

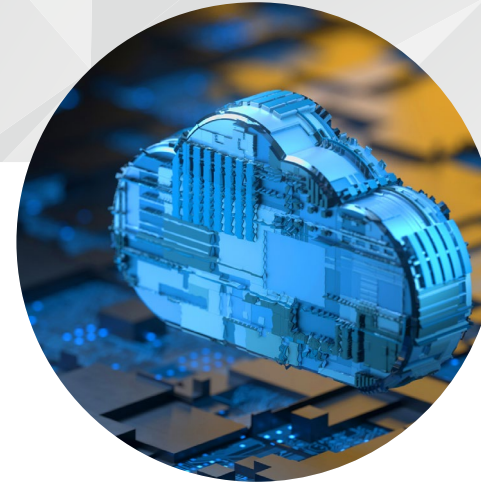
Centralize visibility and simplify policy management with Tufin-Zscaler Cloud Firewall integration

Today's workforce is globally distributed and employees are working from everywhere. With more workloads and applications now in the cloud, keeping the enterprise secure can be a challenge, as employees go directly to the Internet, bypassing traditional security controls. Managing security policies via siloed tools leads to incomplete visibility, and complex, time-consuming daily operation.

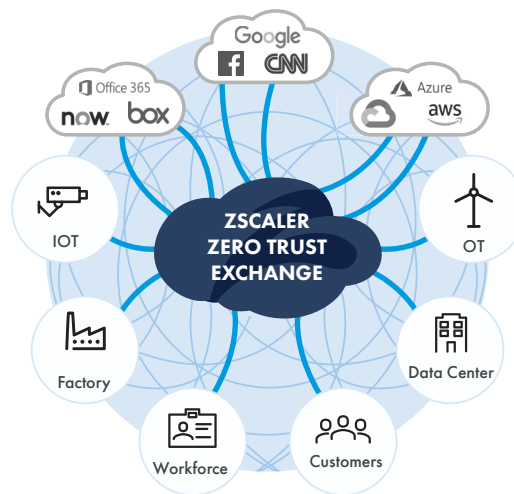
Tufin's integration with the Zscaler Advanced Cloud Firewall, part of the Zscaler Zero Trust Exchange, provides admins with centralized visibility into Zscaler Secure Access Service Edge (SASE) policy rules alongside other vendors' policies, to help simplify and standardize security policy management across the hybrid cloud, directly from the Tufin console.

The Zscaler Zero Trust Exchange provides a full security platform in the cloud, allowing your entire workforce to be secure, regardless of their location. Zscaler ensures users have consistent protection no matter where, or on what device, they connect from. Zscaler Cloud Firewall enables fast and secure off-network connections and local Internet breakouts for all your user traffic, without appliances. Zscaler Cloud Firewall elastically scales across all ports and protocols to handle all your cloud application traffic.

Tufin Orchestration Suite (TOS) is a complete solution for automatically designing, provisioning, analyzing, deploying, and auditing network security changes from the application layer, down to the network layer. Tufin provides advanced automation capabilities to increase business agility, improves accuracy through elimination of manual errors, and ensures continuous compliance via a single console. Tufin's unified security policy empowers network and IT security teams to effectively safeguard complex, heterogeneous environments through a central interface for defining and enforcing policy controls over firewalls, switches, Software Defined Networking (SDN), private and public cloud platforms and Kubernetes, down to any level of segmentation.



Zero Trust Architecture



Benefits

- Reduce complexity and increase control by managing enterprise security policies, all from a single console
- Faster resolution of security and connectivity issues by identifying overly permissive rules, rule certification status, and more
- Easy detection and troubleshooting analysis with Zscaler Cloud Firewall rule change tracker – view and compare policy changes at any point in time
- Reduce time and effort invested in audit preparation, whereby auditors gain instant visibility into policy changes

Key features include:

Rule Viewer

Tufin's Rule Viewer provides network administrators an instant view of Zscaler Cloud Firewall rules directly from the Tufin console, for fast analysis. Users can view rule attributes—sources, destinations, users, applications. The Rule Viewer also provides rule metadata, such as when the rule was last modified, the certification status if rule certification is being enforced via Tufin, and if the rule is overly permissive and should therefore be modified or removed.

The screenshot displays the Tufin dashboard's Zscaler Cloud Firewall rule viewer. At the top, a summary bar shows: Last hit: N/A, Last modified: 6 days ago, Cert. Exp.: None, Permissiveness: N/A, Shadowed: N/A, and Violations: N/A. Below this, the device is identified as 'Zscaler' and the domain as 'Default'. The main area is divided into several sections: SOURCE (14.14.14.1/32, 10.10.0.0-10.10.11.11, 13.13.13.0/24), DESTINATION (www.test.com, 30.30.0.0/16, test2.ru, 15.15.15.15/32, test1.co.il, 20.20.0.0-20.20.20.5), SERVICE (Any (ipv4)), ACTION (a red circle with a slash), COMMENT (No comment), MISCELLANEOUS (Time: Any, Location: No data), SOURCE USER (Any), and APPLICATION (APNS, Microsoft Office365, OFFICE365, M365COMMON, LOGMEIN, NetworkApplicationGro..., DICT, CHAP, LOGMEINRESOLVE).

Tufin dashboard: Zscaler Cloud Firewall rule viewer

Rule Change Tracker

To ensure continuous compliance and enable faster troubleshooting, Tufin monitors and highlights Zscaler Cloud Firewall rule changes—what was changed, when, by whom, and whether there's a comment or a reference associated with it. Tufin records every policy revision, maintaining a complete policy history as it evolves over time. Administrators can quickly retrieve and view the Zscaler policy as it existed at a previous point in time. A side-by-side comparison helps admins review changes to identify and fix misconfigurations. This can be invaluable when a change unexpectedly blocks access to a critical asset, enabling auditors to immediately view what has changed since the last audit.

The screenshot shows the Tufin dashboard's Revision History and Change Comparison tool. The top section displays a table of revisions for 'Zscaler' with columns: Revision, Action, Changed on, Received on, Administrator, Installed on, GUI client, Audit log, Policy package, Global policy, Ticket ID, and Comment. Below this, there are buttons for 'Filter', 'View Policy', 'Compare', and 'Generate Report'. The main area is a 'Comparison' view showing two side-by-side tables for 'Zscaler - Revision 1' and 'Zscaler - Revision 2'. The tables have columns: NO., Name, Source, Destination, Locations / Location Groups, and Users / Dep. The comparison highlights changes between the two revisions, such as the addition of a new source IP and the removal of a user.

Tufin dashboard: Revision history and change comparison

Rule filter

Admins can filter rules by locations, apps, URL category, and users, for faster resolution of security and connectivity issues.

The screenshot displays the Tufin SecureTrack Rule Viewer interface. At the top, the search filter is set to 'vendor = ZSCALER'. Below the search bar, it indicates that 47 rules were found. The main area shows a list of rules, each with a unique ID and name. Rule 10 is 'Zscaler Proxy...' with a ZIA icon. Rule 11 is 'Firewall_7' with a ZIA icon. Rule 12 is 'Firewall_4' with a ZIA icon. Rule 13 is 'Office 365 O...' with a ZIA icon. Each rule entry includes a list of source and destination IP ranges, actions, and status indicators. The right side of each rule entry shows 'Last hit' and 'Last modified' information. For example, rule 10 has 'Last hit: N/A' and 'Last modified: Yesterday'. Rule 12 has 'Last hit: N/A' and 'Last modified: Yesterday'. Rule 13 has 'Last hit: N/A' and 'Last modified: Yesterday'. The 'Permissiveness' column shows 'N/A' for rules 10, 11, and 13, and 'High' for rule 12. The 'Shadowed' column shows 'N/A' for all rules.

Tufin dashboard: Rule viewer

With Tufin and Zscaler, organizations can centrally manage and apply consistent and effective segmentation policies across their multi-vendor, hybrid cloud environment.

Learn more at tufin.com/supported-devices-and-platforms/zscaler

About Tufin

Tufin (NYSE: TUFN) 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 company's Tufin Orchestration Suite™ to increase agility in the face of ever-changing business demands while maintaining a robust security posture. The Suite reduces the attack surface and meets the need for greater visibility into secure and reliable application connectivity. With over 2,000 customers since its inception, Tufin's network security automation enables enterprises to implement changes in minutes instead of days, while improving their security posture and business agility.

www.tufin.com



tufin
The Security Policy Company.

Copyright © All rights reserved. Tufin, Unified Security Policy, Tufin Orchestration Suite and Tufin logo are trademarks of Tufin. All other product names mentioned herein are trademarks or registered trademarks of their respective owners. You may not copy, reproduce, photograph, translate, transmit, make available to the public, make derivative works, perform in public, rent, broadcast or make any commercial use of the publication in full and / or in part without prior written approval.

DP20220219