

DEPLOYMENT GUIDE

Fortinet and OneLayer Integration Guide



Overview

Fortinet and OneLayer have partnered to provide integrated security for LTE and 5G private networks. The joint solution includes real-time device identification, segmentation, policy enforcement, anomaly detection, and zero-trust security. This addresses the unique security challenges of private cellular networks and IoT devices, safeguarding against threats and preventing lateral movement between networks.

Architecture Overview

The OneLayer bridge integrates with the cellular packet core with the control and data planes. OneLayer OneID identifies and fingerprints the devices and correlates their cellular identifiers, such as IMEI and IMSI, to their IT network identifiers, such as IP address and MAC address, to enable securing the devices on the private cellular network, including devices behind cellular routers.

Device information, such as IPs and device types, is shared with the FortiGate Next-Generation Firewall (NGFW), enabling the creation of segmentation and security policies for enforcement between the cellular network and other enterprise networks. The FortiGate NGFW allows policies based on the device identity and context to mitigate unauthorized access. OneLayer applies segmentation policies inside the cellular network to prevent lateral movement between cellular devices.



FortiGate Configuration

Integrating the Fortinet FortiGate and the OneLayer OneID requires a two-way configuration to synchronize devices, groups, and policies automatically.

Step 1: FortiGate Configuration

API-based integration (recommended)

Create a new API token for OneLayer:

- 1. On the FortiGate GUI, select System > Admin Profiles > Create New.
- 2. Configure the firewall topic with read and write permissions.
- 3. Create a REST API Admin.
 - a. On the FortiGate GUI, select System > Administrators > Create New > REST API Admin.
 - b. Populate the fields as shown below:

≡ Q.			>_	0 -	¢.	😫 admin 👻
New REST API Admin						
Username Comments Administrator profile PKI Group CORS Allow Origin	<name-of-your-choice></name-of-your-choice>					
Restrict login to trusted	nosts					
	OK Can	cel				

- 4. In 6.4.2 and earlier, the Trusted Host must be specified to ensure your local host can reach FortiGate. For example, to restrict requests as coming from only 10.20.100.99, enter 10.20.100.99/32. The Trusted Host is created from the Source Address obtained in Step 1: Determine your Source Address.
- 5. Click OK, and an API token will be generated.
- 6. Copy and paste the key into the designated field in the OneLayer platform as described in Step 2 of this document. Note the API token, as it is only shown once and cannot be retrieved again.
- 7. Click Close to complete the creation of the REST API Admin.

CLI integration: Create a new user for OneLayer.

Step 1: Create a new user for OneLayer to access FortiGate for the integration.

- 1. Go to System > Administrators and click "Create New." Enter the details for the user account and enter the details as shown in the screenshot below.
- 2. Enter the Username, Password, and Comments.
- 3. Select the Type of the user to be "Local User."
- 4. Set Administrator Profile to "super_admin."
- 5. Enable Restrict login to trusted hosts and put in the IP of the OneLayer.
- 6. Click OK.

B Dashboard	>	New Administrator				
Security Fabric	>	Username	opelaver-admin			FortiToken Cloud
- Network	>	Time	Local User			E FortiToken Cloud Dashboard
O System	0 ~	Type	Match a user on a remote se	Over group		
Administrators	슈		Match all users in a remote s	erver group		⑦ Documentation
Admin Profiles			Use public key infrastructur	e (PKI) group		Online Help Online Help Online Help
Firmware		Password		æ		an video rutonais (5
Sattinas		Confirm Password	•••••	۲		
Replacement Messages FortiGuard Feature Visibility Certificates	0	Comments Administrator Profile	Cannot reuse old password Write a comment super_admin	rds T	0/255	
Balicy & Objects		Force Password Change				
Security Profiles	>	Two-factor Authenticat	tion			
User & Authentication	>	Restrict login to trusted	d hosts			
♥ WiFi & Switch Controller	>	Restrict admin to guest	account provisioning only			
M Log & Report						

Step 2: OneLayer Configuration

1. In the OneLayer dashboard, go to the Integrations page, and click on Fortinet.



Fortinet Integration page:

- 1. Choose a use case (currently available is policy groups update).
- 2. Configure the API token.
- 3. Select the groups to synchronize with FortiGate; options include all or specific groups.
- 4. Configure groups prefix (default: None).
- 5. Activate.

i oi une	t		Filatin
Policy Groups	Update:		
API Token:	Type token		
Group configuration:	All groups	~	
Group prefix:	None		
	Latest change: 2023/64/22 13:21		
Similar integr	ations:		
Similar integr	ations:		Pente



www.fortinet.com

Copyright © 2023 Fortinet, Inc. All rights reserved. FortiGate*, FortiGate*, FortiGate*, FortiGate*, FortiGate*, and FortiGate*, FortiGate*, and FortiGate*, FortiGate*, 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 may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsed, with a purchaser that expressly warrants that the identified product will perform accerding to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims 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 of the publication shall be applicable.

December 13, 2023 4:25 PM 2313502-0-0-EN