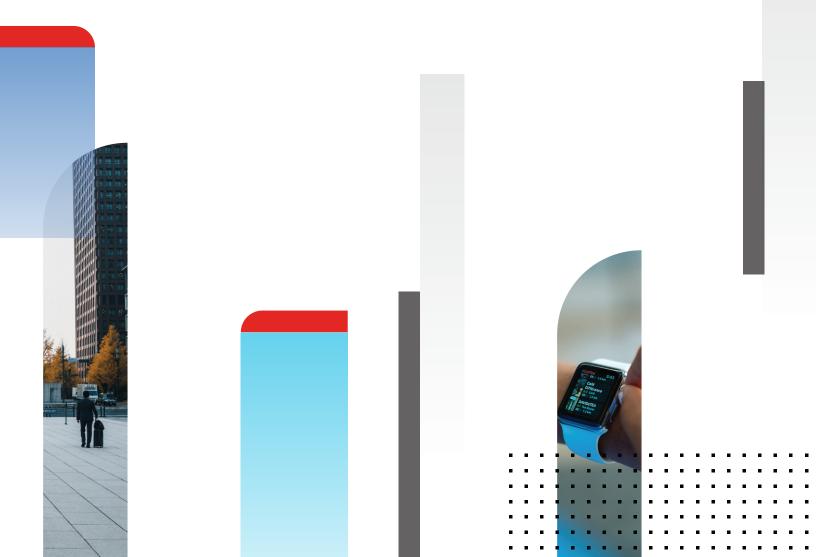


DEPLOYMENT GUIDE

Aislelabs Integration with Fortinet Wifi



Aislelabs Integration with Fortinet WiFi

Introduction
Aiselabs Flows Integration with Fortinet FortiGate
Data Flow Diagram and Prerequisite
Aislelabs Connect Integration with Fortinet FortiGate 4
Data Flow Diagram and Prerequisite
Aislelabs Flow Integration with Fortinet FortiWLC WiFi
Data Flow Diagram and Prerequisite

Introduction

This document shows the integration with Fortinet WiFi infrastructure with Aislelabs Flow and Connect Products. Most Fortinet products are turn-key compatible with Aislelabs solution suite, and do not require any additional hardware or components. If your specific hardware model is not listed here, contact us. You can request detailed integration information and assistance for the deployed integration by contacting support@aislelabs.com.

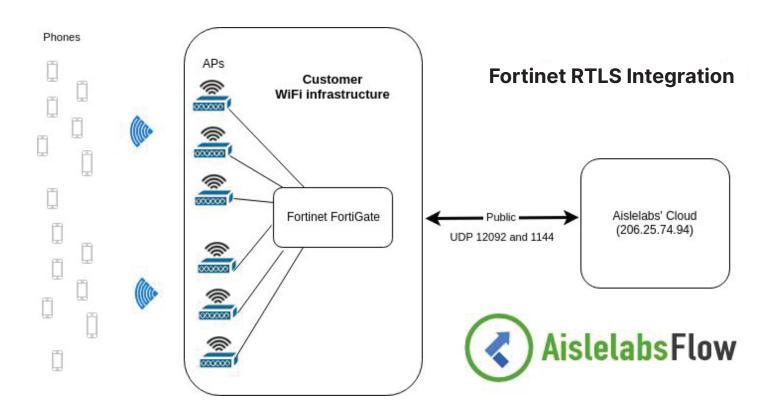
Learn more about Aislelabs and products at www.aislelabs.com.

Aiselabs Flow Integration with Fortinet FortiGate

Using Real-time Location Service (RTLS) for Anonymous Wi-Fi Location Analytics

Data Flow Diagram and Prerequisite

- 1. Complete list of AP MAC address, Public IP of your FortiGate
- 2. Enable bidirectional UDP port 12092 and port 1144 traffic on the firewall between Aislelabs and the FortiGate



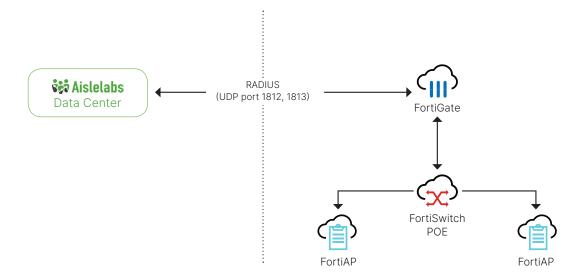
Requirement	Туре	Firewall Rule	Comments
Outgoing UDP port 12092 and 1144 requests	Required	Allow outgoing UDP 12092 and 1144 from FortiGate to Aislelabs	
Incoming UDP 12092 and 1144 requests	Required	Allow Incoming UDP 12092 and 1144 from Aislelabs to FortiGate	
Incoming acknowledgement packets	Required	Allow UDP acknowledgement packet back to controller (sent from Aislelabs as response)	Allow UDP acknowledgement packet, either by allowing all incoming UDP traffic or using stateful firewall NAT
Fortinet Controller Access	Optional	Create a user account and send us	Optional, and if provided, this will allow us to configure the service on your account directly

Aiselabs Connect Integration with Fortinet FortiGate

Using Fortinet FortiAP for Wi-Fi Marketing

Data Flow Diagram and Prerequisite

The controller will be able to send data to our RADIUS IP over UDP port 1812 and 1813 and receive data back. The easiest way to achieve this is by NAT, but site-to-site VPN can also be used. In this case via VPN.



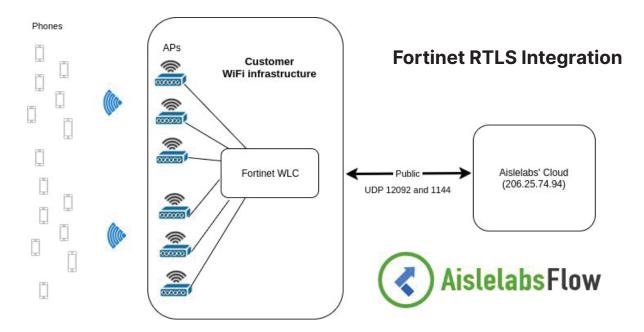
Requirement	Туре	Firewall Rule	Comments
Outgoing UDP 1812 and 1813 requests	Required	Allow outgoing UDP 1812, 1813 from FortiGate Controller to Aislelabs	
Incoming acknowledgement packets	Required	Allow UDP acknowledgement packet back to FortiGate Controller (sent from Aislelabs as response)	Allow UDP acknowledgement packet, either by allowing all incoming UDP traffic or using stateful firewall NAT
FortiGate Controller Access	Optional	Create a user account and send us	Optional, and if provided, this will allow us to configure Social WiFi on your controller directly

Aiselabs Flow Integration with Fortinet FortiWLC WiFi

Using Real-time Location Service (RTLS) for Anonymous Wi-Fi Location Analytics

Data Flow Diagram and Prerequisite

- 1. Complete list of AP MAC address, Public IP of your Fortinet WLC
- 2. Enable bidirectional UDP port 12092 and port 1144 traffic on the firewall between Aislelabs and the Fortinet Controller



Requirement	Туре	Firewall Rule	Comments
Outgoing UDP port 12092 and 1144 requests	Required	Allow outgoing UDP 12092 and 1144 from Fortinet Controller to Aislelabs	
Incoming UDP 12092 and 1144 requests	Required	Allow incoming UDP 12092 and 1144 from Aislelabs to Fortinet Controller	
Incoming acknowledgement packets	Required	Allow UDP acknowledgement packet back to controller (sent from Aislelabs as response)	Allow UDP acknowledgement packet, either by allowing all incoming UDP traffic or using stateful firewall NAT
Fortinet Controller Access	Optional	Create a user account and send us	Optional, and if provided, this will allow us to configure the service on your account directly



www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet*, FortiGate*, 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. 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, slighted by Gritnet's General Coursel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics expressly identified in such binding written contract, slighted be binding on Fortinet's and, in such verind, will be binding on 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 publicable. 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 publicable. 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 in all be papilicable.

June 28, 2021 10:01 PM