How to Configure Wi-Fi AP Authentication

https://campus.barracuda.com/doc/23336/

The Barracuda CloudGen Firewall F-Series can parse authentication information contained in the syslog stream of supported wireless access points. Wi-Fi access points typically use authentication services such as RADIUS servers to authenticate users before allowing them to connect. The Barracuda CloudGen Firewall F-Series monitors the syslog files sent by the Wi-Fi access points for the username and the associated IP address of logged-in users. Depending on the access point, the Barracuda CloudGen Firewall F-Series receives login and/or logout information.

Supported Wi-Fi access points

- Aerohive (login only)
- Ruckus (login and logout)
- Aruba (login only)
- Aruba Instant (login only)

Video

Watch the following video to see the Barracuda CloudGen Firewall F-Series receive user information via Wi-Fi Access Point authentication from an Aerohive Access Point:

Videolink:

https://campus.barracuda.com/
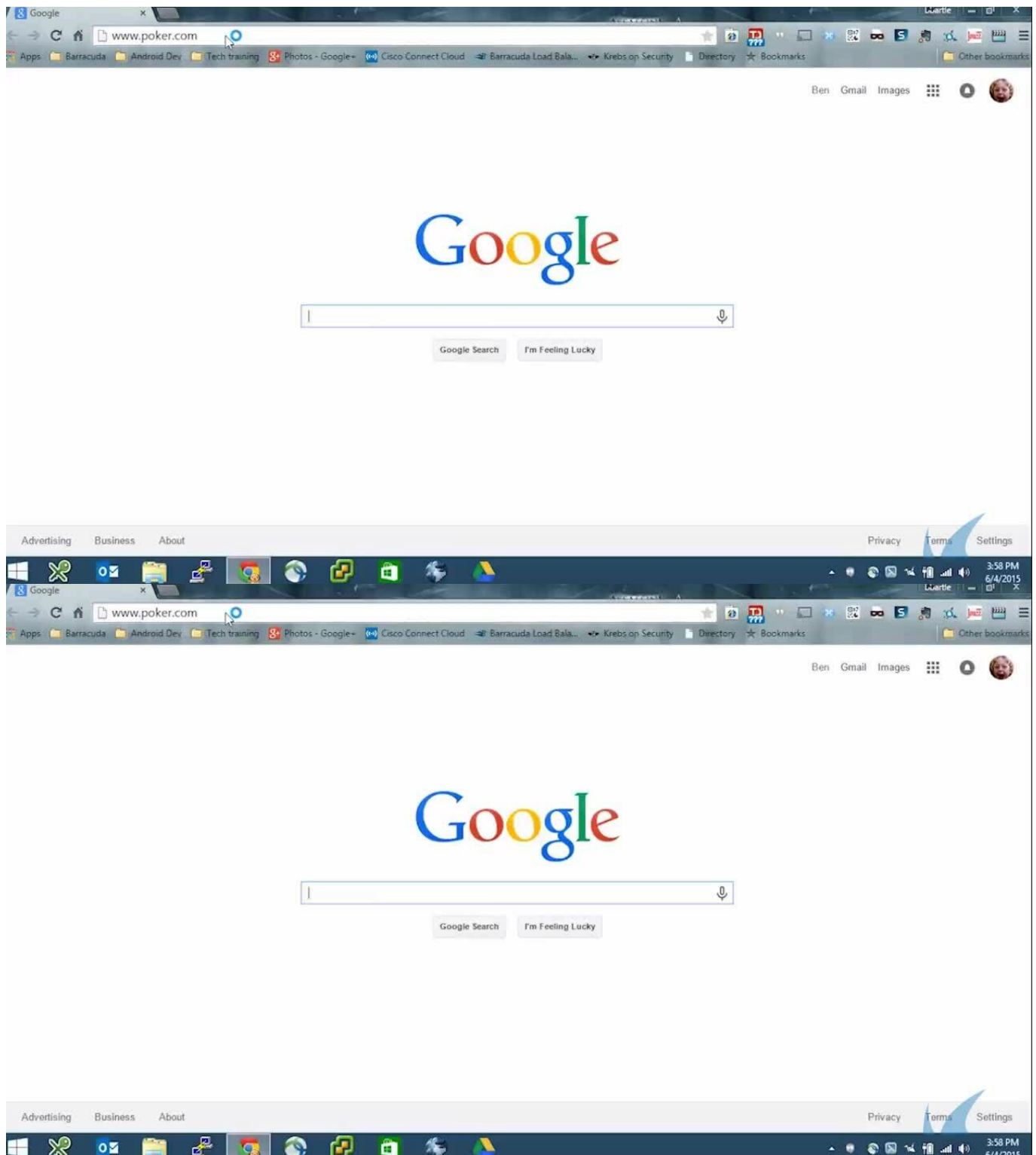
Before you Begin

Configure the Wi-Fi access point to stream the syslog to the Barracuda CloudGen Firewall F-Series. For more information, see:

- Wi-Fi AP Authentication Aerohive Configuration
- Wi-Fi AP Authentication Aruba Configuration
- Wi-Fi AP Authentication Ruckus Wireless Configuration

Step 1. Configure a Box Level IP Address

Add an IP address to the box level that can be reached by the wireless access point.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. Click **Lock**.
3. Click **+** to add an **Additional Local IP**.
4. Enter a **Name**.
5. Select the interface from the **Interface Name** drop-down list.
6. Enter the **IP Address** and **Associated Netmask**.
7. Click **OK**.
8. Click **Send Changes** and **Activate**.

Step 2. Configure Wi-Fi AP Authentication

If the Wi-Fi access point is using an SSL-encrypted connection, the certificate can be imported from a PEM or PKCS12 file. For non-standard Wi-Fi Access Point syslog streaming ports, change the port in Advanced View and edit the port in the **BOX-AUTH-WIFI-SYNC** rule accordingly.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Authentication**.
2. Click **Lock**.
3. In the left menu, click **Wi-Fi AP Authentication.**
4. Set **Activate Scheme** to **yes**.

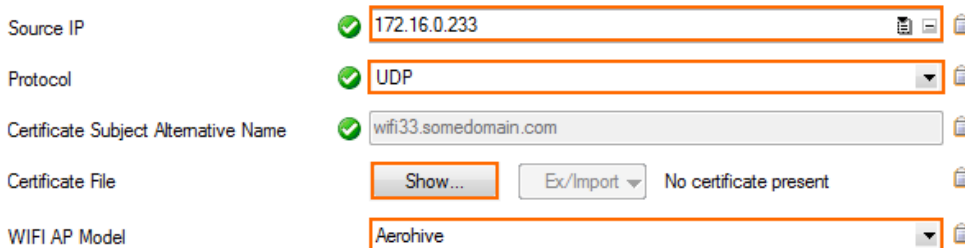5. Click **+** to add a **Wi-Fi AP Endpoint**. The **Wi-Fi AP Endpoints** window opens.
6. Enter the **Source IP**. This is the IP address of your Wi-Fi access point.
7. Select the **Protocol** used by the Wi-Fi access point to send the syslog.
    - UDP
    - TCP
    - SSL
8. (SSL only) Enter the **Certificate Subject Alternative Name** for the SSL certificate.
9. (SSL only) Click **Ex/Import** and import the **Certificate File**.
10. Select the manufacturer of your Wi-Fi access point from the **Wi-Fi AP Model** drop-down list.

11. Click **OK**.
12. Click **Send Changes** and **Activate**.

You can now use the authentication information from your Wi-Fi access point. Go to **Firewall > Users**. All users with **Wi-Fi-AP** in the **Origin** column are authenticated via the Wi-Fi access point.

Figures

3. wifi01.png
4. wifi02.png