tufin The Security Policy Company.

SecureChange+™

Change Design Automation and Rule Lifecycle Management

Overview

SecureChange+ delivers the compliance monitoring, policy management and risk mitigation that comes with SecureTrack+, as well as full-spectrum change design automation, rule lifecycle management and complete topology visibility.

Many businesses today struggle to manage thousands of network devices and cloud resources from multiple vendors, with manual and error-prone changes that take weeks to implement and require significant resources. These manual processes are risky and often noncompliant with corporate policy or industry regulations. Frequently, the security policies themselves lack documentation and are not reviewed nor justified.

SecureChange+ is an end-to-end, automated policy change design solution, enabling you to automatically build least-privilege access rules across all major firewall, SDN and cloud platforms. Automated risk identification and impact simulation is built into the network change process, with real-time visibility into every network or cloud change and its impact on security posture.

Automation is a must in order to achieve agility, while consistently enforcing security policy across your hybrid environment.

> *"We also integrate **Tufin SecureChange** with our ITSM ticketing system, ServiceNow, where a ticket triggers a workflow... facilitating easy and centralized tracking. Tufin Designer can run across multi-vendor firewalls and highlight rules and interfaces."*
>
> — Security Engineer, Fortune 500 Travel Company

Customizable Workflows

SecureChange+ workflows are fully customizable to address multiple use cases and constant organizational changes.

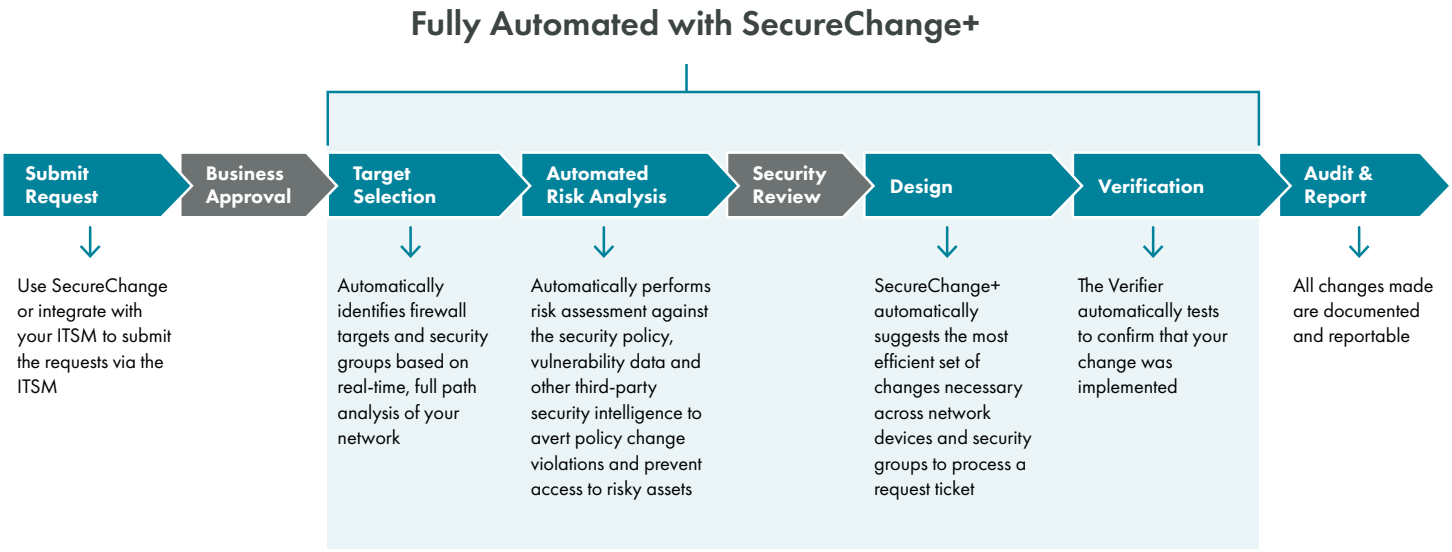
Each workflow is a multi-step, graphical process – from request submission to the fully automated stages of target firewall selection, risk assessment, design, and verification. This process removes the bottlenecks in everyday manual operations and eliminates the risk of configuration errors. All workflows are audit-ready, tracking and documenting the full change history.

Key Features

- Customizable automated workflows
- Integrates fully into ITSM processes
- Automated change design and validation
- Topology mapping
- Visual path analysis
- Fast, accurate troubleshooting
- Efficient target selection
- Checks changes against vulnerability data
- Automated rule recertification process

Outcomes

- Save thousands of work hours per year typically spent on rule cleanup, change design, recertification and audit prep.
- Achieve continuous compliance, virtually eliminating the risk of config errors.
- Minimize risk and vulnerability exposure.
- Reduce downtime with fast troubleshooting.
- Every change is documented providing more granular auditability.



Access Request Workflow - a unified change process enables collaboration and visibility across teams.

For every change request, Tufin conducts risk analysis against the selected Unified Security Policy, as well as data retrieved from either Tufin's Vulnerability-based Change Automation module or a third-party tool, such as a SIEM, SOAR or endpoint security solution. These potential risks and violations will be instantaneously flagged.

Tufin integrates with leading ITSM providers and other solutions that use REST API (ServiceNow, Remedy and others), to deliver seamless change workflows, whereby opening a ticket in your ITSM solution triggers a change design workflow within Tufin.

Several readily available workflows can be customized to fit your organization's business processes, such as:

Access Request / Access Decommissioning

Automatically identifies all devices on the network path between the source and destination, checks for security risks and network impacts, then updates the rule base to enable access or removal of access.

Group Modification

Creates and modifies network groups across different firewall vendors.

Rule Modification

Designs changes to existing rules.

Rule Recertification

Identifies expiring or expired rules, maps them to their business owners, and triggers an automated recertification or decertification process.

The Industry's Most Advanced Topology Mapping Delivers Real-Time, Holistic Visibility

SecureChange+ is powered in part by the industry's most advanced topology model. SecureChange+ connects to network devices, such as multi-vendor firewalls, routers, NGFWs, SDNs, and cloud services, retrieving all routing tables, as well as accounting for common network technologies, such as NAT, MPLS, IPSEC VPN, to create your topology view. This vendor-agnostic network topology map, delivers centralized visibility and control on-premises and in the cloud.

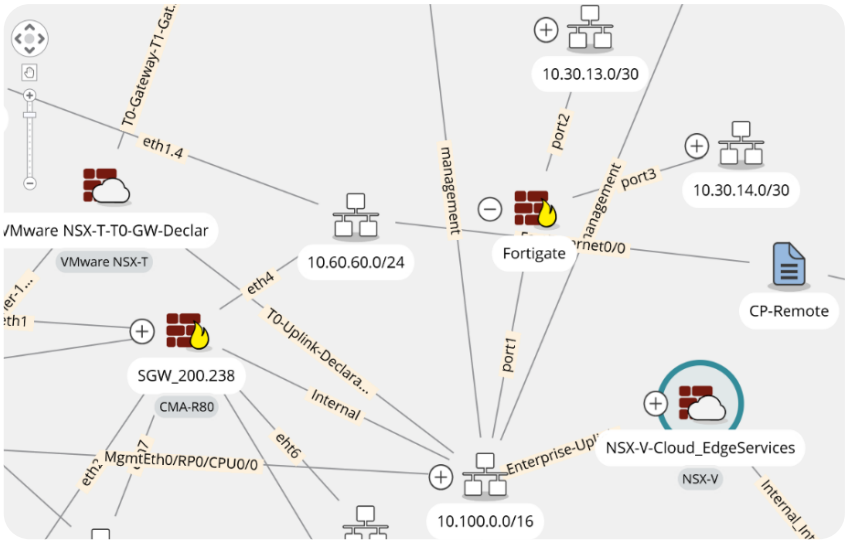
Tufin's topology intelligence lets you use the routing information from your devices to make informed decisions about your network's security.

Within SecureChange+ workflows, topology intelligence is used to:

- Suggest target firewall devices for access requests
- Calculate and show the necessary changes needed for the access request
- Verify the access request was successfully added

Rapid Troubleshooting

- Users can run topology analysis queries, showing the current path from source to destination and the relevant security policies on each network device along the way to understand if the path in question is allowed or blocked.



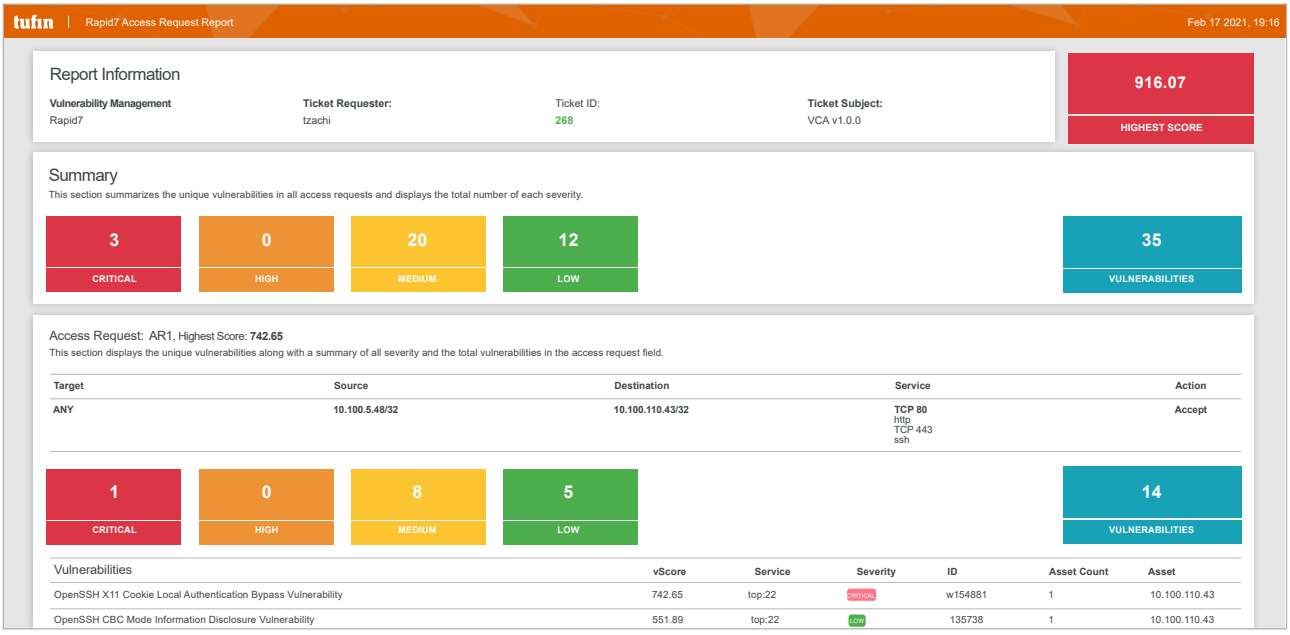
Tufin's Topology Map

Unmatched Scalability

The topology map is expandable, allowing customers to add generic network devices and nonstandard configurations. Tufin supports thousands of devices and 100M+ routes, providing real-time, accurate network topology analysis.

Vulnerability-based Change Automation (VCA)

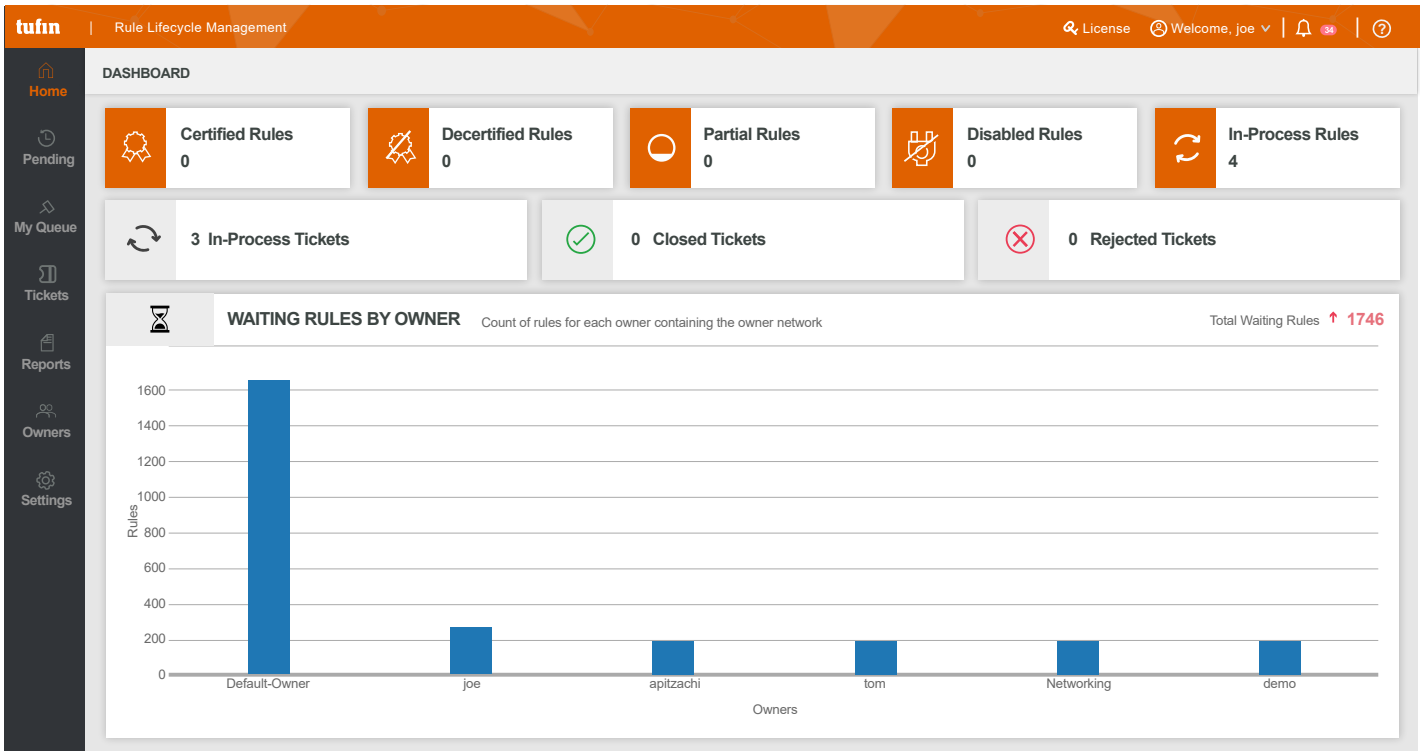
Tufin's Vulnerability-based Change Automation module enables you to expand your risk-based access request workflows to reflect the results of vulnerability scan results. You can automatically check source and destination assets for known vulnerabilities prior to granting access or connectivity.



VCA Dashboard

Rule Lifecycle Management (RLM)

Rule Lifecycle Management enables orchestration of rule recertification. It integrates with configuration management databases to map network owners, identify inactive owners for rule reassignment, and orchestrate certification across the right set of rule owners. You can automatically identify expiring or expired rules and map them to their owner(s), enabling simple recertification or decertification of the rule. This allows you to operationalize more frequent rule reviews.



RLM Dashboard

Customer Success

A **multinational bank** **eliminated a 12-month recertification backlog.**

The team automated rule review and recertification workflows with variable rule expiration timeframes.

Now they review rules daily.

www.tufin.com

tufin
The Security Policy Company.

DP20221014