RSA® NETWITNESS® Packets Implementation Guide

Garland Technology EdgeLens® 9.2.1

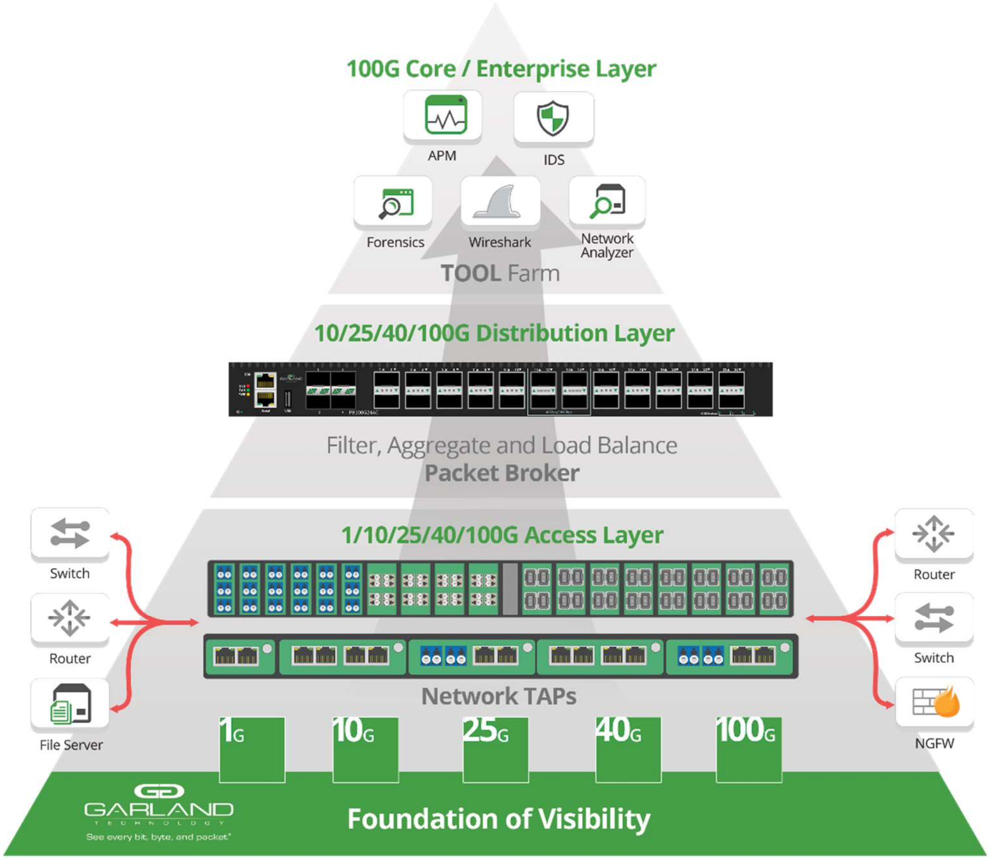
Daniel R. Pintal, RSA Partner Engineering

Last Modified: December 19, 2018

Solution Summary

Garland Technology provides the industry's most reliable and economical test access point (TAP) solutions. Paired with the RSA NetWitness Suite, Analysts have a clear vision of their network by providing the security operations staff with the means to hunt and remediate threats within the network.

RSA NetWitness Tested Features	
Garland EdgeLens 9.2.1	
Flow / Traffic Mapping	Yes
De-duplication	No



Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Garland Technologies EdgeLens with RSA NetWitness. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

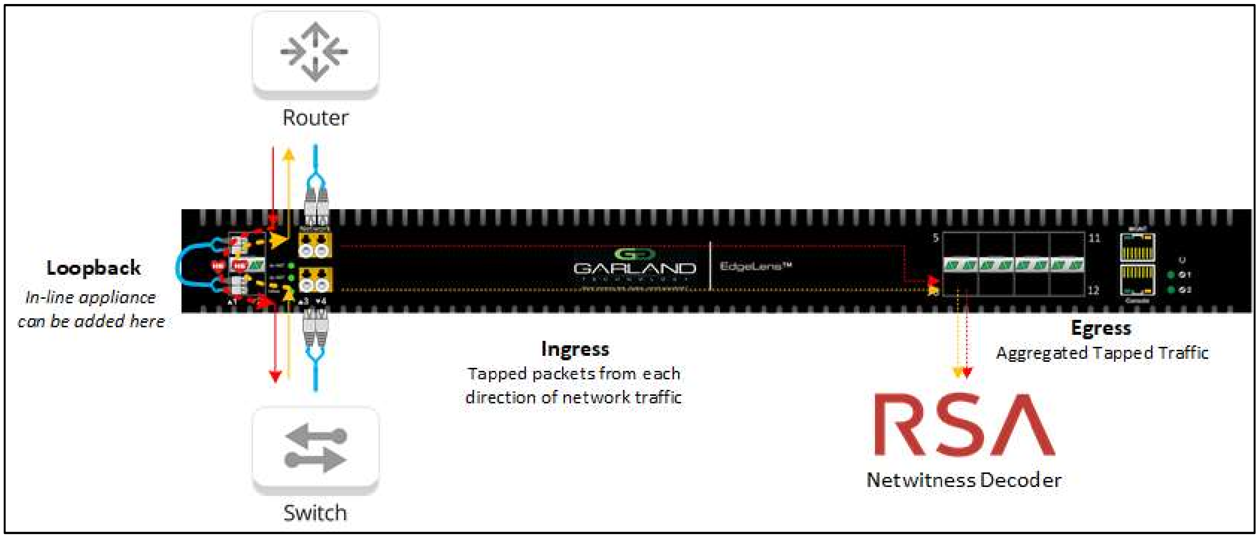
All Garland Technologies EdgeLens components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

! Important: The configuration shown in this Implementation Guide is for example and testing purposes only. It is not intended to be the optimal setup for the device. It is recommended that customers make sure Garland Technologies EdgeLens is properly configured and secured before deploying to a production environment. For more information, please refer to the Garland Technologies EdgeLens documentation or website.

Garland Technologies EdgeLens Configuration

Deployment Design Overview

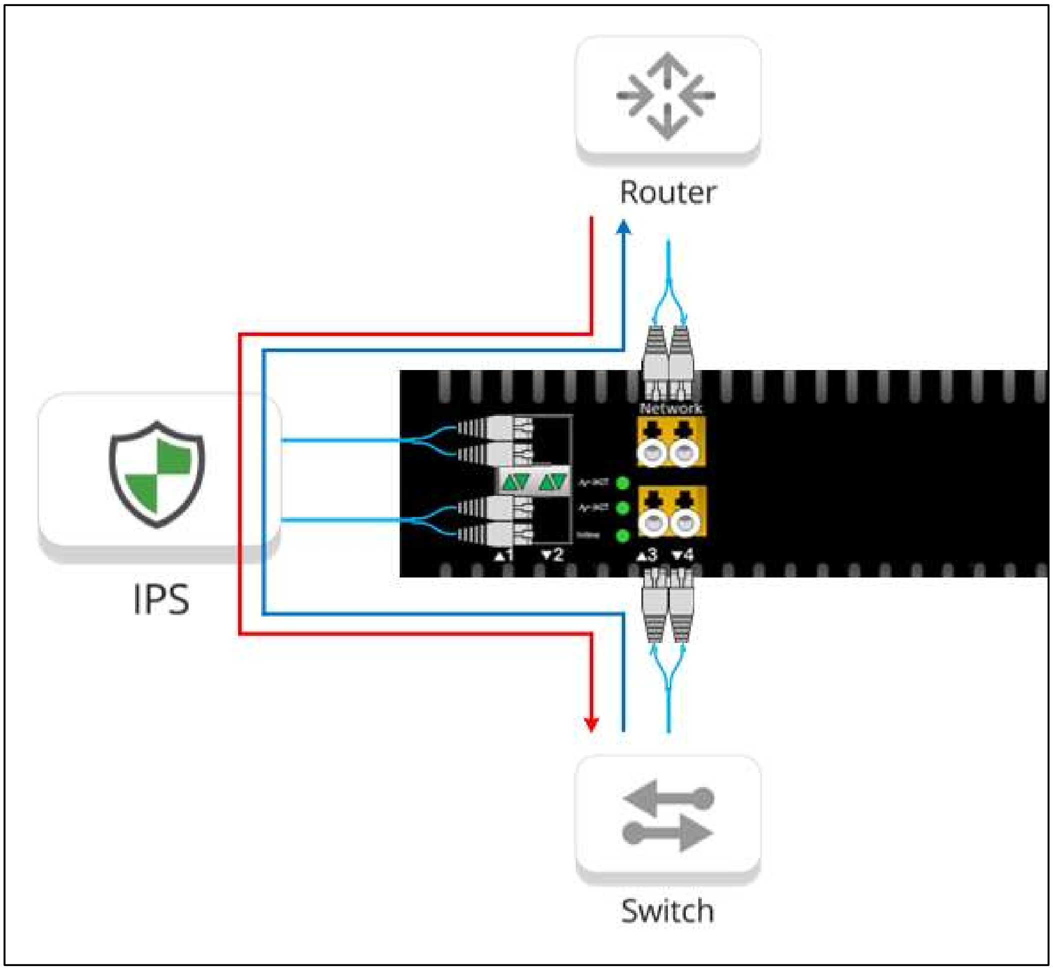
This section provides instructions for setting up the Single Segment EdgeLens (INT10G2SRBP10SFP+) to aggregate tapped North and Southbound production traffic and egress the monitor traffic over to the RSA NetWitness Decoder.


Router
Loopback
In-line appliance can be added here
GARLAND
EdgeLens™
Ingress
Tapped packets from each direction of network traffic
Egress
Aggregated Tapped Traffic
RSA
Netwitness Decoder
Switch

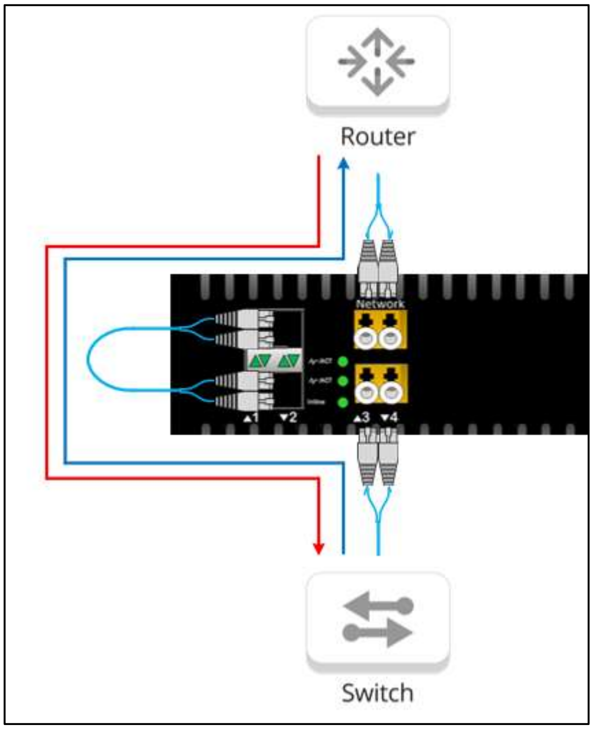
Connecting the Network Interfaces

The INT10G2SRBP10SFP+ EdgeLens has a Bypass Tap built into the chassis. The Bypass Tap is designed to fit in-line between two (2) network devices and redirect the traffic over to an in-line appliance that can be placed physically out-of-band.

The Bypass Tap removes the in-line tool as a point of failure within the network. The Bypass Monitor Ports will inject a heartbeat packet that will pass through the inline appliance and get stripped off on receipt by the adjacent Bypass Monitor Port. If this heartbeat fails to return, then the Network Ports will fail open, allowing network traffic to continue flowing around the un-responsive in-line appliance.

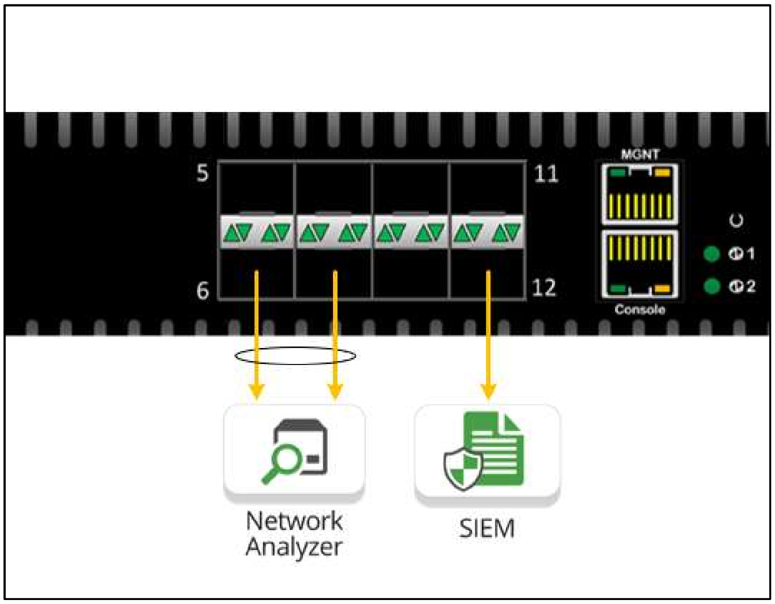


For the sake of this integration, the monitor ports will be looped together by cabling the two together. In an actual environment, these monitor ports would connect directly to an appliance that needs to sit in-line with the traffic flow. Having the monitor ports connected will allow the heartbeats to pass through and keep the link up and running:

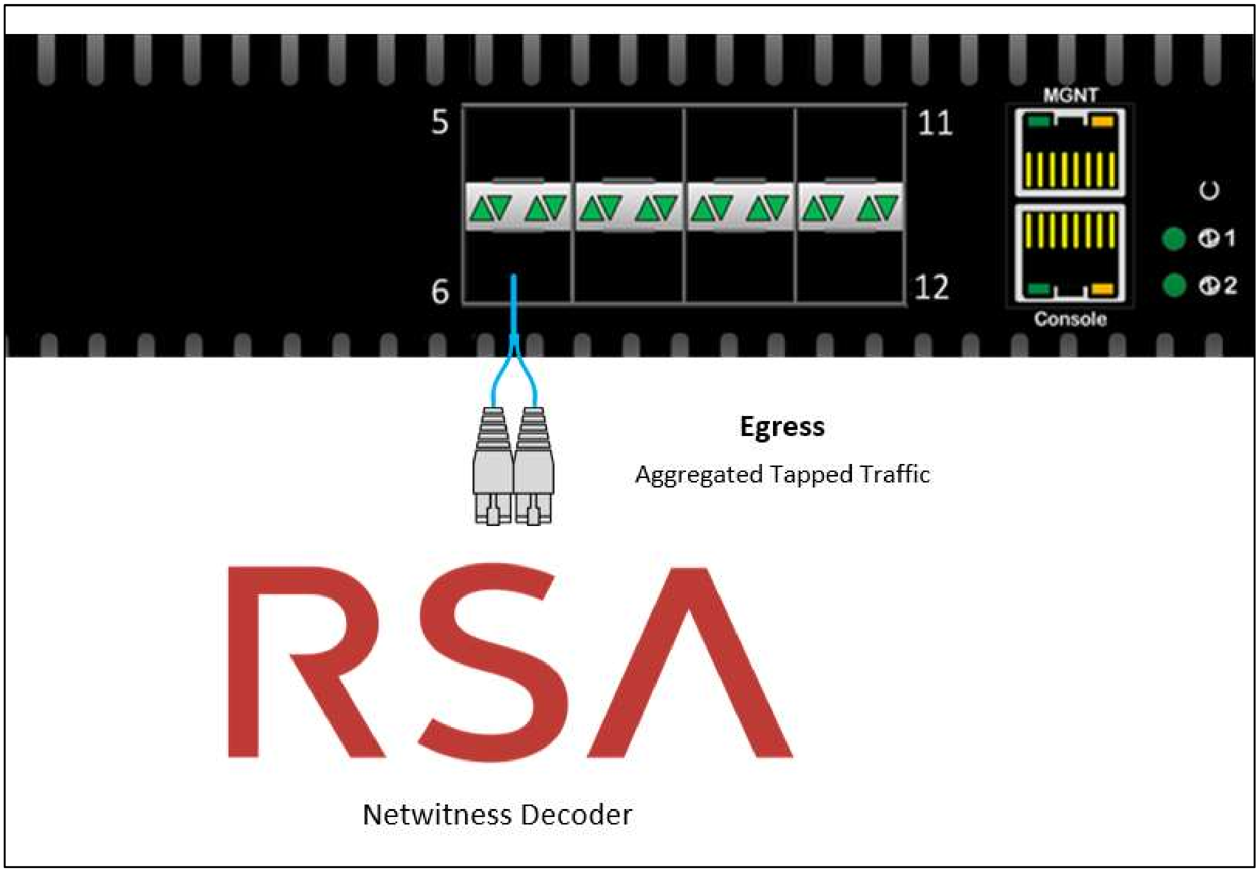


Connecting the Monitor Interfaces

On the opposite side of integrated Bypass Taps are a set of eight (8) 1/10G SFP+ packet broker monitor ports. These ports are used to egress monitor traffic. Filtering, Aggregation, and Load Balancing are supported on these packet broker monitor ports.



During this integration, one (1) of these packet broker monitor ports will be cabled into a virtual machine running RSA NetWitness Packet Decoder using a port that is set to **Promiscuous Mode**. For the sake of this integration, use Port 6 to connect the EdgeLens to the RSA NetWitness Packet Decoder.



Configuring the Management IP of the EdgeLens

With the physical connections made, the next step is to set up the EdgeLens for configuration. The default management IP address for the EdgeLens is **10.1.1.1** but can initially be set through the CLI by using the serial port and a terminal emulation software like PuTTy.

To connect a computer using a serial connection:

1. Open the terminal emulation software and use the below settings to establish a connection:
   - Bits per second: **115200**
   - Data bits: **8**
   - Parity: **None**
   - Stop: **1**
   - Flow Control: **None**
2. Use the following credentials to log in to the device under the Administrator account:
   - User name: **root**
   - Password: **gtroot1**
3. After logging in, a device prompt will display on the screen: **Switch#>**
   1. To configure the Management Web GUI IP address, use the following CLI commands:

      ```
      end
      configure terminal
      interface cpu0
      ip address {<ip_address> <subnet_mask>}
      ```

   2. Set the gateway IP address with the following com m ands.

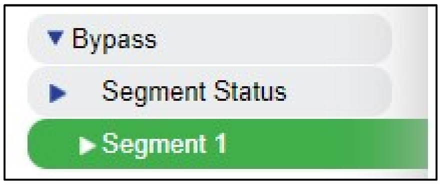
      ```
      end
      configure terminal
      ip route 0.0.0.0 0.0.0.0 <gateway_ip>
      ```

   3. The Management Web GUI can now be accessed by entering the Management IP address into a Chrome or Firefox web browser and using the following credentials:

      ```
      User name: root
      Password: gtroot1
      ```

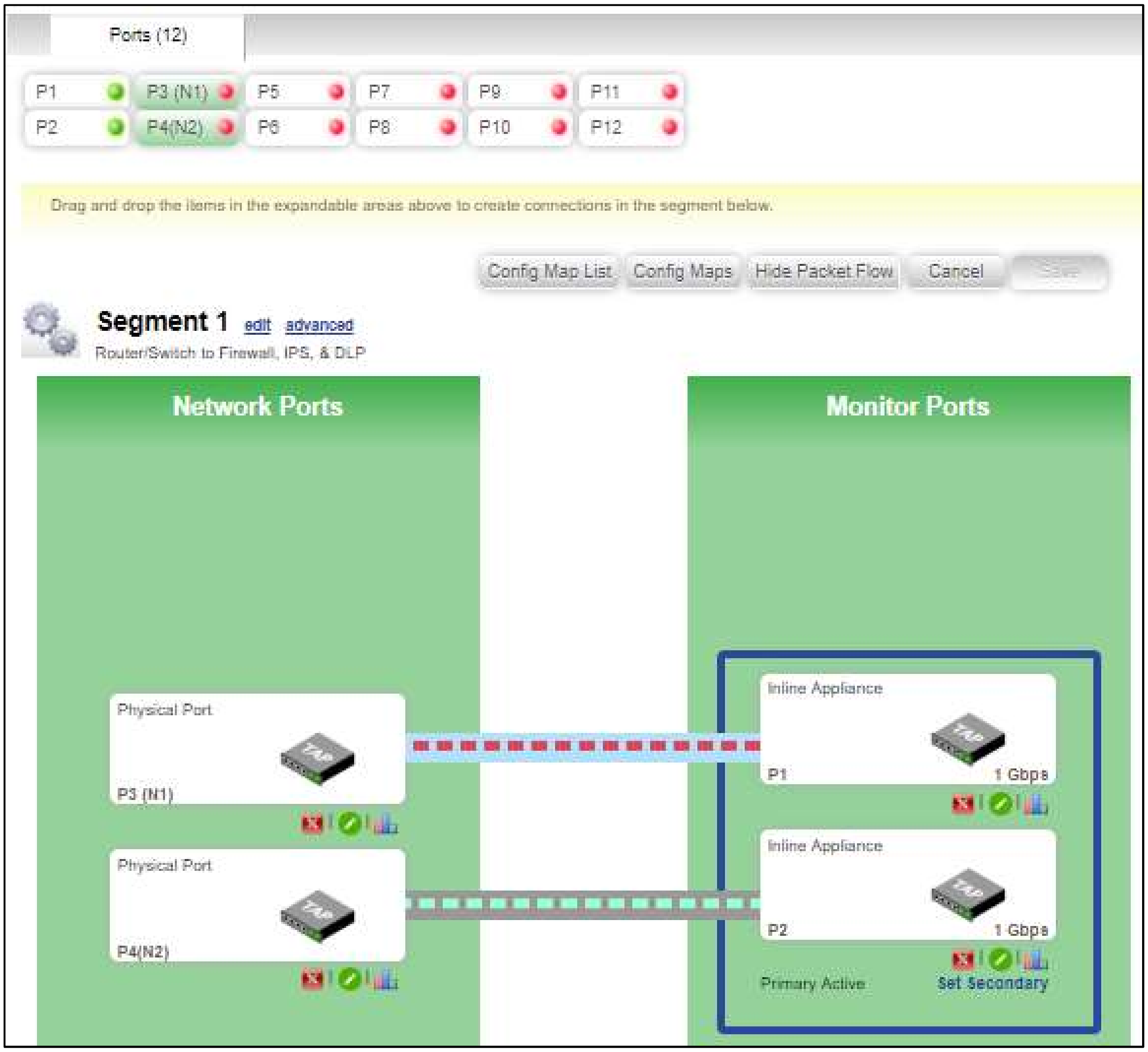
Configuring Bypass Segments

To configure the Bypass Taps on the EdgeLens, look on the left side of the Management Web GUI for a menu. Locate the section in the menu called **Bypass** and expand it out to show **Segment Status** with **Segment 1**.



This will display a screen that shows the current configuration of the bypass taps. By default, the bypass segments should already be configured for each group of fixed LC ports and their corresponding SFP+ ports residing on their immediately left.

Bypass Segment configurations will allow the tapped traffic going into the fixed LC ports to be directed to the monitor ports, allowing traffic to flow through the in-line appliance. No additional changes should be needed to have traffic pass through the EdgeLens.

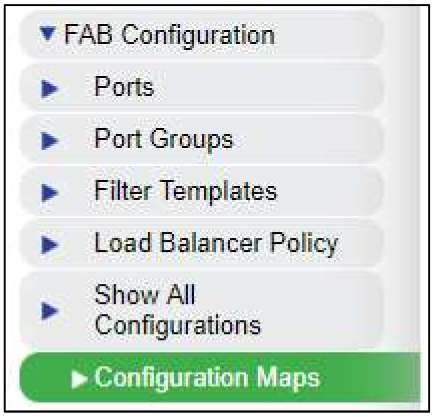


Drag and drop the items in the expandable areas above to create connections in the segment below.

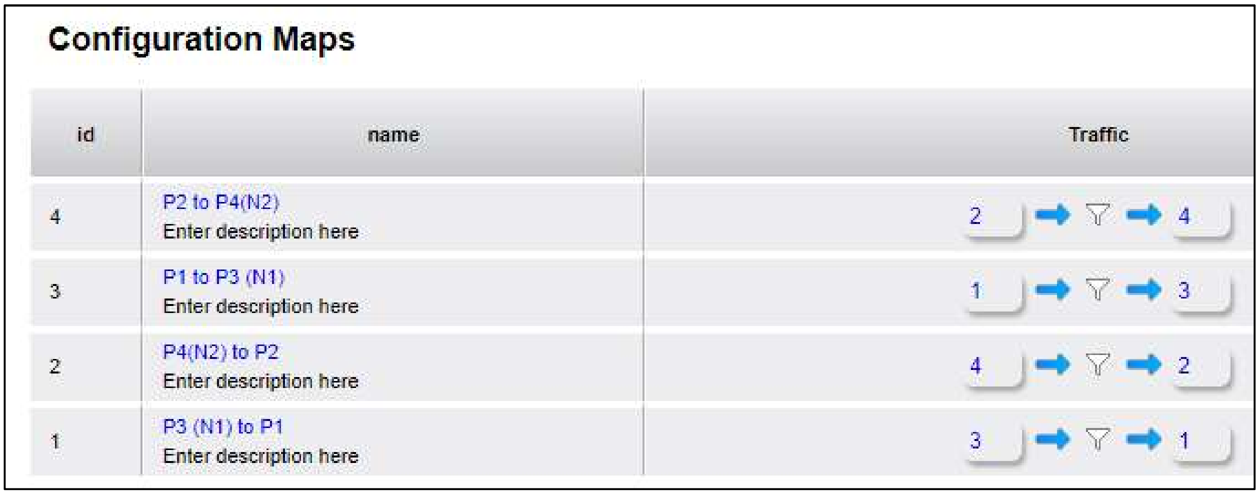
Segment 1 edit advanced
Router/Switch to Firewall, IPS, & DLP

Configuring Packet Broker Ports

To configure the Packet Broker ports on the EdgeLens, look on the left side of the Management Web GUI for the section in the menu called **FAB Configuration** and expand it out to show **Configuration Maps**.



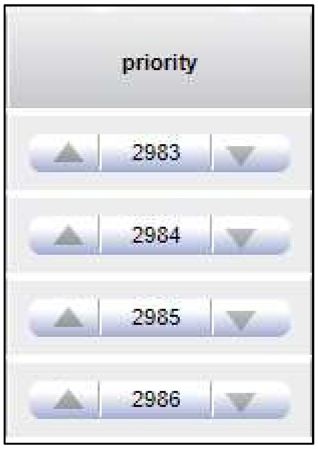
This will display all the port mapping configurations on the EdgeLens, including the port maps used for the Bypass segments which were automatically created:



Configuration Maps

id	name	Traffic
4	P2 to P4(N2) Enter description here	2 → ▽ → 4
3	P1 to P3 (N1) Enter description here	1 → ▽ → 3
2	P4(N2) to P2 Enter description here	4 → ▽ → 2
1	P3 (N1) to P1 Enter description here	3 → ▽ → 1

On the right-hand side of this table is a column called **Priority**.



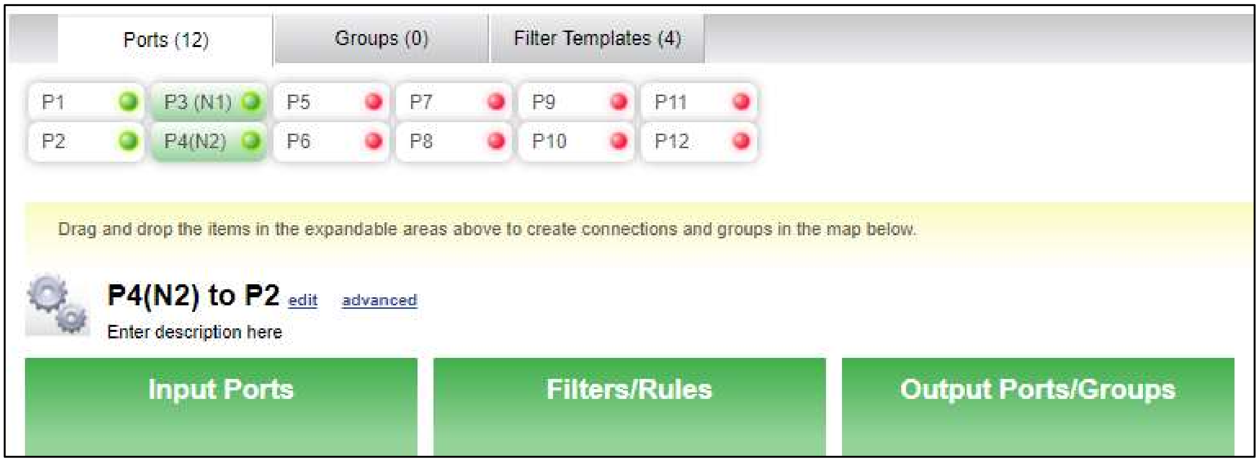
These numbers work in a top-down fashion where the lower number of priority gets processed first. As soon as incoming traffic matches a map the traffic is forwarded, and the processing stops. Any configuration maps after the map that the traffic mapped with will not be evaluated.

For this integration, we want the traffic to be directed to the both inline appliance and out a packet broker port to an out-of-band appliance: the NetWitness Packet Decoder.

To create this port map, click on the map labeled **P4 (N2) to P2** to highlight the map that evaluates traffic that comes into the lower network interface. Then, click **Edit** in the top right corner. A new screen will display that will be used to configure port maps.

In this screen, the available ports and their numbers will display at the top of the screen with either a Green or Red dot that indicates if the port has link or not.

Below these ports are three panes labeled **Input Ports**, **Filters/Rules**, and **Output Ports/Groups**. These panes are used to build the Port Map Configuration.



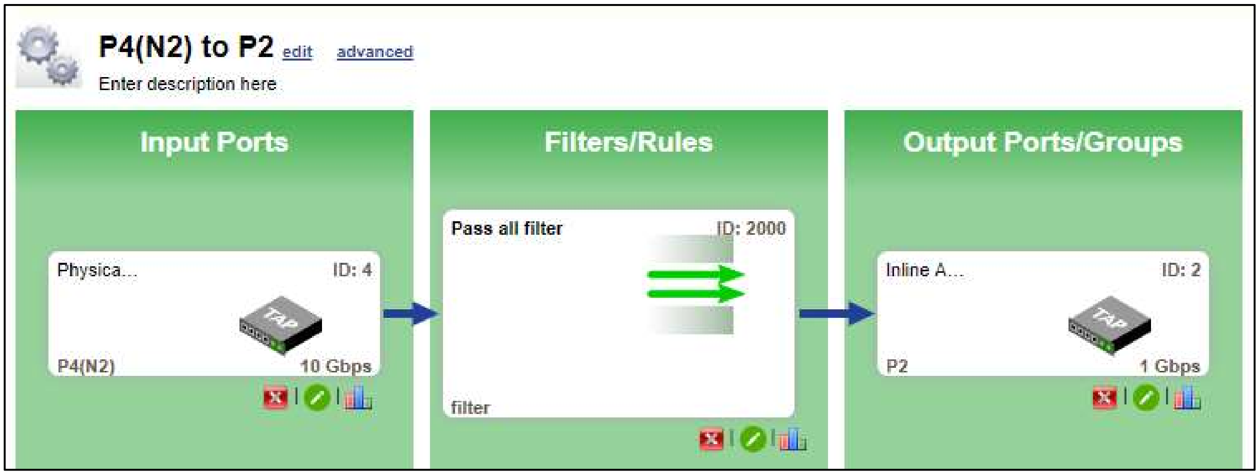
Drag and drop the items in the expandable areas above to create connections and groups in the map below.

P4(N2) to P2 edit advanced

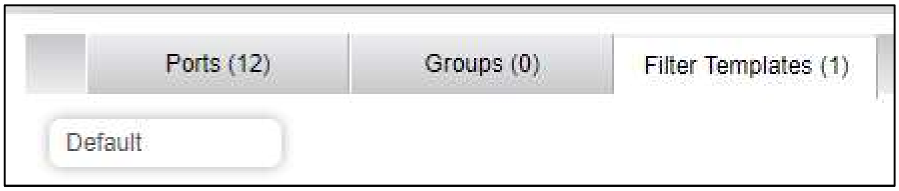
Enter description here

Configuring Maps on the EdgeLens is an interactive, drag-and-drop process of grabbing the port from the top and pulling it down to the pane that corresponds to how you want the traffic to flow through the ports: In (Input Ports) or out (Output Ports/Groups).

Ingress ports will only capture traffic that is coming **IN** to the port. Even though the other direction of traffic may be sent out of the port, it won't be captured. Since this specific map was automatically configured from the bypass segment, the P4(N2) ingress port is already in place and nothing will need to be done.



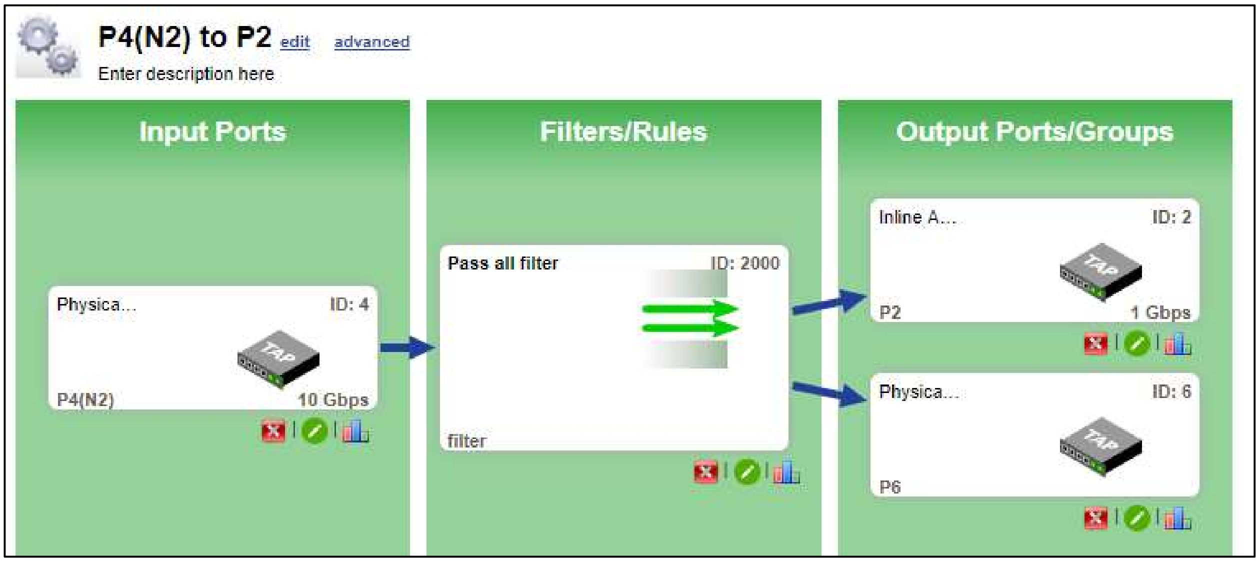
The next step is to insert a filter to use. At the top of page, there are tabs for Ports, Groups, and Filter Templates. Select the **Filter Templates** tab.



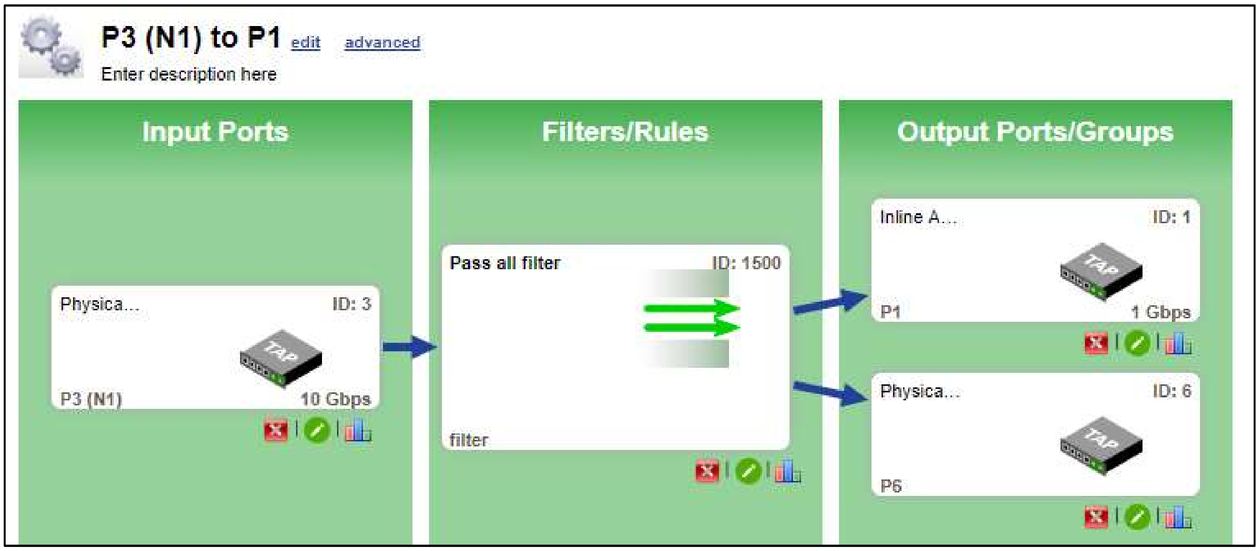
The Default filter is a pass-all filter. Since this configuration map was automatically generated, the pass all filter will already be in place and nothing will need to be changed.

The last step is to choose a port to egress traffic out of to the network tool. Port 2 is already in place from the Bypass segment map and will send the traffic to the inline tool. In this integration, we will want a second copy of the ingress traffic sent out a separate port to the NetWitness Packet Decoder.

At the top, click back to the **Ports** tab. From here, drag a port down to the **Output Ports/Groups** pane and below the existing Port 2. This will add another port for a second copy of the traffic to flow out of. For the sake of this integration, use Port 6. After adding the second port, press the **Save** button to complete**.**



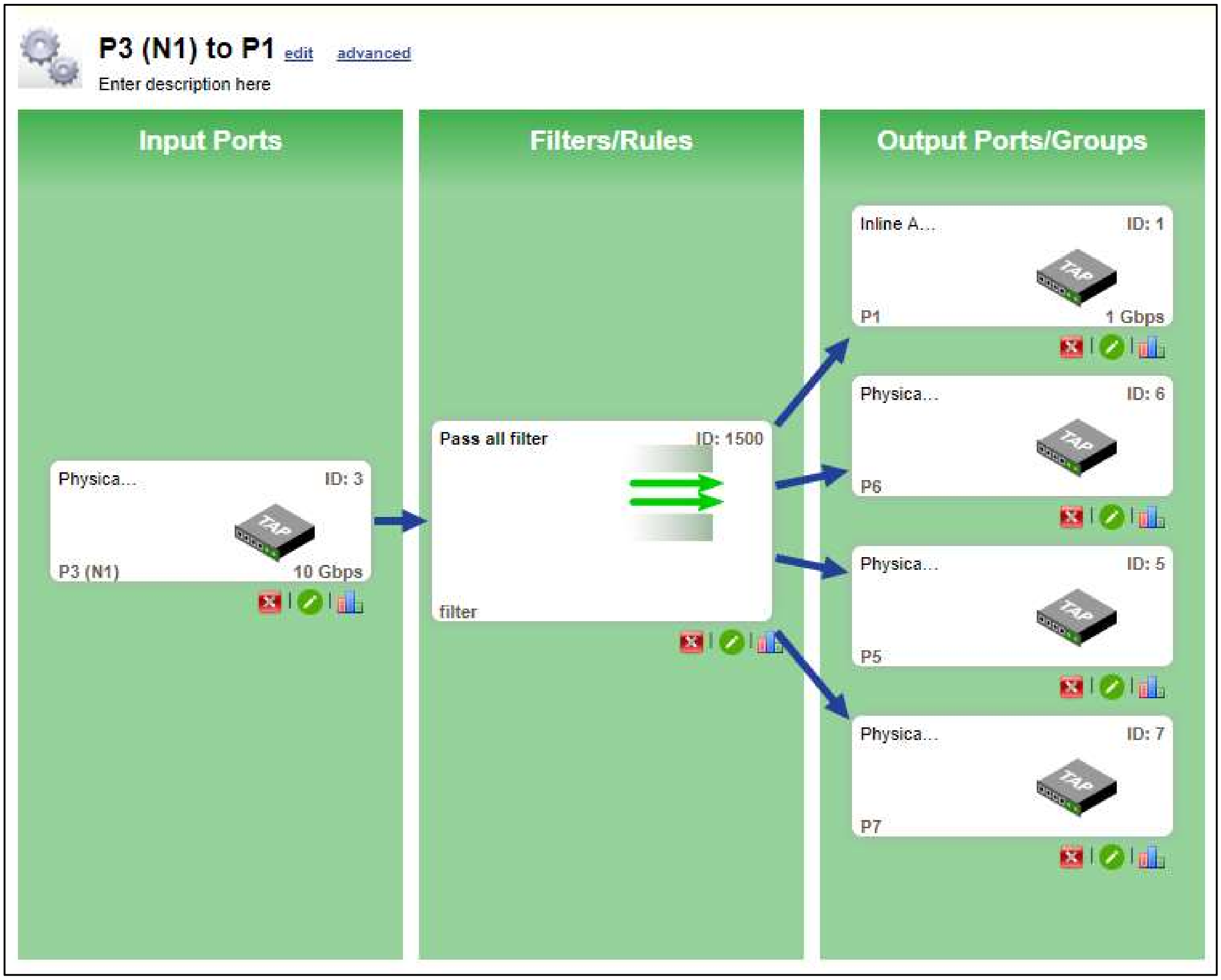
Now follow the same steps again for **P3 (N1) to P1**.



Having both P4 (N2) and P3 (N1) sending traffic to Port 6 will aggregate both North and South bound traffic out a single monitor link to the NetWitness Packet Decoder.

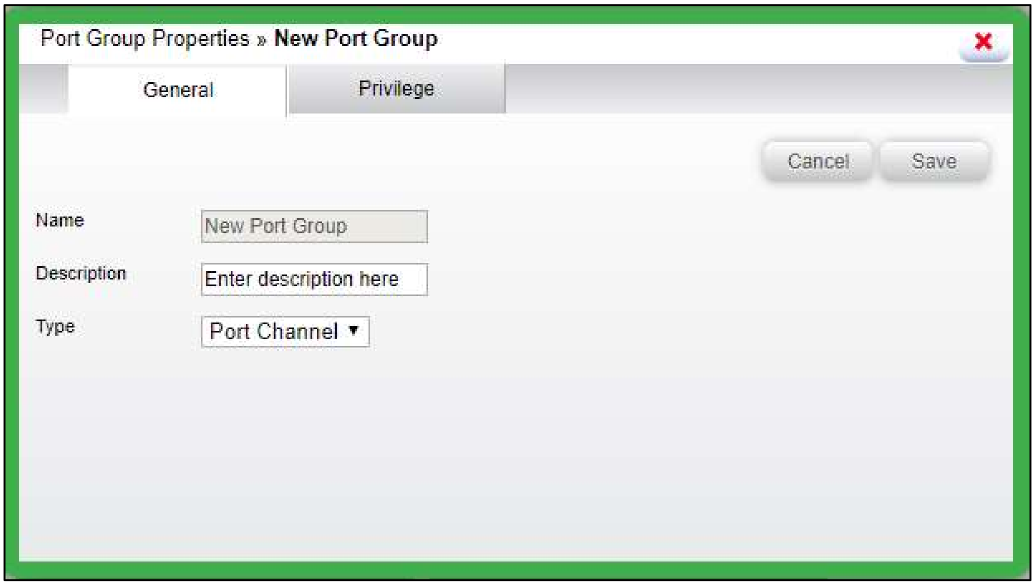
Optional: Send traffic to multiple tools

If the same traffic needs to go to more than one tool, additional egress ports can be assigned to regenerate the traffic multiple times. To do this, simply choose another port for egress traffic and drag it below the existing egress port in the **Output Ports/Groups** pane. This will update the pane to reflect the multiple separate streams of traffic.



Optional: Load balanced Egress Port

In some cases, the ingress traffic throughput may exceed the capacity of what the egress port can handle. For example, if two streams running at 6 Gbps are collected as ingress traffic, the aggregated total will be 12 Gbps, which will oversubscribe a 10Gbps port. To accommodate for this, a port channel can be created to expand the capacity of the egress ports. To configure a port channel or Load Balanced Group, grab an unused port and drag it on top of an existing **egress port**. This will open a new menu for creating the new load balanced port group. A load balanced port group will evenly distribute traffic between the ports used in the port group.



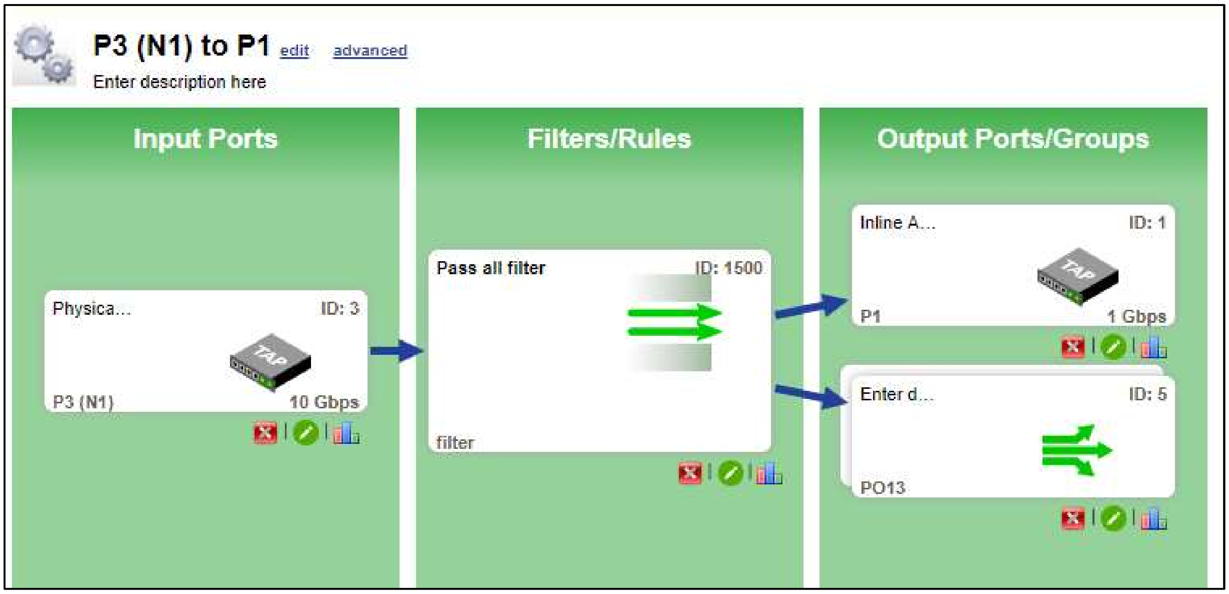
Port Group Properties » **New Port Group**

Name: New Port Group

Description: Enter description here

Type: Port Channel ▾

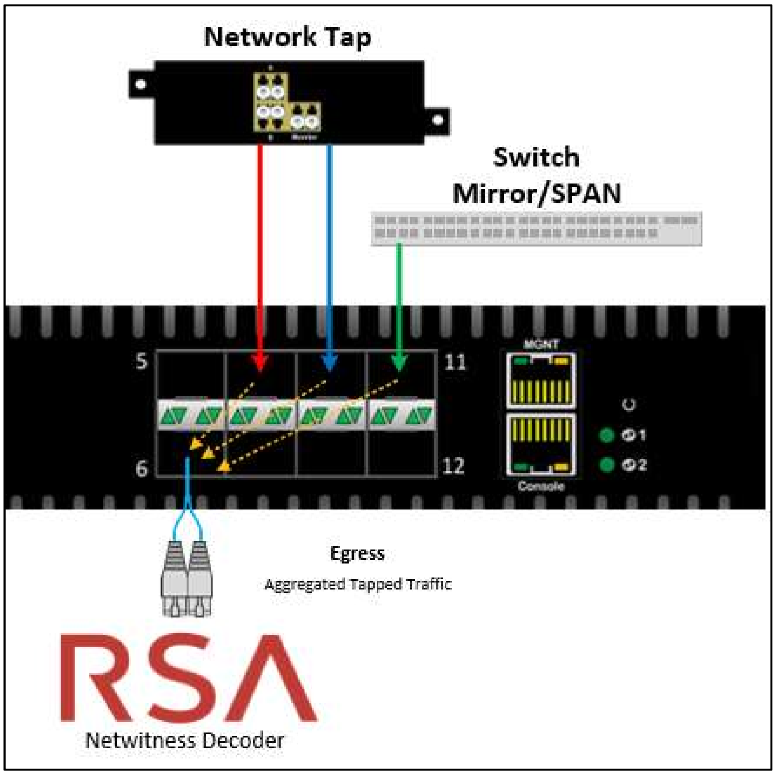
Leave the Type as Port Channel, provide a relevant Description of the Port Group, and then click **save**. This will update the Output Ports/Groups pane to reflect the port channel.



Using a load balanced Egress Port Group with two (2) 10G ports will allow 20 Gbps of throughput at the cost of requiring two (2) ports on the network tool. As more ports are added to the port group, the throughput capacity as will the number of ports required on the network tool.

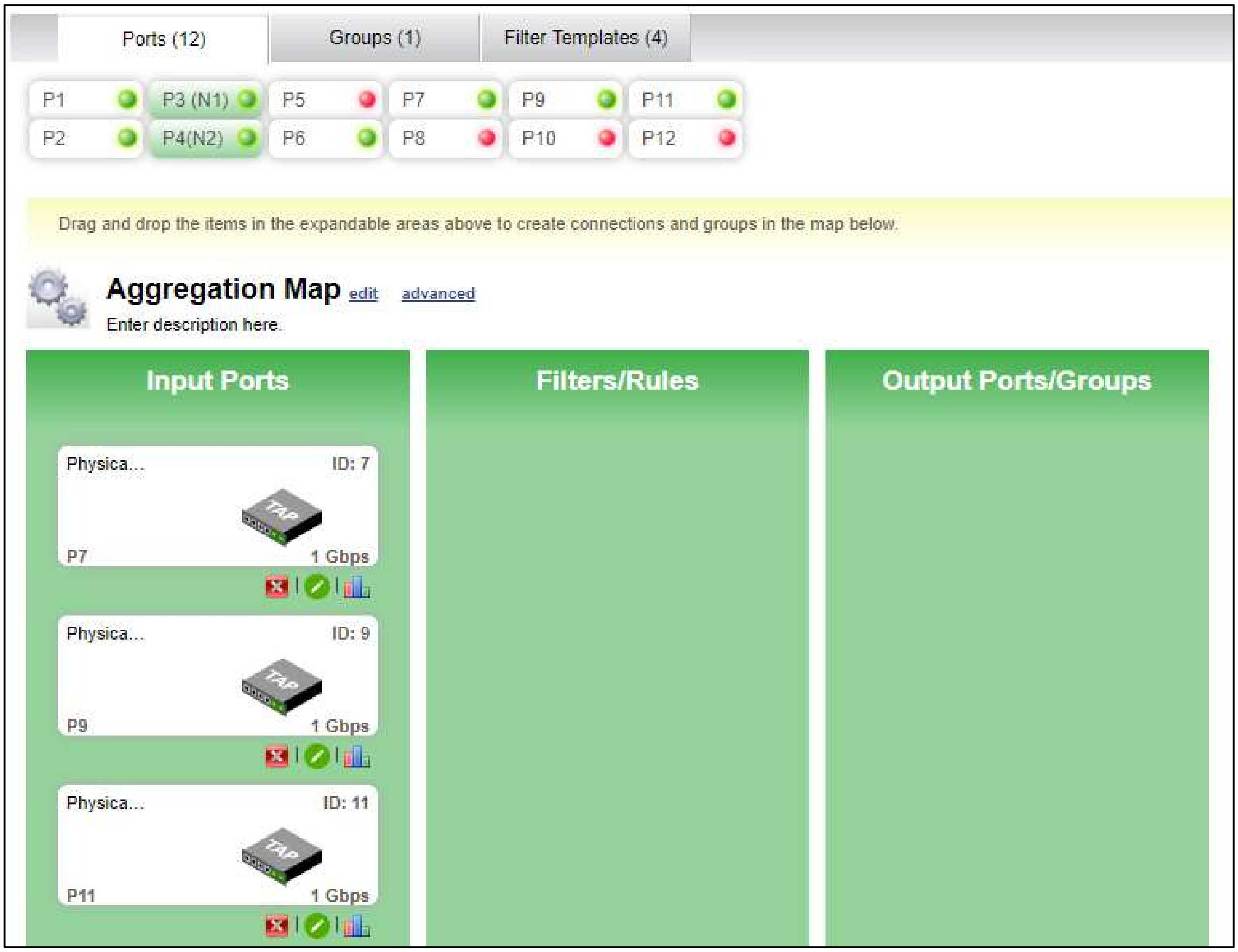
Optional: Ingress TAP/SPAN port Filtering

The location of the Network Link tapped by the EdgeLen's integrated Tap determines what type of traffic is captured. If the EdgeLens is positioned near the WAN link, you would see inbound and outbound traffic, but may miss the internal East / West traffic. Additional sources of traffic can be either captured with either another Network Tap or generated by a switch's SPAN/Mirror port. These additional monitor links can be aggregated together with the traffic captured from the EdgeLens by utilizing the available Packet Broker ports.



Setting up multiple Ingress ports from the Packet Broker ports will require a new Configuration Map to be created that is separated from the Bypass Segment maps.

To create a new port map, go to the **Configuration Maps** page and click **New** in the top right corner. This will take you to a blank configuration map. Start by adding the Ingress ports by pulling P7, P9, and P11 down into the **Input Ports** pane:



Drag and drop the items in the expandable areas above to create connections and groups in the map below.

Aggregation Map

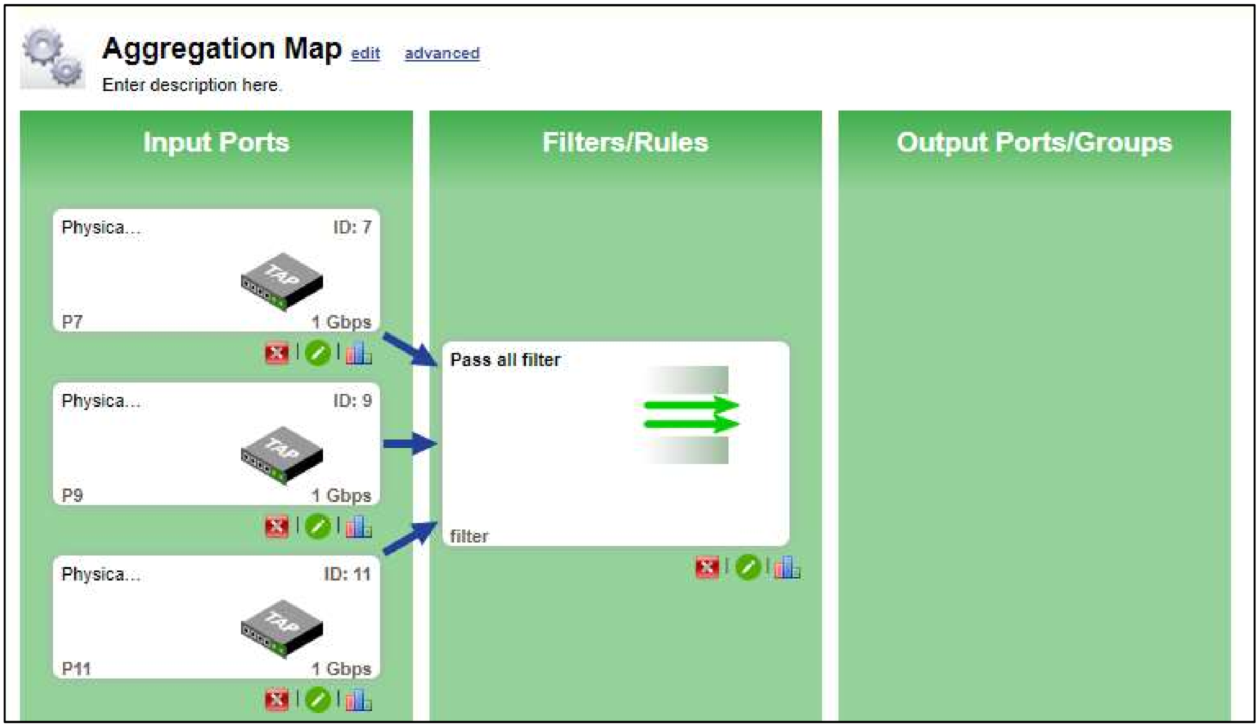
Enter description here.

Physica... ID: 7
P7 1 Gbps

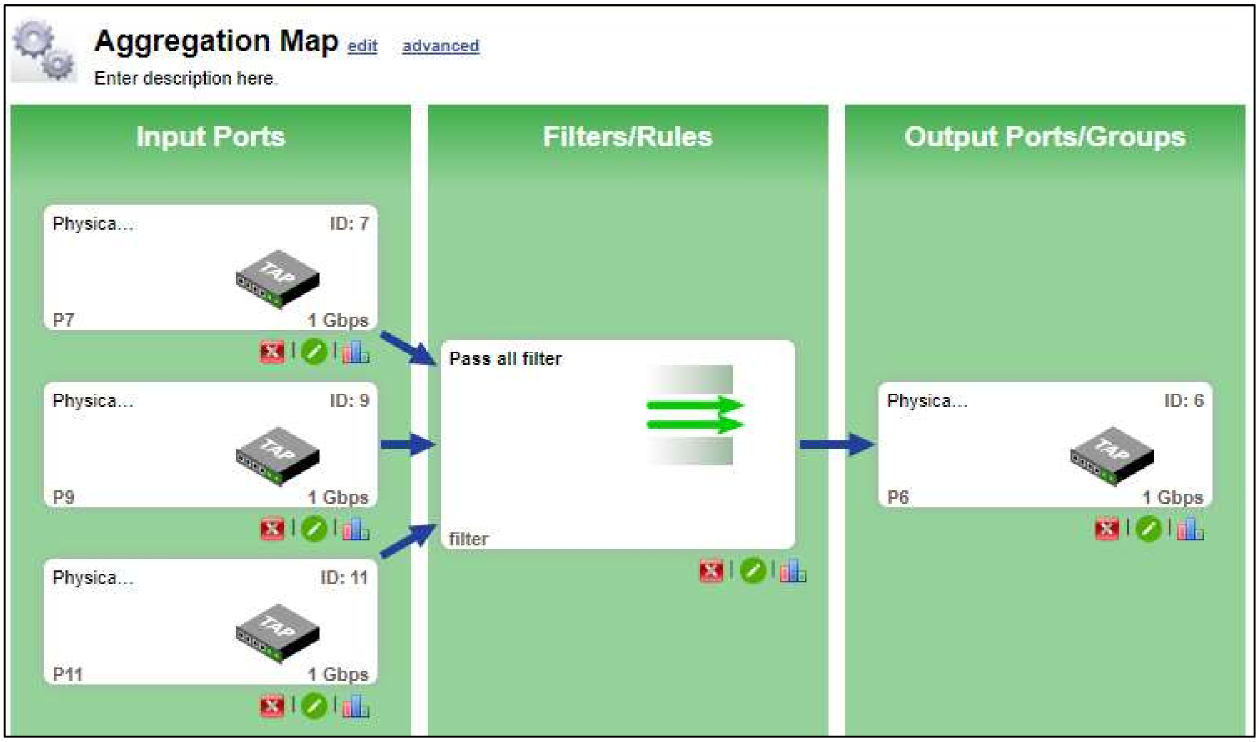
Physica... ID: 9
P9 1 Gbps

Physica... ID: 11
P11 1 Gbps

Next, go to the Filter Templates tab at the top and pull down the Default filter to the **Filters/Rules** pane.



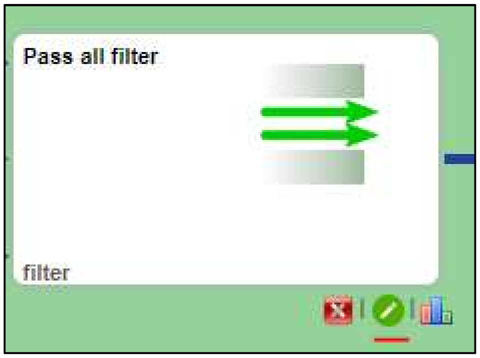
Notice that three (3) separate arrows are pointing from the Input Ports into the Filter. This represents three (3) different sources of data being aggregated together and evaluated by the filter. To finish the port mapping, go to the Ports tab at the top and drag down P6 into the **Output Ports/Groups** pane.



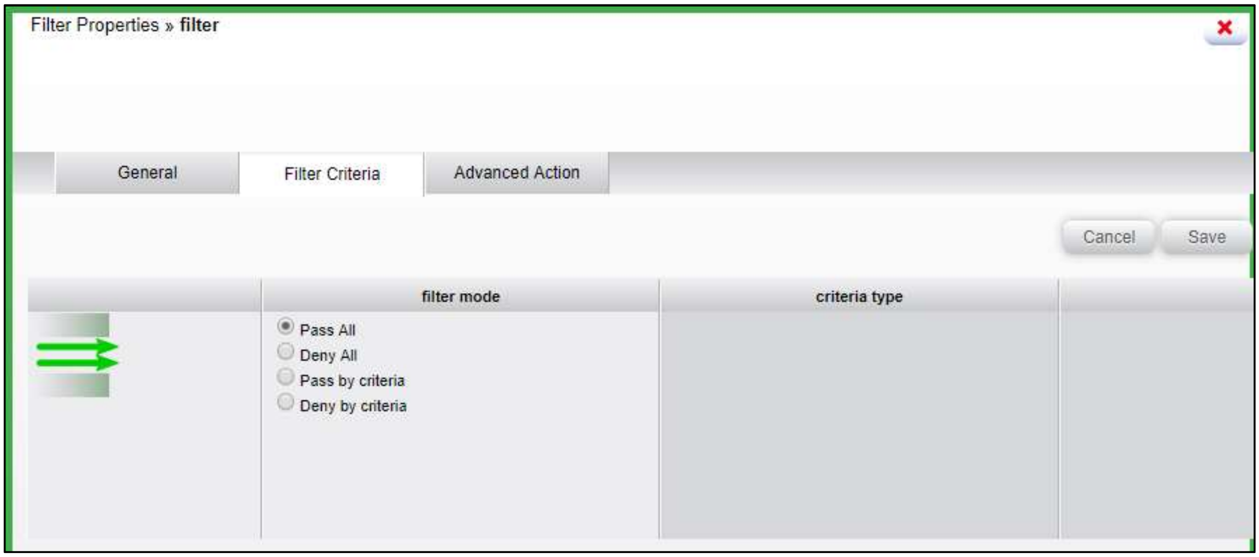
This Configuration map takes in traffic from three (3) different sources, aggregates the traffic together, and egresses out a single egress port. Since Port 6 is used again, the Mirror/SPAN port and Tap monitor ports traffic will be aggregated together with the previously defined EdgeLens traffic.

When aggregating multiple ports together, understanding the throughput utilization of each link is important. If the amount of throughput exceeds the throughput the Egress port is capable of handling, then packets will start to drop. This can be remedied by creating a Load Balanced Port Group as covered earlier, or by filtering out traffic to only pass what the Network Tool on the other end needs. For example, the network tool may not need to see multicast or broadcast traffic. If this is that case, a **deny filter** can be configured to drop this additional, unnecessary traffic.

To configure a filter, click the green circle with a pencil in the middle of it



This will open the Filter Configuration page.



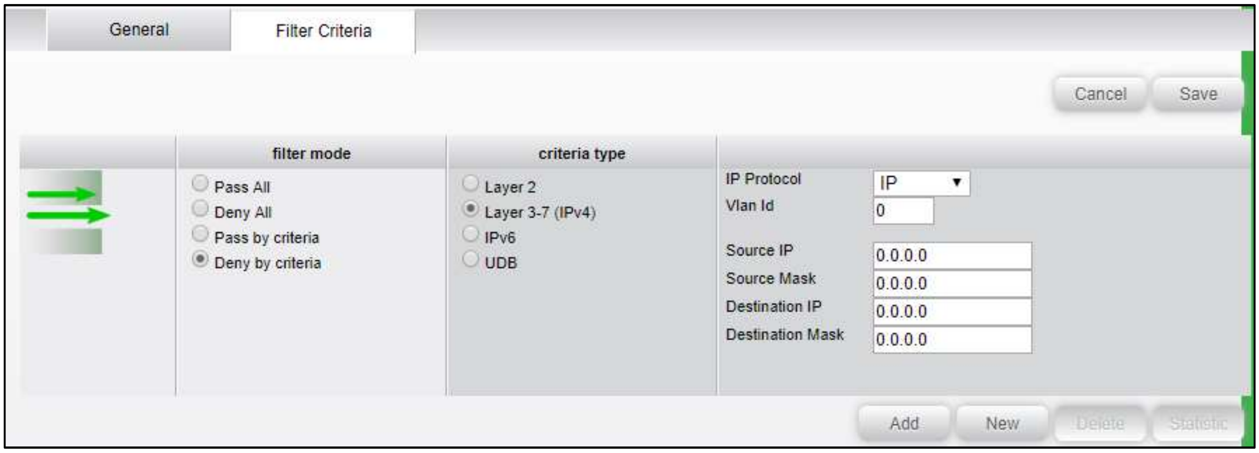
Filter Properties » **filter**

filter mode

- ● Pass All
- ○ Deny All
- ○ Pass by criteria
- ○ Deny by criteria

criteria type

By default, the filter is set to Pass All traffic. For this example, change the selection to **Deny by criteria** and then select **Layer 3-7 (IPv4)**.



filter mode

- ○ Pass All
- ○ Deny All
- ○ Pass by criteria
- ● Deny by criteria

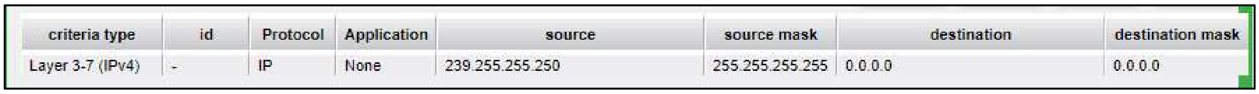
criteria type

- ○ Layer 2
- ● Layer 3-7 (IPv4)
- ○ IPv6
- ○ UDB

IP Protocol: IP ▾
Vlan Id: 0
Source IP: 0.0.0.0
Source Mask: 0.0.0.0
Destination IP: 0.0.0.0
Destination Mask: 0.0.0.0

This will allow you to input specifics about the header of the packets you do not being sent to your Network Tools.

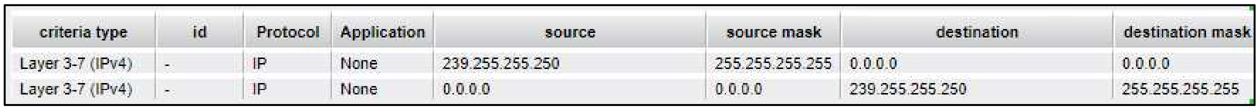
For this example, let’s say the Network Tool has no use for Simple Service Discovery Protocol (SSDP) traffic. SSDP traffic uses the IP address 239.255.255.250 /32. To create a deny filter for this, first enter in 239.255.255.250 into the **Source IP** field and 255.255.255.255 into the **Source Mask** field. Then Press **Add**.



criteria type	id	Protocol	Application	source	source mask	destination	destination mask
Layer 3-7 (IPv4)	-	IP	None	239.255.255.250	255.255.255.255	0.0.0.0	0.0.0.0

This creates a filter looking for any packet that specifically has 239.255.255.250 as the Source IP. This filter will drop any SSDP packet being sent from a device, but traffic being sent to SSDP will still be sent to the tool. To block both directions of SSDP, another filter will need to be added looking for 239.255.255.250 in the Destination IP.

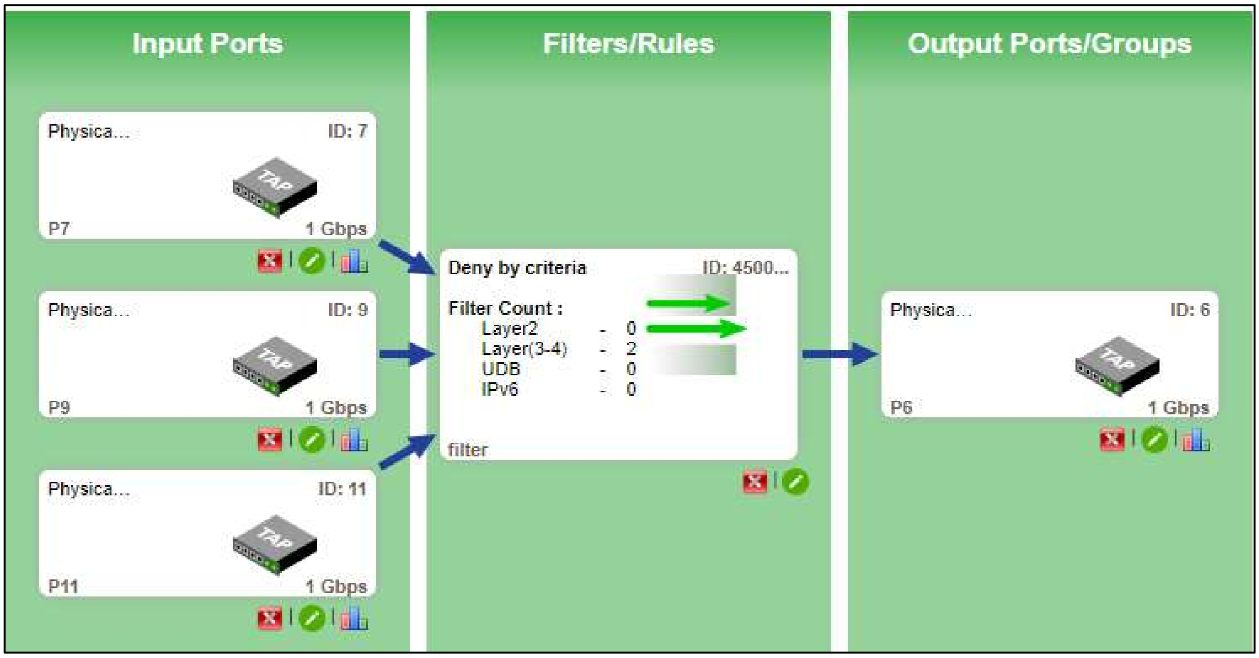
Follow the same process except using the **Destination IP** and **Destination Mask** fields instead.



criteria type	id	Protocol	Application	source	source mask	destination	destination mask
Layer 3-7 (IPv4)	-	IP	None	239.255.255.250	255.255.255.255	0.0.0.0	0.0.0.0
Layer 3-7 (IPv4)	-	IP	None	0.0.0.0	0.0.0.0	239.255.255.250	255.255.255.255

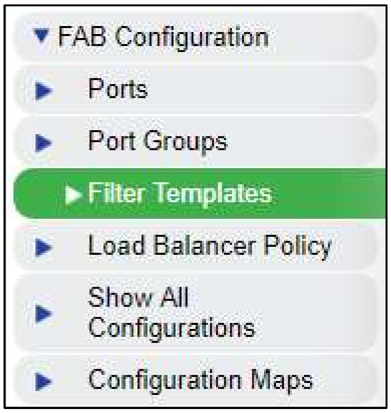
Each filter added to this table get processed as part of an **OR** function. As traffic comes in from the three ingress ports, it will be processed by the filter. The Filter will first inspect the traffic to see if the Source IP is 239.255.255.250. If it is, it will drop the packet. If it is not, it will move down the list and inspect the Destination IP to see if it is 239.255.255.250. Again, if it matches, the packet will be dropped. If it doesn't match, the packet will pass on through to the egress port and out to the Network Tool.

Press **Save** to create this new filter.

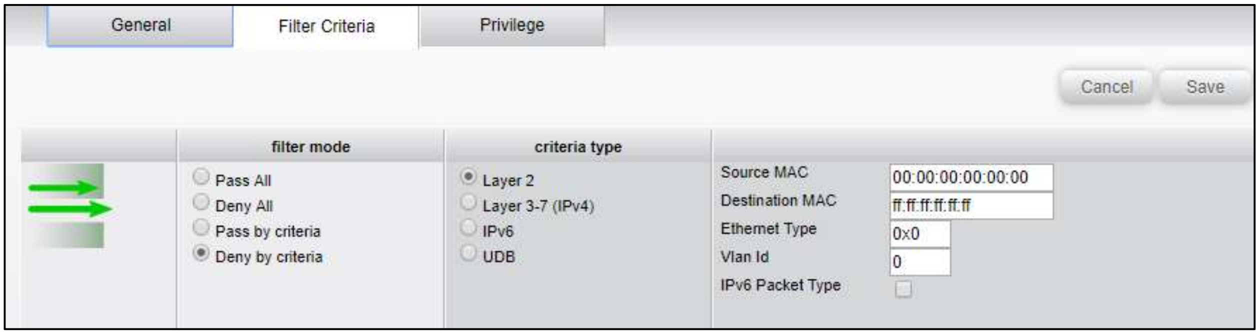


The Configuration Map will update to reflect the new filter.

Egress Filters can also be added for another layer of packet filtering. Instead of being added through the drag-and-drop process, Egress filters are assigned to the port itself. To create an egress filter, first expand the **Fab Configuration** panel on the left and click **Filter Templates.**



The Filter Templates page is where you can create re-usable filters. Press **New** in the upper right corner to open the Filter Configuration page and start a new filter template. For this example, we'll create a deny filter to drop broadcast traffic from being sent to the Network tool.



filter mode

- ○ Pass All
- ○ Deny All
- ○ Pass by criteria
- ● Deny by criteria

criteria type

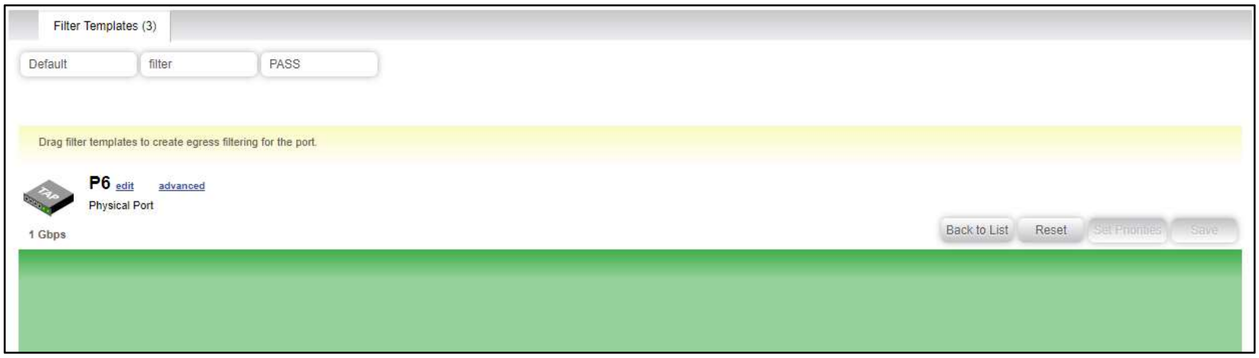
- ● Layer 2
- ○ Layer 3-7 (IPv4)
- ○ IPv6
- ○ UDB

Source MAC	00:00:00:00:00:00
Destination MAC	ff:ff:ff:ff:ff:ff
Ethernet Type	0x0
Vlan Id	0
IPv6 Packet Type	□

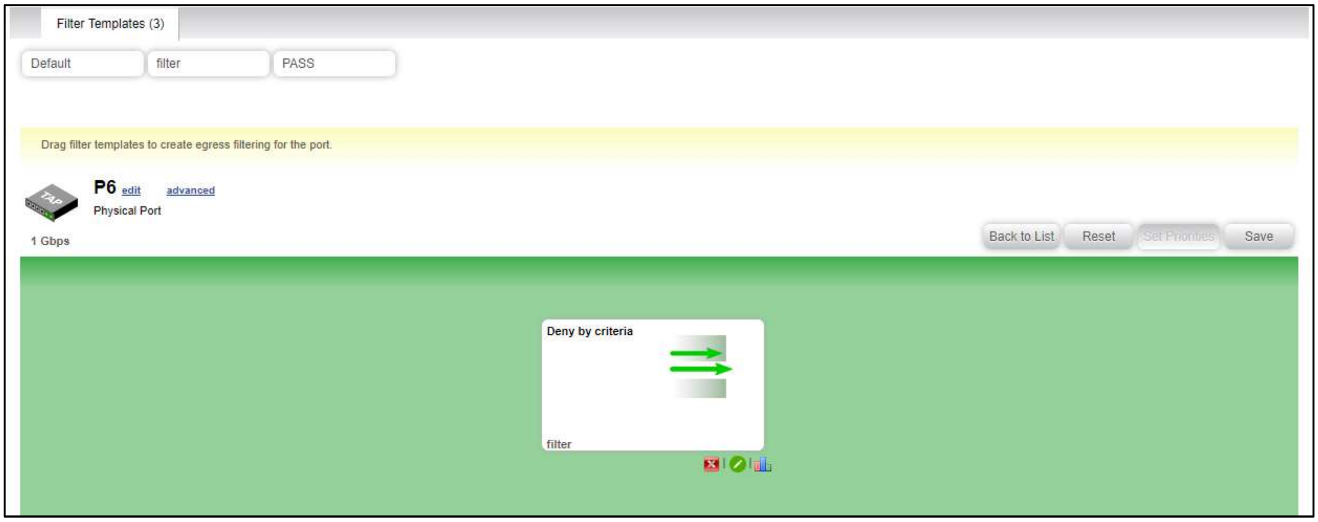
! Important: Filters created in the Filter Template will only look at one *AND* condition at a time. To add additional statements to create an *OR* filter, the filter must be added to a Configuration Map and then edited from there.

The next step is to assign the filter to the egress port itself. To do this, expand the **FAB Configuration** panel on the left and click **Ports**. Click on the name of the port you wish to add the filter directly to. In this example, click on **P6**

A configuration page will open for the port:



Here you can drag and drop created filter templates to be evaluated by the Port.



With the filter in place on the Port, all traffic going through this port will be evaluated against this filter. If the packet matches the deny filter, it will be dropped instead of being sent out.

Conclusion

The EdgeLens integrated bypass tap system provides the means to capture production network traffic and seamlessly integrate a new in-line appliance into the network. The Packet Broker ports on the EdgeLens system are used to send traffic to out-of-band tools like the RSA NetWitness Packet Decoder. These Packet Broker ports can be configured to look at specific ingress sources to either aggregate or isolate East, West, North, or Southbound traffic.

In this integration guide, both directions of network traffic will be captured, aggregated, and sent to RSA NetWitness. Depending on where the EdgeLens is tapping in the network architecture will determine what type of traffic is seen. If the EdgeLens is placed near the WAN, then inbound and outbound traffic will be seen but possibly not East West traffic from internal devices to internal servers. Additional taps will be required to achieve full visibility in the network.

Certification Checklist for RSA NetWitness

Date Tested: December 19, 2018

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA NetWitness	11.1	Virtual Appliance
Garland Technology EdgeLens	9.2.1	Proprietary OEM

NetWitness Test Cases	Result
Packet Collection	
TCP data consumed by the Decoder	✓
UDP data consumed by the Decoder	✓
Other packet data consumed by the Decoder	✓
Inline Heartbeat	
Monitor the health of inline network tools	✓
Traffic Mapping	
Mapping network service ports to dedicated ports	✓
Port Load Balancing	
Create port channel to increase throughput capacity	✓
Traffic Filtering	
Create filters to pass or deny specific network packets to out-of-band tools	✓

✓ = Pass ✗ = Fail N/A = Non-Available Function