tufin The Security Policy Company.

CRA-F Hong Kong Monetary Authority: Proactive Measures to Boost Your Organization's Cybersecurity Position

The Hong Kong Monetary Authority issued the Cybersecurity Fortification Initiative (CFI) in 2016 with a view to raising the cyber resilience of Hong Kong's banking system. The initiative is underpinned by three pillars, including the Cyber Resilient Assessment Framework (C-RAF). The C-RAF is a risk-based framework for authorized institutions to assess their own risk profiles and benchmark the level of defence and resilience that would be required to accord appropriate protection against cyber attacks.

This document maps the capabilities provided by Tufin Orchestration Suite against four of the C-RAF requirements.

Tufin for CRA-F at-a-glance

CRA-F Requirements	Tufin Functions and Features
3.2.1 Changes to firewall rules are reviewed before becoming effective. CRA-F 3.2.1 requirement	Tufin's SecureChange automates a change workflow that can include a "what if" risk assessment that simulates the impact of the proposed network change and approval of the firewall rule changes. The Tufin SecureTrack module can automatically generate least-privilege policies and illuminate the changes necessary for cloud security groups and cloud firewalls, if using SecureCloud.
3.2.1 The firewall rules are regularly audited or verified on a risk-based approach at least annually.	With SecureTrack Tufin clients have been able to implement daily rule audits. Tufin's SecureTrack logs every change on every device or cloud resource - physical or virtual. Users are able to view all rules by vendor, device and policy across their entire enterprise – on-premises and cloud. It enables continuous compliance with real-time, vendor-agnostic alerting for policy violations, and it allows users to quickly identify rules for decommissioning.
3.2.1 The enterprise network is segmented in multiple, separate trust or security zones with defence-in-depth strategies (e.g. logical network segmentation, hard backups, air-gapping, etc.) to mitigate the risk of cyber attacks.	SecureTrack delivers vendor-agnostic, end-to-end visibility, and allows users to set and manage accurate segmentation policies across the hybrid cloud environment. It provides a realtime hybrid network topology map and segmentation policy orchestration, irrespective of the network infrastructure or cloud platform.
4.3.2 Automated tools are installed to detect unauthorised changes to critical system files, firewalls, IPS, IDS, or other security devices.	Tufin's SecureTrack makes it possible to manage the entire network-layer, next-generation and IPv6 firewalls, as well as network security infrastructure - including routers, switches, load balancers and more — from a central platform. It provides always-on audit logging, continuously checks rules against policy and delivers real-time violations alerts with the option to automate workflows for exceptions handling or remediation proposals.

© Copyright 2022 Tufin. All rights reserved.

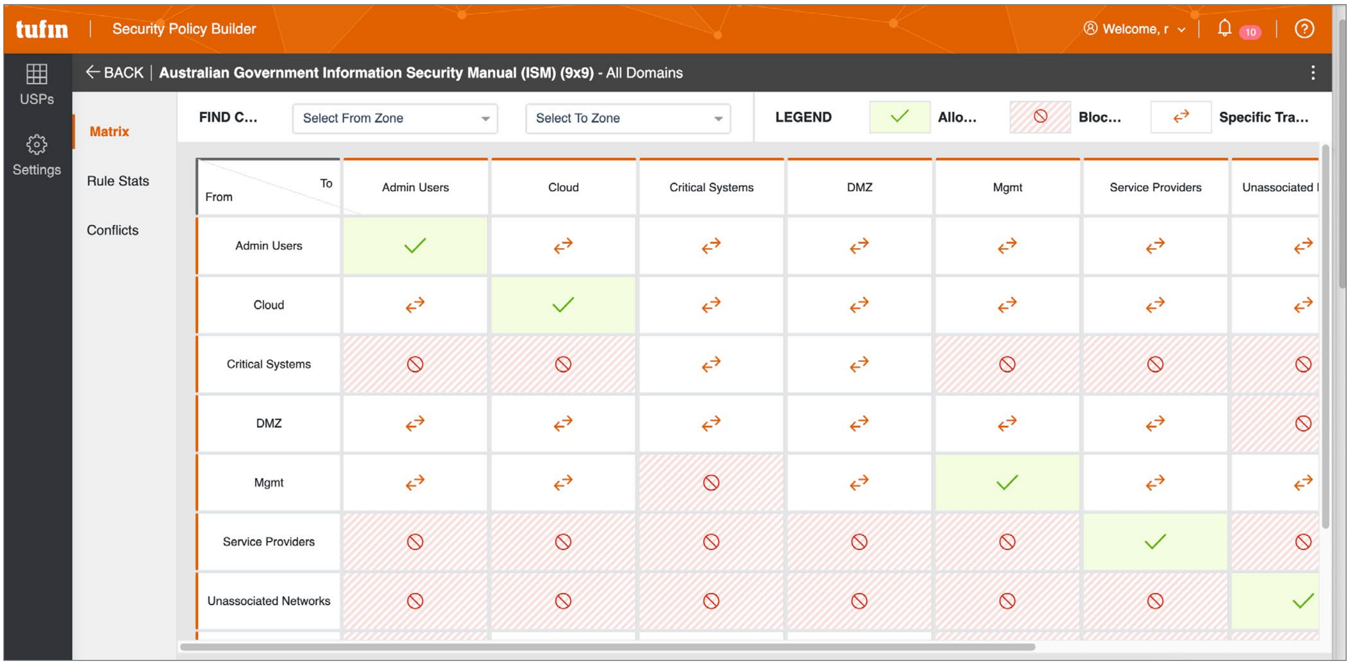
CRA-F 3.2.1 requirement -

Changes to firewall rules are reviewed before becoming effective

Tufin Functionality Supporting CRA-F

Tufin provides end-to-end, fully customisable network change workflows that automate changes across the hybrid environment. These automated/semi-automated workflows reduce the time it takes to fulfill change requests, because Tufin translates between zones, tags, and namespaces, and from security group rules to firewall rules, and designs and implements the required access changes.

As part of this workflow, Tufin can automate review and risk assessment to ensure continuous compliance. SecureChange carries out this integrated risk assessment step by vetting the change against an organisation's security policy, as well as external third-party data (e.g., vulnerability score, SIEM, SOAR, or endpoint security data) to enforce compliance and prevent regulatory violations and associated fines.



From \ To	Admin Users	Cloud	Critical Systems	DMZ	Mgmt	Service Providers	Unassociated I
Admin Users	✓	⇄	⇄	⇄	⇄	⇄	⇄
Cloud	⇄	✓	⇄	⇄	⇄	⇄	⇄
Critical Systems	⊘	⊘	⇄	⇄	⊘	⊘	⊘
DMZ	⇄	⇄	⇄	⇄	⇄	⇄	⊘
Mgmt	⇄	⇄	⊘	⇄	✓	⇄	⇄
Service Providers	⊘	⊘	⊘	⊘	⊘	✓	⊘
Unassociated Networks	⊘	⊘	⊘	⊘	⊘	⊘	✓

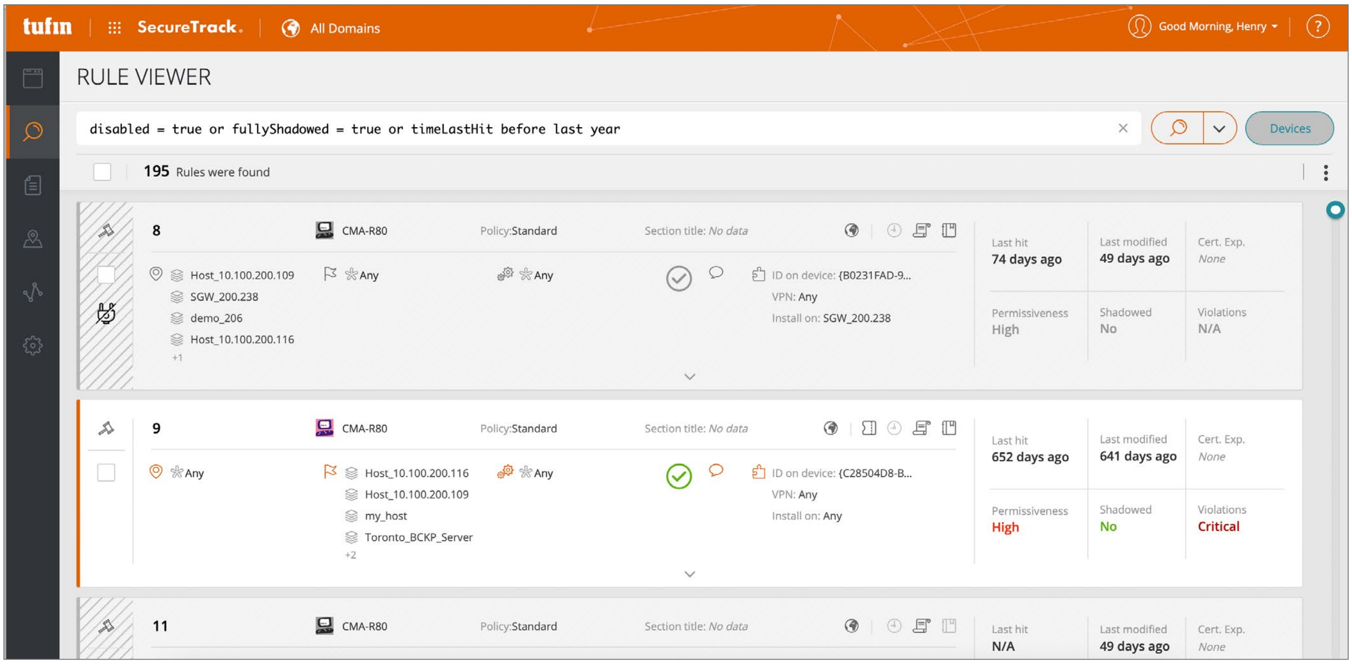
CRA-F 3.2.1 requirement -

Firewall rules are regularly audited or verified on a risk-based approach at least annually

Tufin Functionality Supporting CRA-F

With Tufin's SecureTrack, organisations can review and recertify rules across their hybrid, multi-cloud environments — with full topology visibility and always-on audit trail. Using the Tufin dashboard, organisations can perform daily rules reviews against their unified security policy, because expired and shadowed rules are immediately enumerated in the dashboard, and real-time alerts are generated as violations occur. Further, SecureTrack provides automated processes for approvals, exceptions handling and proposed remediation.

© Copyright 2022 Tufin. All rights reserved.



```
disabled = true or fullyShadowed = true or timeLastHit before last year
```

195 Rules were found

8 | CMA-R80 | Policy:Standard | Section title: *No data*

Host_10.100.200.109
SGW_200.238
demo_206
Host_10.100.200.116
+1 | Any | Any | ID on device: {B0231FAD-9...
VPN: Any
Install on: SGW_200.238

Last hit: 74 days ago | Last modified: 49 days ago | Cert. Exp.: *None*
Permissiveness: High | Shadowed: No | Violations: N/A

9 | CMA-R80 | Policy:Standard | Section title: *No data*

Any | Host_10.100.200.116
Host_10.100.200.109
my_host
Toronto_BCKP_Server
+2 | Any | ID on device: {C28504D8-B...
VPN: Any
Install on: Any

Last hit: 652 days ago | Last modified: 641 days ago | Cert. Exp.: *None*
Permissiveness: High | Shadowed: No | Violations: Critical

11 | CMA-R80 | Policy:Standard | Section title: *No data*

Last hit: N/A | Last modified: 49 days ago | Cert. Exp.: *None*

Rule Viewer Enumerating Fully Shadowed Rules

CRA-F 3.2.1 requirement -

The enterprise network is segmented in multiple, separate trust or security zones with defence-in-depth strategies (e.g. logical network segmentation, hard backups, air-gapping, etc.) to mitigate the risk of cyber attacks

Tufin Functionality Supporting CRA-F

Tufin allows security teams to confidently build a segmentation strategy with the most comprehensive ecosystem integration, topology mapping and automation. Tufin can see through the firewall into the cloud, providing automated policy generation, impact assessment and lifecycle management. This enables clients to set and apply micro-segmentation policies automatically, accelerating the journey to a state of zero-trust maturity.

In the cloud, Tufin monitors traffic, automatically learns the app/workload communication flows, and creates an editable whitelist policy, using natural high-level language to define segmentation policies and create security “guardrails”. Clients receive real-time alerts when configuration attempts are in violation of policy. The result is proactive protection of your cloud-native resources and workloads, which are often provisioned and configured using CI/CD processes and tools.

For IP-based segmentation, organisations can use the Tufin Unified Security Policy (USP) matrix to create security policies and control what traffic is allowed between zones. Additionally, Tufin’s Automatic Policy Generator (APG) can analyze and reduce an enforcement point’s rule base based on how granular you’d like access to be. Users can either upload logs or have the solution “listen” to network access use over a period of time in order to provide an optimized rule set.

Finally, the Security Policy Builder, further enables security teams to easily analyze access between segments throughout the network (cloud and on-premises), to create a visual model, and — most importantly — recommend a comprehensive, access-based security policy based on the analysis of existing access in addition to available compliance-based models (e.g. PCI-DSS, NERC).

All historical decisions regarding access are based on the risk framework of network segmentation, while all network access change implementations can be implemented, verified, and tracked through Tufin SecureChange.

© Copyright 2022 Tufin. All rights reserved.

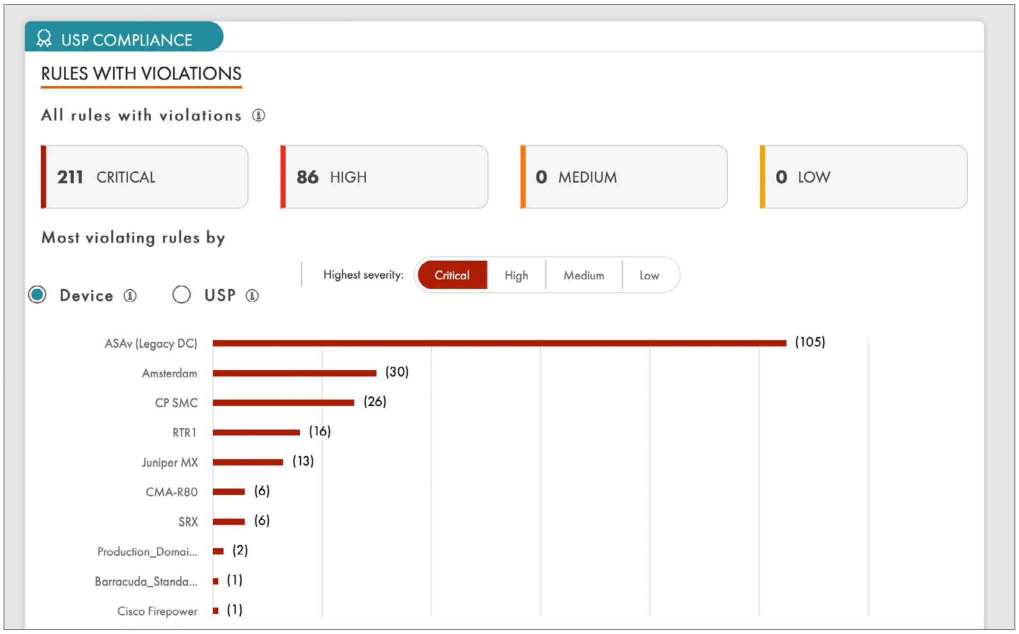
CRA-F 4.3.2 requirement -

Automated tools are installed to detect unauthorised changes to critical system files, firewalls, IPS, IDS, or other security devices

Tufin Functionality Supporting CRA-F

The SecureTrack provides an at-a-glance view of the security and compliance violations in the organisation's on-premises and multi-cloud environments by device. The Violating Rules report shows all the violations that apply to a specified rule, along with the severity, the creation date of the violation, the security requirement that causes the violation, and the recommended action to mitigate the violation where available.

In the cloud, Tufin automatically and continually evaluates DevOps toolchain activity, and alerts when any cloud resource is attempted to be configured in a manner that violates security policy.



USP COMPLIANCE

RULES WITH VIOLATIONS

All rules with violations ⓘ

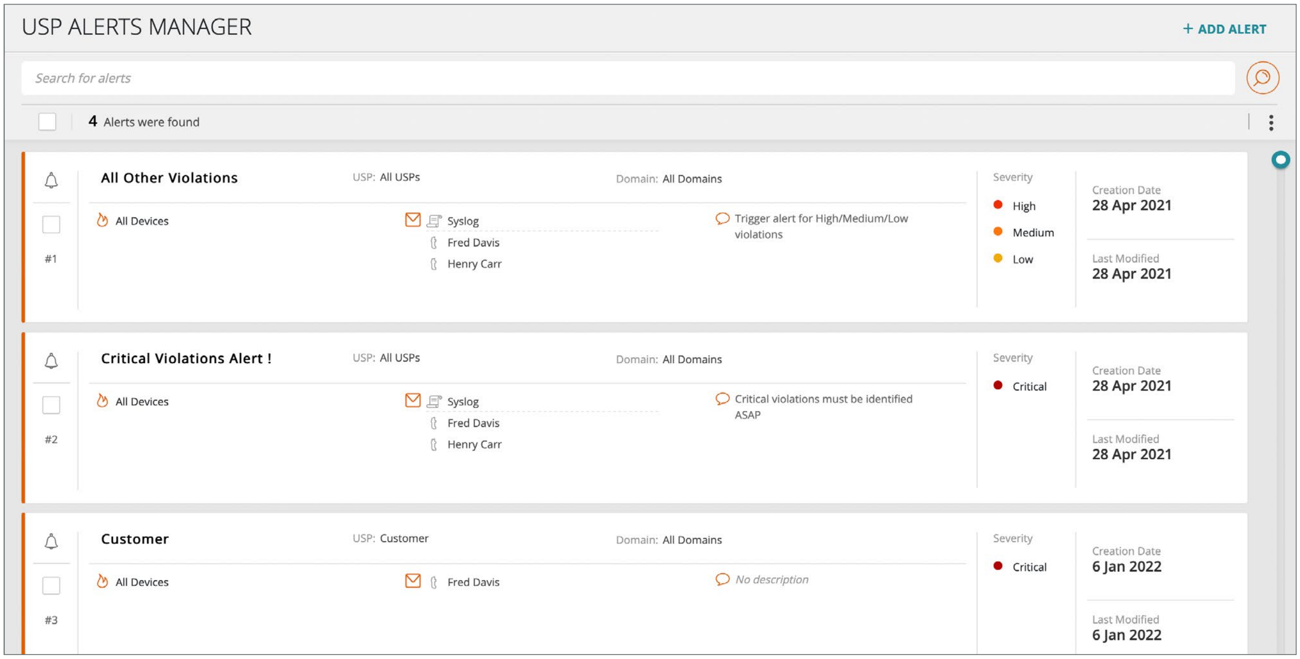
211 CRITICAL | **86** HIGH | **0** MEDIUM | **0** LOW

Most violating rules by

● Device ⓘ ○ USP ⓘ

Highest severity: Critical | High | Medium | Low

At-a-Glance View of All Violations Across Resources



USP ALERTS MANAGER

+ ADD ALERT

Search for alerts

□ **4** Alerts were found

□ #1 **All Other Violations** USP: All USPs Domain: All Domains
All Devices — Syslog, Fred Davis, Henry Carr — Trigger alert for High/Medium/Low violations
Severity: High, Medium, Low
Creation Date 28 Apr 2021
Last Modified 28 Apr 2021

□ #2 **Critical Violations Alert !** USP: All USPs Domain: All Domains
All Devices — Syslog, Fred Davis, Henry Carr — Critical violations must be identified ASAP
Severity: Critical
Creation Date 28 Apr 2021
Last Modified 28 Apr 2021

□ #3 **Customer** USP: Customer Domain: All Domains
All Devices — Fred Davis — *No description*
Severity: Critical
Creation Date 6 Jan 2022
Last Modified 6 Jan 2022

Unified Security Policy Violation Alerts Manager

© Copyright 2022 Tufin. All rights reserved.

Conclusion

Tufin delivers the most comprehensive, vendor-agnostic security policy management solution available, enabling highly regulated organizations to reduce the time and resources required to implement changes and maintain compliance. Network security and cloud teams can implement access changes in minutes instead of days, enable consistent security policy across their complex, fragmented hybrid and multi-cloud environments, and systematically apply network security policy to existing DevOps processes. With Tufin's automation capabilities, organizations can easily design and enforce a Unified Security Policy, proactively monitor environments for potential security and/or compliance risk, and more easily meet compliance and audit obligations.

Tufin® is the leader in Network Security Policy Orchestration for enterprise cybersecurity. More than half of the top 50 companies in the Forbes Global 2000 turn to Tufin to simplify 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 award-winning Tufin Orchestration Suite™ to increase agility in the face of everchanging business demands while maintaining a robust security posture. The Suite 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 2,000 customers spanning all industries and geographies; its products and technologies are patentprotected in the U.S. and other countries. Find out more at www.tufin.com.

tufin
The Security Policy Company.

Copyright © All rights reserved. Tufin, Unified Security Policy, Tufin Orchestration Suite and Tufin logo are trademarks of Tufin. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. You may not copy, reproduce, photograph, translate, transmit ,make available to the public, make derivative works, perform in public, rent , broadcast or make any commercial use of the publication in full and / or in part without prior written approval.