SOLUTION BRIEF

Fortinet and Tufin OT Security Solution

Visibility, Compliance, and Control for OT Environments

Executive Summary

The Tufin Orchestration Suite allows all stakeholders to achieve unified visibility of network topology and security policies, from control networks to the edge. This joint solution allows customers to ensure that these critical network segments remain secure and all compensating controls remain strictly enforced, maintaining a zero-trust approach to operational technology (OT) security.

Challenge

Legacy OT systems used to be isolated from traditional IP-based networks. Increasing smartness and interconnectedness of OT devices has led to a convergence of IT and OT, and as a result, OT devices are no longer treated as a black box from the network perspective. This convergence poses unique challenges to enterprise security teams, as they struggle to maintain security while providing connectivity to OT devices that may not have been designed with enterprise security in mind and often lack proper embedded security controls.

OT devices often monitor or control critical processes, such as energy generation, manufacturing systems, or utilities distribution. A compromise or interruption of these systems could have a serious impact on the organization, as well as public safety and welfare. Even noncritical OT devices can pose a serious risk to the organization's security posture. Attackers are keenly aware of the weaknesses and shortcomings of the security in OT, and they will often target OT devices in a bid to compromise a network. Compromised and connected OT devices can serve as a beachhead for attackers to launch attacks from within the network.

Joint Solution

Tufin and Fortinet have partnered to deliver an industry-leading security solution to enable resource agility and fuel growth in organizations. The integration of the Tufin Orchestration Suite and Fortinet FortiGate, FortiManager, FortiSIEM, and FortiSOAR, enabled through the Fabric-Ready Program in the Fortinet Open Fabric Ecosystem, delivers unmatched security policy visibility, and change management in complex and heterogeneous environments while maintaining continuous compliance and business agility.

Joint Solution Components

Tufin Orchestration Suite

Automate security policy visibility, risk management, provisioning, and compliance across multivendor, hybrid, and cloud environments. Eliminate the security bottleneck and increase the business agility of your organization.

FortiGate

FortiGate next-generation firewalls (NGFWs) are network firewalls powered by purpose-built security processing units (SPUs) including the latest NP7 (Network Processor 7). They enable security-driven networking and are ideal network firewalls for hybrid and hyperscale data centers.

Joint Solution Components

- FortiGate
- FortiManager
- FortiSIEM
- FortiSOAR
- Tufin Orchestration Suite

Joint Solution Benefits

- Fortinet Security Fabric platform for broad visibility and easy management of security and network operations across environments
- Unified dashboard for security policy management across diverse network firewalls, private cloud, and public cloud
- Automated change management for improved security, compliance, and business agility
- Efficient and effective security incident response with advanced network intelligence and automation
- Continuous compliance with enterprise and industry regulations
- Policy change requests enrichment with endpoint information and events, allowing more informed decisions and reduced risk

FORTINET Fabric-Ready

FortiManager

An integral part of the Fortinet Security Fabric, FortiManager supports network operations use cases for centralized management, best practices compliance, and workflow automation to provide better protection against breaches.

FortiSIEM

FortiSIEM brings together visibility, correlation, automated response, and remediation in a single, scalable solution. It reduces the complexity of managing network and security operations to effectively free resources, improve breach detection, and even prevent breaches.

FortiSOAR

Integrated into the Fortinet Security Fabric, FortiSOAR security orchestration, automation, and response (SOAR) remedies some of the biggest challenges facing cybersecurity teams today. Allowing security operations center (SOC) teams to create a custom automated framework that pulls together all of their organization's tools unifies operations, eliminating alert fatigue and reducing context switching. This allows enterprises to not only adapt but also optimize their security process.

Joint Solution Integration

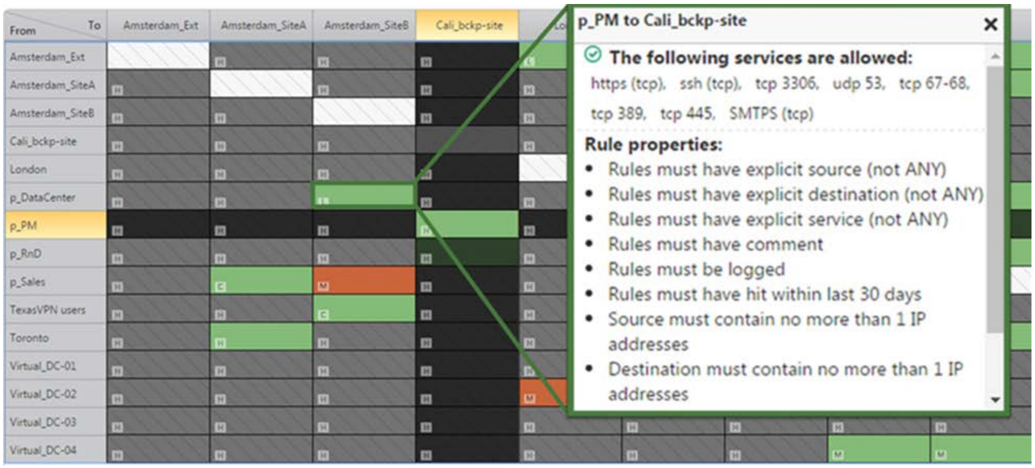
The Tufin-Fortinet joint solution delivers unparalleled visibility, compliance, and control across complex OT environments, ensuring that access to the critical network segments is managed securely and all compensating controls are strictly enforced, maintaining a zero-trust approach to OT security.

Tufin leverages security policy and other network configuration information from FortiGate and FortiManager, including diverse multivendor devices, to provide organizations with a holistic view of the entire network ecosystem, originating from individual control networks to the edge devices. All stakeholders are provided with a single, unified awareness of the network topology and the security policies governing these complex environments.

Tufin's Unified Security Policy (USP) allows organizations to define granular security policy requirements, codifying industry regulations, company policies, and best practices into a framework that can be enforced across a hybrid IT environment. Violations of the organization's USP can be sent to FortiSIEM for aggregation and alerting or sent to FortiSOAR for incident handling.

Security policy changes, both routine and in response to a security incident, can be optimized and automated by Tufin. Tufin incorporates configuration management database (CMDB) and event data from FortiSIEM, unified compliance standards, and best practices, as well as an accurate understanding of network topology to ensure continuous compliance and business agility throughout the change management life cycle. Tufin's customizable change workflows enable organizations to define processes that help to involve multiple stakeholders in the design and approval of network changes, thus allowing IT and OT teams to collaborate in ensuring a state of cc

If a security incident occurs within the OT network, Tufin's network visibility and change automation can be combined with FortiSIEM and FortiSOAR to make more intelligent automated incident handling decisions and implement effective threat containment actions.



p_PM to Cali_bckp-site

The following services are allowed:

https (tcp), ssh (tcp), tcp 3306, udp 53, tcp 67-68, tcp 389, tcp 445, SMTPS (tcp)

Rule properties:

- Rules must have explicit source (not ANY)
- Rules must have explicit destination (not ANY)
- Rules must have explicit service (not ANY)
- Rules must have comment
- Rules must be logged
- Rules must have hit within last 30 days
- Source must contain no more than 1 IP addresses
- Destination must contain no more than 1 IP addresses

Figure 1: Tufin's zone-based Unified Security Policy enables policy optimization, network segmentation, and continuous compliance across a hybrid network.

Joint Use Cases

Use Case 1

Visibility Across Network Boundaries—The Tufin Orchestration Suite provides complete visibility into network topology and security policies across a hybrid network environment, including network devices acting as gateways to OT networks. Both IT and OT teams are provided with a single, unified awareness of the network from edge devices to internal network devices.

Use Case 2

Unified Compliance and Change Management—Tufin's Unified Security Policy allows organizations to define granular security policy requirements, which can be used to detect and prevent security and compliance violations, leading to a stable and secure OT environment. Tufin's customizable change workflows allows organizations to implement consistent design and approval processes that will also mirror their existing manual processes.

About Tufin

Tufin (NYSE:TUFN) simplifies management of some of the largest, most complex networks in the world, consisting of thousands of firewalls 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 Tufin Orchestration 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. Find out more at www.tufin.com.

FORTINET®

www.fortinet.com