

Case Study

# Blue Cross Blue Shield of Massachusetts - Empowering a Lean Security Team with Tufin



## The Challenge

The network security team at Massachusetts' largest health insurer<sup>1</sup>, Blue Cross Blue Shield of MA (BCBSMA), has a wide range of network responsibilities that includes implementing Software Defined Networks (SDNs), managing migrations, applying effective security controls, and maintaining business-critical network connectivity. With 95% of BCBSMA's workforce dependent on this infrastructure to work effectively from home, the network security team must ensure its infrastructure is always up and running. The team set out to improve its security posture by automating policy management and more proactively identifying security risks through centralized visibility and control across its multi-vendor, hybrid network.

## Why Tufin

Like other large organizations, BCBSMA maintains a complex network of on-premises, SDN and public cloud environments with firewalls from multiple vendors. It must manage adherence to its own security standards as well as regulatory standards. BCBSMA has been able to quickly identify risky configurations and manage security policies with Tufin Orchestration Suite.

## The Results

### Continuous Compliance with Regulatory Standards

BCBSMA leverages Tufin to identify rules that violate compliance or business standards as well as proactively protect against new, risky requests. The network security team is alerted when risks are found via Tufin's real-time continuous monitoring, and regularly checks Tufin's security risk reports. These measures empower the team to proactively identify high and critical risks for immediate remediation, and flag medium-severity risks for less urgent remediation.

Risk	Name	Type	Instances
N01	Critical	Risky Microsoft services can enter Internal and/or DMZ networks	Risky rules 11
N02	Critical	Risky R-services can enter Internal and/or DMZ networks	Risky rules 12
N03	High	TFTP services can enter Internal and/or DMZ networks	Risky rules 11
N04	High	Microsoft SQL services can enter Internal and/or DMZ networks	Risky rules 13
N05	High	NFS services can enter Internal and/or DMZ networks	Risky rules 11
N06	High	LDAP services can enter Internal and/or DMZ networks	Risky rules 11
N07	High	TCP small services can enter Internal and/or DMZ networks	Risky rules 11
N08	High	Finger services can enter Internal and/or DMZ networks	Risky rules 11

  

ID	NAME	SOURCE	DESTINATION	VPN	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT	RISK
2.1		Any, environment	SWW_200,238	Any	Any	Accept	None	SGW_200,238	Any		N01 N02 N03 N04 N05 N06 N07 N08
2.8		Any	blm2_206 Host_10.100.200.1 Host_10.100.200.1 Any Host SGW_200,238 Tervnet_BSCP_Ser...	Any	Any	Accept	Log	Any	Any		N01 N02 N03 N04 N05 N06 N07 N08

View of rules deemed critical or high risk, providing drill down to the device, the rule and its instances

Screenshot of a risk report showing for all devices, SDNs and public clouds the rules deemed critical or high risk, providing drill down to the device, the rule and its instances.

<sup>1</sup> <https://tinyurl.com/y29pcmoa>

In addition, the information that Tufin SecureTrack makes available provides visibility into the organization’s firewall and security group policies, and makes it is easy to identify risky rules and services. With SecureTrack’s topology and traffic visibility, the network security team can determine which rules can be eliminated with confidence that connectivity is not disrupted.

## Proactively Report on Risks

BCBSMA’s network security team scores the organization regularly against benchmarks and industry standards, and provides BCBSMA’s CIO, CISO, and board of directors with visibility into the organization’s security risk. At monthly meetings, the team presents metrics via reports that include policy compliance status, change reports, risks mitigated and benchmark scores.

## Proactively Manage Audit Readiness

BCBSMA also consistently assesses its policies against its security policy benchmark to proactively identify and remediate non-compliant policies. Proactively managing its audit score in turn empowers the team to monitor and modify connections that will impact its rule base or audit performance, such as permissiveness, redundant rules, shadowed rules, inactive rules, or rules that have large numbers of IP addresses. This helps ensure the team is ready to pass its next audit, and is proactively managing its security posture.

When the security team changes any firewall, SDN or security group policy, it uses Tufin’s policy and change tracking tool to quickly understand what was changed and whether connectivity was removed inadvertently. This visibility makes it easy to rolling back changes, and determine whether a new risk was inadvertently introduced.

With Tufin’s security policy orchestration suite, BCBSMA has tightened its firewall and security group policy management, optimized security policies, and is able to proactively identify and manage network security risks across its complex, multi-vendor, heterogeneous network. By leveraging Tufin’s automation, BCBSMA’s small network security team can accomplish all this efficiently.

## 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.

The screenshot displays a 'Best Practice Audit Report' for 'Best Practice Audit CP and Fortinet'. It includes a 'Summary' table with columns for Category, Critical, High, Medium, Low, and Total. The table lists various policy categories such as Rule Base, Objects Cleanup, Performance, Firewall Gateway, Users Cleanup, Logging, and Check Point Performance, along with their respective counts for each severity level and a total count.

Category	Critical	High	Medium	Low	Total
<b>Common Best Practices (for all firewall vendors)</b>					
Rule Base	0 (of 2)	5 (of 6)	3 (of 3)	0 (of 0)	8 (of 11)
Objects Cleanup	0 (of 0)	0 (of 0)	1 (of 3)	1 (of 3)	2 (of 6)
Performance	0 (of 0)	0 (of 0)	0 (of 0)	1 (of 1)	1 (of 1)
<b>Check Point Best Practices</b>					
Firewall Gateway	0 (of 0)	0 (of 2)	0 (of 0)	0 (of 0)	0 (of 2)
Rule Base	0 (of 0)	3 (of 9)	2 (of 4)	1 (of 2)	6 (of 15)
Users Cleanup	0 (of 0)	0 (of 0)	0 (of 0)	0 (of 3)	0 (of 3)
Logging	0 (of 0)	0 (of 1)	0 (of 1)	0 (of 0)	0 (of 2)
Check Point Performance	0 (of 0)	1 (of 2)	0 (of 0)	0 (of 0)	1 (of 2)
<b>Total</b>	<b>0 (of 2)</b>	<b>9 (of 20)</b>	<b>6 (of 11)</b>	<b>3 (of 9)</b>	<b>18 (of 42)</b>

Screenshot of the Best Practices Audit Report which identifies critical, high, medium and low risk policies for a specified (set of) devices, zones or domains.