

Security Policy Orchestration for Forcepoint™ Stonesoft® Next Generation Firewall

Technology Partner Solution Brief

Forcepoint™ & Tufin® Provide Secure, Manageable & Compliant Networks

Enterprise IT and security experts are under increasing pressure to respond to complex network changes and keep up with growing business demands. Lack of network visibility hinders the ability to deliver services and applications with the security, speed and accuracy required.

Together, the Tufin Orchestration Suite™ and Forcepoint™ Stonesoft® Next Generation Firewall (NGFW) provide advanced network protection and visibility, enabling agile and risk-free policy changes. Using advanced analysis and automation technologies, the change processes are orchestrated across heterogeneous networks, devices, servers and applications.

Automatic Network Security Change Design & Implementation

The Forcepoint-Tufin solution significantly shortens the time previously required to make network security changes by automating every step of the change workflow, including design and implementation. Automated design is based on cutting-edge network topology simulation that identifies the relevant policies and the optimal change to rules and objects. A detailed change plan is then suggested and, once approved, the changes are automatically provisioned across network devices. This ensures quick and accurate processes while significantly reducing risk to your organization's network.

Reduce the Attack Surface with Central Policy Enforcement

Understanding and enforcing network segmentation is a major challenge for IT experts. Tufin's Security Zone Matrix simplifies this task by visually mapping the desired network zone-to-zone traffic flow and instantly providing detailed insights on your network segmentation across physical networks and hybrid cloud platforms.

Highlights & Benefits

- **Proactively analyze network changes** to avoid increased risk and security policy violations
- **Implement network security changes in minutes** with automated provisioning
- **Reduce audit preparation by up to 70%** with continuous policy compliance
- **Gain visibility and control of network security policy management** across heterogeneous environments from a single console
- **Increase business agility** by modeling and/or troubleshooting application connectivity changes
- **Reduce the attack surface** by effectively managing network segmentation and optimizing security policies

UNIFIED SECURITY POLICY → Corporate Matrix (Physical + AWS)

From \ To	Amsterdam_Ext	Amsterdam_SiteA	Amsterdam_SiteB	AWS_DB	AWS_Exchange	Virtual_DC-01	Toronto	Cali_bckp-site	London	p_DataCenter
Amsterdam_Ext	Allow only	Block all	Block all	Block all	Block only	Block only	Allow only	Block all	Allow only	Block all
Amsterdam_SiteA	Block all	Allow only	Block all	Allow only	Block only	Block only	Block all	Block all	Block all	Block all
Amsterdam_SiteB	Block all	Block all	Allow only	Allow only	Block only	Block only	Block all	Block all	Block all	Block all
AWS_DB	Block all	Block all	Allow only	Allow only	Allow only	Allow only	Allow only	Allow only	Allow only	Allow only
AWS_Exchange	Block all	AWS_Exchange to Amsterdam_SiteA ✗		Allow only	Block only	Allow only	Allow only	Allow only	Allow only	Allow only
Virtual_DC-01	Allow only	Allow only	Block all	Allow only	Block only	Allow only	Block all	Block all	Block all	Block all
Toronto	Allow only	Allow only	Block all	Allow only	Block only	Allow only	Block all	Block all	Block all	Block all
Cali_bckp-site	Block all	Block all	Block all	Allow only	Allow only	Block all	Block all	Allow only	Block all	Block all
London	Block all	Block all	Block all	Allow only	Allow only	Block only	Block only	Block all	Allow only	Block all
p_DataCenter	Block all	Block all	Allow only	Allow only	Allow only	Allow only	Allow only	Block all	Block all	Block all

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)

Tufin's Security Zone Matrix -- simplified, centralized control of your network and security policy management

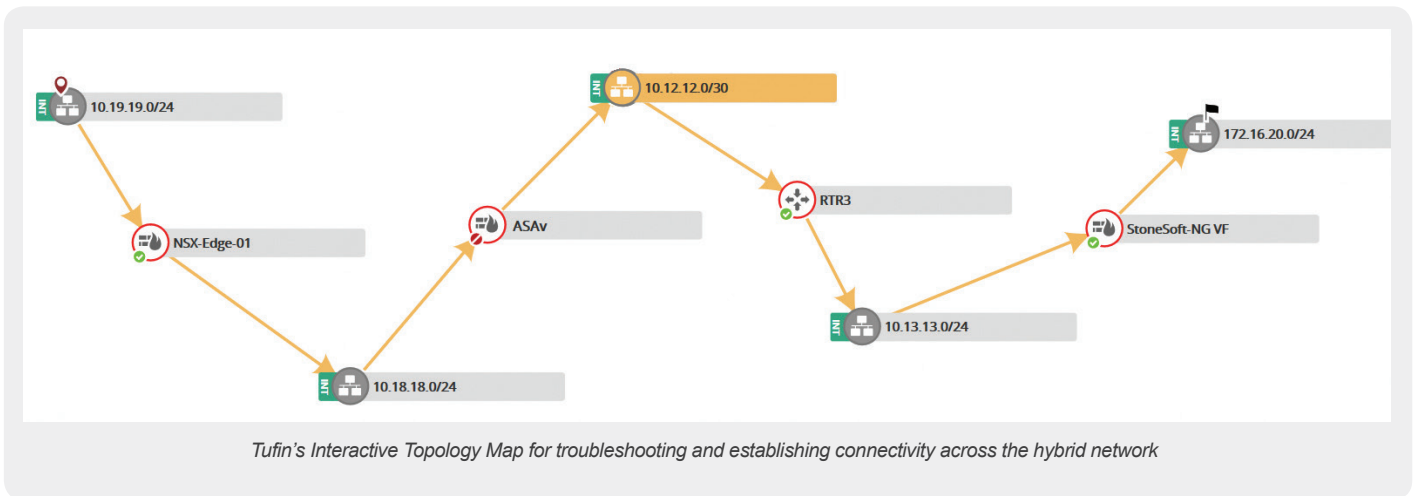
Continuous Regulatory Compliance with Industry Standards

The Tufin Orchestration Suite provides a closed-loop process for enforcing, verifying and documenting compliance with industry standards such as PCI DSS, NERC CIP and SOX. Every firewall policy change is monitored in real-time to identify and address potential violations and provide an accurate, updated audit reports. In addition, Tufin offers proactive compliance analysis for staged applications and policy changes to ensure safe deployment.

Optimize Your Firewalls

The Tufin Orchestration Suite helps enterprises to optimize next-generation firewalls across heterogeneous environments with:

- Optimization of next-generation firewall policies by identifying rules and objects that are misconfigured, risky or unused
- Recommendations for aligning next-generation firewall policies with industry best practices
- Firewall analysis and reporting tools that enable security teams to achieve better productivity
- Built-in, customizable workflows for network and firewall changes



Gain Insight and Control over Complex Networks from a Single Console

The integration of Tufin with Forcepoint ensures that customers can monitor and manage the Forcepoint™ Stonesoft® Next Generation Firewall as part of the overall heterogeneous network, including physical and virtual network devices as well as cloud platforms. The central console reduces complexity and allows managing security and connectivity from the application layer to the network layer.

About Tufin Orchestration Suite™

Tufin® is the leader in Network Security Policy Orchestration, serving more than half of the top 50 companies in the Forbes Global 2000. Tufin simplifies management of some of the largest, most complex networks in the world, consisting of thousands of firewall and network devices and emerging hybrid cloud infrastructures. Enterprises select the award-winning Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. Tufin reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. Its network security automation enables enterprises to implement changes in minutes with proactive risk analysis and continuous policy compliance. Tufin serves over 1,800 customers spanning all industries and geographies; its products and technologies are patent-protected in the U.S. and other countries.

About Forcepoint Stonesoft Next Generation Firewall

Forcepoint™ was created to empower organizations to drive their business forward by safely embracing transformative technologies – cloud, mobility, Internet of Things (IoT), and others – through a unified, cloud-centric platform that safeguards users, networks and data while eliminating the inefficiencies involved in managing a collection of point security products. The Forcepoint™ Stonesoft® Next Generation Firewall (formerly Intel Security/McAfee NGFW) integrates application control, sophisticated evasion prevention and an intrusion prevention system (IPS) into a single solution that is cost-effective and easy to deploy. It has a proven capability to identify advanced evasion techniques (AETs) that evade other devices, and delivers exfiltration protection using both application and endpoint intelligence.