tufin

Adhering to the Risk Management Framework (RMF) with Tufin Orchestration Suite

NIST Special Publication 800-37

Solution Brief

The Risk Management Framework (RMF) was developed by the National Institute for Standards and Technology (NIST) and U.S. federal agencies, to help Department of Defense and federal agencies manage risks to and from Information Technology (IT) systems more easily, efficiently and effectively. RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring. The RMF also promotes near real-time risk management and ongoing information system and common control authorization through the implementation of continuous monitoring processes.

Tufin Provides Broad Support for NIST 800-53 Control Families

The Tufin Orchestration Suite addresses and supports many of the control families categorized as "High" in NIST Special Publication (SP) 800-53 Revision 4. Tufin provides visibility, compliance and automation of network access policies across the hybrid network. An independent analysis by Coalfire maps Tufin core capabilities to FISMA control requirements.

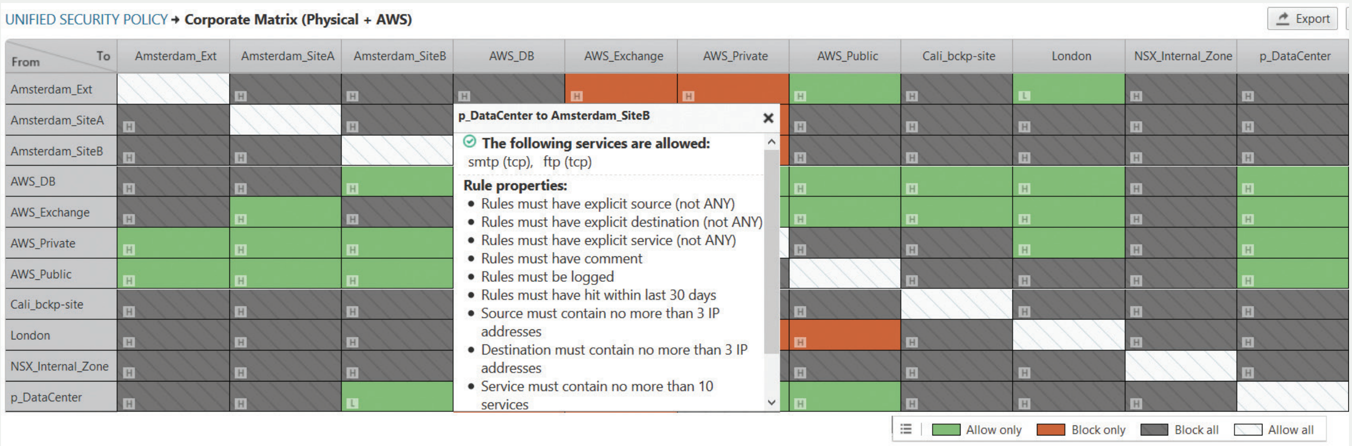
According to the applicability guide the Tufin Orchestration Suite is "a useful tool to support or address relevant technical FISMA High requirements." It helps provide visibility across hybrid networks "to define and confirm security authorization boundaries and their associated network policies for control enforcement." The Tufin solution provides broad support for FISMA High requirements from the Access Control (AC) and Configuration Management (CM) families of requirements. It also provides support for the Audit and Accountability (AU), Incident Response (IR), System and Communication Protection (SC), and System and Information Integrity (SI) control families.

Access Control: Designing and Enforcing Consistent Network Segmentation

The Tufin Orchestration Suite utilizes a Unified Security Policy (USP) that defines and enforces a central, zone-based segmentation matrix to strengthen the security posture and meet regulatory requirements. The USP matrix can be configured as a blacklist or whitelist policy and can accommodate zones based on IP address or defined security groups. Tufin provides a central console for identifying and addressing high-risk access across vendors and platforms and allows for the execution of proactive risk analyses for access changes.

Highlights and Benefits:

- Define and enforce a central, consistent network segmentation policy for adhering to access control mandates
- Embed change controls in a pre-defined, auditable workflow for network access changes
- Ensure continuous compliance with RMF by providing real time monitoring and proactive risk analysis
- Cut audit preparation efforts with automated audit trail and customizable audit reports
- Increase agility and efficiency by automating network changes



UNIFIED SECURITY POLICY → **Corporate Matrix (Physical + AWS)**

From \ To	Amsterdam_Ext	Amsterdam_SiteA	Amsterdam_SiteB	AWS_DB	AWS_Exchange	AWS_Private	AWS_Public	Cali_bckp-site	London	NSX_Internal_Zone	p_DataCenter
Amsterdam_Ext	⬜	⬛ H	⬛ H	⬛ H	🟧 H	🟧 H	🟩 H	⬛ H	🟩 L	⬛ H	⬛ H
Amsterdam_SiteA	⬛ H	⬜	⬛ H				⬛ H	⬛ H	⬛ H	⬛ H	⬛ H
Amsterdam_SiteB	⬛ H	⬛ H	⬜				⬛ H	⬛ H	⬛ H	⬛ H	⬛ H
AWS_DB	⬛ H	⬛ H	🟩 H				🟩 H	🟩 H	🟩 H	⬛ H	🟩 H
AWS_Exchange	⬛ H	🟩 H	⬛ H				🟩 H	🟩 H	🟩 H	⬛ H	🟩 H
AWS_Private	🟩 H	🟩 H	🟩 H				⬛ H	⬛ H	🟩 H	⬛ H	🟩 H
AWS_Public	🟩 H	🟩 H	🟩 H				⬜	⬛ H	⬛ H	⬛ H	🟩 H
Cali_bckp-site	⬛ H	⬛ H	⬛ H				⬛ H	⬜	⬛ H	⬛ H	⬛ H
London	⬛ H	⬛ H	⬛ H				🟧 H	⬛ H	⬜	⬛ H	⬛ H
NSX_Internal_Zone	⬛ H	⬛ H	⬛ H				⬛ H	⬛ H	⬛ H	⬜	⬛ H
p_DataCenter	⬛ H	⬛ H	🟩 L				🟩 H	⬛ H	⬛ H	⬛ H	⬜

p_DataCenter to Amsterdam_SiteB ✕

✓ **The following services are allowed:**
smtp (tcp), ftp (tcp)

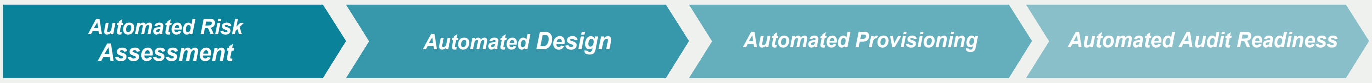
Rule properties:
- Rules must have explicit source (not ANY)
- Rules must have explicit destination (not ANY)
- Rules must have explicit service (not ANY)
- Rules must have comment
- Rules must be logged
- Rules must have hit within last 30 days
- Source must contain no more than 3 IP addresses
- Destination must contain no more than 3 IP addresses
- Service must contain no more than 10 services

🟩 Allow only 🟧 Block only ⬛ Block all ⬜ Allow all

Unified Security Policy – Zone-to-Zone Based Connectivity Matrix

Configuration Management: Automating a Policy-Centric Change Process

The Tufin Orchestration Suite manages the entire security policy change lifecycle across an organization's security, network, and application ecosystem. Groups that have been performing change control using just a ticketing system or email and spreadsheets to manage changes will significantly improve their ability to create, approve, and execute changes, which will also enhance their ability to meet or exceed any applicable service level agreements (SLAs). The customizable workflow's ability to model changes prior to implementation can significantly reduce implementation times and negative impacts to the business due to misconfigured changes. Post-implementation confirmation that changes have been implemented as requested reduces rework. Organizations that use other tools to make changes can seamlessly integrate their change management system with Tufin SecureChange. This gives organizations real-time compliance validation that adds value to not only the operations teams, but audit, compliance, and reporting functions as well



Automated Risk Assessment

Proactive risk analysis of each access change against the enterprise network security policy

Automated Design

Recommended network changes based on accurate topology modeling, path analysis and security policy

Automated Provisioning

Zero-touch implementation across all leading firewall and cloud platforms

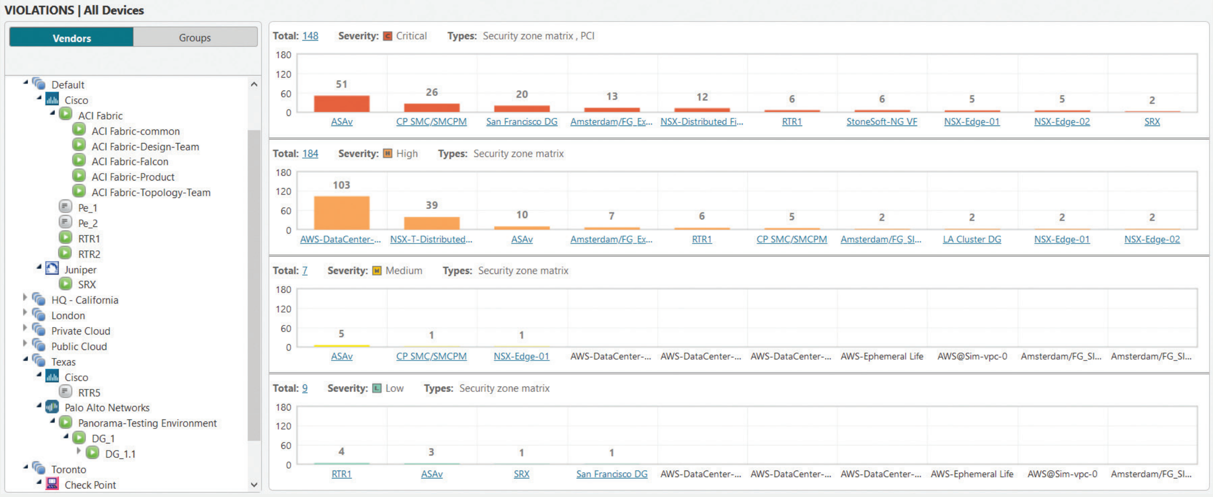
Automated Audit Readiness

Continuous compliance by enforcing an auditable change process that prevents overly permissive access and ad hoc changes

Tufin SecureChange automates network changes to gain agility and security

Continuous Compliance and Audit Readiness

The Tufin Orchestration Suite ensures continuous compliance and cuts audit preparation efforts with real time monitoring and alerts. Identifying violations and unauthorized changes supports RMF and other security framework tasks, and enforces accountability, transparency, and consistency with your network security policies. Data enrichment and automated audit trail are used to generate a variety of customizable audit reports that comply with FISMA Low, Moderate and High impact levels.



Violations Dashboard: Identify and Alert on Violations in Real Time

About Tufin

Tufin (NYSE: TUFN) 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 company's Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. The Tufin Orchestration Suite reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. With over 2000 customers since its inception, Tufin's network security automation enables enterprises to implement changes in minutes instead of days, while improving their security posture and business agility. Find out more at www.tufin.com.

Technology Partners

aws, bmcsoftware, Blue Coat, Check Point SOFTWARE TECHNOLOGIES LTD., Microsoft Azure, cisco, f5, servicenow, FORTINET, intel Security, JUNIPER NETWORKS, openstack, paloalto NETWORKS, vmware

tufin
www.tufin.com