & Tufin Orchestration Suite

Benefits

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

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 and 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 elements for achieving audit readiness and preventing your next cyber breach. Organizations who leverage the synergy of Cisco Tetration Analytics together with Tufin Orchestration Suite will dramatically increase their business agility without sacrificing security and propel their business transformation.

About Tufin

Tufin is the leader in Network Security Policy Orchestration, serving more than half of the top 50 companies in the Forbes Global 2000. Tufin simplifies management of some of the largest, most complex networks in the world, consisting of thousands of firewall and network devices and emerging hybrid cloud infrastructures. Enterprises select the award-winning Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. Tufin reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. Its network security automation enables enterprises to implement changes in minutes with proactive risk analysis and continuous policy compliance. Tufin serves over 2,100 customers spanning all industries and geographies; its products and technologies are patent-protected in the U.S. and other countries. Find out more at www.tufin.com.

www.tufin.com