tufin The Security Policy Company. + EUROPEAN CENTRAL BANK

Solution Brief

Ensuring Continuous Compliance with ECB Open Banking Network Security Mandates

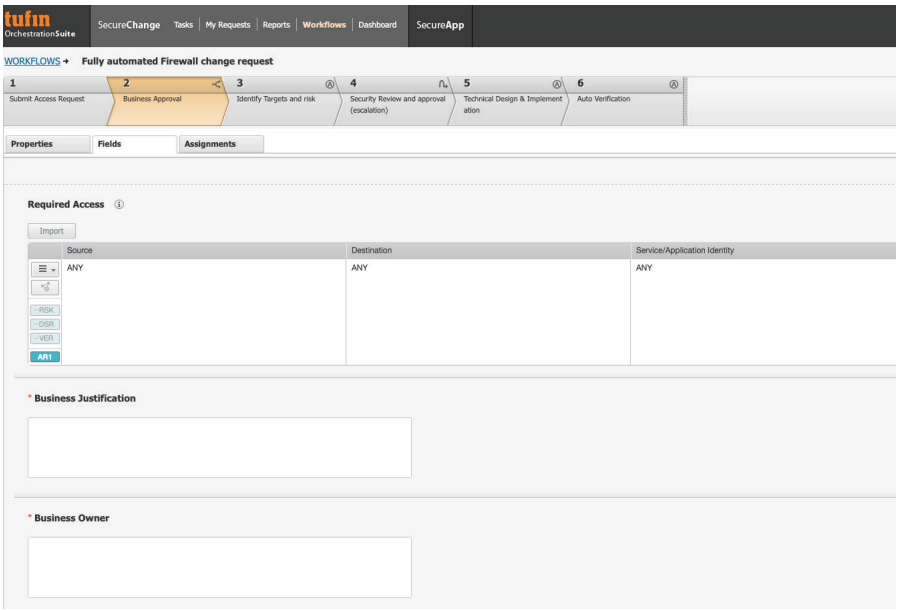
The ECB network security requirements for Open Banking, or the Revised Payment Service Directive (PSD2), requires EU's financial institutions to raise the standards of their processes and documentation. An ECB audit requires financial institutions to justify all access rules; ensure least-privilege access; institute segregation of duties; and establish professional, documented, and auditable practices for managing network access. Demonstration of compliance needs to be recertified every 180 days.

Tufin has been a primary choice of financial institutions (FI) across Europe, and the world, with over 700 FI customers globally. While Tufin is trusted for helping customers gain visibility and control of their network security posture, we also help clients fulfill ECB network security compliance with a single, centralized solution that spans their entire multi-vendor, multi-platform environment.

Business Justification and Ownership of All Access Rules

The ECB aims to ensure that application and network access is justified and properly implemented. Organizations must prove that they maintain an inventory of their access requests, and that each request has a business owner and business-level justification. Furthermore firms need visibility into how access requirements map to firewall and object-level rules, that the rules adhere to the firm's security standards, and that access is properly implemented.

Tufin provides an application-centric approach to defining, identifying, provisioning, documenting, and managing network access. The Tufin Orchestration Suite enables modeling connectivity and visualizing the access rules that map to each application. Automated workflows fully document access requests, business justification and ownership, which through the provisioning engine can be automatically implemented as well as automatically checked for continuous compliance. Audit readiness is assured on an ongoing basis by documenting every step in the workflow.



Screenshot from Tufin SecureChange showing the access change provisioning workflow. The workflow enables ECB compliance as it requires business justification and ownership, approval, and is a "standardised and reproducible" process that can't be "compromised or circumvented" with full documentation/audit trail capture.

Benefits to Your Business:

- Ensure continuous compliance and audit readiness with ECB network security mandates
- Simplified management of least privilege and segmented access through visualization, application level to device level rule translation, and a full network topology across your multi-vendor network
- Customizable security policy change workflow integrated with your ticketing system
- Documentation of connectivity through a central console
- Automated recertification workflow
- Centralized visibility and control of network access across vendors and platforms

Least Privilege Access Control and Segregation of Duties

The ECB seeks to ensure that firms have appropriate security solutions in place to protect networks against abuse or attacks. Network access must be kept to a strict minimum following the "least privilege" principle, restricted only to those systems, applications, and individuals for which access is required and justified from a business perspective. Further, firms are required to implement segregation of duties as well as pay special attention to the segregation of IT environments.

Tufin's granular, role-based access control capabilities allow firms to establish and enforce segregation of duties related to requesting, approving, designing, administering, and provisioning access. Tufin simplifies the complexity of visualizing and managing segmentation, down to the most granular level. Zone-to-zone segmentation enables firms to define network zones that can connect, and the network traffic that is allowed or blocked between them. Least privilege network access is accomplished by restricting access only to resources, applications, and individuals that have a justifiable business need.

Tamper-Proof Recertification

Previously accepted manual management of network access, often through spreadsheets, and emails is inaccurate, non-scalable, and no longer compliant with ECB regulations. Firms must employ professional, repeatable, and auditable practices to manage network access. They must also establish an effective process for recertifying and, if necessary, revoking access every 180 days with a process that includes rule justification, recertification date, sign-off approvals, and a tamper-proof audit trail. Financial institutions that cannot meet the ECB regulations must present a remediation plan to demonstrate the ability to comply in the near future; else, they risk heavy penalties that may include a requirement to shutdown an application until compliant.

Tufin provides an automated, policy-based rule review process, including an of out-of-the-box recertification workflow to enable customers to enforce access recertification every 180 days (or any frequency desired). It offers compliance alerts and enables initiating a workflow for review, approval, and, if necessary, revocation. A decision to revoke access can lead directly to an automated, documented process for rule decommissioning. Tufin automates the identification of risky and undocumented rules and allows documenting required access, justification, status and adherence to standards. Compliance can be demonstrated at the push of a button with a full audit trail.

Tufin's multi-vendor platform works with:

Network & Cloud Platforms

FORCEPOINT · vmware NSX · CISCO · JUNIPER NETWORKS · Symantec · Microsoft Azure · Check Point SOFTWARE TECHNOLOGIES LTD. · paloalto NETWORKS · f5 · FORTINET · aws · openstack

Solutions Integrations

bmc Remedy · IBM Service Desk · Qualys · RSA Archer GRC · RAPID7 · TANIUM · ARISTA · hp HP Service Manager · Nessus · splunk> · Radar · servicenow · <VA> vARMOUR · Cisco Tetration

The Only Complete Solution for ECB Network Security Audit Readiness

The Tufin Orchestration Suite scales with your network to bring you into compliance, keep you in compliance, and make it easy to prove compliance at any point in time for your network today and your increasingly complex network of the future.

Tufin will not only help your organization stay compliant with ECB, but also help mitigate and manage network policy risk, increase the speed of implementing access requests from days to minutes, lift the productivity of your team, and improve your overall security posture; all while maximizing business agility.

Over 2,300 of the world's largest global organizations trust Tufin to simplify and automate their security policy management across complex hybrid environments. Gain confidence, transparency and compliance of your security posture.

tufin The Security Policy Company.

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**.

[1] https://www.ecb.europa.eu/pub/pdf/other/assessmentguidesecurityinternetpayments201402en.pdf
[2] Frequency not explicitly stated in the regulations, 180 days is commonly recommended by audit firms