tufin The Security Policy Company.

EUROPEAN CENTRAL BANK

EUROSYSTEM

ECB PSD2 Requirements for Network Security

The Directive Explained in 3 Essential Steps: A How-to Guide to Comply

Introduction

The ECB Audit for compliance with Open Banking, also referred to as the Revised Payment Service Directive, or PSD2, is requiring EU's global financial institutions to raise the standards of their network security processes and audit trails. An ECB audit requires proof of "least privilege principles"; "adequate segregation"; "proper implementation;" and "professional, documented, auditable practices" for network access management. There are many piecemeal tools available which will enable partial fulfillment; however, Tufin provides one centralized and comprehensive solution that will empower an organization to meet all of the ECB audit requirements related to network security policy access.

Beyond fulfilling the ECB network security audit requirements, the Tufin Orchestration Suite (TOS) helps firms gain full visibility and control of their network security policy across their entire, hybrid, multi-vendor network. This allows firms to increase the productivity of their network, security, and compliance teams, and ensure security guardrails are in place to maintain continuous compliance. TOS enables organizations to minimize their attack surface and improve their security posture, even as their network's vendors and cloud platforms continue to expand.

Impending Deadline

The regulation driving these requirements, the European Union's Payment Services Directive (PSD), was passed in 2007, with security requirements elaborated upon in the European Central Bank Assessment Guide for the security of Internet payment published in 2014[1] . EU Member States were given until 13 January 2018[2] to transpose it into national law. The implementation deadline, originally in 2019, has been extended to **31 December 2020**. As it has already been extended, additional extensions are unlikely. The penalties for not complying are unknown, if they require applications to be decommissioned until the issue is resolved, the consequences could be severe.

[1] European Central Bank Assessment Guide for the security of internet payments, February 2014 https://tinyurl.com/y8n3wscm

[2] Guidelines on the security measures for operational and security risks of payment services under Directive (EU) 2015/2366 (PSD2) https://tinyurl.com/yb94vq4b

REQUIREMENT
1
Least
Privilege

Least privilege access defined for all applications

4.1[3]: In designing, developing and maintaining internet payment services,. . . pay special attention to the . . . proper implementation of ***the "least privilege" principle*** *as the basis for sound identity and access management.*

The ECB is seeking to ensure that a firm's access requirements are least privilege, limited to only who needs access. Need is defined as having a business-level justification. The justification needs to be defined at an application-level and be collectively exhaustive in terms of inclusive of every application in use.

The Directive - Requirement #1: **Least Privilege - Application Inventory**

Collectively exhaustive application access discovery:

All applications within the financial institution that require access to the network need to be identified, along with their associated access requirements

Section 3.2[4,5]: *PSPs should identify, establish and* ***regularly update an inventory*** *of the information assets, such as ICT systems, their configurations, other infrastructures and* ***also the interconnections with other internal and external systems . . .***

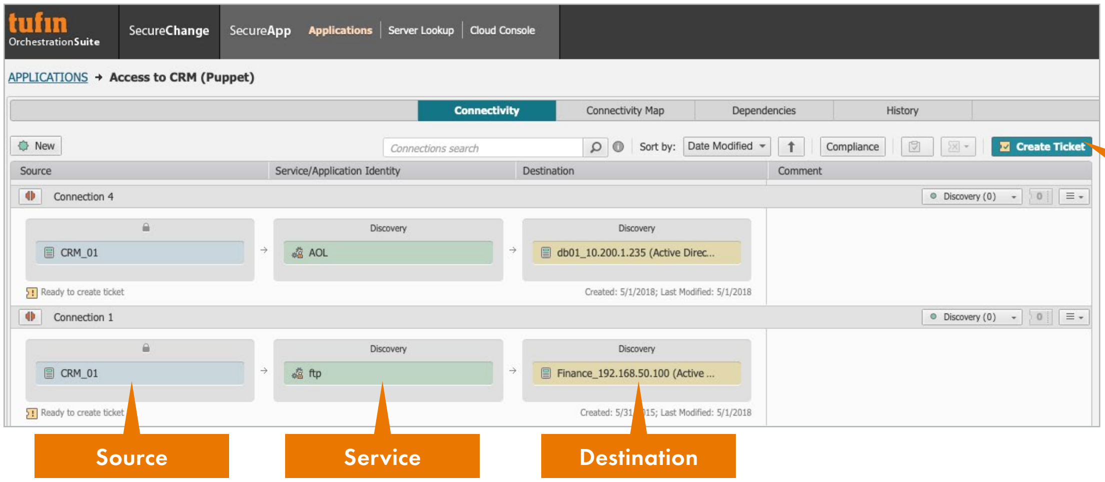
Section 4.1.2[6]: *...the* ***access privileges*** *. . . associated with each system product (e.g.. . application) and the users to which they need to be allocated* ***should be identified and reviewed*** *on a regular basis*

Tufin's Capabilities to Fulfill Least Privilege - Application Inventory

Tufin provides connection discovery functionality for automated identification of application connectivity. Tufin also provides off-the-shelf integrations with network performance monitoring/application discovery applications for fully automated application discovery.

Tufin supports automated application connection discovery for all devices made available or configured within TOS. As traffic is continuously monitored the system is collectively exhaustive based on its identification of all device traffic, and any new application connections as they are automatically added to the network.

Developing and maintaining a comprehensive inventory of all applications and their connectivity is burdensome to say the least. As organizations need to manage a rapidly growing level of application connectivity, tracking all applications without a centralized, comprehensive and automated solution can lead to misconfigurations or blind spots, which will lead to non-compliance. With an automated solution for managing access rules for all apps across any network device, platform, and environment, the burden of continuously maintaining an accurate inventory and associated connectivity will be lifted.



APPLICATIONS → Access to CRM (Puppet)

Source	Service/Application Identity	Destination	Comment
Connection 4			
CRM_01	Discovery AOL	Discovery db01_10.200.1.235 (Active Direc...	
Ready to create ticket		Created: 5/1/2018; Last Modified: 5/1/2018	
Connection 1			
CRM_01	Discovery ftp	Discovery Finance_192.168.50.100 (Active ...	
Ready to create ticket		Created: 5/31/2015; Last Modified: 5/1/2018	

Screenshot showing two new application connections automatically discovered by SecureApp.

There is an option to create a ticket to send these application connections through the workflow process to ensure business ownership and justification are secured, along with reviews and approvals.

[3] https://tinyurl.com/y8n3wscm

[4] Section 3.2 page 7 https://tinyurl.com/yb94vq4b

[5] Inventory requirements also referenced in section 4.5.59 of https://www.vab.de/wp-content/uploads/2019/11/ENT_EBA-Guidelines_ICT-security-risk-management_13122018.pdf

[6] Page 19, https://tinyurl.com/y8n3wscm

REQUIREMENT
1
Least
Privilege

Least privilege access for all network access

The Directive - Requirement #1: **Least Privilege - Justification & Owner**

Application access requirements[7] - defined, justified and owned:

Access requirements for each application must be defined based on need which ties to a business level justification. Each access requirement must also have a business owner.

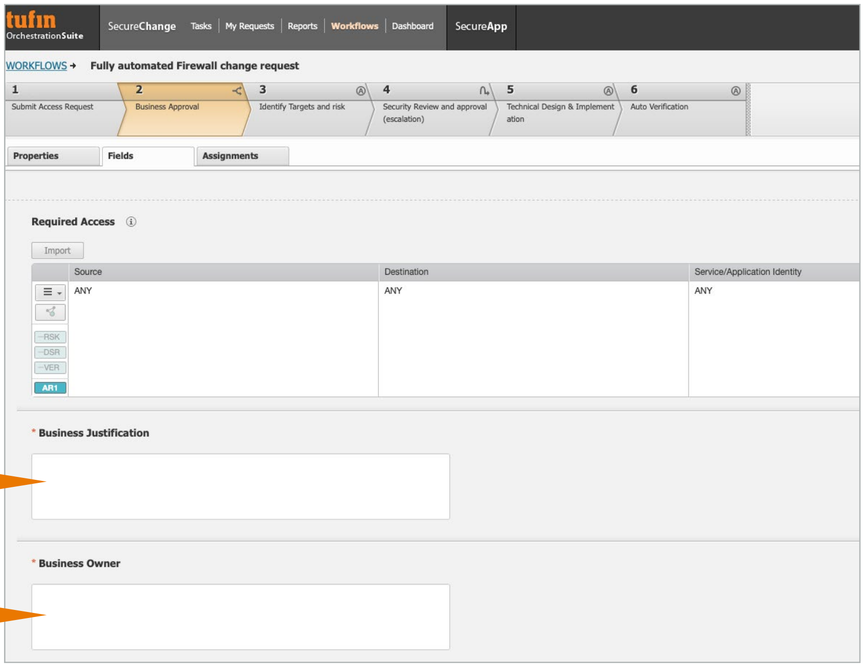
4.9[8] *access control: Physical and* ***logical access*** *to ICT systems should be permitted only for authorised individuals. . . . PSPs should institute controls that reliably restrict such access to ICT systems to those with a* ***legitimate business requirement****. Electronic access by applications to data and systems* ***should be limited to the minimum*** *that is required to provide the relevant service*

4.4.3 - 34(e)[9] *page 21 Access management: access rights should be granted, removed or modified in a timely manner, according to predefined approval workflows* ***involving the business owner***

Tufin's Capabilities to Fulfill Least Privilege - Justification and Owner

The Tufin Orchestration Suite (TOS) allows the capture and tracking of the business justification[10] for a network connectivity or change request. This is supported at both the device-level and application-level to match your business needs and enhance stakeholder (e.g. security, app teams) collaboration. Requirements that the requester/owner, business justification and approval fields are populated prior to provisioning can be embedded into your access request workflow. TOS includes out-of-the-box and customized workflows, which can be embedded into your existing ITSM workflows. Tufin offers off-the-shelf integrations with leading ITSM solutions.

Screenshot of Tufin's SecureChange OOTB workflow for provisioning network access. The workflow includes business justification, risk assessment, approval, security review, technical design, engineering design review, implementation and verification. By capturing request justification and ownership, this component of the requirement is fulfilled.



WORKFLOWS → Fully automated Firewall change request

1 Submit Access Request
2 Business Approval
3 Identify Targets and risk
4 Security Review and approval (escalation)
5 Technical Design & Implementation
6 Auto Verification

Required Access

Source	Destination	Service/Application Identity
ANY	ANY	ANY

* Business Justification

* Business Owner

Request Justification

Ownership

As development speed continues to increase and networks continue to expand, organizations will need to manage an increased level of access requests. Automatically tracking all of these access requests, and their associated justification and approvals, through one unified system will save time, and ensure consistency. Tufin simplifies the complexity of defining, approving, and managing network change requests while embedding it into a best-practices process and enabling full documentation.

[7] Definition of application access: which applications or systems can access each application, which we've simplified by describing as who has access to who, and what has access to what.

[8] Page 9 https://tinyurl.com/yb94vq4b

[9] Page 21 https://www.vab.de/wp-content/uploads/2019/11/ENT_EBA-Guidelines_ICT-security-risk-management_13122018.pdf

[10] https://web.tufin.com/hubfs/resources/products/Tufin_Secureapp_Datasheet.pdf

REQUIREMENT
1
Least
Privilege

Least privilege access for all network access

The Directive - Requirement #1: **Least Privilege - Need-to-know**

Least Privilege:

Least privilege definition must be based on the minimum requirements.

4.5[11, 12] *In designing, developing and providing payment services, **PSPs should ensure** that segregation of duties and **'least privilege' principles are applied**. . .*

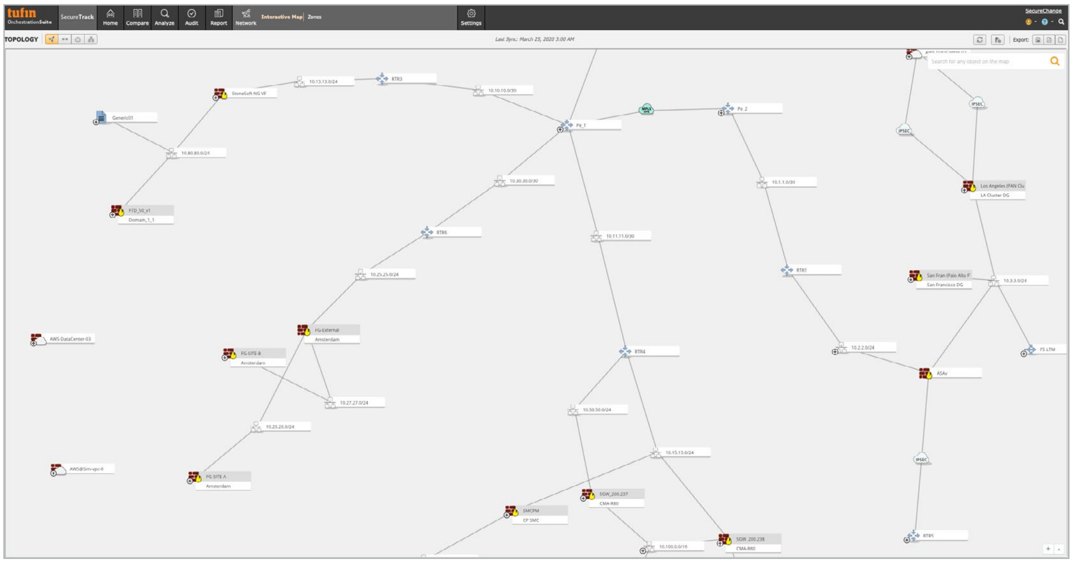
4.6[13] *. . . PSPs should ensure that the . . . routing, [and] processing,. . of sensitive payment data . . is adequate, relevant and **limited to what is necessary** ...*

4.10[14] *access control: PSPs should manage **access rights** to information assets and their supporting systems **on a 'need-to-know' basis**.*

4.1.2[15] ***privileges** should be allocated to users . . . **i.e. the minimum requirement** for their functional role only when needed*

Tufin's Capabilities to Fulfill Least Privilege - Need-to-know

Application-based least privilege access is defined by the application-level justification requirement, explained above. If the access that is justified is the only access granted, then least privilege is accomplished. This is essentially a requirement for segmentation with justification and ownership for each segment. TOS simplifies the complexity of visualizing and managing segmentation. To effectively manage and control communication routes, Tufin enables customers to decouple segmentation policy from the underlying network so it can be applied to any app or workload everywhere. This spans the datacenter and into the cloud, treating the cloud as an extension of the datacenter and vise-versa. This enables customers to define and consistently enforce the centralized access policy, independent of where the apps/ workloads run. In addition, through logs ingested from managed network devices, Tufin automatically recommends an optimized rule base to limit traffic to what is used or needed by the organization.



Screenshot of a network topology view enabled by Tufin SecureTrack. Least privilege access requires a granular-level of segmentation. The Tufin topology, along with the underlying Automatic Policy Generator, simplifies the complexity of understanding, visualizing, setting and managing segmentation.

[11] Page 8 https://tinyurl.com/yb94vq4b

[12] Also in section 4.1 page 18 of https://tinyurl.com/y8n3wscm

[13] Page 9: https://tinyurl.com/yb94vq4b

[14] Page 9: https://tinyurl.com/yb94vq4b

[15] Page 19 2nd bullet https://tinyurl.com/y8n3wscm

REQUIREMENT
2
Proper
Implementation

Proper implementation with segregation of duties

4.1[16]: In designing, developing and maintaining internet payment services, PSPs and payment schemes should pay special attention to the adequate ***segregation of duties*** *in information technology (IT) environments and . . .* ***proper implementation*** *of the "least privilege" principle as the basis for sound identity and access management...*

The ECB is seeking to ensure that an organization has visibility into how their justified connectivity requests, defined at an application layer, map to their security policy layer - to their firewall and object-level access rules. This needs to also include proof that only the justified requests are in-force, i.e. that the application level access required is "properly implemented" in a manner that ties back to the rule owners and approvals. Further they need to ensure separation of duties.

The Directive - Requirement #2: Proper Implementation - What Was Defined Corresponds to What is Implemented

Application access mapped to security policies:

Once the application level access requirements are established and justified, per set 1 above, firms need to demonstrate that their security policies, that their actual firewall rules or security group policies, support the access requirements. ECB requires not just that each application access request has a business owner, but that each policy rule has a business owner as well. In other words, ECB requires a complete mapping of every single policy rule to its application access (and associated owner).

2.5[17] PSPs should ensure that the aforementioned ***internal control model*** *has sufficient authority, independence, resources and direct reporting lines.*

4.1[18]. . .and the ***proper implementation*** *of the "least privilege" principle as the basis for sound identity and access management...*

*4.2.1[19] . . .****firewalls with appropriate rules to allow only legitimate connections***

Tufin's Capabilities to Fulfill Proper Implementation - Security Device Translation

Tufin automatically converts application level connectivity requests to device level access requests, with mappings, documentation and audit trails. When a change request pertaining to application connectivity is submitted, Tufin SecureChange identifies the relevant network route, and each of the network devices along that route that needs to be updated. The Automatic Policy Generator (APG) then designs policy changes and provisions the changes to the relevant devices using an automated workflow for automated implementation. The whole process is documented, hence an audit trail is generated.

The below diagram further explains Tufin's application connectivity to security policy mapping capability.

An application connectivity request, initiated by an application owner or user, is demonstrated on the left- a request may entail for example that a portal needs input from a database and a CRM and sends output to a server. The picture on the right illustrates the conversion to the information needed to deploy that portal, to convert those application connections to security policies, for example the source IP addresses, destination IP address, and service for every connection along the route.

[17] Page 6 https://tinyurl.com/yb94vq4b

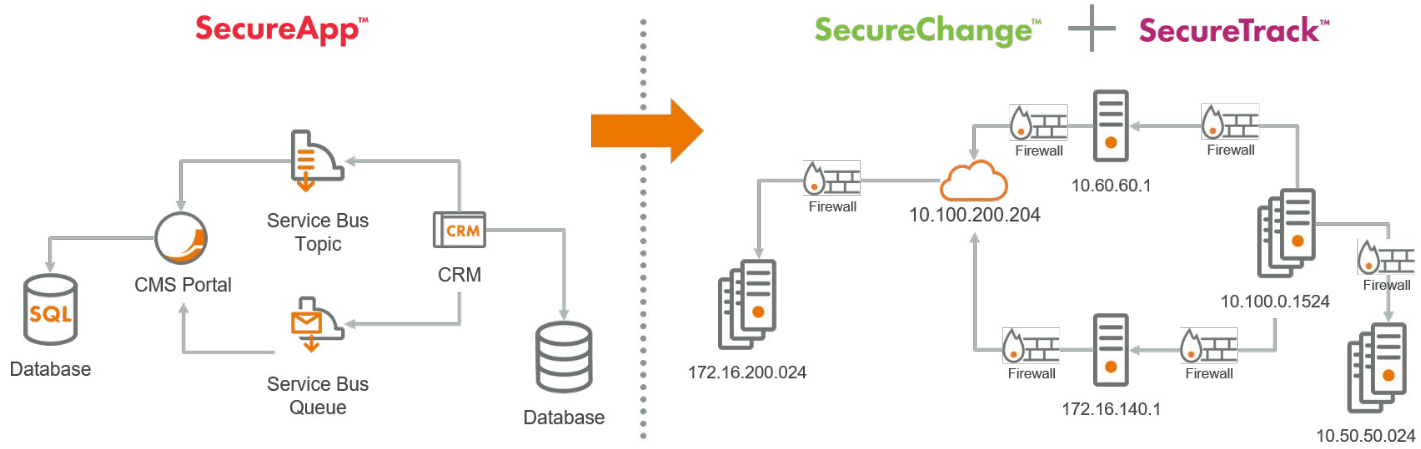
[18] Page 18 https://tinyurl.com/y8n3wscm

[19] Page 19, 3rd bullet https://tinyurl.com/y8n3wscm

REQUIREMENT
2
Proper Implementation

Proper implementation with segregation of duties

Tufin's Capabilities to Fulfill Proper Implementation - Security Device Translation



TOS allows application owners to submit application connectivity change requests at the application level, and then automatically translates those change requests into specific network security policies, whereby the resulting policy change requests enter the organization's existing network change request queue.

Tufin provides end-to-end automation for application connectivity changes.

[18] Page 6 https://tinyurl.com/yb94vq4b

[19] Page 18 https://tinyurl.com/y8n3wscm

[20] Page 19, 3rd bullet https://tinyurl.com/y8n3wscm

REQUIREMENT
2
Proper
Implementation

Proper implementation with segregation of duties

The Directive - Requirement #2: Proper Implementation - Meet Organization's Standards

Security policies comply with standards:

Now that security policies, based on application connectivity requirements, have been defined, ECB requires that the organization confirms that the policies adhere to the firm's standards.

Tufin's Capabilities to Fulfill Proper Implementation - Comply with Standards

Compliance with standards is embedded into the network change request workflow provided by Tufin. Tufin has a centralized repository of an organization's standards/desired policies, the Unified Security Policy (USP). With automation, only changes that have been evaluated against the USP and meet security mandates will be provisioned. As mentioned above, Tufin converts a change request to a policy change, and automatically checks the policy changes against this USP. If a change would violate the desired security policies, alerts can be set or workflow exception paths can be followed.

Tufin continuously monitors connectivity for compliance. If a non-compliant change request is provisioned outside of the workflow, presuming it is running on a device that Tufinwas set to monitor, TOS will alert relevant users of the violation. TOS further can suggest options and policies to remediate the violation.

TOS enables you to proactively assess risk and compliance before and after changes are made.

The Directive - Requirement #2: Proper Implementation - Separation of Duties

Separation of duties:

Firms need to define and have a means of enforcing a separation of duties.

*4.2[22] PSPs should **establish and implement a 'defence-in-depth' approach by instituting multi-layered controls** ... such as the four-eyes principle, two-factor authentication, network segmentation and multiple firewalls.*
*4.5[23] . . . **PSPs should ensure that segregation of duties** and 'least privilege' principles are applied. PSPs should pay special attention to the segregation of IT environments, in particular to the development, testing and production environments.*
*4.1.2[24] **Administrative privileges** should be assigned to users through a **different user ID** from that used for normal business use . . . may necessitate role-based access control or at least equivalently strong access control models.*

Tufin's Capabilities to Fulfill Proper Implementation Separation of Duties

Tufin provides role-based access and control capabilities to allow organizations to establish and enforce separation of duties. Roles support limiting the ability to request or approve an access request from those with permission to provision changes.
For example, TOS has a business owner role whereby this role is allowed to review policy revisions and run queries, audits and reports, however only administrators are allowed to add or configure monitored devices. Predefined roles include auditor, business owner, requester, security administrator, and system administrator.

Tufin's role-based capabilities make it easy for organizations to institute separation duties related to requesting, approving, designing, and provisioning access requests.

[21] Page 18 https://tinyurl.com/y8n3wscm

[22] Page 8 https://tinyurl.com/yb94vq4b

[23] Page 8 https://tinyurl.com/yb94vq4b

[24] European Central Bank Assessment Guide for the security of internet payments, February 2014, https://tinyurl.com/y8n3wscm p19 6th & 9th bullets

Recertification with tamper-proof audit trail

*4.1.2[25]. . . an effective **recertification process** for assessing and, if necessary, revoking privileges should be in place and carried out at regular intervals*

The ECB is seeking to ensure that a firm has "sound," professional, reliable and auditable network security access processes, and is recertifying its compliance every 180 days.

The Directive - Requirement #3: Recertification - Reliable Process

Documented professional, repeatable, and reliable network security process:

Firms need to demonstrate a "sound" process for requesting, approving, provisioning and confirming compliance of all connections, with application-level justification and ownership of all connections.

*4.13[26] Access control: The operation of products, tools and procedures related to access control processes should **protect the access control processes from being compromised or circumvented**.*

*4.1.2[27] . . .an authorization process and a **record of all privileges allocated** should be maintained, with privileges not being granted until the authorisation process is complete.*

*2.4.3[28] . . .ensure that the method to generate the risk assessments is **standardised and reproducible**. . . results of the risk assessment submitted to senior management for approval.*

Tufin's Capabilities to Fulfill Recertification - Reliable Process

Procedures for network policy management within today's organizations with fragmented, multi-vendor networks often revolve around tribal knowledge with policies either tracked manually through spreadsheets or in an employee's head. This is not acceptable for an ECB audit. A documented and auditable process, outside of a spreadsheet, needs to be in place.

Tufin provides tracking and controls to enable centralized security policy management across firewalls, including next-generation firewalls, in a multi-vendor, hybrid environment with full documentation, defined workflows, and visibility of the process, changes and utilization. Configurable workflows provide an automated process for requesting, analyzing, designing, provisioning, and verifying changes to firewall rules with comprehensive documentation.

[25] Section 4.1.2 2nd bullet, page 19 https://tinyurl.com/y8n3wscm

[26] Page 10 https://tinyurl.com/yb94vq4b

[27] Page 19 3rd bullet https://tinyurl.com/y8n3wscm

[28] Page 15 https://tinyurl.com/y8n3wscm

REQUIREMENT
3
Recertification

Recertification with tamper-proof audit trail

The Directive - Requirement #3: Recertification - Effective Recertification Process

Tamper-proof Recertification:

The access request, provisioning and monitoring process needs to be recertified regularly in a tamper-proof manner with an authorized sign-off.

*4.10[29] Access control: . . .. Access rights should be **periodically reviewed**.*

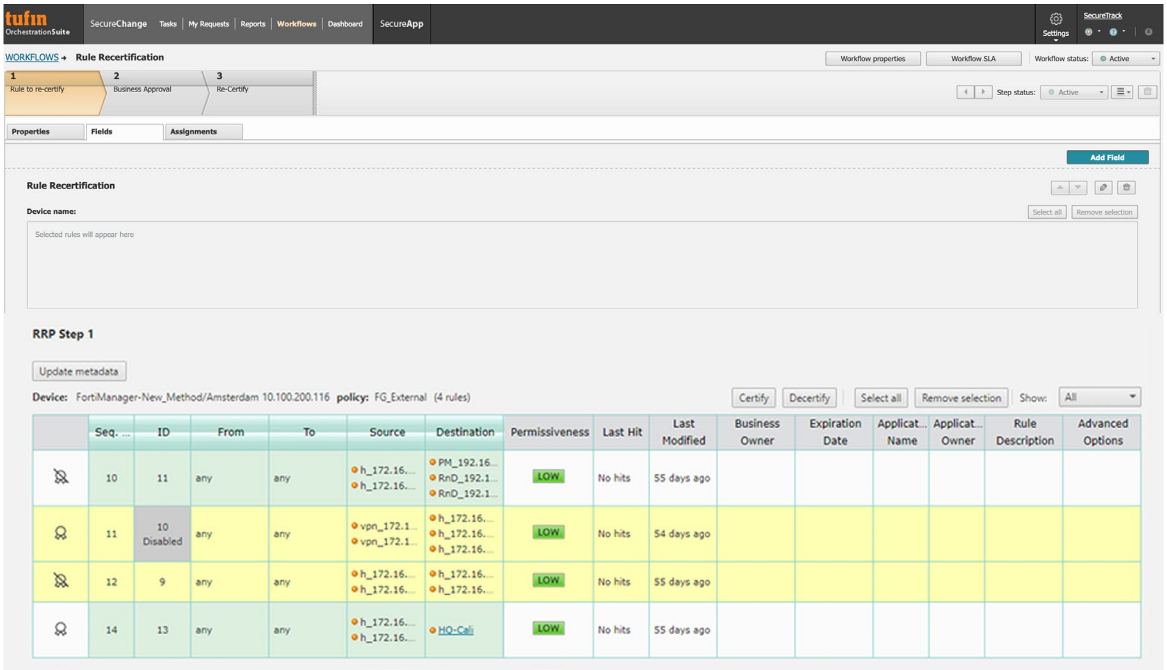
*4.1.2[30] . . ..**the access privileges** . . . **should be** identified and **reviewed on a regular basis**.*

*4.1.2[31] . . .an **effective recertification process** for assessing and, if necessary, revoking privileges should be in place and carried out at regular intervals.*

Tufin's Capabilities to Fulfill Recertification - Tamper-proof

TOS provides automated reporting capturing granular level and summary level access change status and compliance, providing full accountability. Reporting is robust, it can be based on data, or rich meta data, for the access (usage data, policy violations, ownership, comments, etc.). Full accountability is assured as each change is stored with the administrator's name, approval, time and status. Recertification data is protected against alteration. Compliance can be demonstrated at the push of a button with instant documentation. The solution is dynamic, it grows and scales with your network to maintain and demonstrate compliance in the short-term and long-term.

As business needs evolve, the underlying policies and rule bases become large, more intricate and more complex. An automated and dynamic system will enable you to keep up.



Rule Recertification

Workflow status: Active

1 Rule to re-certify | 2 Business Approval | 3 Re-Certify

Step status: Active

Rule Recertification

Device name:

Selected rules will appear here

RRP Step 1

Device: FortiManager-New_Method/Amsterdam 10.100.200.116 policy: FG_External (4 rules)

Show: All

	Seq. ...	ID	From	To	Source	Destination	Permissiveness	Last Hit	Last Modified	Business Owner	Expiration Date	Applicat... Name	Applicat... Owner	Rule Description	Advanced Options
	10	11	any	any	h_172.16... h_172.16...	PM_192.16... RnD_192.1... RnD_192.1...	LOW	No hits	55 days ago						
	11	10 Disabled	any	any	vpn_172.1... vpn_172.1...	h_172.16... h_172.16... h_172.16...	LOW	No hits	54 days ago						
	12	9	any	any	h_172.16... h_172.16...	h_172.16... h_172.16...	LOW	No hits	55 days ago						
	14	13	any	any	h_172.16... h_172.16...	HQ-Cali	LOW	No hits	55 days ago						

Rule recertification workflow screenshots, the top half of the picture shows the beginning of the rule recertification workflow where the rules to recertify are chosen, the bottom half shows an individual's certification approval screen.

[29] Page 9 https://tinyurl.com/yb94vq4b

[30] Section 4.1.2 2nd bullet, page 19 https://tinyurl.com/y8n3wscm

[31] Section 4.1.2 4th bullet, page 19 https://tinyurl.com/y8n3wscm

REQUIREMENT
3
Recertification

Recertification with tamper-proof audit trail

The Directive - Requirement #3: Recertification - Reporting

Executive Level Reporting:

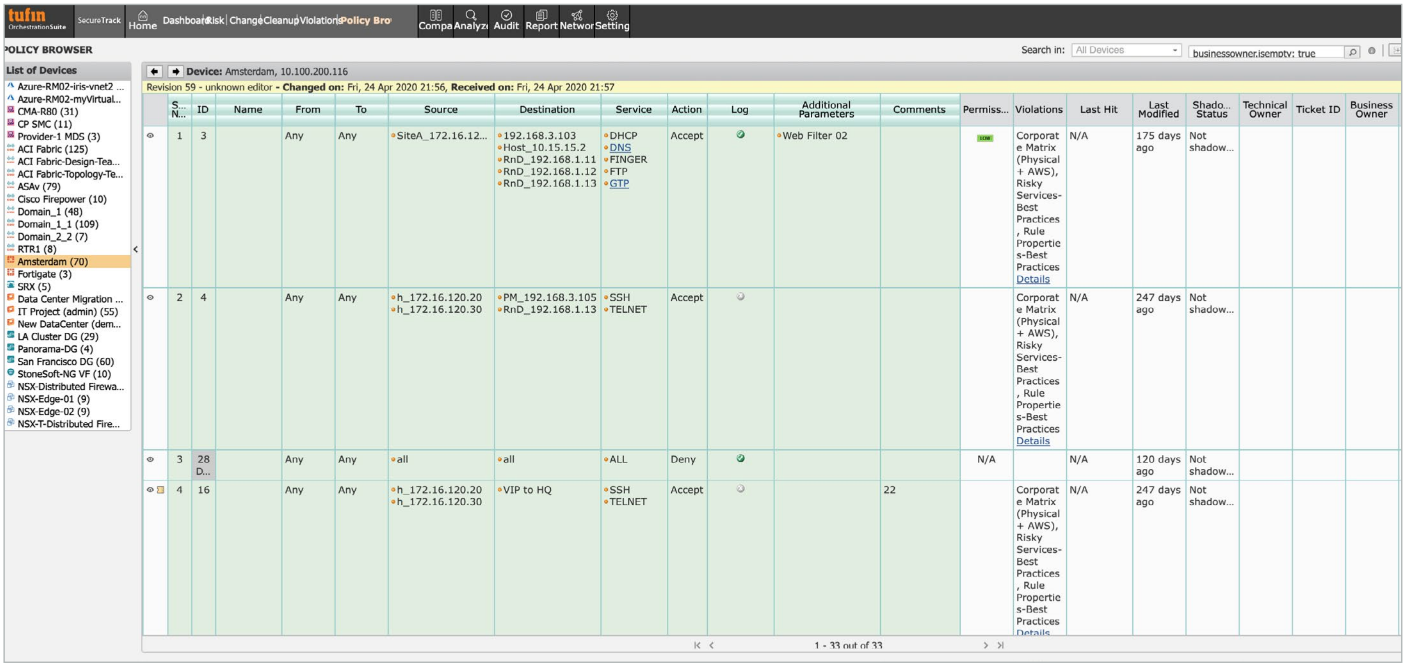
The regulation requires sufficient authority and oversight for implementation, including direct reporting to management. An automation system can support this requirement through providing the relevant management reporting and alert capabilities.

From section 2.5[32] *. . . control model has sufficient authority, independence, resources and* ***direct reporting lines to the management body*** *and, where relevant, to the senior management.*

Tufin's Capabilities to Fulfill Recertification - Reporting

TOS includes management reports (see list of standard reports and opt-in reports) that provide overviews of risk, implementation and compliance status. For example the Security Risk Report summarizes the current risk posture and calculates the risk score. The report can be run at the organizational level or per gateway, and indicates risk trends in addition to the current state. To determine the Security Score, the report uses your compliance policies, defined per ECB standards, and a group of predefined risk factors taken from leading industry standards. You can set your own priorities and customize the report to exclude specific policies, zones or risk factors. Reports can be scheduled for automatic, periodic execution and emailed to all relevant security officers.

With robust reporting, TOS can help security admins, managers, compliance and risk teams maintain ECB network security compliance.



POLICY BROWSER

Search in: All Devices businessowner.isempty: true

List of Devices

Azure-RM02-iris-vnet2 ...
Azure-RM02-myVirtual...
CMA-R80 (31)
CP SMC (11)
Provider-1 MDS (3)
ACI Fabric (125)
ACI Fabric-Design-Tea...
ACI Fabric-Topology-Te...
ASAv (79)
Cisco Firepower (10)
Domain_1 (48)
Domain_1_1 (109)
Domain_2_2 (7)
RTR1 (8)
Amsterdam (70)
Fortigate (3)
SRX (5)
Data Center Migration ...
IT Project (admin) (55)
New DataCenter (dem...
LA Cluster DG (29)
Panorama-DG (4)
San Francisco DG (60)
StoneSoft-NG VF (10)
NSX-Distributed Firewa...
NSX-Edge-01 (9)
NSX-Edge-02 (9)
NSX-T-Distributed Fire...

Device: Amsterdam, 10.100.200.116

Revision 59 - unknown editor - **Changed on:** Fri, 24 Apr 2020 21:56, **Received on:** Fri, 24 Apr 2020 21:57

	S... N...	ID	Name	From	To	Source	Destination	Service	Action	Log	Additional Parameters	Comments	Permiss...	Violations	Last Hit	Last Modified	Shado... Status	Technical Owner	Ticket ID	Business Owner
	1	3		Any	Any	SiteA_172.16.12...	192.168.3.103 Host_10.15.15.2 RnD_192.168.1.11 RnD_192.168.1.12 RnD_192.168.1.13	DHCP DNS FINGER FTP GTP	Accept	✓	Web Filter 02		LOW	Corporate Matrix (Physical + AWS), Risky Services-Best Practices, Rule Properties-Best Practices Details	N/A	175 days ago	Not shadow...			
	2	4		Any	Any	h_172.16.120.20 h_172.16.120.30	PM_192.168.3.105 RnD_192.168.1.13	SSH TELNET	Accept	○				Corporate Matrix (Physical + AWS), Risky Services-Best Practices, Rule Properties-Best Practices Details	N/A	247 days ago	Not shadow...			
	3	28 D...		Any	Any	all	all	ALL	Deny	✓			N/A		N/A	120 days ago	Not shadow...			
	4	16		Any	Any	h_172.16.120.20 h_172.16.120.30	VIP to HQ	SSH TELNET	Accept	○		22		Corporate Matrix (Physical + AWS), Risky Services-Best Practices, Rule Properties-Best Practices Details	N/A	247 days ago	Not shadow...			

1 - 33 out of 33

Screenshot showing a report that lists all rules that do not have a business owner.

[33] Guidelines On Security Measures For Operational And Security Risks Under PSD2 12/01/2018 https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

REQUIREMENT
3
Recertification

Recertification with tamper-proof audit trail

The Directive - Requirement #3: Recertification - Monitoring

Continuous Monitoring:

The regulation requires continuous monitoring.

Section 3.4   PSP should ensure that they continuously monitor threats and vulnerabilities. . .

Guideline 5 : PSPs should establish and implement processes and capabilities to continuously monitor business functions, supporting processes and information assets

Tufin's Capabilities to Fulfill Recertification - Continuous Monitoring

TOS is a real-time system. It continuously checks firewall and device level rules against your organization's security mandates . The automated change management workflow process and embedded proactive risk analysis ensure that access granted is a legitimate connection with an expiration date, and that it complies with policy. The automated risk analysis engine identifies policy violations and ensures adherence to the 'least privilege' principle. Tufin's interactive network topology map provides a graphic display of network areas and devices along with the full access path between any specified source and destination, providing visual confirmation that implemented rules are operational. The solution is dynamic to grow and scale with your network

[34] (Guidelines On Security Measures For Operational And Security Risks Under PSD2 12/01/2018) page 7 https://eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-security-measures-for-operational-and-security-risks-under-the-psd2

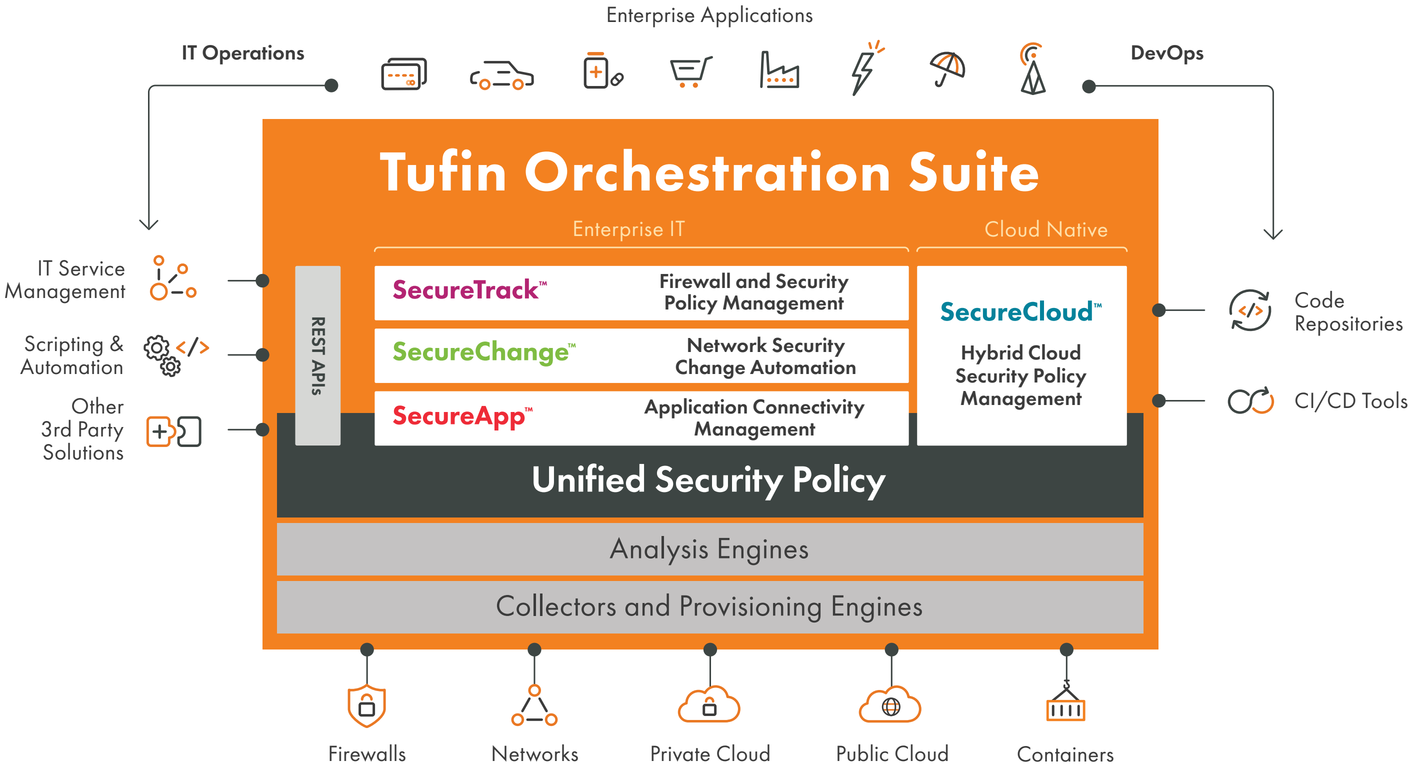
[35] (Guidelines On Security Measures For Operational And Security Risks Under PSD2 12/01/2018) page 10 https://tinyurl.com/yb94vq4b

Conclusion:

The Tufin Orchestration Suite helps organizations achieve ECB least privilege access, demonstrate compliance, and recertify regularly. It provides real-time monitoring for continuous compliance, and includes documentation and audit trails for audit readiness.

The platform will dynamically grow with your network, and works across your multi-vendor environment, including on-prem devices, as well as public and private cloud. By providing the broadest set of automated processes and the most advanced workflow configuration options, Tufin is an essential solution for complying with ECB audit requirements related to network access security policies.

Tufin will not only help your organization stay compliant with ECB, but also help enhance your network visibility, increase the productivity of your team, and improve your overall security posture. Tufin provides a best-in-class, integrated, dynamic and professional solution for meeting all of the ECB network security audit requirements as well as sound network security policy management for the state of your network today and in the future.


Enterprise Applications
IT Operations
DevOps
Tufin Orchestration Suite
Enterprise IT
Cloud Native
IT Service Management
Scripting & Automation
Other 3rd Party Solutions
REST APIs
SecureTrack™
Firewall and Security Policy Management
SecureChange™
Network Security Change Automation
SecureApp™
Application Connectivity Management
SecureCloud™
Hybrid Cloud Security Policy Management
Code Repositories
CI/CD Tools
Unified Security Policy
Analysis Engines
Collectors and Provisioning Engines
Firewalls
Networks
Private Cloud
Public Cloud
Containers