

DEPLOYMENT GUIDE

Fortinet and Tufin SecureTrack



Table of Contents

Overview	3
Deployment Prerequisites	3
FortiManager Configuration	4
Tufin Configuration	6
Conclusion	9

Overview

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network—today and into the future. Only the Fortinet Security Fabric architecture can deliver security features without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 400,000 customers trust Fortinet to protect their businesses. Learn more at https://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

About Tufin

Tufin is the leader in Network Security Policy Orchestration for enterprise cybersecurity. More than half of the top 50 companies in the Forbes Global 2000 turn to Tufin to simplify 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 award-winning 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. Its network security automation enables enterprises to implement changes in minutes with proactive risk analysis and continuous policy compliance. Tufin serves over 1,900 customers spanning all industries and geographies; its products and technologies are patent-protected in the U.S. and other countries. Find out more at www.tufin.com.

Deployment Prerequisites

- 1. Fortinet FortiManager version 5.x (tested with versions 5.4.2 and 5.6.0)
- 2. Tufin Orchestration Suite SecureTrack version 17.1 GA.2 build 93488





Figure 1: Architecture overview.

FortiManager Configuration

Create and configure an administrator account for tufin to use.

- 1. Create and configure an administrator account for Tufin to use.
- 2. From System Settings go to Admin > Administrators > Create New.

System Settings 🗸							🌅 admin 🗸
Dashboard	+	Create New 🕑 Edit 🖞	Delete di Column Si	sttings 🗸 🖽	Table View \sim		
응 All ADOMs		▲ User Name		Type	Profile	ADOMs	Policy Packages
O Network		A admin		LOCAL	Super_User	All ADOMs	All Packages
њ на							
2 Admin 🗸							
Administrators							
Profile							
Remote Authentication Server							
Admin Settings							
Certificates							
Local Certificates							
CA Certificates							
CRL							
皓 Event Log							

3. Enter a username, new password and confirm the password. Set the Admin Profile to Super_User and click OK at the bottom.

User Name	tufin	
Avatar	+ Change Photo - Remove Photo	
Comments		
		0/127
Admin Type	LOCAL	-
New Password	•••••	•
Confirm Password	•••••	P
Admin Profile	Super_User	-
Administrative Domain	All ADOMs All ADOMs except specified ones	Specify
Policy Package Access	All Packages Specify	
Trusted Hosts	OFF	
Meta Fields >		

4. The screen should look like the image below.

System Settings ~									🕗 admin 🗸
Dashboard	+	Create New	🕑 Edit	🗊 Delete	🐔 Column Settin	gs ~ [🗉 Table View 🗸		
All ADOMs		▲ User Name	2			Туре	Profile	ADOMs	Policy Packages
© Network		Q. admin				LOCAL	Super_User	All ADOMs	All Packages
in HA						LOCAL	Super_User	All ADOMs	All Packages
2 Admin	-	U unn							
Administrators									
Profile									
Remote Authentication Server									
Admin Settings									
Certificates	-								
Local Certificates									
CA Certificates									
CRL									
皓 Event Log	1								

5. Enable the Web Service from the Network settings.

Name	port1
IP Address/Netmask	10.101.32.64/255.255.255.0
IPv6 Address	::/0
Administrative Access	🗹 HTTPS 🗹 HTTP 🗹 PING 🗹 SSH 🗌 TELNET 🗌 SNMF 🗹 Web Service
IPv6 Administrative Access	HTTPS HTTP PING SSH TELNET SNMP Web Service
IPv6 Administrative Access Service Access	HTTPS HTTP PING SSH TELNET SNMP Web Service FortiGate Updates Web Filtering
IPv6 Administrative Access Service Access Default Gateway	HTTPS HTTP PING SSH TELNET SNMP Web Service FortiGate Updates Web Filtering 10.101.32.254
IPv6 Administrative Access Service Access Default Gateway Primary DNS Server	HTTPS HTTP PING SSH TELNET SNMP Web Service FortiGate Updates Web Filtering 10.101.32.254 208.91.112.52

- 6. Remote Procedure Call (RPC) needs to be set to read-write when using FortiManager version 5.2.3 and above (see link to the Technical Note at the end for more details).
- 7. Connect to the FortiManager CLI to change the Tufin administrator account permissions.
- 8. Enter the following CLI commands:



- 9. Configure FortiManager to send Syslog to the Tufin IP address.
- 10. From System Settings go to Advanced > Syslog Server and click Create New.

System Settings 🗸			
Dashboard	+ Create New	🗹 Edit 🏦 Delete	🕑 Test
H All ADOMs	□ ▲ Name		IP or FQDN: Port
Network	No entry found.		
击 HA			
Admin >			
Certificates			
Event Log			
Task Monitor			
& Advanced			
SNMP			
Mail Server			
Syslog Server			
Meta Fields			
Advanced Settings			

- 11. Enter a Name.
- 12. Enter the IP Address or FQDN of the tufin server.
- 13. Click OK.

Create New Syslog Server	Settings
Name	tufin
IP address (or FQDN)	10.101.32.69
Syslog Server Port	514

Tufin SecureTrack Configuration

- 14. Configure tufin SecureTrack to monitor FortiManager.
- 15. Go to Settings > Monitoring.

tufin Orchestration Swite	e Compane Analyze Audit Ru	eport Network Settings Ny 1	Settings Monitoring Configuration	
Manage Devices Device Groups TOP Plugins	Timing Finewall OS Monitoring			
Honitored Devices	Start monitoring a new d	levice:		
() M43 - 54.2 () Front Gate: VM64 () FortiGate: VM64 () Lab FM6 () Front () Front Fortigment () Fortigment	Web Services*		Select Device	CISCO. Select Device
	(5)	FORCEPOINT	FORTIDET	(intel) Security 🛡
	Select Device	Select Device	Select Device	Select Device

16. Click the Fortinet panel > Select Device > FortiManager.

F
Select Device
Fortigate
FortiManager

- 17. Enter a Name for Display.
- 18. Enter the IP address of the FortiManager.
- 19. Select Basic firewall management if using FortiManager 5.2 and earlier.
- 20. Select Advanced management if using FortiManager 5.4 and above.
- 21. Click Next.

Seneral Settings		
Device Type	Fortinet FortiManager	
ame for Display	FortiManager	
Get revisions from		
IP Address	1.2.3.4	
) Offline File		
Anagement Mode The Management N You must select the M	ode cannot be edited after it has been saved. anagement Mode that matches the FortiManager vi	ersion running on your device.
Basic firewall manage	ement (compatible with FortiManager 5.2.4 and earlier)	
 Advanced managem equires FortiMana 	nt using Administrative Domains (ADOMs) with automat per 5.4 and above)	ted provisioning

- 22. Enter the username and password configured previously.
- 23. Click Retrieve Certificate and wait for confirmation it was retrieved.
- 24. Click Next.

lser name	tufin	
assword		
onfirm Password		
Connection configurati	n	
Connection type	JSON API	
Port number		
* Leave empty to use Retrieve Certificate	default port (443)	
Certificate retrieved	retrieved	
	trieved successfully.	
his certificate was r		
his certificate was r		
'his certificate was r		
'his certificate was r		

- 25. Select the desired Monitoring Settings, either Default or Custom.
- 26. Click Next.

ew Fortinet FortiManager Stage 3 of 4	
Monitoring Settings	
Custom	
	Cancel < Prev Next >

27. Click Save.

ew Fortinet FortiManager Stage 4 of 4	
Click 'Save' to save your changes	
You have completed the configuration of this device.	
	Cancel < Prev Save

28. Click Import Administrative Domains and Managed Devices.

lew Fortinet FortiManager Stage 4 of 4	
SecureTrack will start monitoring this device shortly. You can view policy revisions in Compare view. For more information see our online help.	
Import Administrative Domains and Managed Devices	
Add another Fortinet FortiManager	
Your changes have been saved.	
	Cancel d Date
	Cancel < Prev Done

- 29. Select the Administrative Domains and Managed Devices to import.
- 30. Select the desired Features.
- 31. Click Import.

	Select: all none
FortiManager Administrative Domains and Managed Devices ☐ 2 root ☐ 2 FGVM040000101072	
eatures ionniony © Enable Topology	

32. The configuration is now complete.

The Home Dashboard should look like this:



Summary

Fortinet and Tufin have developed an integrated offering for comprehensive network security policy orchestration. Together, the Tufin Orchestration Suite with Fortinet FortiGate firewalls and FortiManager network security management products reduce attack surface for mitigation of cyber threats. The joint offering enables IT security teams to manage complex heterogeneous physical networks and cloud platforms through a single pane of glass, providing advanced visibility and risk-free policy modifications. Based on advanced analysis and automation technologies, network security policies are orchestrated across the enterprise networks, leveraging the advanced capabilities and unparalleled security protection of Fortinet FortiGate firewalls.

FortiManager Administration Guide Technical Note on enabling RPC in FortiManager Solution Brief Solution Overview Video Tufin Knowledge Center



www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet*, FortiGate*, FortiGate*, and FortiGuard*, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results. Nothing metric respective owners. The product variables, different network environments and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results. Nothing metric respective owners. The protonet and other results and vary. Network variables, different network environments and other results. Nothing verges or implied, except to the externet Fortine enternet contract, signal burchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance in the same ideal conditions as in Fortinet's listers. Fortinet internal lab tests. Fortinet disclams in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version in shall be applicable.