Wi-Fi AP Authentication Aruba Configuration

https://campus.barracuda.com/doc/73719689/

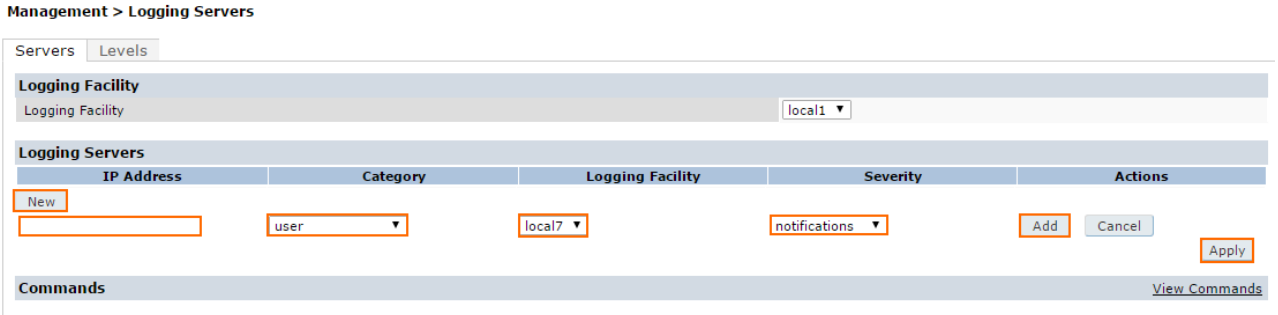
To authenticate users connected to Aruba access points, you must stream the syslog containing the authentication data to the Barracuda CloudGen Firewall F-Series.

Reference Devices/Versions:

- Aruba Controller 651 Version 6.4.1.0
- Aruba AP 105
- Aruba Instant

Enable Syslog Streaming on the Aruba AP

1. Log into the Aruba Mobility Controller.
2. Click the **Configuration** tab.
3. In the **MANAGEMENT** section of the left menu, click **Logging**.
4. In the **Logging Servers** section, click **New**:
   - **IP Address** – Enter the management IP address of the Barracuda CloudGen Firewall F-Series.
   - **Category** – Select **user**.
   - **Logging Facility** – Select the logging facility to be able to differentiate between multiple Aruba APs.
   - **Severity** – Select **notifications**.
5. Click **Add**.
6. Click **Apply**



7. Click the **Levels** tab.
8. Set the **Logging Levels** in the **User logs** section to **notifications**.

	User logs	notifications
	all	notifications
	captive-portal	notifications
	vpn	notifications
	dot1x	notifications
	radius	notifications
	voice	notifications
	client-match	notifications
	mapc	notifications
	pan	notifications

9. Click **Apply**.

Verify that the Firewall is Receiving the Syslog Data

On the Barracuda CloudGen Firewall F-Series, go to **LOGS** and open **Box > Control > AuthService_wifiap.log**. After successfully authenticating, you will see a `logged in user  with IP` line in the log. The Wi-Fi access point name is also listed.

Box\Control\AuthService_wifiap | <new Log>

Select Log File: Box\Control\AuthService_wifiap | Reload Log File Tree

Time	Type	TZ	Message
2015 09 23 11:00:02	Info	+02:00	[config] protocol: udp
2015 09 23 11:00:02	Info	+02:00	[config] model: aerohive
2015 09 23 11:00:02	Info	+02:00	[config] source-ip: 192.168.0.37
2015 09 23 11:00:02	Info	+02:00	[config] protocol: udp
2015 09 23 11:00:02	Info	+02:00	[config] model: aruba
2015 09 23 11:00:02	Info	+02:00	[config] source-ip: 10.17.133.103
2015 09 23 11:00:02	Info	+02:00	[config] protocol: udp
2015 09 23 11:00:03	Info	+02:00	[main] listening on udp 10.17.133.1:514
2015 09 23 11:00:03	Info	+02:00	[main] listening on tcp 10.17.133.1:514
2015 09 23 11:00:03	Info	+02:00	[main] listening on ssl 10.17.133.1:6514
2015 09 23 11:00:03	Info	+02:00	[main] listening on udp 10.17.76.133:514
2015 09 23 11:00:03	Info	+02:00	[main] listening on tcp 10.17.76.133:514
2015 09 23 11:00:03	Info	+02:00	[main] listening on ssl 10.17.76.133:6514
2015 09 23 11:00:03	Info	+02:00	[main] listening on udp 192.168.0.1:514
2015 09 23 11:00:03	Info	+02:00	[main] listening on tcp 192.168.0.1:514
2015 09 23 11:00:03	Info	+02:00	[main] listening on ssl 192.168.0.1:6514
2015 09 23 11:00:33	Info	+02:00	[auth] udp:10.17.133.103 (type aruba): logged in user user2 with IP 172.17.70.32

Figures

1. aruba01.png
2. aruba_03.png
3. aruba_Logs.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.