Visibilità, conformità e automazione per Amazon Web Services (AWS)

Informazioni sulla soluzione combinata

L'utilizzo del cloud è in rapida ascesa in tutti i settori industriali e in ogni parte del mondo. AWS è stato indicato come leader nel mercato IaaS (Infrastructure as a Service)[1]. Moltissime aziende utilizzano o sono in procinto di utilizzare AWS per acquisire maggiore agilità nella fornitura di nuovi servizi e applicazioni per i clienti[2].

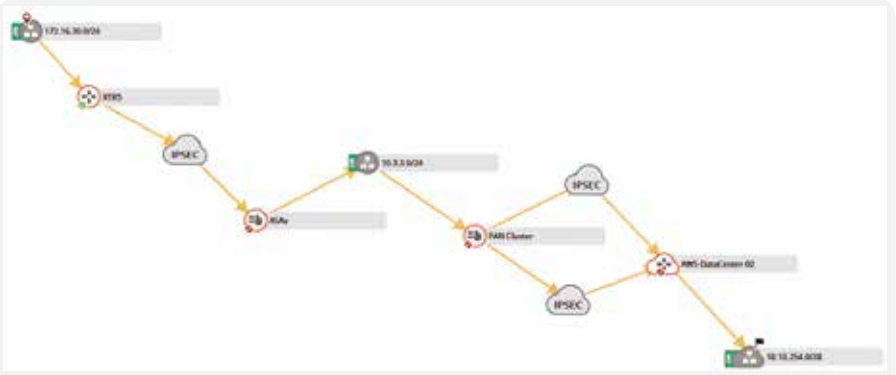
Anche se molte aziende ospitano nuove applicazioni in AWS o fanno migrare quelle esistenti, ci sono ancora domande in sospeso per quanto concerne la definizione e l'implementazione delle policy di sicurezza in AWS. Per evitare ritardi e godere dell'agilità ottimale offerta da AWS, i team preposti alla sicurezza spesso non vengono coinvolti nelle modifiche quotidiane alla sicurezza e alla connettività di AWS o addirittura nel setup iniziale dei gruppi di sicurezza AWS.

Oltre alle sfide di visibilità e applicazione in AWS, molte aziende che iniziano a utilizzare AWS avranno infrastrutture fisiche e virtuali che continueranno a gestire. Questi ambienti eterogenei di cloud pubblico, privato e reti fisiche aumentano le sfide create da visibilità condivisa, sicurezza e connettività tra fornitori e piattaforme e possono mettere in serio pericolo il livello di sicurezza, la conformità alle normative e anche la disponibilità di applicazioni fondamentali per la mission.

Visibilità centralizzata tra reti AWS e On-Premise

La visibilità è essenziale per gestire sicurezza e connettività in una rete eterogenea. I team preposti alle operazioni di rete e alla sicurezza che non hanno visibilità all'interno dei gruppi di sicurezza AWS e delle regole non possono identificare violazioni alle policy o prepararsi per gli audit. Con Tufin possono avviare un'individuazione automatica di istanze AWS, applicazioni e connettività di applicazione, tag, gruppi di sicurezza e regole, restando aggiornati con il monitoraggio delle modifiche in tempo reale. Grazie a questa visibilità, possono anche avviare analisi per identificare violazioni alla policy di sicurezza dell'organizzazione o linee guida del settore.

Inoltre, l'utilizzo di piattaforme multiple e fornitori all'interno della rete ibrida rende incredibilmente complessa la visualizzazione della connettività per applicazioni che spaziano da AWS a infrastruttura on-premise. Grazie alla gestione centrale di piattaforme cloud pubbliche e private e di firewall fisici e router, Tufin consente di visualizzare la connettività dell'applicazione utilizzabile per risolvere guasti o pianificare modifiche e migrazioni.



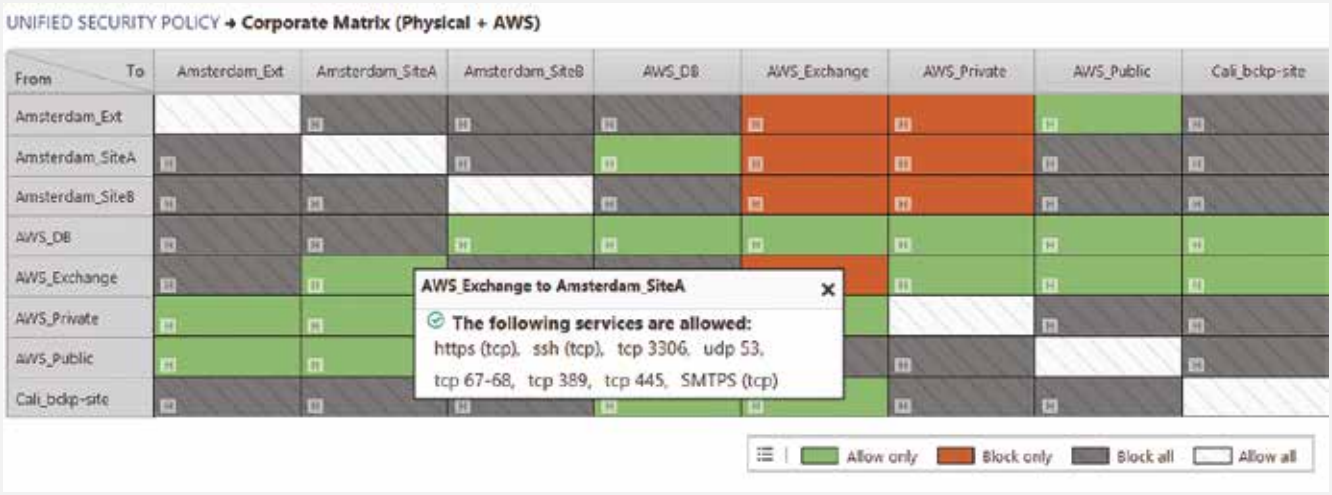
L'analisi del percorso di topologia interattiva Tufin visualizza la connettività tra AWS e firewall on-premise

Vantaggi per le attività:

- Visibilità di sicurezza in AWS e nella rete eterogenea
- Aumento dell'agilità grazie all'orchestrazione di policy di sicurezza attiva su cloud e on-premise
- Automazione delle operazioni di sicurezza per AWS per stabilire controlli integrati
- Garanzia di una stretta segmentazione e conformità delle policy in AWS e nella rete ibrida
- Riduzione della preparazione delle verifiche fino al 70% con conformità continua
- Risoluzione errori e provisioning della connettività per applicazioni nord-sud

Conformità alle policy e disponibilità alle verifiche per applicazioni AWS

I controlli di sicurezza e conformità definiti e applicati in sede spesso non vengono implementati nelle piattaforme cloud. Ciononostante, le applicazioni ospitate in AWS devono allinearsi con le policy dell'organizzazione per proteggere dati e sistemi sensibili e contenere il successivo attacco informatico. Tufin aiuta i clienti a definire e applicare una Unified Security Policy™ a livello centrale, in grado di rafforzare la segmentazione della rete, implementando una conformità costante con standard interni e di settore quali PCI DSS, SOX, NERC CIP v5 e ISO 27001. Applicando una conformità continua, le organizzazioni non solo evitano le sanzioni associate alla mancanza di conformità, ma possono anche ridurre l'impegno profuso nella preparazione delle verifiche fino al 70%. I team di sicurezza non vengono così bypassati da team cloud grazie all'adozione di un controllo di policy di sicurezza integrato che non ritarda la release di nuove applicazioni e servizi.



La policy di sicurezza unificata Tufin rafforza la segmentazione da zona a zona in AWS e rete ibrida

Massimizzare l'agilità tramite l'automazione end-to-end

L'agilità è il fattore più importante dal punto di vista della competitività nel panorama commerciale di oggi. Tuttavia, per le applicazioni nord-sud che si estendono tra AWS e infrastruttura on-premise, l'agilità può essere limitata a causa dei diversi sistemi di gestione e orchestrazione. Un'applicazione può avere pieno provisioning in AWS, ma deve attendere l'accesso ad un database di tipo data center tramite firewall fisici e router prima di essere lanciata. Con la gestione centrale Tufin e il processo di modifica completamente automatizzato, i clienti possono implementare i requisiti di connettività end-to-end all'interno della rete eterogenea.

Il processo di modifica fornito da Tufin comprende l'analisi automatizzata del rischio per conformità policy integrata, design automatizzato e provisioning per firewall e piattaforme cloud e verifica automatizzata per aumentare la produttività e accelerare la release.

Tufin offre provisioning automatizzato per le modifiche ai gruppi di sicurezza AWS e guida gli utenti alla definizione del corretto gruppo di sicurezza da modificare. Sulla base dell'orchestrazione end-to-end, Tufin offre inoltre un processo automatizzato per la migrazione delle applicazioni in AWS. Il modello di connettività di applicazione può essere duplicato e sottoposto a provisioning in AWS con un'interfaccia utente simile a un'installazione guidata e l'applicazione originale può essere poi revocata con il processo Tufin per aumentare la sicurezza di rete.

Tufin

Tufin® è leader nell'orchestrazione delle policy di sicurezza delle reti ed è partner di oltre la metà delle 50 maggiori compagnie citate in Forbes Global 2000. Tufin semplifica la gestione di alcune tra le più grandi e complesse reti al mondo, costituite da migliaia di firewall e dispositivi di rete e da innovative infrastrutture cloud ibride. Le aziende scelgono la pluripremiata Tufin Orchestration Suite™ per risultare più agili nel far fronte ai requisiti commerciali in continua evoluzione e preservare al contempo una robusta infrastruttura di sicurezza. Tufin riduce le superfici di attacco e risponde alle esigenze di maggiore visibilità all'interno dei sistemi di connettività applicativa sicuri e affidabili. L'automazione della sicurezza di rete consente alle aziende la rapida implementazione delle modifiche, con analisi proattiva dei rischi e conformità costante alle policy. Tufin vanta oltre 1.800 clienti in tutti i settori industriali e in ogni parte del mondo. I prodotti e le tecnologie Tufin sono brevettate negli Stati Uniti d'America e in altri Paesi.

[1] Gartner Magic Quadrant for Cloud Infrastructure as a Service, report mondiale, Lydia Leong et al, pubblicato il 3 agosto 2016

[2] RightScale 2016 State Of The Cloud Report

tufin
www.tufin.com

SB-11-16

amazon web services