tufin The Security Policy Company.

SecureTrack™

Security Policy Management for the Hybrid Cloud

Overview

Today, organizations are witnessing growing network complexity, such as hundreds of firewalls from different vendors, thousands of routers and switches, and private clouds. Software-defined networks using micro-segmentation technologies, such as VMware NSX and Cisco ACI, public clouds with built-in security controls, and containers running in Kubernetes, often in multi-cloud environments, are also prevalent. This results in **complex fragmented networks** that provide an enormous attack surface vulnerable to hackers.

While many firewalls and cloud vendors offer different levels of visibility and policy management capabilities for their respective platform and infrastructure components, **most organizations still lack a unified, comprehensive security policy governing who can talk to whom, and what can talk to what across the hybrid network.** Without full visibility, IT teams are struggling with managing their complex, fragmented networks, and configuring policy rules using disparate solutions. This leads to inconsistent security policy enforcement, re-work due to manual errors, excessive time spent on routine tasks, and challenges when decommissioning rules, servers, or applications.

Tufin SecureTrack enables organizations to achieve vendor-agnostic, end-to-end visibility, and set and manage accurate segmentation policies across the hybrid cloud environment, to mitigate exposure, and prevent lateral movement. SecureTrack provides a real-time hybrid network topology map and segmentation policy orchestration, irrespective of the network infrastructure or cloud platform. Segmentation/micro-segmentation policies are generated based on real-time visibility into application/workload communication flows, using enforcement points (e.g. firewalls, cloud-native firewalls, etc.) currently deployed throughout the hybrid environment. Policy generation does not require any in-depth knowledge of different firewalls' network capabilities, nor does it require additional agents or proxy.

Key Features

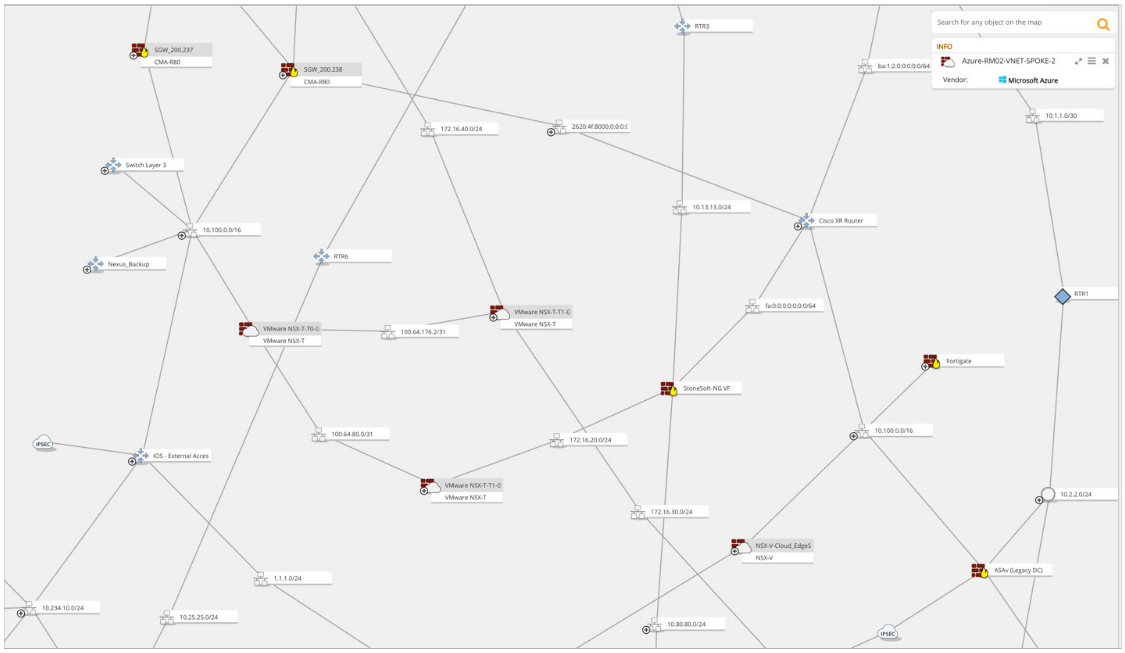
Real-time Topology Map Across the Hybrid Cloud

SecureTrack discovers an organizations' network topology and provides admins with a dynamic, visual map. The topology map is created by connecting to all network security devices and infrastructure components, such as multi-vendor firewalls, routers, NGFWs, SDNs, and cloud services, retrieving all routing tables, as well as considering common network technologies, such as IPSec VPN, MPLS, NAT, and more to create accurate topology view.

This process results in a highly accurate model of the hybrid environment that allows users to immediately start monitoring actual traffic, perform 'what-if' analysis, troubleshoot connectivity, and identify anomalies, such as misconfigurations and potential threats, while remaining infrastructure-agnostic.

Benefits:

- Set and manage segmentation or micro-segmentation policies across the hybrid cloud, irrespective of the underlying infrastructure
- Detect access violations and quickly mitigate risk by using accurate topology and policy data, regardless of the infrastructure
- Optimize policies and vet access changes by using automated policy generation and path analysis
- Gain comprehensive visibility across on-premise and hybrid cloud
- Enable continuous compliance with real-time monitoring and alerts for policy violations and regulatory compliance risks
- Maintain audit readiness with a fully documented audit trail
- Ensure continuous compliance for regulations, e.g., PCI-DSS, SOX, NERC CIP, and others



Tufin SecureTrack Topology View

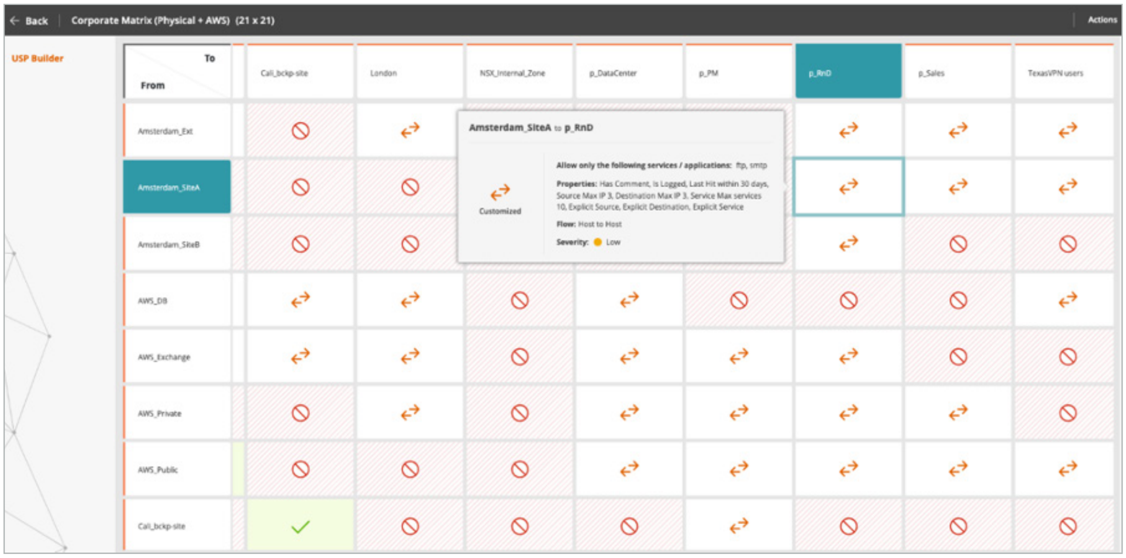
Segmentation Policy Generation and Management

With Tufin SecureTrack, users can define the desired state of security by establishing a baseline of allowed and blocked traffic between security segments and **apply it throughout the hybrid network**.

A dashboard view provides an overview of the rule changes and highlights risks, such as access anomalies, policy violations, and compliance violations that are alerted and flagged, providing **end-to-end visibility** of the hybrid environment's security posture.

In addition, Tufin provides pre-built rulesets and violation alerts for key **compliance mandates** (e.g. PCI-DSS, NERC CIP, GDPR, SOX, HIPAA, and NIST). Once defined, policies are automatically distributed and enforced.

Users can also deploy SecureTrack's advanced search and analysis capabilities to look for security groups, rules, objects, and more, across their infrastructure.



Corporate Matrix (Physical + AWS) (21 x 21)

To From	Cali_bckp-site	London	NSX_Internal_Zone	p_DataCenter	p_PM	p_RnD	p_Sales	TexasVPN users
Amsterdam_Ext	⊘	⇄				⇄	⇄	⇄
Amsterdam_SiteA	⊘	⊘				⇄	⇄	⇄
Amsterdam_SiteB	⊘	⊘				⇄	⊘	⊘
AWS_DB	⇄	⇄	⊘	⇄	⊘	⊘	⊘	⇄
AWS_Exchange	⇄	⇄	⊘	⇄	⇄	⇄	⊘	⊘
AWS_Private	⊘	⇄	⊘	⇄	⇄	⇄	⇄	⊘
AWS_Public	⊘	⊘	⊘	⇄	⇄	⇄	⇄	⇄
Cali_bckp-site	✓	⊘	⊘	⊘	⇄	⊘	⊘	⊘

Amsterdam_SiteA to **p_RnD**

⇄ Customized

Allow only the following services / applications: ftp, smtp

Properties: Has Comment, Is Logged, Last Hit within 30 days, Source Max IP 3, Destination Max IP 3, Service Max services 10, Explicit Source, Explicit Destination, Explicit Service

Flow: Host to Host

Severity: ● Low

Tufin SecureTrack Unified Security Policy and segmentation matrix

Policy Optimization and Cleanup

SecureTrack helps define **least privilege policies**. Using Tufin's Automated Policy Generator (APG), SecureTrack identifies overly permissive rules and how to limit them in order to **optimize rules** based on actual activity. The APG ensures least privilege compliance without breaking connectivity.

In addition, to minimize the attack surface, SecureTrack analyzes the actual usage of policy rules and labels each rule based on its usage. SecureTrack also analyzes object usage within each rule, indicating specific network objects and services that are no longer in use, and are candidates for decommissioning.

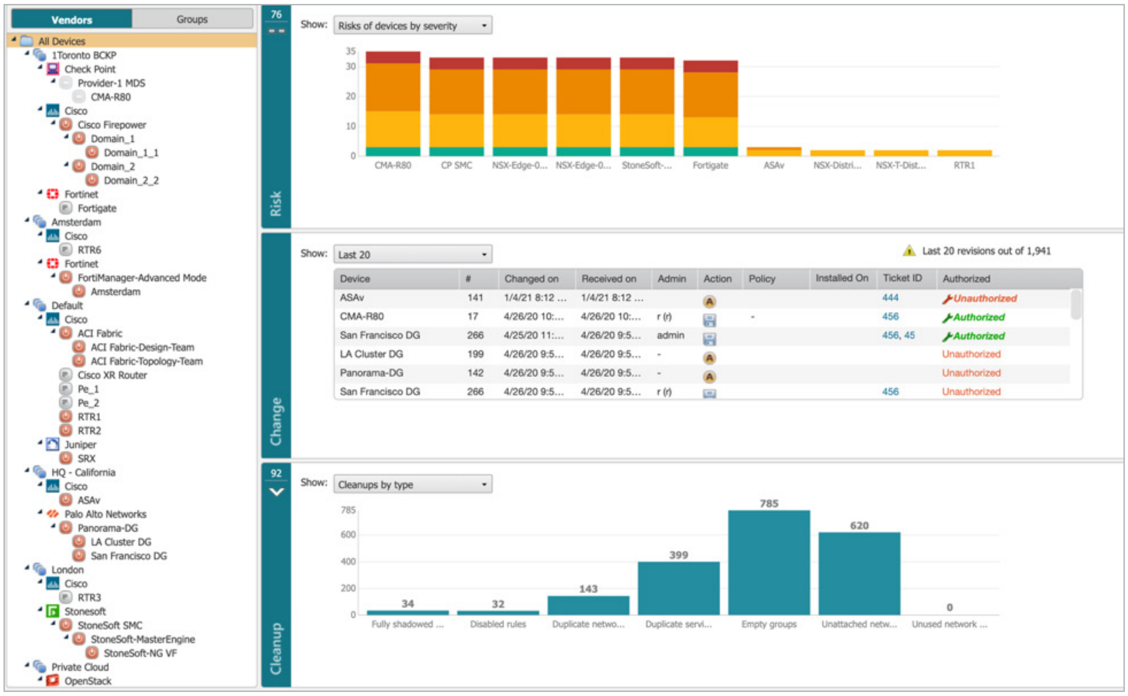
For security purposes and to enhance device performance, SecureTrack makes recommendations regarding the position of specific rules – placing the heavily-used rules at the top of the rule base and moving the least-used rules to the bottom. SecureTrack also indicates rule shadowing – places where rules overlap, or effectively "hide" other rules – so that rules can be easily re-positioned, and essentially, optimized.

In turn, policy optimization becomes exceedingly important prior to app migration. The ability to use searches from SecureTrack in the migration process, makes it very easy to remove dozens of unused network object groups and unused rules, and ensure least privilege policies, irrespective of the app/workload location in the network.

Real-time Monitoring and Alerts

Tufin SecureTrack provides statistics on and visibility into rule utilization and trigger rates to help **optimize policies**. Tufin automatically detects **unused, shadowed, redundant, and overly permissive rules**, and highlights them for fast mitigation.

Further, SecureTrack develops a full audit trail. It collects and records policy changes, providing a central console that monitors, displays, and compares policy revisions, irrespective of the firewall or platform, in real-time. Users can view what has changed, by whom, when, and why.



- All Devices
  - 1Toronto BCKP
    - Check Point
      - Provider-1 MDS
        - CMA-R80
    - Cisco
      - Cisco Firepower
        - Domain_1
          - Domain_1_1
        - Domain_2
          - Domain_2_2
    - Fortinet
      - Fortigate
  - Amsterdam
    - Cisco
      - RTR6
    - Fortinet
      - FortiManager-Advanced Mode
        - Amsterdam
  - Default
    - Cisco
      - ACI Fabric
        - ACI Fabric-Design-Team
        - ACI Fabric-Topology-Team
      - Cisco XR Router
      - Pe_1
      - Pe_2
      - RTR1
      - RTR2
    - Juniper
      - SRX
  - HQ - California
    - Cisco
      - ASAv
    - Palo Alto Networks
      - Panorama-DG
        - LA Cluster DG
        - San Francisco DG
  - London
    - Cisco
      - RTR3
    - Stonesoft
      - StoneSoft SMC
        - StoneSoft-MasterEngine
          - StoneSoft-NG VF
  - Private Cloud
    - OpenStack

Device	#	Changed on	Received on	Admin	Action	Policy	Installed On	Ticket ID	Authorized
ASAv	141	1/4/21 8:12 ...	1/4/21 8:12 ...		A			444	*Unauthorized*
CMA-R80	17	4/26/20 10:...	4/26/20 10:...	r (r)	💾	-		456	*Authorized*
San Francisco DG	266	4/25/20 11:...	4/26/20 9:5...	admin	💾			456, 45	*Authorized*
LA Cluster DG	199	4/26/20 9:5...	4/26/20 9:5...	-	A				Unauthorized
Panorama-DG	142	4/26/20 9:5...	4/26/20 9:5...	-	A				Unauthorized
San Francisco DG	266	4/26/20 9:5...	4/26/20 9:5...	r (r)	▭			456	Unauthorized

Tufin SecureTrack Dashboard

Troubleshooting Connectivity

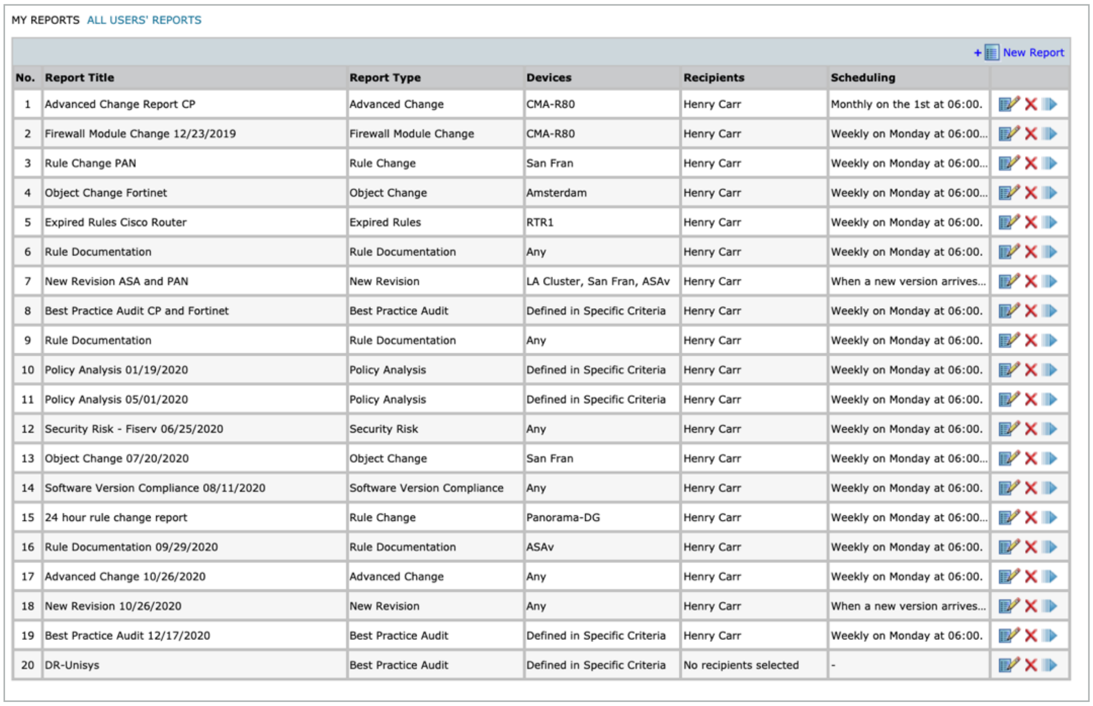
Based on SecureTrack's accurate topology modeling and path analysis, network and security teams can quickly and accurately troubleshoot and remediate network outages across the multi-vendor, hybrid environment, and properly plan connectivity changes.

For example, if an app availability issue is detected, users can deploy Tufin's interactive topology map to run path analysis to view East-West and North-South traffic. By entering the security group or IP address as source/destination, Tufin calculates and maps the path across any environment or alert on unavailable traffic routes. Based on the app or workload's connectivity requirements, users can also change rules that block traffic.

Auditing and Continuous Compliance

SecureTrack provides predefined compliance segmentation policy templates, whereby all rules can be compared to these policies to comply with industry standards. SecureTrack also provides automatic audit reports that test current firewall configuration against corporate security policy, as well as a configurable checklist of standards. Along with a list of violations, Tufin's audit reports provide information on how to resolve or mitigate the infraction. Specific reports, such as the PCI-DSS audit and the Cisco Device Configuration Report (DCR), are already designed according to the requirements of the industry standard. Audit reports can be scheduled for automatic or periodic execution, and forwarded to all relevant security officers.

SecureTrack supports periodic audits with continuous change tracking, and a comprehensive audit trail that provides full accountability, and demonstrates implementation of a separation of duties. Change reports can be generated at any time to show the configuration changes that were made, to both the rule base and to the firewall operating system.



No.	Report Title	Report Type	Devices	Recipients	Scheduling	
1	Advanced Change Report CP	Advanced Change	CMA-R80	Henry Carr	Monthly on the 1st at 06:00.	✎ ✕ ▶
2	Firewall Module Change 12/23/2019	Firewall Module Change	CMA-R80	Henry Carr	Weekly on Monday at 06:00...	✎ ✕ ▶
3	Rule Change PAN	Rule Change	San Fran	Henry Carr	Weekly on Monday at 06:00...	✎ ✕ ▶
4	Object Change Fortinet	Object Change	Amsterdam	Henry Carr	Weekly on Monday at 06:00...	✎ ✕ ▶
5	Expired Rules Cisco Router	Expired Rules	RTR1	Henry Carr	Weekly on Monday at 06:00.	✎ ✕ ▶
6	Rule Documentation	Rule Documentation	Any	Henry Carr	Weekly on Monday at 06:00.	✎ ✕ ▶
7	New Revision ASA and PAN	New Revision	LA Cluster, San Fran, ASAv	Henry Carr	When a new version arrives...	✎ ✕ ▶
8	Best Practice Audit CP and Fortinet	Best Practice Audit	Defined in Specific Criteria	Henry Carr	Weekly on Monday at 06:00.	✎ ✕ ▶
9	Rule Documentation	Rule Documentation	Any	Henry Carr	Weekly on Monday at 06:00.	✎ ✕ ▶
10	Policy Analysis 01/19/2020	Policy Analysis	Defined in Specific Criteria	Henry Carr	Weekly on Monday at 06:00.	✎ ✕ ▶
11	Policy Analysis 05/01/2020	Policy Analysis	Defined in Specific Criteria	Henry Carr	Weekly on Monday at 06:00.	✎ ✕ ▶
12	Security Risk - Fiserv 06/25/2020	Security Risk	Any	Henry Carr	Weekly on Monday at 06:00.	✎ ✕ ▶
13	Object Change 07/20/2020	Object Change	San Fran	Henry Carr	Weekly on Monday at 06:00...	✎ ✕ ▶
14	Software Version Compliance 08/11/2020	Software Version Compliance	Any	Henry Carr	Weekly on Monday at 06:00.	✎ ✕ ▶
15	24 hour rule change report	Rule Change	Panorama-DG	Henry Carr	Weekly on Monday at 06:00...	✎ ✕ ▶
16	Rule Documentation 09/29/2020	Rule Documentation	ASAv	Henry Carr	Weekly on Monday at 06:00.	✎ ✕ ▶
17	Advanced Change 10/26/2020	Advanced Change	Any	Henry Carr	Weekly on Monday at 06:00.	✎ ✕ ▶
18	New Revision 10/26/2020	New Revision	Any	Henry Carr	When a new version arrives...	✎ ✕ ▶
19	Best Practice Audit 12/17/2020	Best Practice Audit	Defined in Specific Criteria	Henry Carr	Weekly on Monday at 06:00.	✎ ✕ ▶
20	DR-Unisys	Best Practice Audit	Defined in Specific Criteria	No recipients selected	-	✎ ✕ ▶

***Download SecureTrack Reporting Essentials** (a Tufin Marketplace app), generate a wide range of operational reports based on SecureTrack data, in a format that is easy to read and understand. Reports can be either vendor-agnostic or vendor-specific.*

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.

The Security
Policy Company.