

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

<https://campus.barracuda.com/doc/73722626/>

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](#).

Reserved IP	<input type="text" value="172.16.0.100"/>	
DHCP Client Identifier	<input type="text"/>	
MAC Address	<input type="text" value="c4:12:e2:02:07:80"/>	

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

Name	IP-Address	Start	End	Relay-ID	Hardware-Address	Hardware-Type
6 Known Client 4 Leases in 5 Ranges (1.1% Load)						
Aerohive: Known Cle... AP1	172.16.0.100				c4:12:e2:02:07:80	ethernet
Aerohive: Pool	1 of 101 Leases - 1.0% used	172.16.0.100	172.16.0.200			

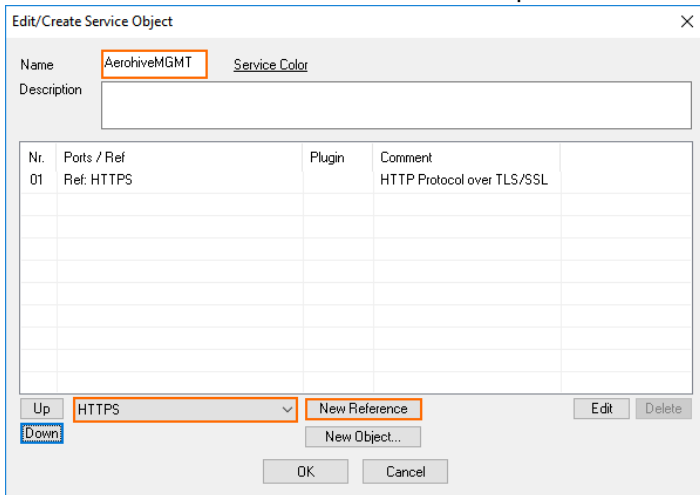
Step 2. Create Service Object for Aerohive Management Traffic

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

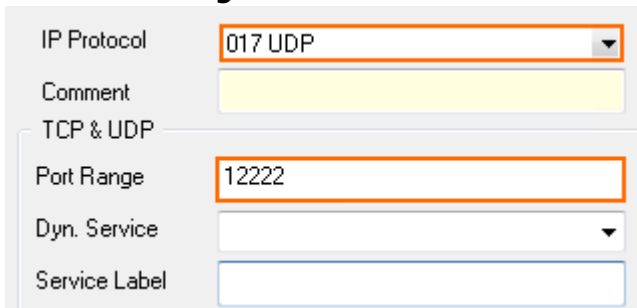
1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual**

server > Assigned Services > Firewall > Forwarding Rules.

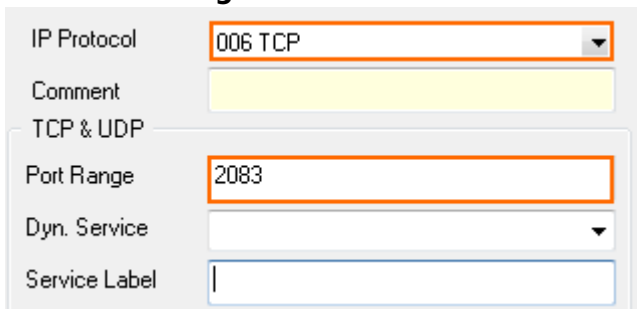
2. In the left menu, click **Services**.
3. Click **Lock**.
4. Right-click the table and select **New**. The **Edit/Create Service Object** window opens.
5. Enter the **Name**. E.g., AerohiveMGMT
6. Select **HTTPS** from the references drop-down list and click **New Reference**.



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



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



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

Edit/Create Service Object ✕

Name Service Color

Description

Nr.	Ports / Ref	Plugin	Comment
01	Ref: HTTPS		HTTP Protocol over TLS/SSL
02	UDP 12222		
03	TCP 2083		

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

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > 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 you are done.

Edit/Create Network Object ✕

General

Type

Name Resolve

Description

Network Color

Include Entries + 🌐 📄 ✕ ✎

IP / Ref / Geo	Comment
172.16.0.100	
172.16.0.101	
172.16.0.102	
172.16.0.103	

Exclude Entries + 🌐 📄 ✕ ✎

IP / Ref / Geo	Comment

Enable L3 Pseudo Bridging


OK Cancel

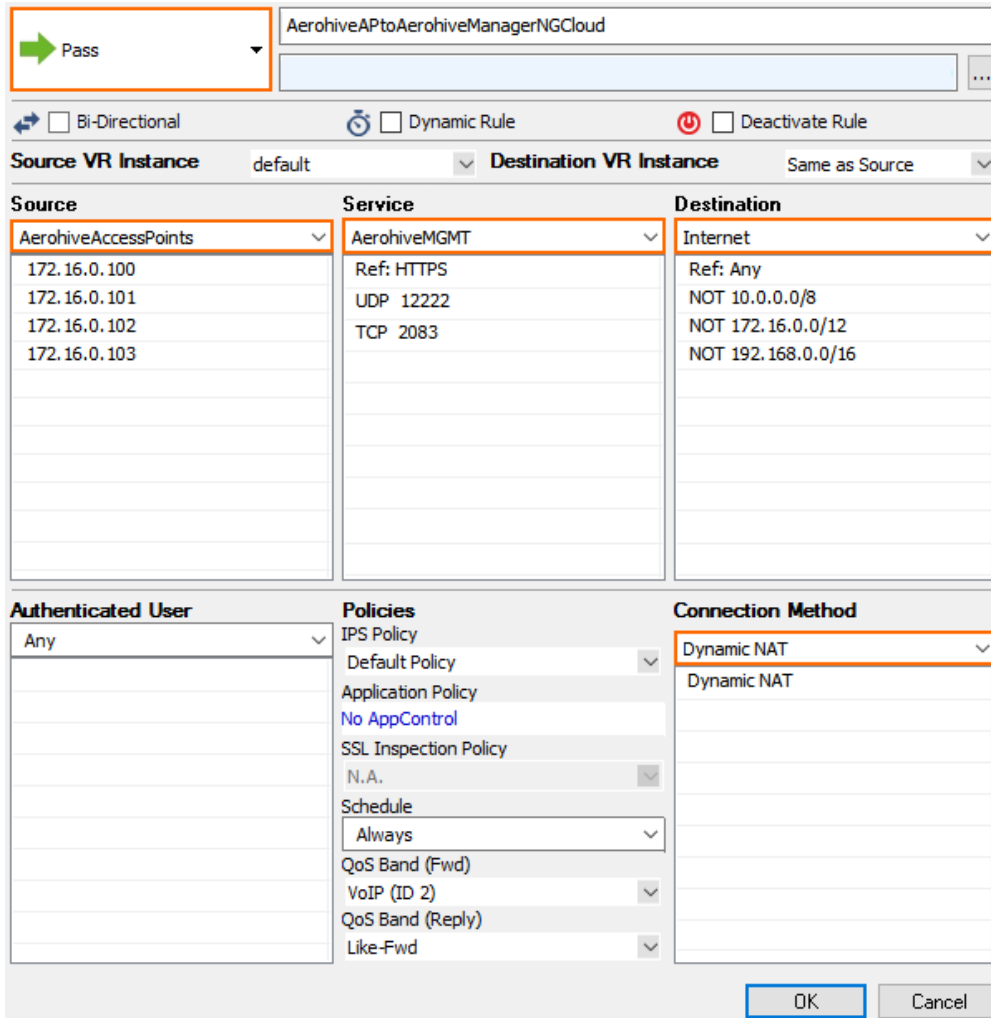
8. Click **OK**.

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 > Virtual Servers > your virtual server > 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.



Pass Bi-Directional Dynamic Rule Deactivate Rule

Source VR Instance: default Destination VR Instance: Same as Source

Source	Service	Destination
AerohiveAccessPoints	AerohiveMGMT	Internet
172.16.0.100	Ref: HTTPS	Ref: Any
172.16.0.101	UDP 12222	NOT 10.0.0.0/8
172.16.0.102	TCP 2083	NOT 172.16.0.0/12
172.16.0.103		NOT 192.168.0.0/16

Authenticated User	Policies	Connection Method
Any	IPS Policy: Default Policy	Dynamic NAT
	Application Policy: No AppControl	Dynamic NAT
	SSL Inspection Policy: N.A.	
	Schedule: Always	
	QoS Band (Fwd):	
	VoIP (ID 2):	
	QoS Band (Reply):	
	Like-Fwd:	

OK Cancel

- Click **OK**.
- Click **Send Changes** and **Activate**.

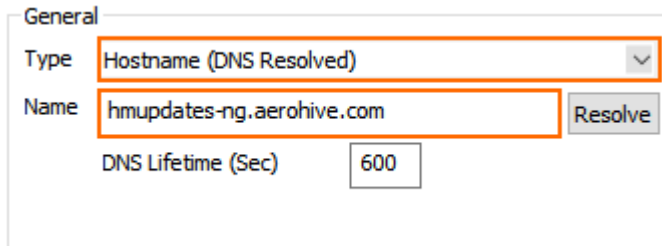
The access points can now communicate with the HiveManager NG.

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

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

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



General


Type: Hostname (DNS Resolved) ▼

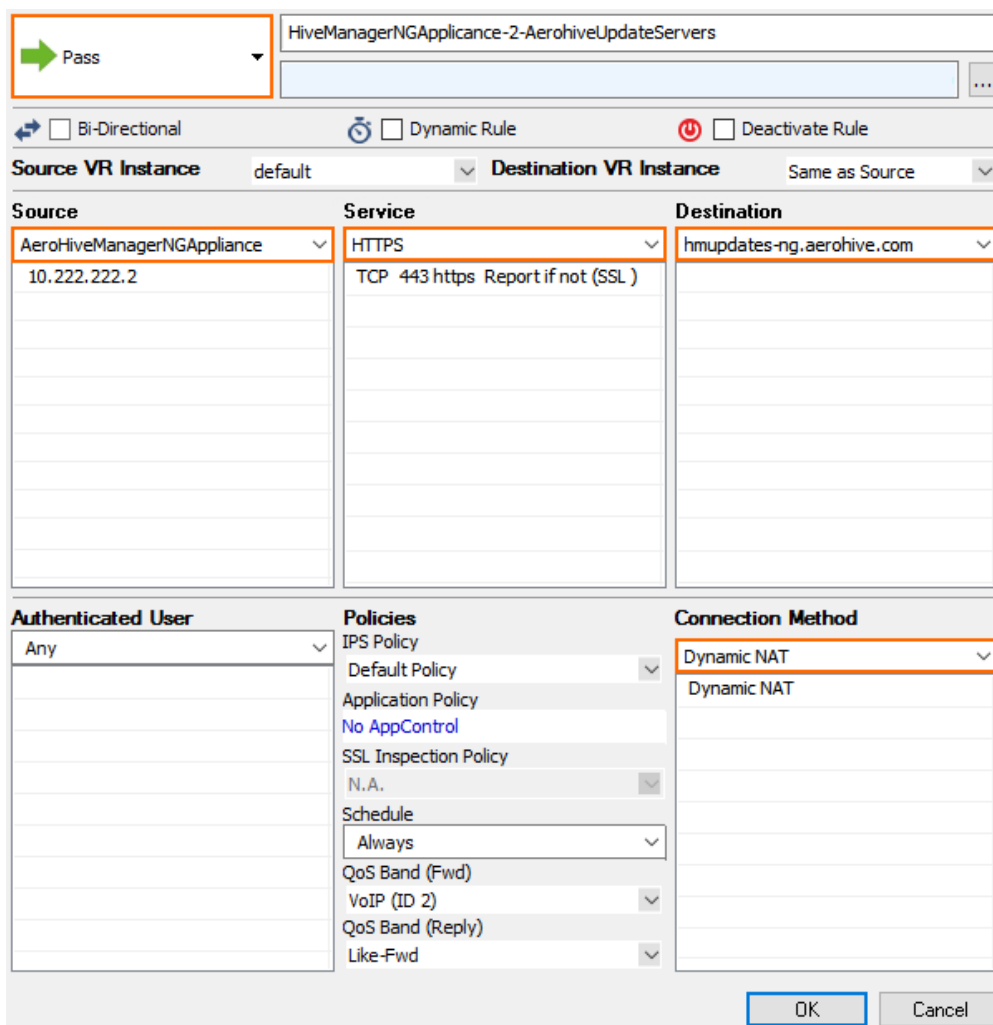
Name: hmupdates-ng.aerohive.com

DNS Lifetime (Sec): 600

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 > Virtual Servers > your virtual server > 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**.



HiveManagerNGAppliance-2-AerohiveUpdateServers

Pass

Bi-Directional Dynamic Rule Deactivate Rule

Source VR Instance: default Destination VR Instance: Same as Source

Source	Service	Destination
AeroHiveManagerNGAppliance 10.222.222.2	HTTPS TCP 443 https Report if not (SSL)	hmupdates-ng.aerohive.com

Authenticated User	Policies	Connection Method
Any	IPS Policy Default Policy Application Policy No AppControl SSL Inspection Policy N.A. Schedule Always QoS Band (Fwd) VoIP (ID 2) QoS Band (Reply) Like-Fwd	Dynamic NAT Dynamic NAT

OK Cancel

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

© Barracuda Networks Inc., 2019 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.