AWS Reference Design Document

Contents

Overview

Amazon Web Services (AWS), Public Cloud and the New Security Challenges

Cloud adoption is proliferating for organizations of all sizes. According to the 2018 RightScale State of the Cloud Report, 92% of enterprises already use public cloud platforms, 64% of which have adopted Amazon Web Services (AWS).

AWS provides organizations flexibility and agility as they extend their operations to virtual networks. As always, new capabilities and deployment models of the cloud introduce new network security challenges, including an increased attack surface, resulting in an increased exposure to cyber threats.

Using Amazon Elastic Compute Cloud (Amazon EC2), companies access flexible computing capacity in the cloud. With EC2, new server instances are provisioned and live in minutes, and spun down just as quickly. This flexibility enables enterprises to rapidly scale their infrastructure as needed, only paying for the actual capacity used. Amazon EC2 frees developers to focus on meeting business needs through a robust infrastructure that scales.

To help secure your cloud-base servers, Amazon provides a tool called AWS Security Groups. Security Groups act as virtual firewalls between your cloud-based server instances, enabling you to manage the communication that is allowed or restricted between all virtual machine (VM) instances in your cloud-based deployment.

However, AWS Security Groups are not a complete solution for mitigating the threats introduced by cloud computing. For example, Security Groups are available only for AWS EC2 and VPC, are isolated to an individual AWS account and region, and do not deliver or manage security for other cloud providers. Organizations that have multiple AWS accounts, distribute their cloud infrastructure across multiple regions, or use private and/or public clouds services provided by other vendors will not have complete security coverage in their cloud environment.

Security at the Speed of DevOps

DevOps is a combination of "development" and "operations," but DevOps involves a lot more than just uniting two departments under one umbrella. DevOps is a culture and process that has a lot in common with agile development.

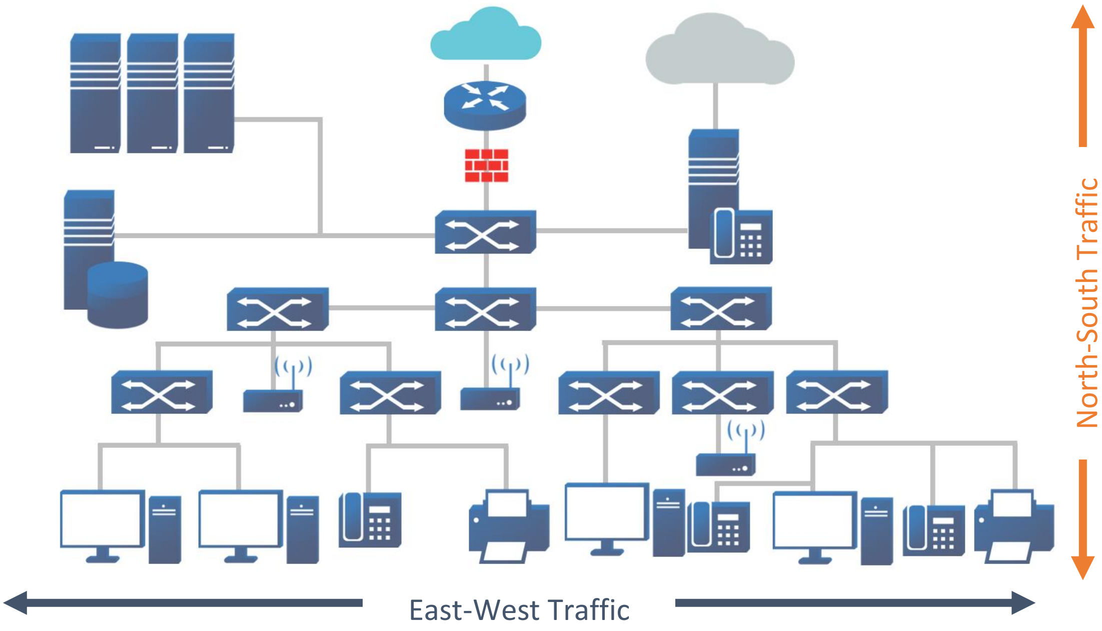
A DevOps workflow typically excludes the extended planning and auditing of code for fear that it will obstruct business agility. For example, application teams cannot deploy fifty changes per day if they must wait for explicit approval for each change. Any pause for approval or audit delays the workflow cycle, prevents rapid application improvement, and hinders the positive effects generated by DevOps.

Security is often not fully embedded into the DevOps toolchain. Moreover, the traditional processes and oversight of ensuring changes to networks, applications, and infrastructure resources is no longer applicable when working with flexible cloud infrastructure. While completely leaving security out of the DevOps process is not a viable choice, if security reviews do not support the agility required by DevOps, then security will be circumvented by the DevOps workflow model.

Security procedures must change to meet the requirements of DevOps by adapting to a new way of enforcement. Security can no longer be a release gateway or a near-final review stage of a release. Security must be integrated throughout every part of the DevOps workflow. This is often referred to a "shift left" for security and it is the only way to ensure security is embedded in rapid development cycles.

Securing East-West and North-South AWS Traffic

East-west traffic is the transfer of data packets from server to server within a data center in the same AWS environment. North-South traffic is the transfer of data packets from an AWS VPC environment to the legacy datacenter or vice versa.



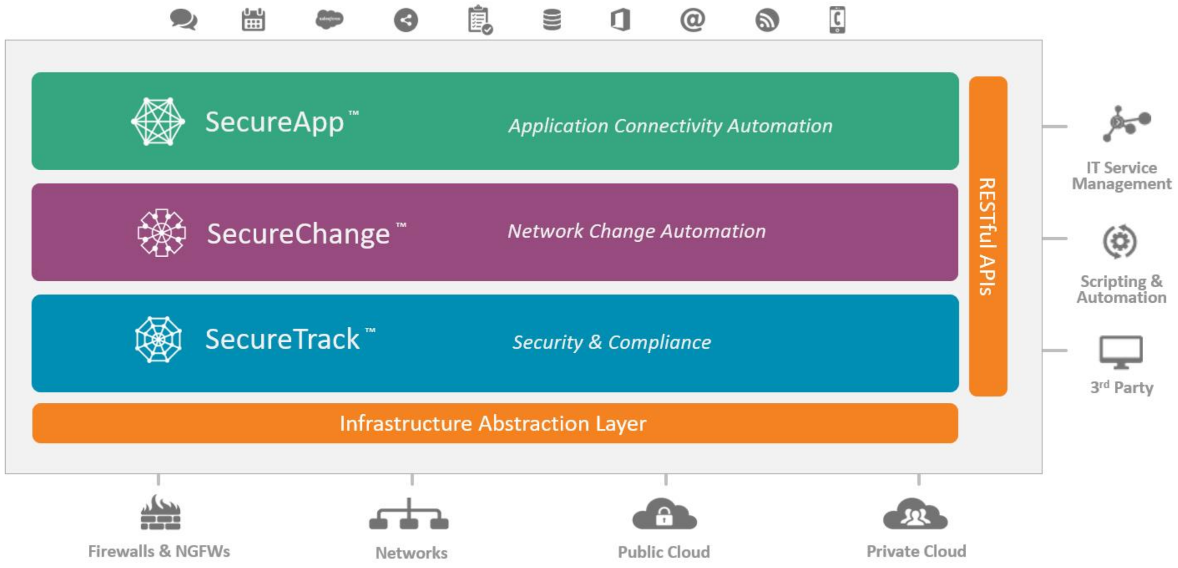
Visibility into both types of traffic – east-west and north-south – is critical for organizations, enabling them to determine the best security practices for their networks and data centers. While many organizations focus on securing external traffic that enters their networks, it is equally important for organizations to monitor internal traffic. Monitoring internal traffic patterns can identify malware or other attacks that have infiltrated the network and also identify insider threats.

Utilizing AWS Security Groups across all your VM instances significantly reduces the attack surface for exploitation and limits the impact of an active attack by restricting east-west traffic.

Tufin Orchestration Suite™ for Amazon Web Services (AWS)

Tufin Orchestration Suite™ is a complete solution for automatically designing, provisioning, analyzing, and auditing network security policy changes from the application layer down to the network layer. With Tufin Orchestration Suite™, IT and security organizations centrally design and manage micro-segmentation, continuously monitor adherence to corporate security policy, identify violations to security policy, and automate changes throughout the entire multi-vendor, multi-platform datacenter through a single pane of glass.

Tufin Orchestration Suite provides centralized management with end-to-end, policy-based change automation of Amazon VPCs, Security Groups, and Instances alongside other cloud platforms and traditional network devices to provide full visibility across the enterprise. Organizations use the Tufin Orchestration Suite to seamlessly extend network security policy management to critical business applications deployed on AWS, while ensuring the enterprise is fully secure and continuously compliant.



Tufin Orchestration Suite integrates with AWS to support the four key security requirements:

- **Visibility** – View and track changes to security policy and configuration in the AWS environment and across the hybrid network.
- **Reactive Security Policy Orchestration –** Define and manage your security policy both within your AWS environment as well as your external data center. Monitor violations to the security policy after changes are provisioned to the AWS environment.
- **Proactive Security Policy Orchestration –** Provide the security team with control by deploying a zone-to-zone access policy matrix and enforcing it as part of DevOps CI/CD pipeline. By deploying a policy-based connectivity matrix reflective of security policy, enterprises ensure adherence to corporate security policy, identify, and understand risk in access changes, and avoid slowing down business agility.
- **Policy-Driven Change Automation** – Automate connectivity changes to ensure adherence to corporate security policy, understand the potential risk, and provision north-south connectivity across AWS security groups and physical firewall and network devices.

The following chapters cover the above use cases in depth while outlining business challenges and how Tufin can help solve them.

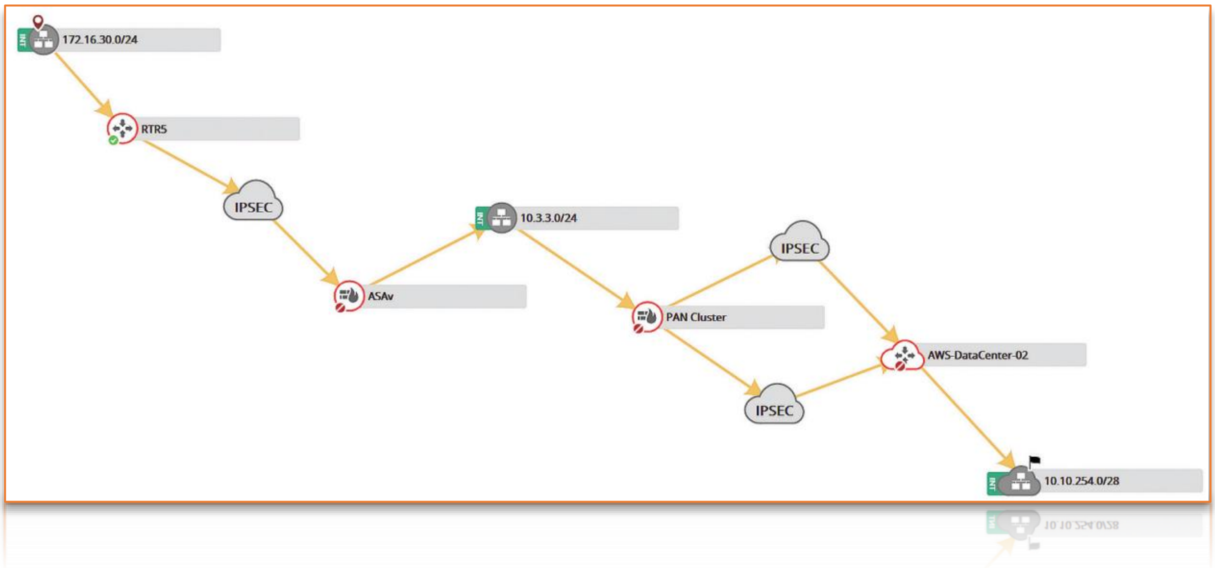
Visibility to AWS Environment – You can't secure what you can't see

Challenge:
Visibility usually ranks first as the key security challenge in public cloud environments. The reason is that often security teams do not have a view into AWS, or even if they have a view, they cannot keep up with the high frequency of access changes. Limited visibility means that there is no way for the security team to understand the impact of changes and, therefore, no way to identify and remediate risks.

Another challenge is the increasing number of consoles when adding AWS to an already heterogeneous network. Security operations managers require visibility into changes across all these enforcing technologies – what was changed and who changed it – without having to use different consoles and dashboards in order to easily identify compliance violations or security risks. In addition to that, using multiple platforms and vendors across the hybrid network makes it extremely difficult to visualize connectivity for applications that span AWS and on-premises infrastructure.

Tufin Solution:
Tufin Orchestration Suite™ serves as the single pane of glass to manage and control security across the hybrid cloud and physical networks. Through a central console, security managers gain the same level of visibility and control in their AWS environment that they are accustomed to in traditional data centers. An accurate audit trail of all changes is available including advanced change monitoring that shows whether changes were made to AWS security groups and the actual details of those changes. The tracking of all changes ensures that reports are readily available for auditors when necessary.

By centrally managing public and private cloud platforms, physical firewalls, and switches and routers, Tufin provides an overall accurate topology map for visualization of connectivity between instances running in the AWS environment and servers running in the legacy datacenter. The visualization is particularly helpful to troubleshoot connectivity failures and to plan changes and migrations.



Tufin Interactive Map path analysis visualizes connectivity across AWS and on-premises firewalls

Reactive Security Policy Orchestration

Challenge:

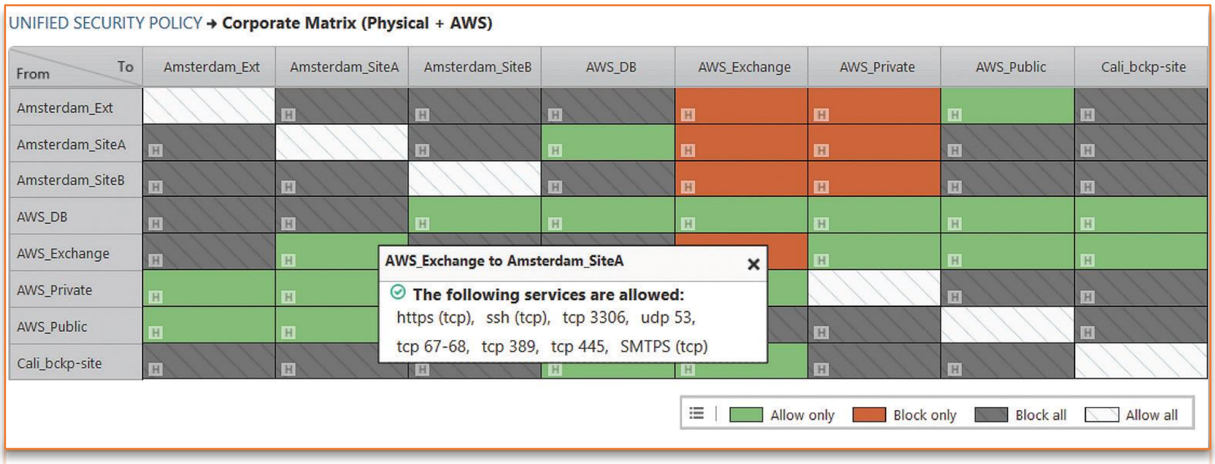
Security and compliance requirements that are defined and enforced on-premises are often not enforced in cloud platforms. At the same time, applications hosted in AWS or spread across AWS and the legacy data center must align with the organization's security policies to both protect sensitive systems and data and to prevent the next cyberattack. Managing and continuously monitoring enterprise security policy becomes more challenging and demanding for the security team in complex, heterogeneous environments.

Throughout changes to the network and hybrid cloud, security managers also face significant challenges in normalizing all the change data for reporting, auditing and management purposes. The pursuit of continuous compliance is a lofty ideal and is pushed further out with the utilization of multiple vendors and increasingly dynamic and frequent changes. Throughout all of the introduced complexity, security admins are accountable for protecting the organization from cyber threats, and therefore must align security policies in the cloud with the way they are defined and enforced in the on-prem network.

Tufin Solution:

Tufin Orchestration Suite helps customers define and enforce a central Unified Security Policy™ that tightens network segmentation and enforces continuous compliance with internal and industry standards such as PCI DSS. Deploying an enforceable continuous compliance model not only reduces the probability of penalties, but also reduces audit preparation efforts by up to 70%. Security teams avoid being bypassed by cloud teams and DevOps through a built-in security policy control that does not delay the delivery of new applications and services.

The screenshot below shows Tufin's zone-based segmentation matrix which is an element of the Unified Security Policy (USP). This matrix represents the different network zones on both the horizontal and vertical axes. The colors of the cells indicate the access permitted between the zones. In the zone segmentation matrix, a green cell indicates that specific services are allowed, a gray cell indicates that all traffic is blocked, and a red cell indicates that some traffic is allowed. Each zone can include IP addresses and/or security groups to represent physical, virtual or public cloud environments.



UNIFIED SECURITY POLICY → **Corporate Matrix (Physical + AWS)**

From \ To	Amsterdam_Ext	Amsterdam_SiteA	Amsterdam_SiteB	AWS_DB	AWS_Exchange	AWS_Private	AWS_Public	Cali_bckp-site
Amsterdam_Ext	□	▨ H	▨ H	▨ H	🟧 H	🟧 H	🟩 H	▨ H
Amsterdam_SiteA	▨ H	□	▨ H	🟩 H	🟧 H	🟧 H	▨ H	▨ H
Amsterdam_SiteB	▨ H	▨ H	□	▨ H	🟧 H	🟧 H	▨ H	▨ H
AWS_DB	▨ H	▨ H	🟩 H	🟩 H	🟩 H	🟩 H	🟩 H	🟩 H
AWS_Exchange	▨ H	🟩 H	▨	▨	🟧	🟩 H	🟩 H	🟩 H
AWS_Private	🟩 H	🟩 H	[illegible]	[illegible]	🟩	□	▨ H	▨ H
AWS_Public	🟩 H	🟩 H	[illegible]	[illegible]	▨	▨ H	□	▨ H
Cali_bckp-site	▨ H	▨ H	▨ H	🟩 H	🟩 H	▨ H	▨ H	□

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)

☰ | 🟩 Allow only 🟧 Block only ▨ Block all □ Allow all

Tufin Unified Security Policy - zone-based segmentation matrix

Tufin's Unified Security Policy can also be used to define and enforce a tagging policy for VMs, to help customers control the proliferation of VMs in public cloud environments.

Operational needs occasionally require an exception to a desired segmentation policy. For example, a specific business application may require non-compliant or risky access in order to run properly, even though it introduces risk to the organization. The Unified Security Policy provides centralized exception management that allows a security administrator to identify and manage exceptions, assign an expiration date to non-compliant rules, and ensure that they are reviewed for approval or removal by a specific date. This process provides the security administrator time to talk with the business application owner and find a way to either change how the application works or change the segmentation policy. All policy exceptions are automatically documented and auditable.

Proactive Security Policy Orchestration

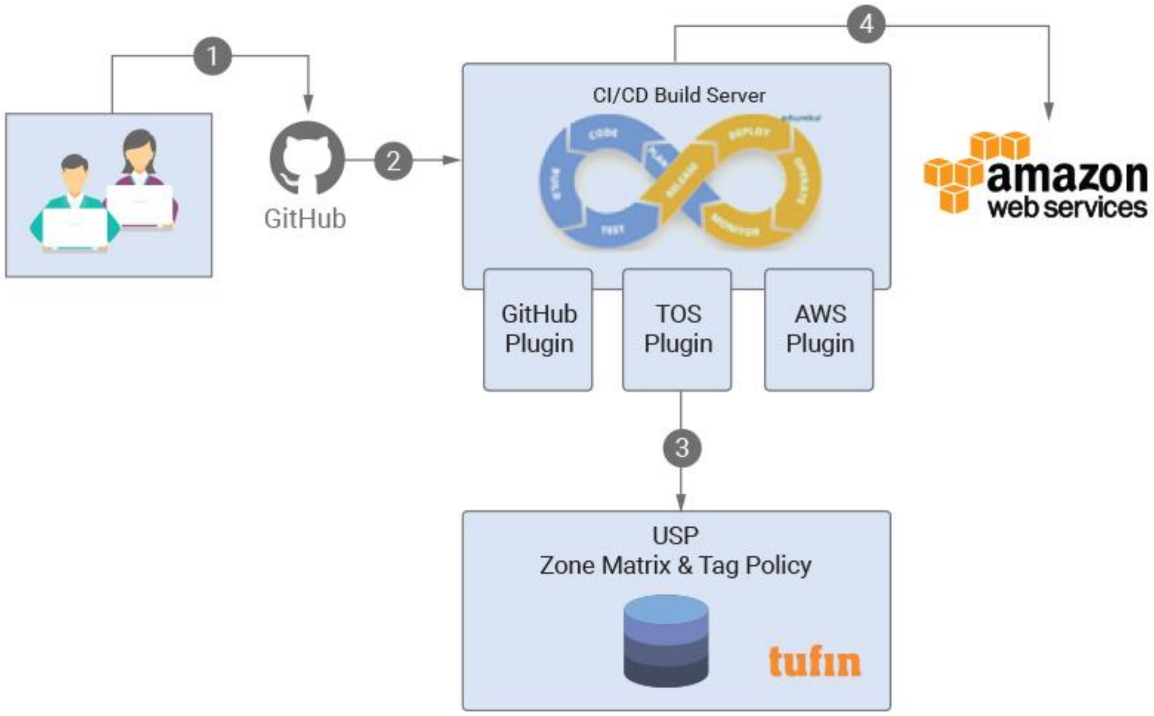
Challenge:

For business leaders, moving to the cloud is all about speed of service delivery, flexibility, scalability and new capabilities and features that would take too long to develop on-prem. The ability to deploy applications and services into cloud environments pushes all facets of IT to move faster than ever before. Amid all this urgency, security teams are perceived as the bottlenecks to rapid development or operation implementations, and obstacles that slow down production code pushes. The challenge facing enterprises today is integrating security and compliance checks directly into DevOps toolchains in a way that meets the business or deployment agility requirements.

Tufin Solution:

Tufin enables enterprises to achieve continuous compliance through the Unified Security Policy by hooking directly into the common DevOps CI/CD frameworks (such as Jenkins) and through API calls that validate the templates for provisioning to the AWS environment.

Consider the example below of DevOps workflow outlined, where DevOps leverages JSON based templates such as CloudFormation to create instances within the AWS (steps 1 and 2). The CloudFormation files are stored in a common files repository, usually GitHub, which serves as the referenceable repository. If changes to Security groups are needed, they will be done on the existing CloudFormation and will overwrite existing Security Groups with new content updated in GitHub. DevOps can integrate security policy checks into the CI/CD toolchain using the Tufin Orchestration Suite API keys. Below (step 3) shows the security groups being configured in CloudFormation and tested for compliance against the Unified Security Policy. Output is logged to job console output and, based on predefined configurations, the job will fail or will proceed.



Policy-Driven Change Automation

Challenge:

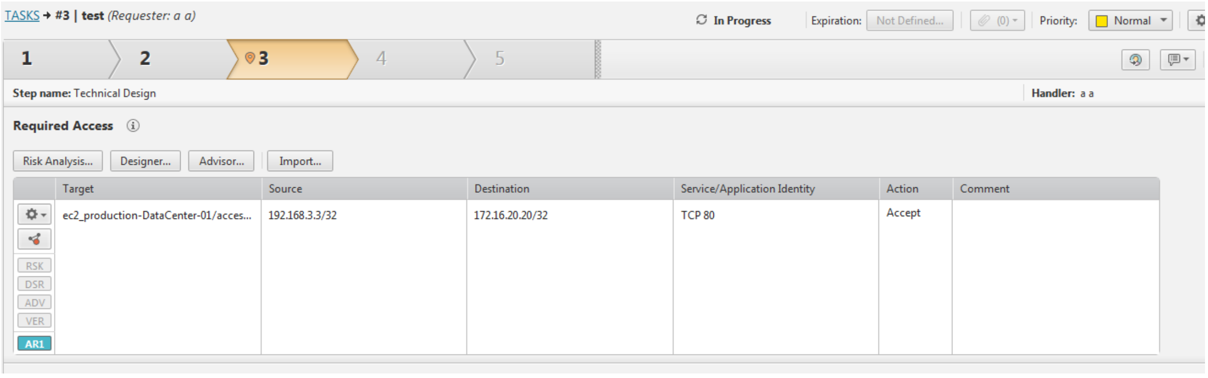
Agility is the most critical competitive factor in today's business landscape. However, for north-south applications spanning across AWS and on-premises infrastructure, agility can be limited due to disparate management and orchestration systems. An application can be fully provisioned in AWS, but it can take days – sometimes weeks – before it is launched to get access to a data center database via physical firewalls and routers. These delays in providing north-south connectivity result in enterprises losing the agility they achieved in the cloud.

Tufin Solution:

Tufin Orchestration Suite provides central management and a fully automated change process, providing end-to-end connectivity across the hybrid network while meeting security policy mandates. End-to-end automation of network security changes with baked-in security and compliance enables both north-south and east-west connectivity by provisioning changes to AWS Security Groups as well as to legacy firewalls.

The change process provided by Tufin Orchestration Suite™ includes automated risk analysis for built-in policy compliance and best practices, automated design and provisioning for both on-prem firewalls and AWS Security Groups, and automated connectivity verification to boost productivity and accelerate delivery. Automated provisioning for changes to AWS Security Groups (or subnets) reduce misconfigurations and ensure accuracy. The automated change design is based on the most accurate topology simulation and efficient path analysis across AWS and other platforms on the market.

While all these capabilities are supported through the SecureChange UI, customers often integrate Tufin workflows and process management into their existing third-party ticketing tools (e.g. ServiceNow or Remedy) through APIs or integration applications to keep their existing business processes and flows unchanged.


TASKS → #3 | test *(Requester: a a)*

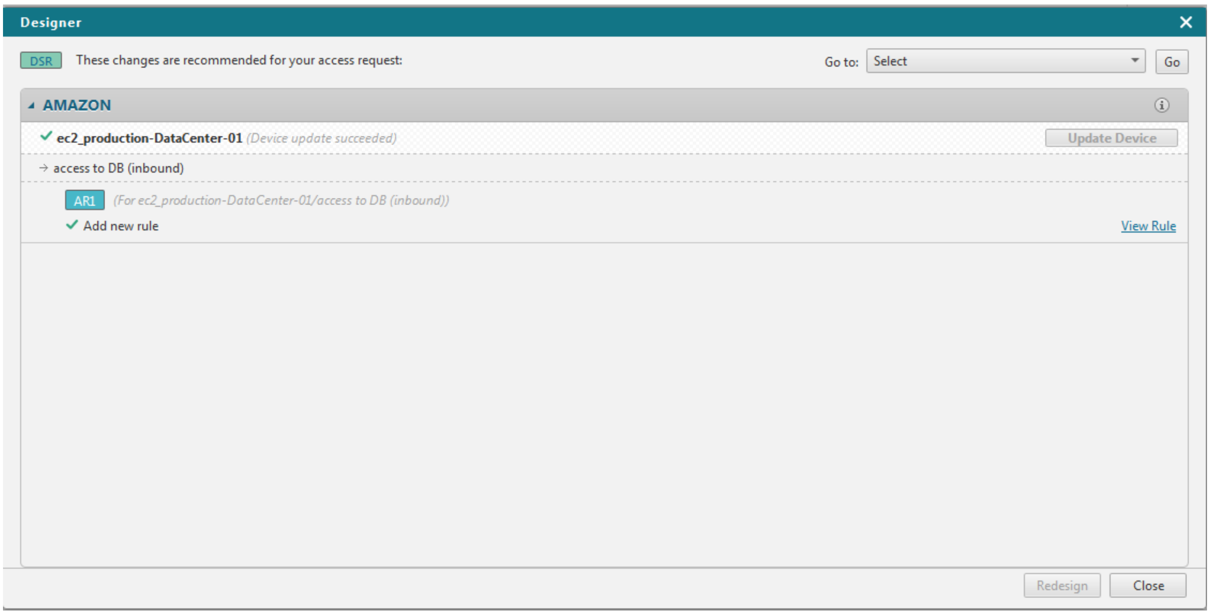
In Progress | Expiration: Not Defined... | (0) | Priority: Normal

Step name: Technical Design

Handler: a a

Required Access

Target	Source	Destination	Service/Application Identity	Action	Comment
ec2_production-DataCenter-01/acces...	192.168.3.3/32	172.16.20.20/32	TCP 80	Accept	


Designer

DSR These changes are recommended for your access request:

Go to: Select

AMAZON

✓ **ec2_production-DataCenter-01** *(Device update succeeded)*

→ access to DB (inbound)

AR1 *(For ec2_production-DataCenter-01/access to DB (inbound))*

✓ Add new rule

Other customers reference applications instead of infrastructure when requesting access changes. Instead of processing changes based on IP addresses and ports, Tufin provides end-to-end automation for application connectivity changes that span public cloud and on-prem environments in order to empower application owners and avoid communication gaps between application teams and network operations teams. Tufin also provides an automated process for application migration and for application decommissioning.

Summary – Integration Key Benefits

The integrated AWS and Tufin Orchestration Suite™ solution delivers visibility, centralized security policy management, and continuous compliance across physical and virtual networks and the hybrid cloud. This strategic integration enables IT organizations and security teams to:

- Reduce complexity by monitoring and managing security policies across the network from a single pain of glass.
- Increase audit readiness by tracking changes to AWS security groups alongside other leading cloud platforms and physical network platforms to identify change details and who made them.
- Ensure compliance and reduce audit preparation efforts by proactively enforcing a Unified Security Policy.
- Ensure application connectivity with a central topology map of the heterogeneous corporate network and topology path analysis to troubleshoot connectivity issues quickly and easily.
- Boost agility with policy-based end-to-end automation of network security changes:
    - Automate proactive risk analysis for continuous compliance.
    - Automate change design based on accurate topology simulation and path analysis.
    - Automate provisioning for north-south connectivity across AWS Security Groups and on-prem network platforms to reduce complexity, eliminate human error, and ensure connectivity.