tufin

Strengthening Data Protection for GDPR Compliance

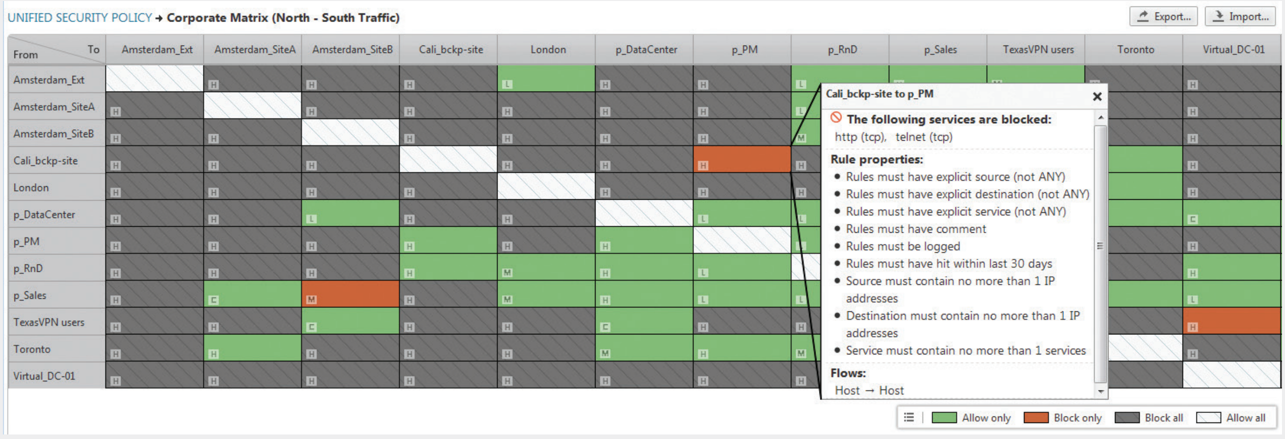
Protect Personal Data with Network Security Policy Management

Solution Brief

The General Data Protection Regulation (GDPR) is a regulation that the European Parliament, Council of the European Union, and the European Commission passed to improve how corporations protect and handle personal data of EU citizens in and outside of the EU. The introduction of GDPR and the steep penalties for non-compliance require global organizations to redefine their corporate security policy. In particular, the definition of what constitutes personal data is significantly broadened by GDPR and requires a more granular view of applications and the users that have access to them. Network Security Policy Management (NSPM), already a standard to meet PCI DSS and other compliance mandates, enables organizations to address certain GDPR requirements by mapping the network topology and establishing a unified security policy for segmentation across the entire hybrid network.

Data Protection by Default and Design (Section 1, Article 25)

To ensure personal data is protected by design, organizations need to define and enforce a unified segmentation policy that spans across the hybrid network. The complexity introduced by a multi-vendor, multi-platform environment makes it difficult to consistently enforce security policy and identify risks. Tufin provides a central solution to help security teams segment the network into zones, define the desired policy for access between zones, and continuously enforce the policy across firewalls, routers, SDN and public cloud platforms.



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	⬜	🟩 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

Data Protection by Design with Tufin Orchestration Suite™
The Unified Security Policy is a zone-to-zone matrix showing the desired network segmentation baseline of the organization

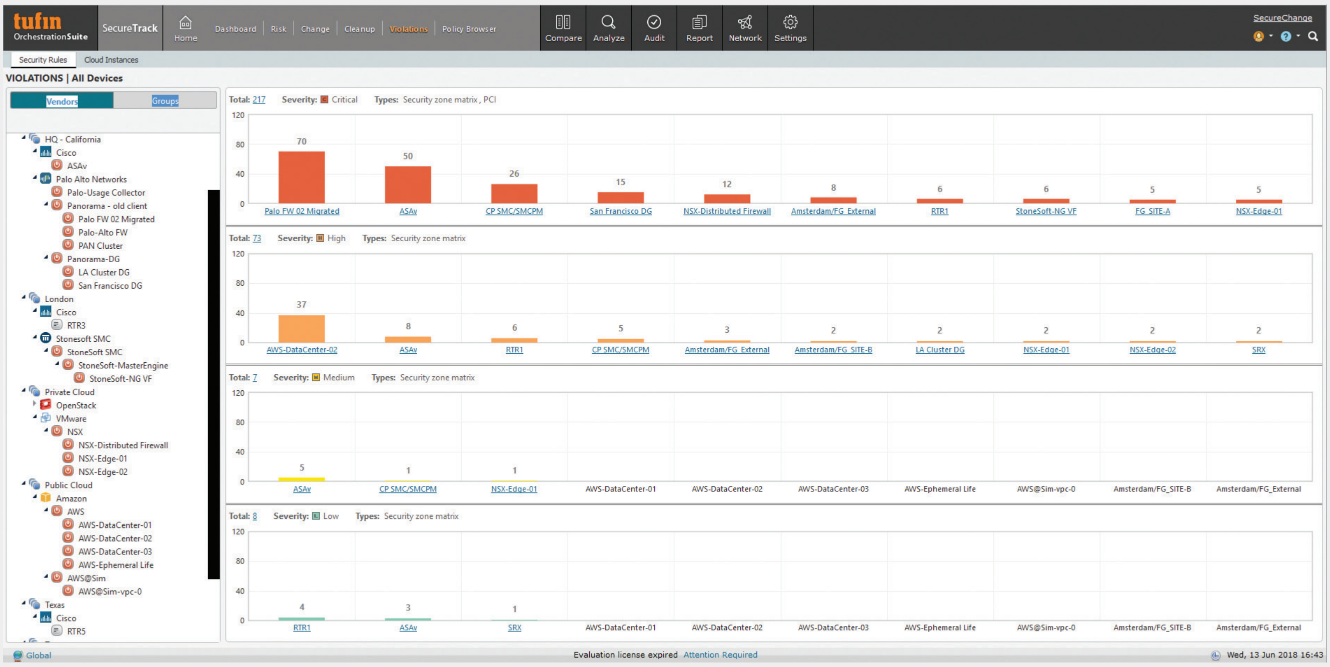
Tufin identifies violations to the unified security policy and enables mitigating them from a central console to retain a state of compliance. Tufin policy-based automation ensures continuous compliance with the desired network segmentation policy. This is done by assessing the risk of new access requests against the unified security policy to identify and prevent potential violations. In addition to that Tufin reduces the exposure of firewall policies by automatically identifying and removing unused and redundant rules, and by tightening permissive rules according to a traffic-based analysis.

Records and Security of Processing Activities (Section 1, Article 30 & Section 2, Article 32)

The requirement to track and report on changes to the network is a critical requirement for all common regulatory mandates, including GDPR. In the course of network expansion and transition – especially through the adoption of private and public cloud – common in-house solutions like documenting changes in Excel become unmanageable and unreportable. Tufin provides a solution for centrally monitoring and reporting on security policy changes across the hybrid network in order to help organizations demonstrate compliance. Tufin also provides a configurable change workflow to ensure the confidentiality and integrity of processing access changes by maintaining separation of duties.

Data Protection Impact Assessment (Section 3, Article 35)

Compliance is an ongoing process that begins with defining the specific benchmarks of compliance for your unique environment. Proactive analysis and real-time assessment of policy changes are required to achieve continuous compliance, protect the organization from cyberattacks, and avoid penalties. Tufin provides a solution for real-time alerts on violations, proactive assessment of risks, and central reports for physical network and hybrid cloud platforms to help organizations demonstrate compliance with GDPR and prepare for audits.



VIOLATIONS | All Devices

Total: 217   Severity: C Critical   Types: Security zone matrix , PCI

Total: 73   Severity: H High   Types: Security zone matrix

Total: 7   Severity: M Medium   Types: Security zone matrix

Total: 8   Severity: L Low   Types: Security zone matrix

Evaluation license expired Attention Required

Wed, 13 Jun 2018 16:43

An Assessment of Safeguards with the Tufin Orchestration Suite™
The violations dashboard summarizes compliance violations by risk level across the next generation network.

Summary: Meeting GDPR Compliance without Compromising Agility

Network Security Policy Management tools enable organizations to eliminate the tradeoff between agility and security. Tufin introduces a policy-driven approach to automating and orchestrating changes across heterogeneous networks. Tufin Orchestration SuiteTM allows network and security teams to implement changes to access policy in minutes while ensuring continuous compliance with internal security policies and external industry regulations, including the above GDPR mandates.

About Tufin

Tufin® is the leader in Network Security Policy Management, 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. Tufin serves over 2,000 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

SB-06-18