

Visibilidade, conformidade e automação para Amazon Web Services (AWS)

Resumo da Solução Integrada

Todos os países e indústrias estão adotando ambientes em nuvem, e a AWS foi considerada a líder no mercado de IaaS (Infraestrutura como Serviço)¹. A maioria das empresas usa ou planeja usar a AWS para agilizar a entrega de novos serviços e aplicativos aos clientes².

Enquanto muitas empresas hospedam novos aplicativos na AWS ou migram aplicativos existentes, ainda há questões em aberto sobre a definição e a aplicação das políticas de segurança na AWS. Para evitar atrasos e obter a agilidade ideal que a AWS oferece, equipes de segurança geralmente não se envolvem em mudanças diárias referentes à segurança e à conectividade em ambientes AWS, ou mesmo na configuração inicial de grupos de segurança da AWS.

Além dos desafios de visibilidade e aplicação na AWS, grande parte das empresas usuárias da AWS ainda possui infraestrutura física e virtual que continuarão gerenciando. Esses ambientes heterogêneos de nuvem pública, nuvem privada e redes físicas apresentam desafios de visibilidade, segurança e conectividade envolvendo todos os fornecedores e plataformas tecnológicas, podendo ameaçar a postura de segurança, a conformidade com as normas e a disponibilidade de aplicativos de missão crítica.

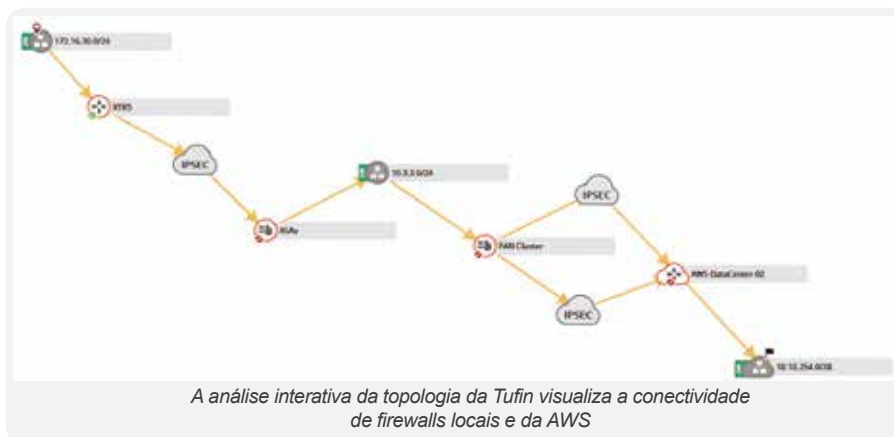
Visibilidade centralizada entre redes AWS e On-Premise

Visibilidade é essencial para gerenciar a segurança e a conectividade em toda a rede heterogênea. Equipes de operações de rede e segurança sem visibilidade das regras e dos grupos de segurança da AWS não conseguem identificar as violações de políticas ou preparar-se para auditorias. Com a Tufin, elas podem executar uma busca automática para encontrar instâncias, aplicativos e conectividade de aplicativos, tags, grupos de segurança e regras da AWS, além de se manterem atualizadas com o monitoramento de mudanças em tempo real. Com base nessa visibilidade, as equipes também podem realizar análises para identificar violações à política de segurança da empresa ou às normas da indústria.

Além disso, o uso de diversos fornecedores e plataformas na rede híbrida dificulta bastante a visualização da conectividade de aplicativos que abrangem a infraestrutura local e da AWS. Com um gerenciamento centralizado de plataformas de nuvem públicas e privadas e firewalls e roteadores físicos, a Tufin consegue fornecer visualização da conectividade de aplicativos que pode ser usada para solucionar falhas ou planejar mudanças e migrações.

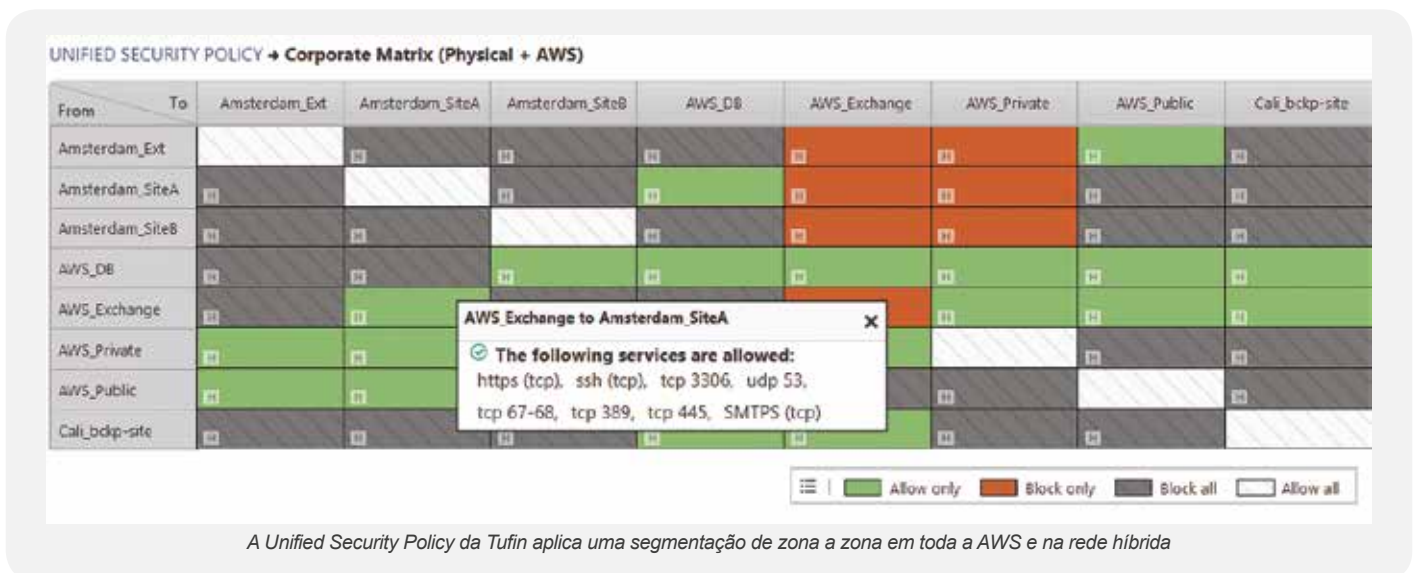
Benefícios para o seu negócio:

- Obtenha visibilidade de segurança na AWS e em toda a rede heterogênea
- Aumente a agilidade com uma orquestração de políticas de segurança que funciona na nuvem e no local
- Automatize operações de segurança para a AWS para estabelecer controles integrados
- Garanta uma segmentação ampla e a conformidade com políticas na AWS e em toda a rede híbrida
- Reduza as preparações para auditorias em até 70% através de uma conformidade contínua
- Solucione problemas e forneça conectividade a aplicativos que se comunicam em ambos os sentidos



Conformidade com políticas e prontidão para auditorias dos aplicativos da AWS

Controles de conformidade e segurança definidos e aplicados no local muitas vezes não são aplicados em plataformas da nuvem. Mesmo assim, aplicativos hospedados na AWS devem estar alinhados com as políticas da organização para proteger dados e sistemas sensíveis e restringir futuros ciberataques. A Tufin ajuda seus clientes a definir e aplicar uma Unified Security Policy™ central que aumenta a segmentação da rede e promove a conformidade contínua com normas internas e da indústria, como PCI DSS, SOX, NERC CIP v5 e ISO 27001. Ao incentivar uma conformidade contínua, as organizações não só evitam as penalidades associadas a falhas no cumprimento das normas, mas também podem reduzir os esforços de preparação para auditorias em até 70%. Equipes de segurança podem evitar o desvio das equipes na nuvem através da adoção de um controle integrado de política de segurança que não atrasa a entrega de novos aplicativos e serviços.



UNIFIED SECURITY POLICY → Corporate Matrix (Physical + AWS)

From	To	Amsterdam_Ext	Amsterdam_SiteA	Amsterdam_SiteB	AWS_DB	AWS_Exchange	AWS_Private	AWS_Public	Calif_bckp-site
Amsterdam_Ext		Block all	Block all	Block all	Block all	Block only	Block only	Allow only	Block all
Amsterdam_SiteA		Block all	Allow all	Block all	Allow only	Block only	Block only	Block all	Block all
Amsterdam_SiteB		Block all	Block all	Allow all	Block all	Block only	Block only	Block all	Block all
AWS_DB		Block all	Block all	Allow only	Allow only	Block only	Allow only	Allow only	Block all
AWS_Exchange		Block all	Allow only	Block all	Block all	Block only	Block only	Block all	Block all
AWS_Private		Block all	Block all	Block all	Block all	Block only	Block only	Block all	Block all
AWS_Public		Block all	Block all	Block all	Block all	Block only	Block only	Block all	Block all
Calif_bckp-site		Block all	Block all	Block all	Block all	Block only	Block only	Block all	Block all

AWS Exchange to Amsterdam_SiteA

The following services are allowed:
https (tcp), ssh (tcp), tcp 3306, udp 53,
tcp 67-68, tcp 389, tcp 445, SMTPS (tcp)

Legend: Allow only (green), Block only (orange), Block all (grey), Allow all (white)

A Unified Security Policy da Tufin aplica uma segmentação de zona a zona em toda a AWS e na rede híbrida

Agilidade maximizada com automação de ponta a ponta

Agilidade é o fator de competitividade mais importante no mundo dos negócios atual. Porém, para aplicativos que se comunicam em ambos os sentidos e abrangem a infraestrutura local e da AWS, a agilidade pode ficar limitada devido a diferentes sistemas de gerenciamento e orquestração. Um aplicativo pode ser totalmente provisionado na AWS, mas precisa esperar o acesso a um banco de dados do data center por meio de firewalls e roteadores físicos antes de ser iniciado. Com o gerenciamento centralizado e o processo de mudanças totalmente automatizado da Tufin, os clientes podem implementar os requisitos de conectividade de ponta a ponta na rede heterogênea.

O processo de mudanças fornecido pela Tufin inclui uma análise de risco automatizada integrada para conformidade com políticas, design e provisionamento automatizado para firewalls e plataformas na nuvem e uma verificação automatizada para aumentar a produtividade e acelerar a entrega.

A Tufin fornece provisionamento automatizado de mudanças a grupos de segurança da AWS e ajuda os usuários a alterarem o grupo de segurança correto. Com base na orquestração de ponta a ponta, a Tufin também oferece um processo automatizado para a migração de aplicativos para a AWS. O modelo de conectividade de aplicativos pode ser duplicado e provisionado na AWS com uma interface de usuário em forma de assistente, e em seguida o aplicativo original pode ser removido com o processo da Tufin para aumentar a segurança de rede.

Sobre a Tufin

A Tufin® é líder em Orquestração de Políticas de Segurança de Redes, atendendo a mais da metade das 50 maiores empresas da Forbes Global 2000. A Tufin simplifica o gerenciamento de algumas das maiores e mais complexas redes do mundo, compostas por milhares de dispositivos de firewall e estruturas de nuvem híbrida em desenvolvimento. Empresas escolhem a solução premiada Tufin Orchestration Suite™ para aumentar a agilidade diante das demandas comerciais em constante mudança enquanto mantêm uma postura robusta de segurança. A Tufin reduz a superfície de ataque e satisfaz a necessidade de maior visibilidade na conectividade segura e confiável dos aplicativos. Sua automação da segurança de redes permite que empresas implementem mudanças em minutos, com análise proativa de riscos e conformidade contínua com as políticas. A Tufin atende a mais de 1.800 clientes de todos os setores e regiões; seus produtos e tecnologias são patenteados nos EUA e em outros países.

¹ Quadrante Mágico da Gartner para Infraestrutura de Nuvem como Serviço, Relatório mundial, Lydia Leong et al, publicado em 3 de agosto de 2016

² Relatório de 2016 da RightScale sobre o estado da nuvem