

Descrizione della Soluzione

# Garanzia di Conformità Costante dell'Open Banking alle Prescrizioni BCE di Sicurezza di Rete

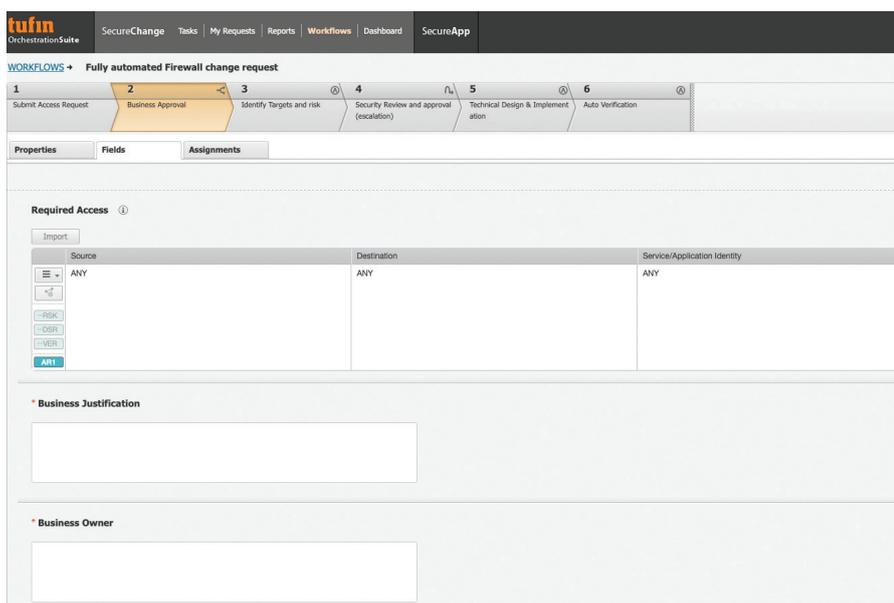
I requisiti di sicurezza di rete della BCE per l'Open Banking o la Direttiva rivista sui servizi di pagamento (PSD2, Payment Service Directive) impongono alle istituzioni finanziarie dell'UE di innalzare gli standard dei loro processi e della documentazione. Una verifica della BCE richiede che le istituzioni finanziarie giustifichino tutte le regole degli accessi, garantiscano gli accessi con privilegi minimi, istituiscano la separazione delle funzioni e stabiliscano procedure professionali, documentate e verificabili per la gestione degli accessi di rete. La dimostrazione di conformità deve essere certificata ogni 180 giorni.

Tufin è stata la scelta preferenziale di Istituzioni Finanziarie (IF) in tutta Europa e nel mondo, con oltre 700 clienti IF a livello globale. Mentre Tufin è affidabile nell'aiutare i clienti ad acquisire visibilità e controllo sulla propria posizione in relazione alla sicurezza di rete, li assiste altresì nel soddisfare la conformità della BCE sulla sicurezza di rete tramite un'unica soluzione centralizzata che abbraccia tutto l'ambiente multi-vendor e multiplatforma.

## Giustificazione e Proprietà Aziendale di Tutte le Regole di Accesso

La BCE mira a garantire che l'accesso alle reti e alle applicazioni sia giustificato e attuato correttamente. Le organizzazioni devono dimostrare di mantenere un inventario delle proprie richieste di accesso e che ciascuna richiesta dispone di un proprietario aziendale e di una giustificazione a livello aziendale. Inoltre le aziende hanno bisogno di visibilità sul modo in cui le condizioni di accesso si associano alle regole a livello di oggetti e firewall, che le regole siano conformi agli standard di sicurezza della società e che gli accessi siano implementati correttamente.

Tufin offre un approccio incentrato sulle applicazioni per la definizione, l'identificazione, il provisioning, la documentazione e la gestione degli accessi di rete. Orchestration Suite di Tufin consente di modellare la connettività e



Schermata di Tufin SecureChange che mostra il flusso di lavoro di provisioning delle modifiche di accesso. Il flusso di lavoro rende possibile la conformità della BCE in quanto richiede la giustificazione e la proprietà aziendale, l'approvazione, ed è un processo "standardizzato e riproducibile" che non può essere "compromesso o eluso" con acquisizione tramite audit trail/documentazione completi.



## Vantaggi per la Vostra Azienda:

- Garanzia di conformità costante e disponibilità alle verifiche in accordo con le prescrizioni di sicurezza di rete della BCE
- Gestione semplificata dei privilegi minimi e dell'accesso segmentato tramite la visualizzazione, la traslazione delle regole dal livello di applicazione al livello di dispositivo e una topologia di rete completa in tutta la vostra rete multi-vendor
- Flusso di lavoro per la modifica delle policy di sicurezza personalizzabile integrato con il sistema di gestione ticket
- Documentazione relativa alla connettività tramite una console centrale
- Flusso di lavoro automatizzato per il rinnovo della certificazione
- Visibilità e controllo centralizzati degli accessi di rete tra fornitori e piattaforme

di visualizzare le regole di accesso associate a ciascuna applicazione. Dei flussi di lavoro automatizzati documentano in maniera esauriente le richieste di accesso, la giustificazione e la proprietà aziendale, che tramite il motore di provisioning possono essere implementate e controllate automaticamente in relazione alla conformità costante. La disponibilità alle verifiche è garantita su base continua tramite la documentazione di ogni fase del flusso di lavoro.

## Controllo dell'Accesso con Privilegi Minimi e Separazione delle Funzioni

La BCE cerca di garantire che le aziende dispongano di soluzioni di sicurezza adeguate volte a proteggere le reti da usi impropri o attacchi. L'accesso alla rete deve essere il più possibile ridotto seguendo il principio del "privilegio minimo", e va limitato solo ai sistemi, alle applicazioni e agli individui per i quali l'accesso è richiesto e giustificato dal punto di vista aziendale. Inoltre, le aziende devono implementare la separazione delle funzioni e prestare particolare attenzione alla segregazione degli ambienti IT.

Le funzionalità di dettaglio del controllo degli accessi basate sui ruoli di Tufin, consentono alle aziende di stabilire e applicare la separazione delle funzioni in relazione alla richiesta, approvazione, progettazione, amministrazione e provisioning degli accessi. Tufin semplifica la complessità della visualizzazione e della gestione della segmentazione fino al livello più dettagliato. La segmentazione per zona consente alle aziende di definire le zone della rete che possono connettersi e il traffico di rete consentito o bloccato tra di esse. L'accesso alla rete con privilegi minimi si ottiene limitando l'accesso solo a risorse, applicazioni e soggetti con necessità aziendali giustificabili.

## Rinnovo della Certificazione

La gestione manuale dell'accesso alla rete precedentemente accettata, spesso tramite fogli di calcolo ed e-mail, è imprecisa, non scalabile e non più conforme alle normative della BCE. Per gestire gli accessi alle reti le aziende devono adottare procedure professionali, ripetibili e verificabili. Devono inoltre stabilire un processo efficace di rinnovo della certificazione, e, se necessario, la revoca dell'accesso, da effettuare ogni 180 giorni tramite un procedimento che includa la giustificazione delle regole, la data di rinnovo della certificazione, la conferma delle approvazioni e un audit trail a prova di manomissione. Gli istituti finanziari che non osservano i regolamenti della BCE devono presentare un piano correttivo per dimostrare la capacità di conformarsi in un futuro prossimo; altrimenti, rischiano di incorrere in pesanti sanzioni che possono includere l'obbligo di disattivare un'applicazione fino a quando non sarà conforme. Tufin fornisce un processo di revisione delle regole automatizzato e basato su policy, che include un flusso di lavoro eccellente per il rinnovo della certificazione che consente ai clienti di applicare il rinnovo della certificazione degli accessi ogni 180 giorni (o con qualsiasi frequenza desiderata). Offre inoltre avvisi di conformità e consente di avviare un flusso di lavoro per la revisione, l'approvazione e, se necessario, la revoca. La decisione di revocare l'accesso può condurre direttamente a un processo automatizzato e documentato per la disattivazione delle regole. Tufin automatizza l'identificazione di regole rischiose e non documentate e consente di documentare l'accesso, la giustificazione, lo stato e l'adesione agli standard richiesti. La conformità può essere dimostrata con la semplice pressione di un pulsante tramite un audit trail completo.

## La piattaforma multi-vendor di Tufin funziona con:

### Piattaforme di Rete e Cloud



### Integrazioni di Soluzioni



## L'Unica Soluzione Completa per la Disponibilità alla Verifica della Sicurezza di Rete della BCE

Tufin Orchestration Suite si adatta alla vostra rete per condurvi alla conformità, mantenervi conformi e semplificare la dimostrazione di conformità per la vostra rete in qualsiasi istante sia nel momento attuale sia per le reti sempre più complesse del futuro. Tufin non solo aiuterà la vostra organizzazione a mantenere la conformità con la BCE, ma contribuirà anche a mitigare e gestire i rischi delle policy di rete, ad aumentare la velocità di implementazione delle richieste di accesso da giorni a minuti, ad accrescere la produttività del vostro team e a migliorare il vostro livello generale in termini di sicurezza, il tutto massimizzando al contempo l'agilità aziendale. Oltre 2300 delle più grandi organizzazioni mondiali si affidano a Tufin per semplificare e automatizzare la gestione delle policy di sicurezza attraverso ambienti ibridi complessi. Ottenete fiducia, trasparenza e conformità per la vostra posizione in termini di sicurezza.

Tufin (NYSE, New York Stock Exchange, Borsa di New York: TUFN) semplifica la gestione di alcune delle reti più grandi e complesse al mondo, costituite da migliaia di firewall e dispositivi di rete e da infrastrutture di cloud ibrido emergenti. Le aziende scelgono Tufin Orchestration Suite™ per aumentare l'agilità in risposta alle esigenze aziendali in continua evoluzione, mantenendo al contempo una solida posizione di sicurezza. Tufin Orchestration Suite riduce le superfici di attacco e soddisfa la necessità di una maggiore visibilità in termini di connettività sicura e affidabile delle applicazioni. Con oltre 2000 clienti dal suo inizio, l'automazione della sicurezza di rete di Tufin consente alle aziende di implementare le modifiche in pochi minuti anziché in giorni, migliorando al contempo la loro posizione di sicurezza e l'agilità aziendale. Ulteriori informazioni sono disponibili all'indirizzo [www.tufin.com](http://www.tufin.com).

<sup>1</sup> <https://www.ecb.europa.eu/pub/pdf/other/assessmentguideinternetpayments201402en.pdf>

<sup>2</sup> Frequenza non esplicitamente indicata nelle normative, 180 giorni sono generalmente raccomandati dalle società di revisione