How to Configure the SNMP Service

https://campus.barracuda.com/doc/79463281/

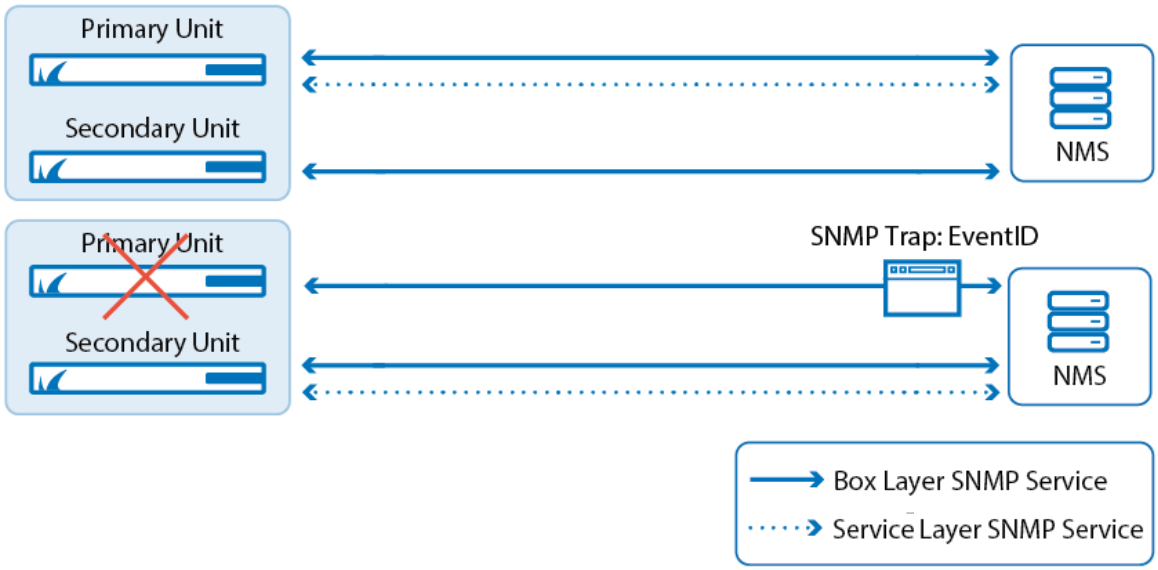
Use the SNMP service to remotely monitor the network and system state of a Barracuda CloudGen Firewall using a network management system (NMS). The SNMP service organizes system information in the form of a Management Information Base (MIB). The MIB contains modules that each contain related objects (OIDs). The OIDs can be queried and in some cases set by the NMS.

An NMS monitors system and network performance for network attached devices. It gathers information from the Barracuda CloudGen Firewall by periodically polling the SNMP services. For important events, you can configure the Barracuda CloudGen Firewall to send SNMP traps to immediately alert the NMS. Further action is dependent on the configuration of the NMS. Usually, the NMS polls a predefined list of objects that are related to the event, classifies the event, and if needed, notifies the administrators about the event. For example, If the system temperature is too high, the NMS polls the fan speeds, system load, and all temperature related OIDs.

On the Barracuda CloudGen Firewall the SNMP service can be installed on the box and the service layer, depending on what the NMS must monitor:

- SNMP Service on the Box layer – By default, the SNMP service runs on the box layer of every Barracuda CloudGen Firewall. SNMP as an infrastructure service on the box layer provides hardware and system information such as fan speeds, temperatures, and system load. In a high availability (HA) setup, running the SNMP service on the box layer permits both units to provide SNMP information. The SNMP service listens on the management IP address.
- SNMP Service on the Service layer – On the firewall's service layer, the SNMP service monitors infrastructure information such as the number and health of the VPN tunnels. In an HA setup, only the active unit is polled. When a HA handover is performed, the SNMP service switches to the HA unit with the services that it monitors; this allows the service layer SNMP service to always be on the same physical unit that the services it monitors are running on.

Follow the instructions in this article to configure the SNMP service and traps. Depending on which SNMP version is supported by the NMS, you can configure SNMPv1 / SNMPv2c or SNMPv3.



Before You Begin

An SNMP service is running on the box layer of every CloudGen Firewall. If you want to use an SNMP service on the firewall's service layer, you must first create the SNMP service.

Configure SNMPv1/SNMPv2c

For SNMPv1 and SNMP v2c, specify the IP addresses and ranges of the SNMP peers that are allowed to receive SNMP information.

1. Open the **SNMP Service Settings** page.

Layer	Path to SNMP Service Settings Page
Box	**CONFIGURATION > Full Configuration > Box > Infrastructure Services > SNMP Service Settings**
Services	**CONFIGURATION > Full Configuration > Box > Assigned Services > SNMP-Service > SNMP Service Settings**

2. In the **SNMP Settings** section, enter the location and contact information for the appliance.
3. In the **SNMPv1 / SNMPv2c Access Groups** section, select **Yes** from the **Use SNMPv1 / SNMPv2c** list.
4. Next to the **Access Groups** table, click the plus sign (**+**) to add an access group.
5. In the **Access Groups** window, enter a name for the access group and then click **OK**.
6. In the **Peers** table, add SNMP peers.
    1. Click the plus sign (**+**) to add an SNMP peer.

2. Enter a name for the peer.
3. In the **Peers** window, specify these settings:
   - **IPv4/IPv6 Address/Mask** – Enter the IP address or range for the peers that are allowed to access the SNMP service.
     For security reasons the SNMP Service will not accept a peer IP address of `0.0.0.0`. Use a specific IP address or range.
   - **Community** – Enter the string that is used to authenticate the peer for SNMPv2c access.
4. Click **OK**.

7. In the **View** table, define access restrictions to specific MIB modules.
   1. Click the plus sign (**+**).
   2. To specify the monitoring view, select one of the following values:
      - **-ALL-** – Allows access to all available MIB modules.
      - **system** – Restricts access to the MIB module "system".
      - **interfaces** – Restricts access to the MIB module "interfaces".
      - **at** – Restricts access to the MIB module "address translation table".
      - **ip** – Restricts access to the MIB module "ip".
8. Click **Send Changes** and **Activate**.

Configure SNMPv3

For SNMPv3, specify the passwords for the users who are allowed to receive SNMP information. The connection is encrypted with AES-128 and SHA-1 ciphers. Passwords can consist of small and capital characters, numbers, and non alpha-numeric symbols, except the hash sign (#).

1. Open the **SNMP Service Settings** page.

Layer	Path to SNMP Service Settings Page
Box	**CONFIGURATION > Configuration Tree > Box > Infrastructure Services > SNMP Service Settings**
Services	**CONFIGURATION > Configuration Tree > Box > Assigned Services > SNMP-Service > SNMP Service Settings**

2. Click **Lock**.
3. In the **SNMP Settings** section, enter the location and contact information for the appliance.
4. In the **SNMPv3 Users** section, select **Yes** from the **Use SNMPv3** list.
5. In the **Users** table, add the users who are allowed to access the SNMP service.
   1. Click the plus sign (**+**) to add a user.
   2. Enter the username and click **OK**.
   3. In the **Users** window, specify these settings:
      - **Authentication Password** – Enter the password used to authenticate this SNMPv3 user. This password must be at least 8 characters long.
      - **Encryption Password** – Enter the password used for SNMPv3 encryption for this user.
   4. Click **OK**.

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

Configure Events to Send SNMP Traps

To configure an event to send SNMP traps to the NMS:

1. Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > Eventing**.
2. Click **Lock**.
3. Click the **Notification** tab.
4. Double-click the notification that you want to send the SNMP trap (e.g., **notification 3**).
5. In the **Detail** window, under the **Server Action** tab, select the **Enable** check box.
6. From the **Type** list, select **3 SNMP**.
7. Specify the following settings for the SNMP trap:
   - **Destination** – Enter the IP address of the NMS. By default, the destination is set to the local broadcast address (255.255.255.255).
   - **Spec Type** – You can choose to select the **Use Event ID** check box or specify a custom **Spec Type**.
   - **Community** – If the SNMP destination is an SNMPv1 or SNMPv2c device, enter the community ID. Only SNMP traps with the correct community string are accepted by the NMS.
8. Click **OK**.
9. Click **Send Changes** and **Activate**.

Figures