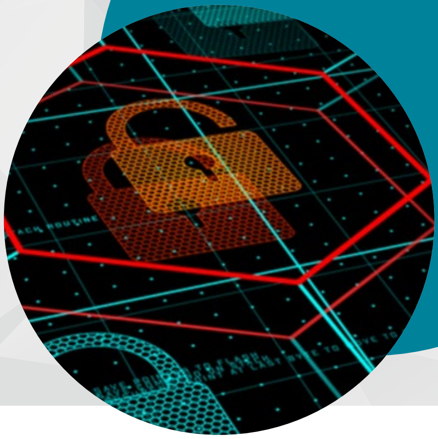
tufin The Security Policy Company.

Aligning Your Security Policy with NIST 800-207 Zero Trust Principles



Introduction

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

The NIST (National Institute of Standards and Technology, part of the U.S. Dept. of Commerce) has released a Zero Trust Security Guide (SP 800-207) that provides practical recommendations for organizations on how to achieve and maintain Zero Trust.

Based on NIST, agencies' traditional approach to network security was that within an organization's network perimeter, services and users were trusted, and therefore, could 'talk'/ connect to one another. It was, for the most part, an open, almost flat network, where any traffic or users were trusted by virtue of being inside the perimeter. This enables unauthorized lateral movement, once an attacker gained access into the perimeter, which is considered one of the main challenges federal agencies face today.

An organization's primary security objective is to effectively "eliminate unauthorized access to data and services, coupled with making the access control enforcement as granular as possible."[1]

To effectively achieve this, and facilitate the process, they need to move the segmentation as close as possible to the resource, also referred to as micro-segmentation, and authenticate and authorize all users, assets, and workflows.

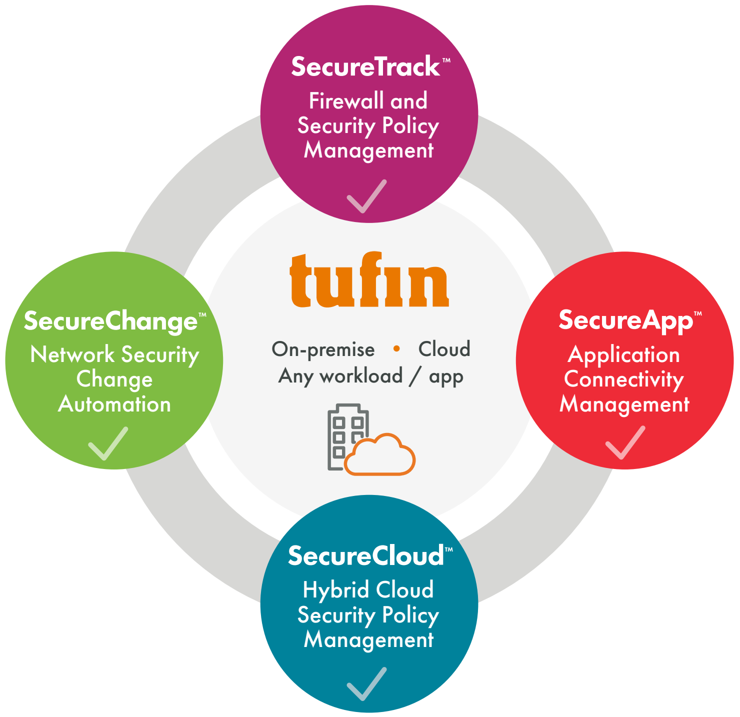
Zero Trust definition by NIST SP 800-207

- Set of network security paradigms that shift network defenses to focus on individual or small groups of resources
- A Zero Trust Architecture (ZTA) strategy defines that no implicit trust is granted to systems based on their physical or network locations
- Access to data resources is granted when the resource is required, and user/device authentication is performed before the connection is established
- ZTA focuses on protecting resources, not network segments, as the network location is no longer viewed as the primary component of the resource's security posture

[1] Source: ZERO TRUST ARCHITECTURE, NIST SP 800-207

How Tufin Enables the Zero Trust Security Model

Tufin Orchestration Suite (TOS) offers a segmentation policy management solution that helps network, security, and cloud teams to embed and maintain Zero Trust practices across their hybrid environment (on-premise and cloud). This is achieved via security automation that drives optimized, least-privilege segmentation, and trusted and secure changes, while ensuring policy adherence and business continuity.


SecureTrack™
Firewall and Security Policy Management
SecureChange™
Network Security Change Automation
tufin
On-premise • Cloud
Any workload / app
SecureApp™
Application Connectivity Management
SecureCloud™
Hybrid Cloud Security Policy Management

- Policy-centric security for any app/workload, anywhere
- Least-privilege performance and allow-listing
- Policy change automation & orchestration
- Open and extensible framework
- Visibility & analytics

Tufin categorically maps to Zero Trust principles in 6 key areas:

1 Complete Visibility & Accurate Topology Modeling

Tufin provides full visibility and control of which apps, workloads, and network security devices (e.g. SDNs, firewalls, NGFW, routers, switches, or security groups) are currently deployed and how they're connected, as well as what can talk to what, and who can talk to whom (e.g. traffic flows) across the multi-cloud, hybrid environment.

Tufin topology map is created by connecting to all of the multi-vendor firewalls, routers, switches, and cloud services, and retrieving all routing tables, as well as taking into account all Network Address Translation (NAT) and port number translation, VPNs, Multiprotocol Label Switching (MPLS), IPV6, security groups, IPAM data, etc.

This results in a precise and highly-accurate model of your hybrid environment, so you can immediately start monitoring actual traffic across environments, and identify anomalies, such as misconfigurations, and potential threats.

Tufin: Key features in support of Zero Trust

Accurate End-to-End Visibility

- Centralized, real-time visibility via a single dashboard of apps and their dependencies, workloads, network platforms, and infrastructure assets
- Visualize traffic flows of network topology and application connectivity throughout on-premise, multi-cloud, and SDN environments
- View apps, objects, services, source and destination, tags, regions, etc.
- View app dependencies and share resources between apps
- Allow search for specific servers, apps, rules, and objects across all network devices
- Application Discovery integration (e.g. Cisco Tetration) automates application discovery and provides real-time visibility into dependency mapping and connectivity monitoring.

2 Security Segmentation

With Tufin, you can consistently and automatically apply any level of segmentation to microservices, network zones, user IDs, or App-IDs (even in the event, for example, the database tier resides in your datacenter, and the app web tier is deployed in AWS public cloud), while using the Tufin solution as an orchestrator/translator between zones, tags, and namespaces, and from security group rules to firewall rules. This ensures segmentation is enforced across cloud environments and datacenters, following the workload anywhere it's deployed.

By mapping apps/workloads/business units/subnets connections (east-west and north-south traffic), you can start modeling security policies and segmentation options. For example, you can locate and prioritize low- and high-value assets, view which assets are most connected, and apply an appropriate segmentation strategy and granular security policy. When deploying a network topology map, you essentially create a shared understanding of security concerns and requirements between the various stakeholders – app owners and network and security personnel.

Tufin provides a path to segmentation. In the cloud, it starts by monitoring traffic and automatically learning the app/workload communication flows, and creates an allow-list policy which you can then edit, using natural high-level language to define segmentation policies. The result is a policy baseline, including deny-list, allow-list, rule properties, and flow restrictions. Further, the policy can be generated as a YAML file, so it can be easily embedded in the SDLC for shift-left security.

For IP/App-ID based segmentation, you can use the Tufin Unified Security Policy matrix to create security policy to control what traffic is allowed between the zones. To quick start your segmentation project, you can use one of Tufin's predefined compliance segmentation policies whereby all rules can be compared to these policies. You can define exceptions to policies, if needed, and once defined, policies are automatically distributed and enforced.

Tufin: Key features in support of Zero Trust

Segmentation Policy Automation & Orchestration

- Centrally set unified security policy and manage all segmentation rules (e.g. deny-list and/or allow-list based on IP addresses, security groups, namespaces, and subnets via a single interface across the multi-vendor, hybrid environment)
- Create logical zones using subnets, IP addresses, security groups, namespaces, etc.
- Define global network security policy alongside rule properties and other variables (e.g. forbid using "Any" in either source/destination/services)
- IPAM integrations deliver on-going, network zone discovery and updates based on accurate IP/DNS zone information for rapid provisioning and updating of network segmentation policy
- Automatic policy generator recommends rules based on traffic data, and permissiveness level
- Automated rule and object provisioning
- Identify rules candidates for cleanup (e.g. redundant, unused rules)
- Use FQDN, EDLs, and CloudGuard objects to define policies or automate changes to policies
- Multi-tenancy support: Assign group access (e.g. master-tenants separation and role-based visibility) to separate network domains, data and reporting segregations (no firewall changes are required)

User Access Control

- Create rules and policies based on User-ID
- Gain complete visibility into User-IDs and their use within the enterprise's security policies
- Visualizes security policies that apply to individual User-IDs, painting a picture of the user's access across the entire enterprise network, inclusive of legacy devices, regardless of the user's location
- Draw roles and permissions from an organization's AD/LDAP groups
- Track, block, and alert on unauthorized user activity
- Log all user activity for investigations and regulatory compliance

3 Policy optimizations via change automation

Tufin provides the ability to visualize network connectivity, assess whether that connectivity is risky, and understand where changes need to be applied. With Tufin, you can implement changes quickly and automatically based on accurate topology path calculations, and policy analysis to ensure fast and precise provisioning of new or changed access. To achieve this, Tufin not only locates the exact applicable rules in all relevant network security devices and infrastructure components, such as firewalls, SDNs, routers, etc., across the hybrid environment, but also very granularly pinpoints which changes in these rules need to be made to enable the required change.

Tufin ensures that every change is vetted by the relevant task owners and meets security and compliance mandates. Tufin also offers pre-defined workflows for common change handling to ensure full user accountability and control with comprehensive audit trails of all changes. These workflows can be integrated into an organization's ITSM, Jenkins, Slack, or other collaboration process.

In addition, Tufin ensures that all policy access changes are designed based on the best optimized path, and via a predefine change window, automatically implement the changes to all relevant firewalls, routers, switches, to ensure an accurate, error-free process.

Zero-Touch Change Automation

- Automatically detect unused rules and objects, shadowed and overly permissive rules, and rule and server candidates for decommissioning
- Optimization of policies (rule clean-up) by identifying misconfigured, expired, risky or unused rules, and objects
- View policies and compare revisions across all multi-vendor network devices and infrastructure components
- Pre-defined and unlimited customizable workflows for rule change management for a vetted, secured access change implementation
- Generate rule usage and unused rules report
- Simulate the impacts of rule changes, prior to implementation, to ensure changes do not result in policy violation/s
- Check rules against corporate policies or risk assessment data from a third-party tool (e.g. vulnerability management solution, SIEM, SOAR, or endpoint security solution) to identify and flag potential risks
- Automatically remove all access associated with a decommissioned servers/apps from relevant firewall targets, irrespective of the device manufacturer/SW vendor
- Impact analysis for controlled app decommission process
- Recommend network changes based on accurate topology modeling, path analysis, and security policy
- Zero-touch rule change implementation across all leading firewalls and routers, and cloud platforms in the hybrid environment
- Identify devices that allow/block requested access, and highlight the changes needed for remediation
- Automatically edit rules as a result of a change, without adding/duplicating rules
- Real-time change notification, tracking and revision control, provide full user accountability
- Automated processes for handling potential security policy violations (e.g. escalations for security approval, exceptions handling, and proposed remediation)
- Set and review time-limited rules (set expiration date on rules, e.g. revoke third-party access to your network)
- Change automation integrations (e.g. ITSM solutions) providing unified change workflows, where opening a ticket in ITSM triggers a workflow within Tufin for automated change design and implementation

4 Monitor and control network changes

Tufin identifies unauthorized changes made directly to network devices outside of the authorized change management and configuration orchestration processes as controlled by Tufin, and alerts via email when policy violations occur. Tufin can also identify when unauthorized personnel attempt unpermitted actions or actions that take place outside of the organizationally defined change processes. The authorized and unauthorized change tracking and reporting from the Tufin dashboard identifies where network security devices were modified outside of the approved workflow and operations windows. Similarly, Tufin can be configured to monitor unusual network activities according to policy based on hit count, zone changes, or anomalous port-specific network behavior.

Tufin: Key features in support of Zero Trust

Risk Analysis

- Run path analysis query from specific source to destination
- View firewall rules that match the queried traffic
- View device interfaces and routing table
- Receive alerts on broken paths
- Ongoing network risk assessment by providing risk score to objects, rules, apps, and workloads
- Track and compare changes to multi-vendor networks' security devices throughout the hybrid environment, irrespective of the technology or infrastructure they operate in
- Provide actionable remediation information for policy violations, rule cluttering, broken connectivity, and misconfigured rules

5 Assess, prioritize and mitigate risk

The challenge with risk has always been that too many critical vulnerabilities are discovered and not enough resources are available to patch them. Moreover, the reality is that vulnerabilities with high CVSS scores aren't necessarily the ones exploitable in your network. For example, a medium-level vulnerability associated with a business asset having multiple access points may be used by an attacker to gain their foothold in your network and move laterally to pivot to other high-value, sensitive assets. As a result, this vulnerability is more prone to exploitation by attackers, and consequently, should be considered a high-level priority for remediation or mitigation.

Organizations need a method of prioritizing the vulnerabilities that should be patched first and find a way to mitigate the risk of exploitation until they can be remediated.

Tufin integrates with leading vulnerability management solutions, including Tenable.io, Tenable.sc, Qualys VMDR, Rapid7 Nexpose, and Rapid7 InsightVM, to provide risk-based network insights that help organizations efficiently prioritize remediation and mitigation efforts by correlating vulnerability data with network insights. By combining vulnerability scanner output with network access data, organizations can understand how these vulnerabilities are contextually exploitable today, enabling security admins to identify and address vulnerabilities that pose the greatest threat to critical business assets.

Tufin: Key features in support of Zero Trust

Identify security gaps

- Immediately gain visibility into all security policies and current configuration (rule bases and ACLs) from all network security vendor devices deployed
- Retrieve vulnerability data (CVSS scores + severity) on high priority segments containing critical assets—view rules govern access to/from a vulnerable asset, underlying services exposing the vulnerabilities, and relevant firewalls that provide access for fast remediation or mitigation, by blocking access to the asset
- Assess your overall security posture and drill down for more information for additional analysis and remediation planning
- Security Operations and Incident Response (SOAR) integrations providing unified real-time network visibility and policy intelligence, to help accelerate incident response based on a rich set of real-time data, while using automated, playbook-driven response

6 Maintain continuous compliance via automation

If done right, automation provides two-fold benefit when it comes to achieving continuous compliance and Zero Trust.

The first benefit is compliance by default, everywhere. With policy automation, you can generate a global policy that is not only optimized for apps/workloads based on least privilege principle and compliant with regulations and other security mandates, but that's also consistently applied everywhere automatically across your hybrid environment.

To help you jumpstart and apply a compliant Zero Trust network, you can use Tufin pre-defined PCI-DSS, HIPAA, NIST, CIS policies where we 'translate' access related requirements into segmentation policy. Any violation is automatically alerted and blocked, and because you define these policies using Tufin, you can apply them, irrespective of the underlying security network infrastructure, SDN, or cloud. If you plan to switch vendor, or migrate to a different environment, you can do this without the need to redefine your policies.

The second benefit is in maintaining compliance, where with automation, you can easily maintain your policy globally. Any change, by default, using automation, will be vetted, tested against the policy, designed and implemented in minutes, with no human errors or misconfigurations.

When it comes to compliance and Zero Trust, automation is a key to helping you integrate security best practices at scale, while dramatically reducing the time it takes to continuously manage them while staying aligned with your organization's security and compliance policies.

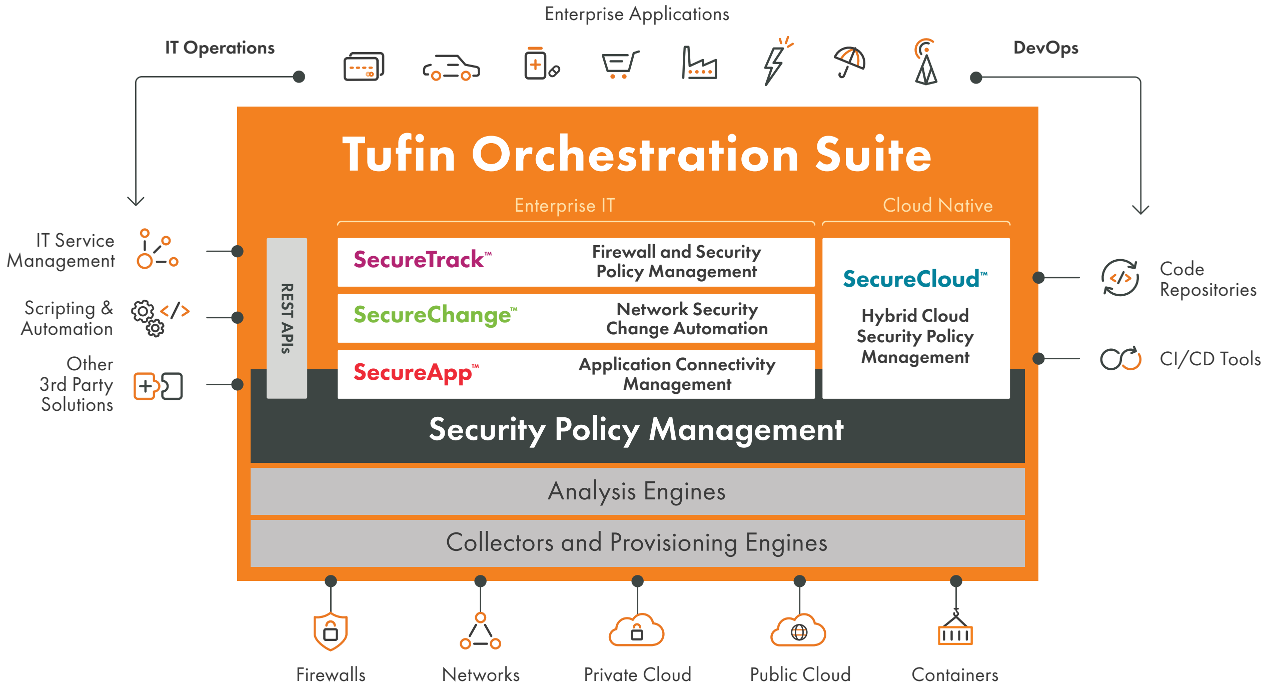
Tufin: Key features in support of Zero Trust

Continuous Compliance

- End-to-end, real-time visibility into network security compliance posture across the hybrid environment (e.g. view risky rules, ports, communication flows, etc.)
- Run automated compliance checks before implementing network access changes
- Full accountability with granular automated audit trails of all access activity, and rule and policy changes
- Automated rule recertification workflows
- Pre-built rulesets and violation alerts for key compliance mandates (e.g., PCI-DSS, NERC CIP, GDPR, SOX, HIPAA, NIST, ISO 27001, CIS, etc.)
- Provide actionable remediation information on detected compliance violations
- Maintain rule clean-ups, rule certification, and rule permissiveness remediation trends
- Generate compliance reports, such as:
  - Risky rule reports
  - Rule order optimization reports
  - Permissive rule reports
  - Policy violation reports

By adopting a Zero Trust approach, you are essentiality adding a heightened level of predictability to your network access practices. By allow-listing what can talk to what and who can talk to whom, you will be able to actually define your intentions in parallel to responding to anomalies. Simply put, this ability is far greater than attempting to guess where the next attacks may come from, or which vulnerabilities will be used by attackers to penetrate your network, and move laterally across your environment.

Tufin Orchestration Suite is uniquely positioned to help U.S. federal agencies and government contractors automate network security controls to protect sensitive assets across the hybrid network, and to meet federal and cybersecurity mandates, such as FISMA, DHS CDM, NIST CSF, etc. To learn more, visit **tufin.com/federal**.



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 2000 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.

tufin The Security Policy Company.