Best Practice - Allow Aerohive Access Points Behind a CloudGen Firewall Access to Hive Manager NG

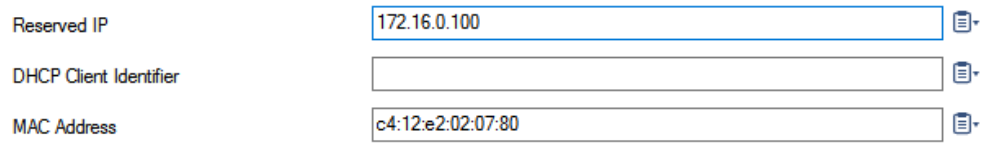
https://campus.barracuda.com/doc/22670/

Aerohive devices running HiveOS such as Aerohive Access Points must be able to communicate with either the cloud or the on-premises HiveManager NG management portal. Create access rules allowing the management traffic from the access points to the HiveManager NG. If an on-premises HiveManager NG appliance is used, the appliance must also be allowed to download firmware updates from the Aerohive cloud.

Step 1. Configure DHCP Reservations for Each AP

To ensure that the access points receive the same DHCP IP each time, configure DHCP reservations for each access point. Alternatively, it is also possible to reconfigure the Aerohive access points to use static IP addresses.

For more information, see How to Configure DHCP IP Address Reservations.



The access points are now listed with their reserved IP addresses on the **DHCP** tab:

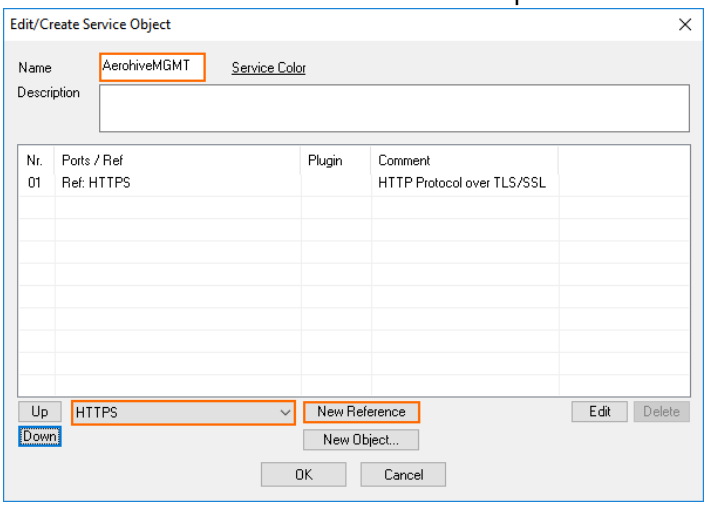
Step 2. Create Service Object for Aerohive Management Traffic

Create a service object for the communication between the access point and the Aerohive HiveManager NG.

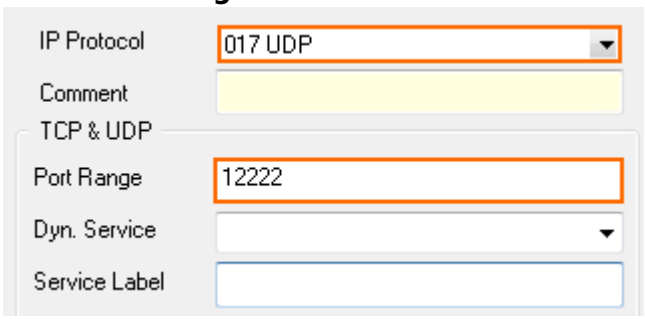
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall >**

Forwarding Rules.

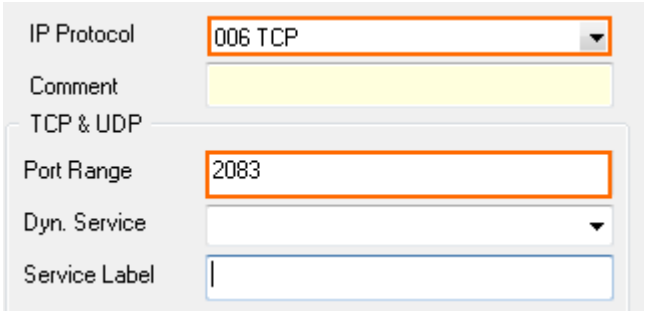
2. In the left menu, click **Services**.
3. Click **Lock**.
4. Right-click the table and select **New.** The **Edit/Create Service Object** window opens.
5. Enter the **Name**. E.g., `AerohiveMGMT`
6. Select **HTTPS** from the references drop-down list and click **New Reference**.



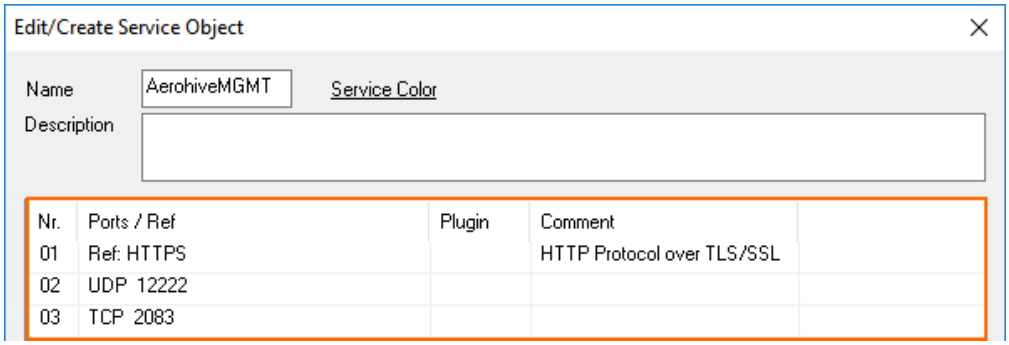
7. Click **New Object** to configure a new object. The **Service Entry Parameters** window opens.
   - **IP Protocol** – Select **017 UDP**.
   - **Port Range** – Enter 12222



8. Click **OK**.
9. Click **New Object** to configure a new object. The **Service Entry Parameters** window opens.
   - **IP Protocol** – Select **006 TCP**.
   - **Port Range** – Enter `2083`.

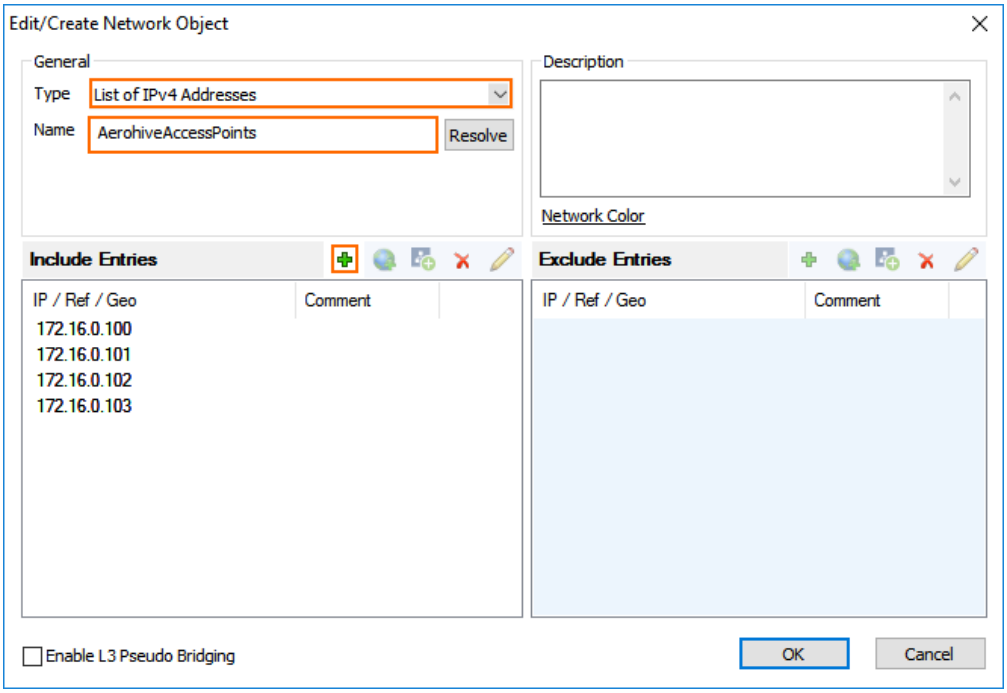


10. Click **OK**.
11. Click **OK**.
12. Click **Send Changes** and **Activate**.



Step 3. Create Network Object Containing the IP Addresses of the Access Points

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, click **Networks**.
3. Click **Lock**.
4. Right-click the table and select **New**. The **Edit/Create Network Object** window opens.
5. From the **Type** drop-down list, select **List of IPv4 Addresses**.
6. Enter a **Name** for the network object. E.g., `AerohiveAccessPoints`
7. For each access point, click **+** in the **Include Entries** section:
   1. **IP** – Enter the IP address of the access point.
   2. **Interface** (optional) – Enter the firewall interface the access point is plugged into.
   3. Click **Insert** to add additional entries, or **Insert and Close** to insert when your are done.



8. Click **OK**.

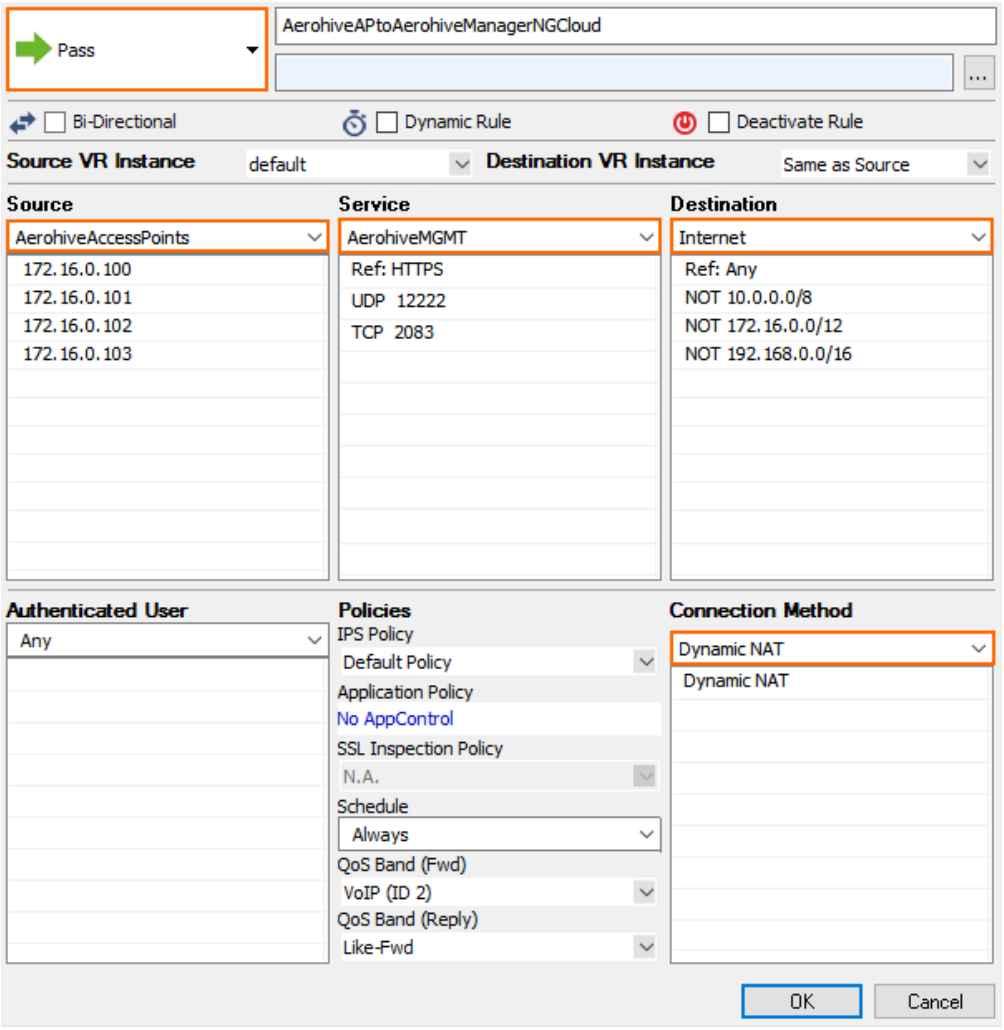
This network object must be updated if access points are removed or additional access points are

added to the network.

Step 4. Create Access Rule to Allow Traffic from the HiveOS Device to the Aerohive HiveManager NG

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Either click the plus icon (**+**) at the top right of the ruleset, or right-click the ruleset and select **New > Rule**.

4. Select **Pass** as the action.
5. Enter a **Name** for the rule.
6. Configure the access rule:
    - **Source** – Select the network object containing the Aerohive access points created in Step 3.
    - **Destination** – Select **Internet** to use Aerohive Manager NG Public Cloud, or enter the IP address of the Aerohive Manager NG appliance.
    - **Service** – Select the service object created in Step 2.
    - **Connection Method** – Select **Dynamic NAT** if you are using Aerohive Manager NG Public Cloud, or **Original Source IP** for the Aerohive Manager NG appliance.



7. Click **OK**.
8. Click **Send Changes** and **Activate**.

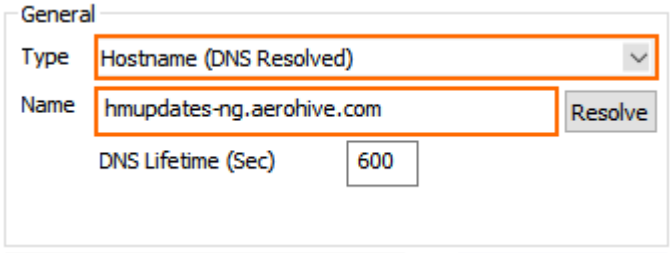
The access points can now communicate with the HiveManager NG.

Step 4. (HiveManager NG Appliance Only) Allow the HiveManager NG Appliance to Download Firmware Updates from the Update Servers

Step 4.1. Create a Hostname Network Object

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. In the left menu, click **Networks**.
3. Click **Lock**.
4. Right-click the table and select **New**. The **Edit/Create Network Object** window opens.
5. Configure the hostname network object:
   - **Type** – Select **Hostname (DNS Resolved)**.

- **Name** – Enter `hmupdates-ng.aerohive.com`

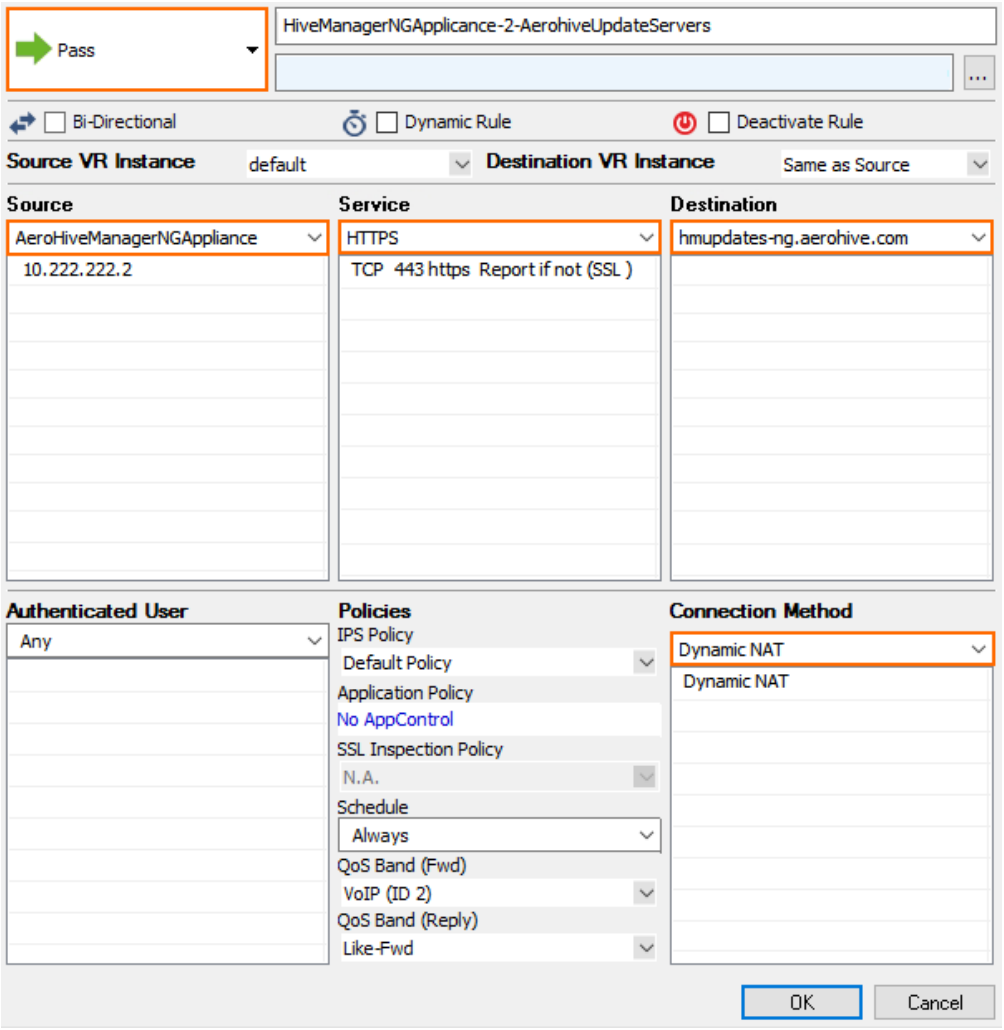


6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Step 4.2. Create an Access Rule to Allow the Appliance to Download Firmware Updates

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Either click the plus icon (**+**) at the top right of the ruleset, or right-click the ruleset and select **New > Rule**.

4. Select **Pass** as the action.
5. Enter a **Name** for the rule.
6. Configure the access rule:
   - **Source** – Enter the IP address of the Aerohive HiveManager NG appliance.
   - **Destination** – Select the hostname network object created in Step 4.1.
   - **Service** – Select **HTTPS**.
   - **Connection Method** – Select **Dynamic NAT**.



7. Click **OK**.
8. Click **Send Changes** and **Activate**.

Your Aerohive devices running HiveOS can now communicate with their on-premises or cloud HiveManager NG.

Figures

1. aerohive_00.png
2. aerohive_00a.png
3. aerohive_01.png
4. aerohive_02.png
5. aerohive_03.png
6. aerohive_04.png
7. aerohive_06.png
8. aerohive_05.png
9. aerohive_07.png
10. aerohive_08.png
11. aerohive_05.png
12. aerohive_09.png