DOCUMENT

Flowroute to Avaya IP Office Port Forwarding on SonicWall v6.5.1.3

DATE

February 25, 2019

REVIEWED BY

David

PROCEDURE

There are five steps to set up port forwarding:

1. Create address objects for the Avaya IP Office and Flowroute WAN IPs
2. Create an address group for Flowroute WAN IPs
3. Create a service object
4. Create an inbound and outbound NAT policy
5. Create a firewall access rule

Step 1: Create necessary Address Objects by going to Manage -> Policies -> Objects -> Address Objects

1. Along the top of the screen, ensure "Address Objects" is selected, change the view to "Custom" and click the "Add" button.

2. In the window that opens:

   a. Name: Enter a friendly name and put the IP address in parenthesis (this comes in handy in the future)
   i.e. "Avaya IP Office (10.11.22.200)"

   b. Zone Assignment: Choose the "LAN" zone, as the phone system resides in the LAN

   c. Type: Choose "Host" as it has a single LAN IP

   d. IP Address: Enter the LAN IP address of the Avaya IP Office.

   e. Click "Add". After you click "Add", the window will remain open. Keep this open to create additional address objects.

(Step 1 continued on next page)

3. Create address objects for Flowroute's Public IPs. This information is subject to change, so you should check flowroute.com to verify the information below is up to date.

Address Object 1:

- Name: Flowroute WAN 1
- Zone Assignment: WAN
- Type: Network
- Network: 147.75.65.192
- Netmask/Prefix Length: 255.255.255.240
- Click "Add"

After you click on "Add" the Address Object will be created, but the window will remain open. You can add the additional three address objects below by simply making the necessary changes to the window and clicking "add".

Address Object 2:

- Name: Flowroute WAN 2
- Zone Assignment: WAN
- Type: Network
- Network: 147.75.60.160
- Netmask/Prefix Length: 255.255.255.240
- Click "Add"

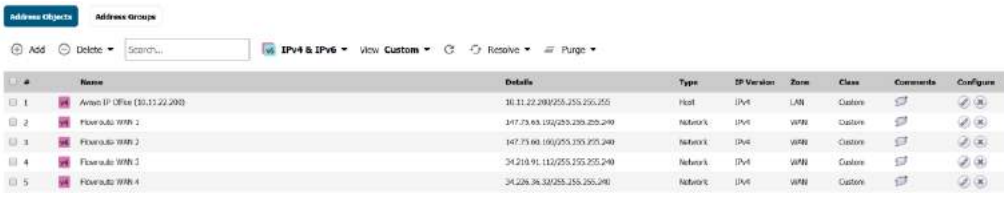
Address Object 3:

- Name: Flowroute WAN 3
- Zone Assignment: WAN
- Type: Network
- Network: 34.210.91.112
- Netmask/Prefix Length: 255.255.255.240
- Click "Add"

Address Object 4:

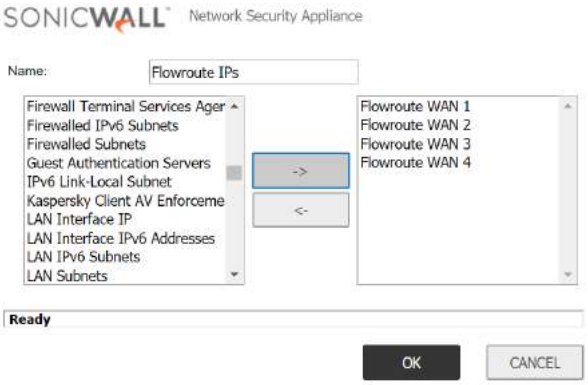
- Name: Flowroute WAN 4
- Zone Assignment: WAN
- Type: Network
- Network: 34.226.36.32
- Netmask/Prefix Length: 255.255.255.240
- Click "Add" and then "Close".

After you click "Close" in the previous step, you will see a window with the address objects you created. Triple check your work!



Step 2: Create an Address Group by click on the “Address Groups” Button and then click on “Add”.

1. In the window that opens:
    a. Name: “Flowroute IP’s”
    b. Find the Flowroute Address Objects created in the previous step and “move” them to the “In Group” column.
    c. Click “OK”



Step 3: Create a Service Object by going to Manage -> Policies -> Objects -> Service Objects

1. Along the top of the screen, ensure “Service Objects” is selected. Change the view to “Custom”, and click “Add”.

2. In the window that opens:
    a. Name: “SIP - UDP 5060”
    b. Protocol: “UDP(17)”
    c. Port Range: “5060” – “5060”
    d. Click “Add”.

3. The “Service Object” Window will remain open. Create an additional “Service Object” as follows:

    a. Name: “Avaya IP Office Audio”
    b. Protocol: “UDP(17)”
    c. Port Range: 46750-50750
    d. Click “Add” and “Close”

    Critical Note: The port range is a value set by Avaya within the IP Office Manager under “System -> LAN 1 -> VoIP -> RTP” and should be verified before going in to production.

Step 4: Create a NAT policy by going to Manage -> Policies -> Rules -> NAT Policy

1. Along the top of the screen change the “View” to “Custom” and click “Add”.

2. In the Window that opens:

   a. Name: This is optional, and a suitable name would be “Flowroute to Avaya Inbound”

   b. Original Source: “Flowroute IPs” (This is the name you created in Step 2.1)

   c. Translated Source: “Original”.

   d. Original Destination: “All WAN IP”

   e. Translated Destination: “Avaya IP Office” (This is the address object you created in Step 1.2)

   f. Original Service: “SIP – UDP 5060” (This is the service object you created in Step 3.2)

   g. Translated Service: “Original”.

   h. Inbound Interface: “Any”

   i. Outbound Interface: “Any”.

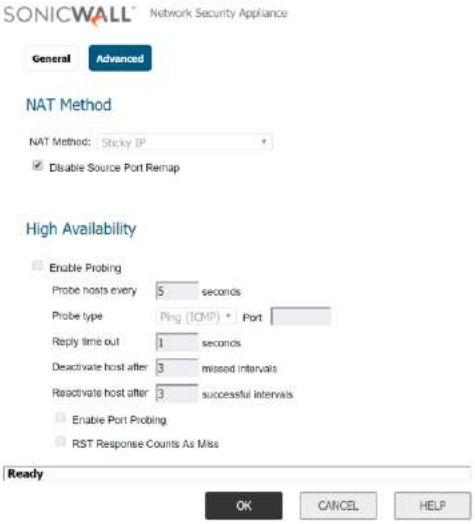
   j. Place a check mark (enable) “Create a reflexive policy”.

   k. Click “Add” and then “Close”.

3. You will be returned to the list of NAT policies. You will see two policies that reference the Avaya IP Office. Find the policy with the “Source Original” as “Avaya IP Office” and click the edit icon.

   Click the “Advanced” button and place a check mark (enable) “Disable Source Port Remap” and click “OK”.

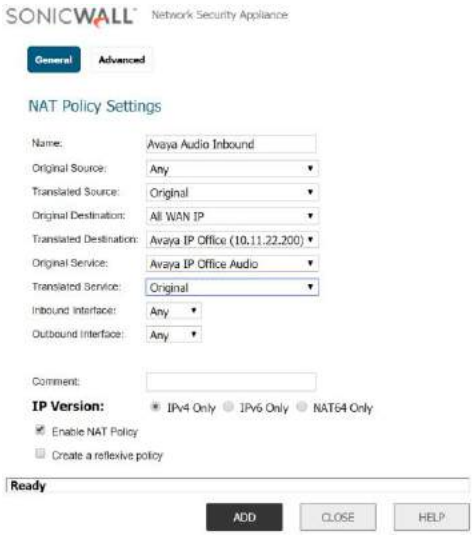
   You will be returned to the list of NAT policies.



(Continue to the next page).

4. Along the top of the screen click “Add” to create another NAT Policy.

   In the Window that opens:



   a. Name: This is optional, and a suitable name would be “Avaya Audio Inbound”

   b. Original Source: “Any”

   c. Translated Source: “Original”.

   d. Original Destination: “All WAN IP”

   e. Translated Destination: “Avaya IP Office” (This is the address object you created in Step 1.2)

   f. Original Service: “Avaya IP Office Audio” (This is the service object you created in Step 3.3)

   g. Translated Service: “Original”.

   h. Inbound Interface: “Any”

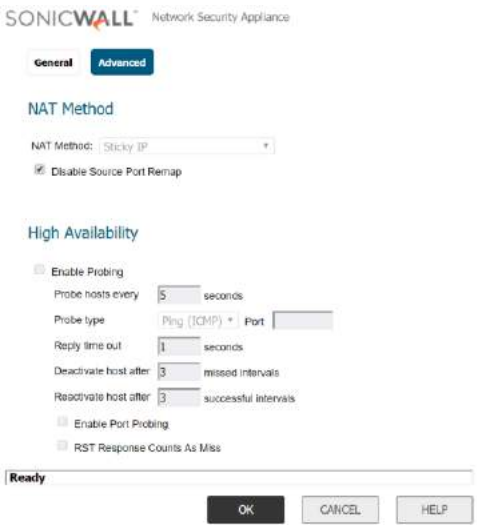
   i. Outbound Interface: “Any”.

   j. Place a check mark (enable) “Create a reflexive policy”. **(Skip for SonicWALL Firmware 6.2.x)**

   k. Click “Add” and then “Close”.

(Skip this step for SonicWALL Firmware 6.2.x)

5. You will be returned to the list of NAT policies. You will see two policies that reference the Avaya IP Office Audio. Find the policy with the “Source Original” as “Avaya IP Office” and click the edit icon.

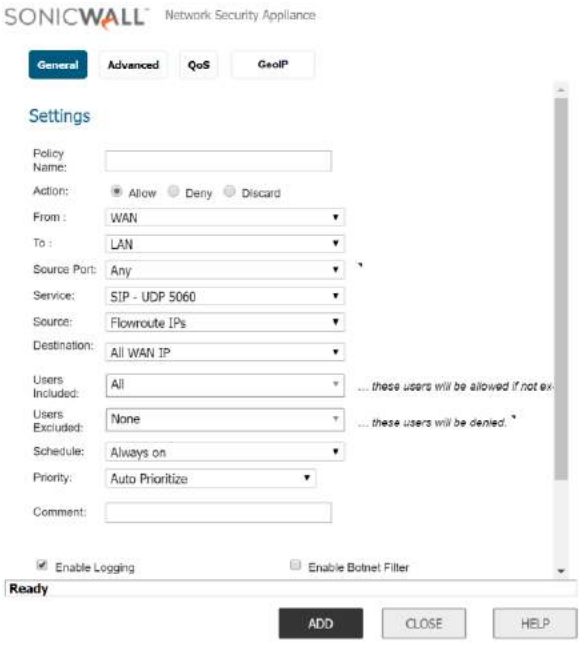


   a. Click the “Advanced” button and place a check mark (enable) “Disable Source Port Remap” and click “OK”.

Step 5: Create an Access Rule by going to Manage -> Policies -> Rules -> Access Rules

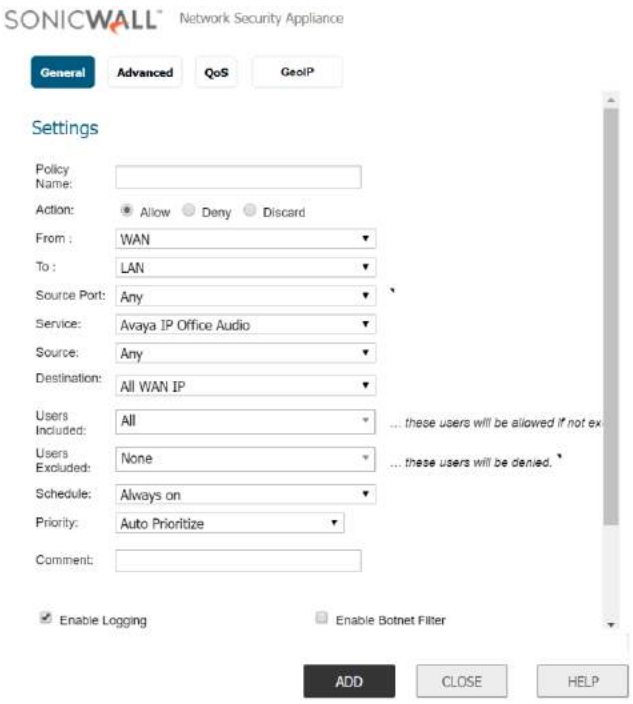
1. Along the top of the screen change the “From” to “WAN”, the “To” to “LAN”, the “View” to “Custom” and click “Add”.

2. In the Window that Opens:



   a. From: WAN (prepopulated)
   b. To: LAN (prepopulated)
   c. Source Port: “Any”
   d. Service: “SIP – UDP 5060” (This is the service object you created in Step 3.2).
   e. Source: “Flowroute IPs” (This is the service group you created in Step 2.1).
   f. Destination: “All WAN IP”
   g. Users Included: Generally “All”.
   h. Users Excluded: Generally “None”
   i. Schedule: Generally “Always On”
   j. All other options are generally left at default.
   k. Click “Add”.

3. The Access Policy Window will remain open. Modify the values to create an additional Access Policy as follows:



   a. From: WAN (prepopulated)
   b. To: LAN (prepopulated)
   c. Source Port: “Any”
   d. Service: “Avaya IP Office Audio” (This is the service object you created in Step 3.3).
   e. Source: “Any”
   f. Destination: “All WAN IP”
   g. Users Included: Generally “All”.
   h. Users Excluded: Generally “None”
   i. Schedule: Generally “Always On”
   j. All other options are generally left at default.
   k. Click “Add” and Close.