Wi-Fi AP Authentication Aerohive Configuration

https://campus.barracuda.com/doc/53248465/

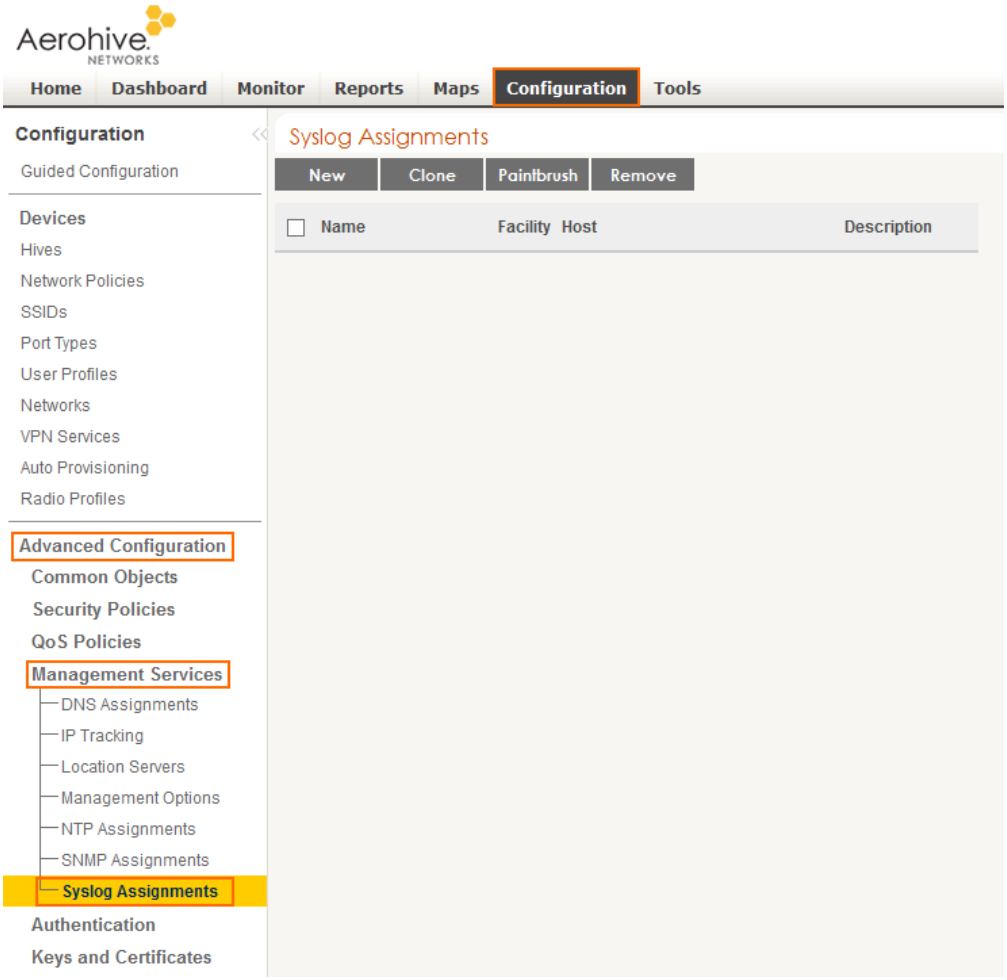
To authenticate users connected to Aerohive access points, you must stream the syslog containing the authentication data to the Barracuda NextGen Firewall F-Series.

Reference Devices/Versions:

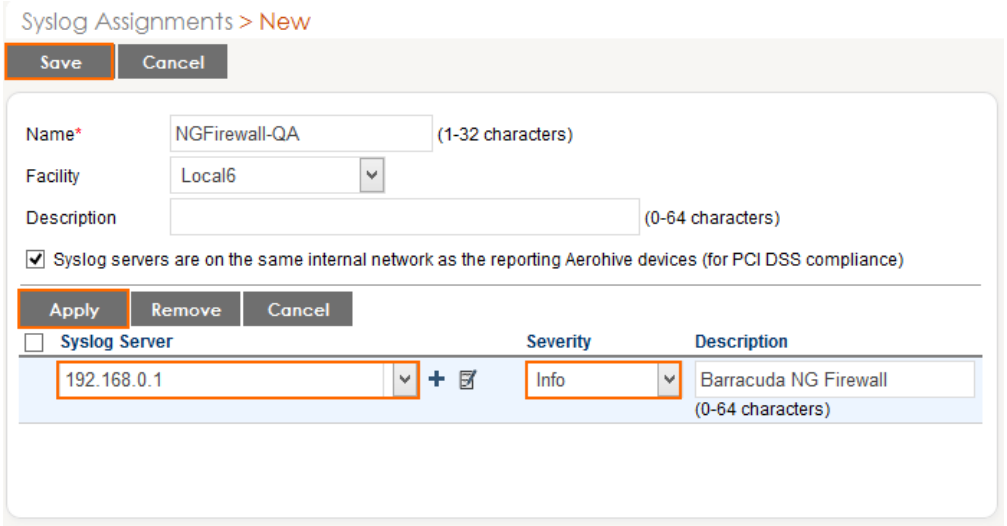
- Aerohive AP230 802.11ac Wireless AP Version 6.4r1a
- Aerohive Networks HiveManager Online 6.4r1

Step 1. Enable Syslog Streaming on the Aerohive AP

1. Log into the Aerohive Networks HiveManager.
2. Go to **Configuration > Advanced Configuration > Management Services > Syslog Assignments**.

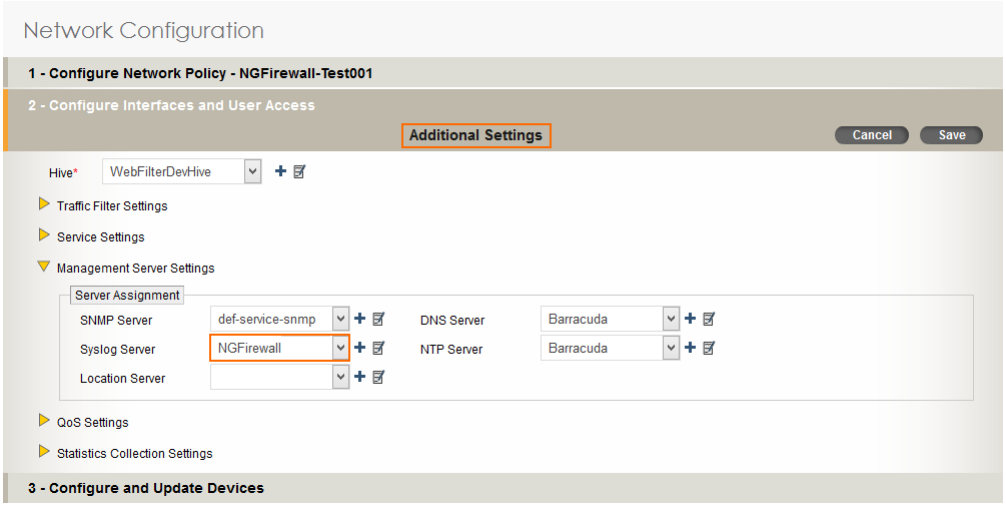


3. Click **New** and configure syslog streaming:
   - **Syslog Server** – Select the IP address of the firewall from the drop down.
   - **Severity** – Select **Info** from the drop down.
4. Click **Apply**.
5. Click **Save**.



Step 2. Add Syslog Configuration to Network Policy on the Aerohive AP

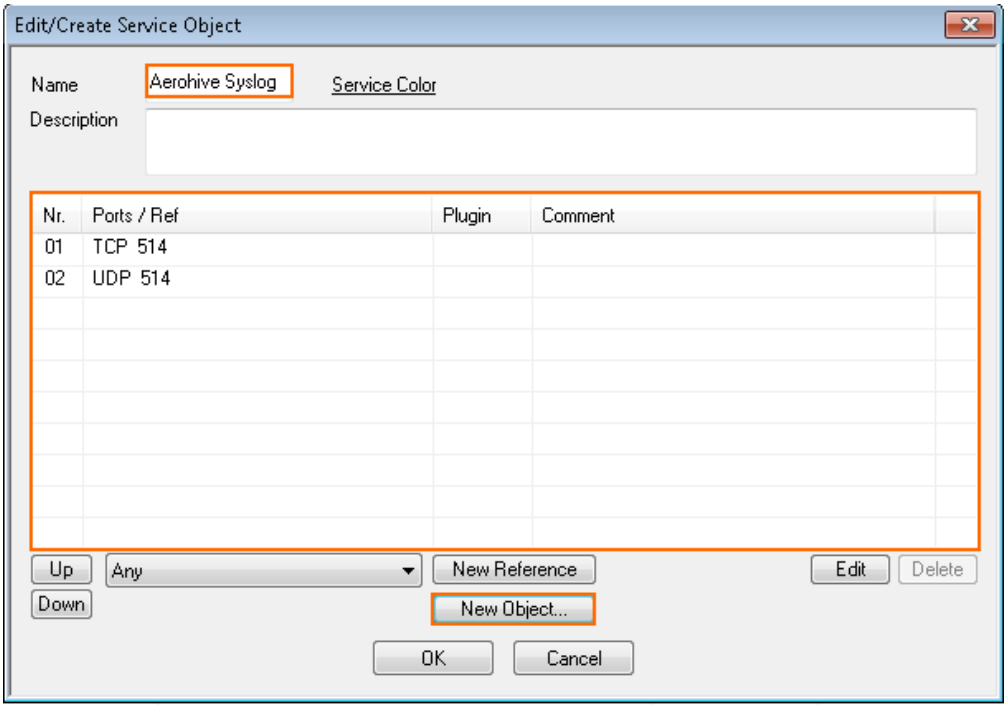
Add the syslog configuration to the **Network Policy** you are using for your access points.



Step 3. Create a Service Object for TCP 514 in Host Firewall

Create a service object for TCP 514. Do not use the **RCMD** service object, as the **rsh** firewall plugin.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Host Firewall Rules**.
2. Click **Lock**
3. In the left menu click **Services**.
4. Right-click the table and select **New**. The **Edit/Create Service Object** window opens.
5. Enter a **Name**.
6. Click **New Object**. The **Service Entry Parameters** window opens.
    - **IP Protocol** – Select **006 TCP**.
    - **Port Range** – Enter 514.
7. Click **OK**.
8. Click **New Object**. The **Service Entry Parameters** window opens.
    - **IP Protocol** – Select **017 UDP**.
    - **Port Range** – Enter 514.
9. Click **OK**.



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

Step 4. Create a Host Firewall Rule

Create a host firewall rule that matches incoming TCP/UDP 514 traffic without using the **rsh** firewall plugin.

1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Host Firewall Rules**.
2. Click **Lock**.
3. Either click the plus icon (**+**) at the top right of the rule set, or right-click the rule set and select **New > Rule**.
4. Select **Pass** as the action.
5. Enter a **name** for the rule. For example, `LAN-DMZ`.
6. Specify the following settings that must be matched by the traffic to be handled by the access rule:
   - **Source** – The source addresses of the traffic.
   - **Destination** – The destination addresses of the traffic.
   - **Service** – Select a service object, or select **Any** for this rule to match for all services.

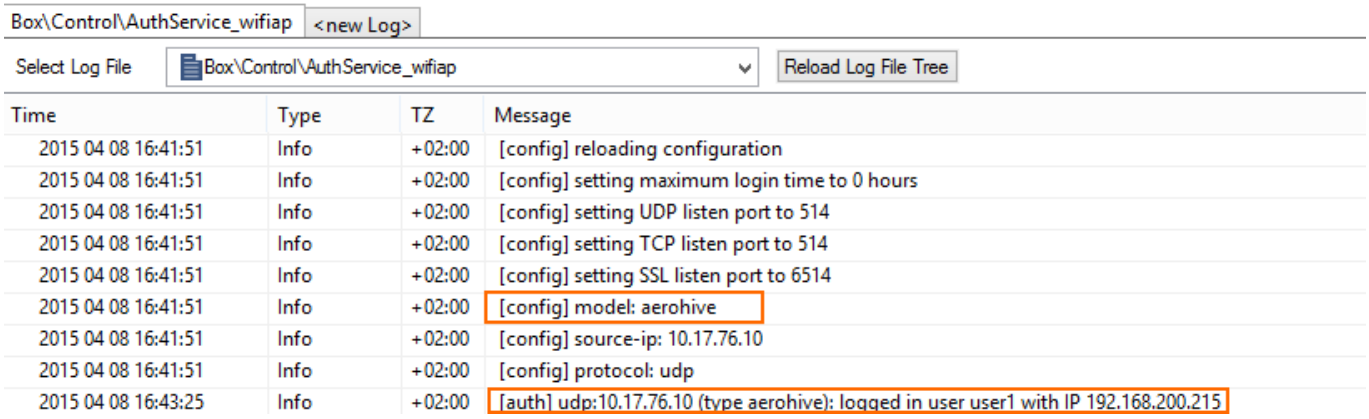
   For the example access rule displayed in the figure above, a network object named **HQ-DMZ** containing the IP address of the DMZ server has been created. For more information, see How to Create Network Objects.
7. Click **OK**.
8. Drag and drop the access rule so that it is the first rule that matches the traffic that you want it

to forward. Ensure that the rule is located *above* the BLOCKALL rule; rules located below the BLOCKALL rule are never executed.

9. Click **Send Changes** and **Activate**.

Verify that the Firewall is Receiving the Syslog Data

On the Barracuda NextGen Firewall F-Series, go to **LOGS** and open the **Box > Control > Serviceable_wifiap.log**. After a successful authentication, you will see a `logged in user <username> with IP <IP address>` line in the log. The Wi-Fi access point name is also listed.



Figures

1. aerohive01.png
2. aerohive02.png
3. aerohive03.png
4. aerohive_service_object.png
5. wifi_log_message_aerohive.png