tufin
The Security Policy Company.

SecureTrack™+

Your Foundation to Platform-Agnostic Network Security Policy Management.

Overview

While many firewalls, SDN, and cloud security solutions offer vendor-specific visibility and management capabilities, no single solution provides visibility into and management of compliance and network security risk at an enterprise scale.

To secure applications and workloads across your hybrid network, you require an environment- and vendor-agnostic solution. Tufin SecureTrack+ offers a holistic view of network access and security configurations, centralizing network security policy management, risk mitigation and compliance monitoring across your entire enterprise.

With a global view into your rule bases across all major firewall, network and cloud platforms, you can easily identify policy violations and unused, expired, shadowed and overly permissive rules that affect your security posture and open doors to cyber attacks.

Fully agnostic to the underlying network infrastructure or cloud platform, SecureTrack+'s Unified Security Policy matrix facilitates holistic management over who can talk to whom, and what can talk to what. With SecureTrack+ you have the enterprise-wide visibility and insights necessary to optimize security policy and execute large network cleanup operations quickly and accurately.

> *"We save countless hours on rule cleanup and compliance reporting, and we can give management visibility without pulling one of our valuable team members from critical tasks."*
>
> — Cybersecurity Manager, Large U.S. Utilities Company

Key Features

- Scales to support thousands of network/cloud resources
- Automatic Unified Security Policy generation, analyzing network access across the entire enterprise network into the cloud
- Automatic firewall rule base optimization, analyzing traffic history to ensure least privilege
- Continuous monitoring of your actual network segmentation to identify risk
- Real-time policy violation alerting
- Automated rule and object clean up
- Context-based vulnerability prioritization

Outcomes

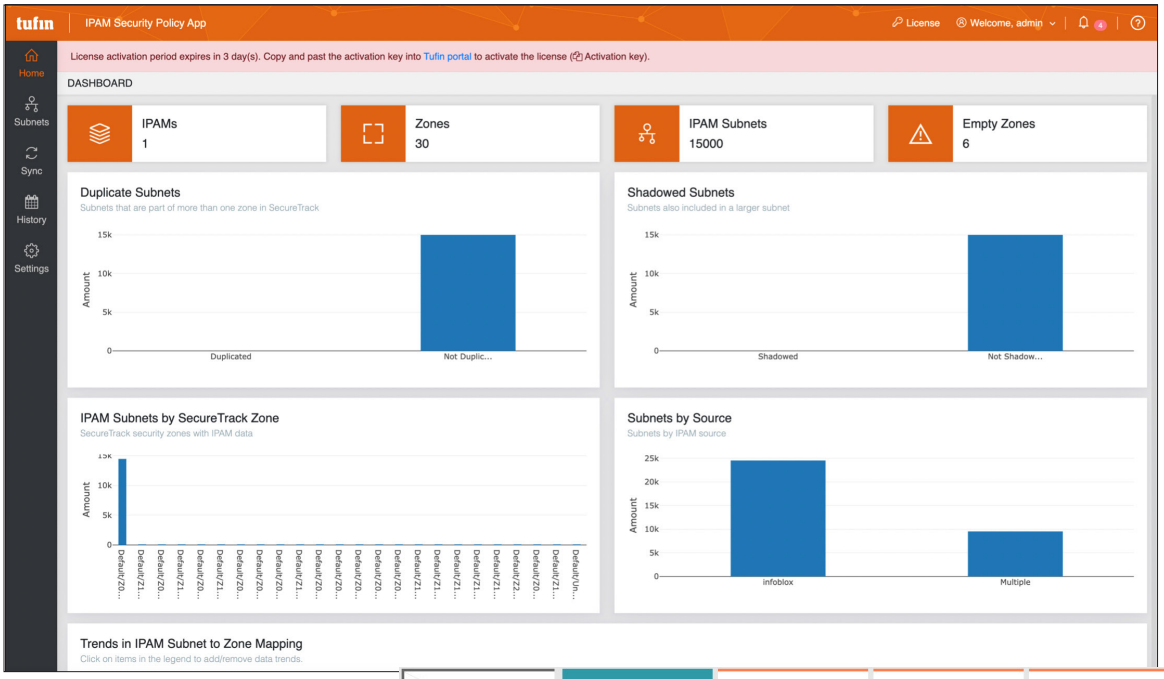
- Centralize and consolidate network security policy management across on-prem and cloud.
- Easily set and manage segmentation policies.
- Dramatically reduce attack surface.
- Prepare for audits in hours, not days or weeks.
- Detect and remediate the most critical vulnerabilities fast.

Security Policy Management

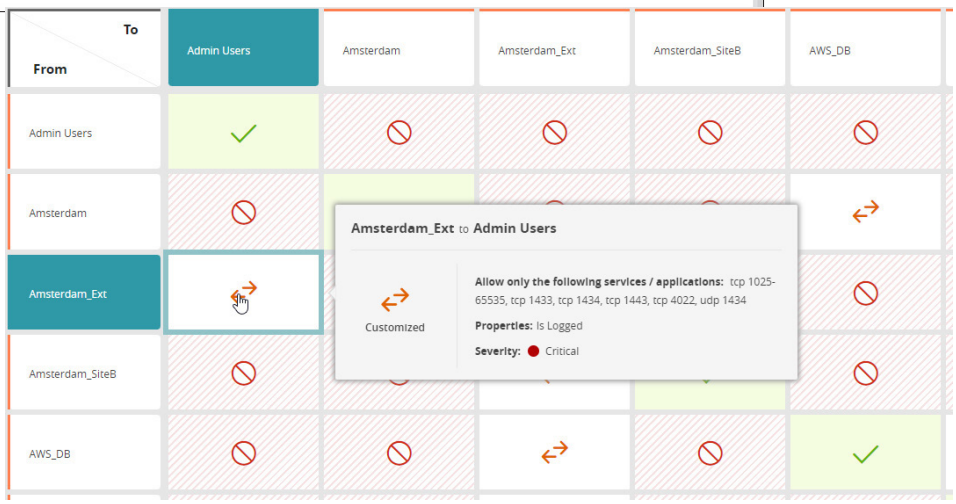
Companies often struggle to implement and adhere to a global security policy. SecureTrack+ automates security policy design, based on your current segmentation, and provides centralized, zone-based policy management. Zones can be defined by subnets, IP addresses or security groups.

- IPAM Integration, automatically populates and maintains any subnet change within user-defined zones, increasing the accuracy of risk assessments and violation alerts.
- Security Policy Builder allows you to easily build, clone or update security policies, defining access permissions from network zone to network zone.

Once your security policy is defined, Tufin highlights the gaps between the desired policy and the actual rulesets as defined within the devices across your network. This consolidates and accelerates policy management—allowing you to improve your security posture while reducing manual, error-prone tasks.



IPAM integration, enables auto-syncing of subnet changes into zones.



Tufin SecureTrack+ Zone-based Unified Security Policy (USP) Management Matrix

Compliance Monitoring and Reporting

Maintaining compliance and passing audits require continuous visibility into your total network infrastructure. SecureTrack+ reporting illuminates all policy changes, risky rules, overly permissive rules, security policy violations and more, across all major network and cloud vendors, to help you ensure compliance and reduce audit burden. You can view vendor-agnostic or vendor-specific reports, customize as needed, and schedule periodic reporting that is sent to all relevant stakeholders.

Reporting Essentials

The topology map is expandable, allowing customers to add generic network devices and nonstandard configurations.

Real-time Policy Violation Alerts

SecureTrack+ monitors network changes and compares them to security/compliance policies. Risks and violations are identified and can be suppressed by establishing an exception.

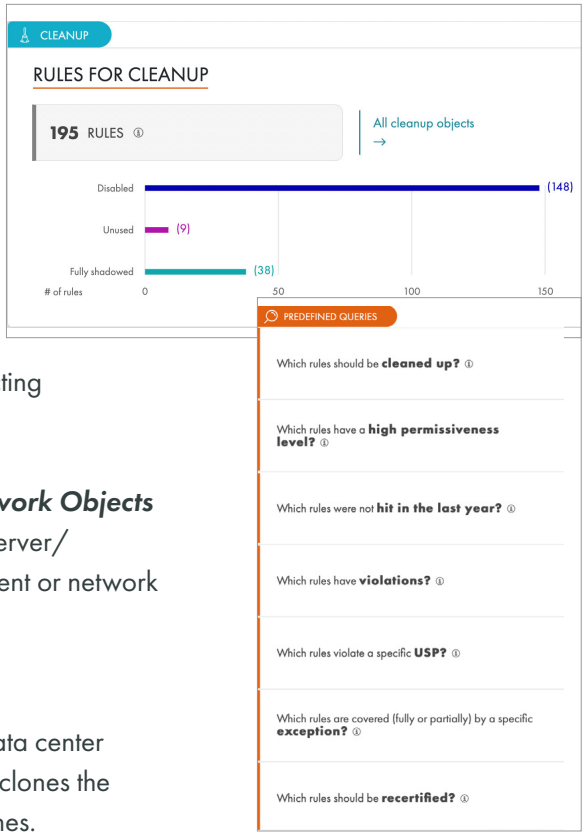
Reduce Downtime with Faster Troubleshooting

SecureTrack+ facilitates root cause identification for change-related outages or unexpected behavior.
A side-by-side comparison of all policy revisions across all monitored devices highlights rule changes and provides additional information as to who made the change, when, and whether there's a comment or a reference associated with it.

Save Time. Improve Security Posture

Reduce Time Spent on Rule Clean Up

Get real-time visibility into unused, shadowed, redundant and overly permissive rules and take advantage of automatic rule decommissioning. Tufin clients have reduced cleanup time by 80%. **(See Case Study: Large Utilities Company)**



Automatic Rule Base Optimization

Automatic Policy Generator creates an optimized rule base by inspecting existing traffic to determine who/what truly requires access.

Automatic Identification and Decommissioning of Unused Network Objects

SecureTrack+ can identify and remove network objects within rules (server/subnet/range) that are no longer needed due to hardware replacement or network architecture changes.

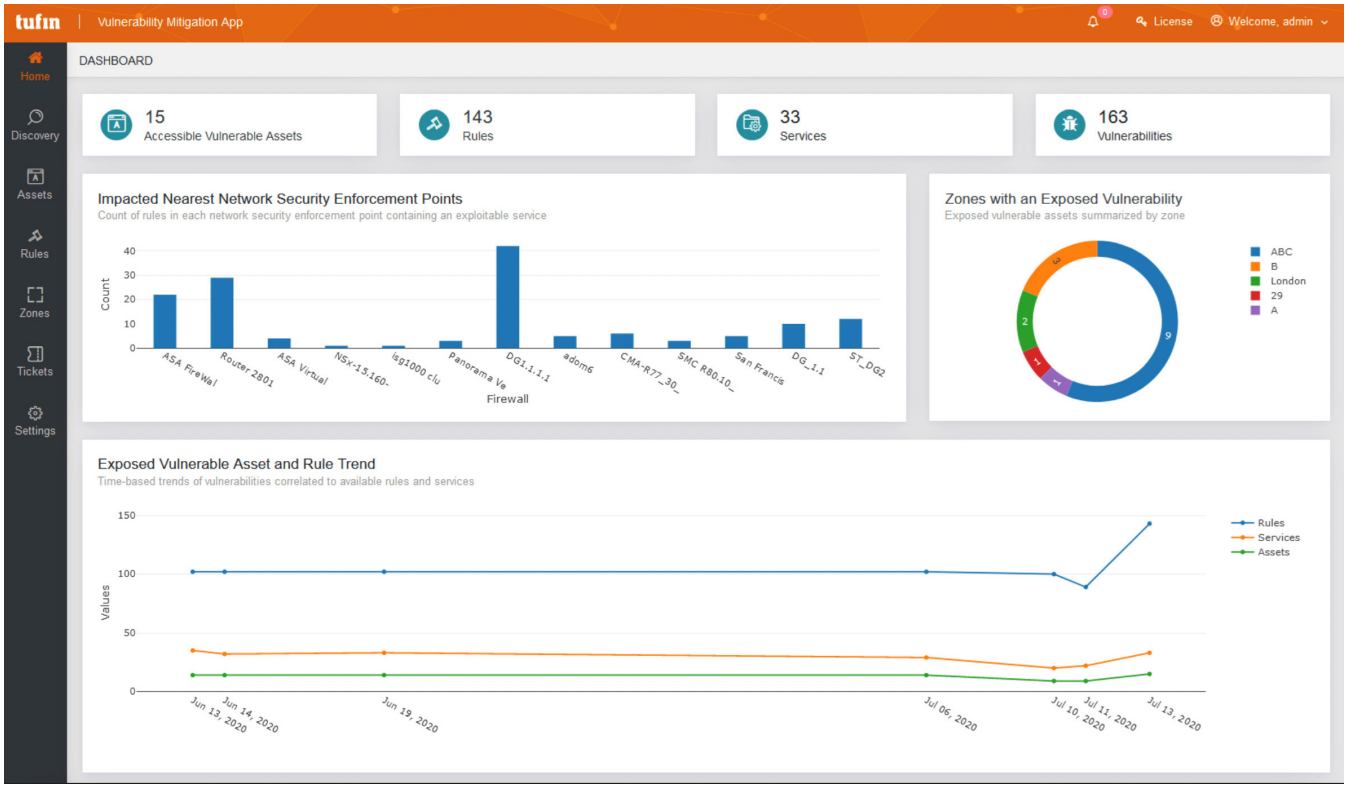
Easier Migrations and Expansions

The Network Object Policy Cloning Workflow is useful for cases of data center migration, hardware expansion and/or hardware replacement, as it clones the security policy of existing servers/subnets/ranges to newly added ones.

Tufin Vulnerability Mitigation

Enrich vulnerability scanner data with network intelligence and business context to prioritize vulnerability remediation.

By combining vulnerability measures (CVSS and severity) with insights into how these vulnerabilities may be accessed and exploited via the network, admins have the context they need to address the vulnerabilities that pose the greatest threats faster.



Vulnerability Mitigation Dashboard

Unmatched Scalability

Tufin is known for its scalability and stability. It makes scaling up and out easy by allowing you to add more worker nodes and remote collectors, so performance is never an issue.