Big Monitoring Fabric

Out-of-band

INFO@BIGSWITCH.COM

MENU BAR OPTIONS

Guide (PDF) with instructions for this module

Lab Topology & options to access the Big Monitoring Fabric Controller

Reference Configuration

INTRODUCTION

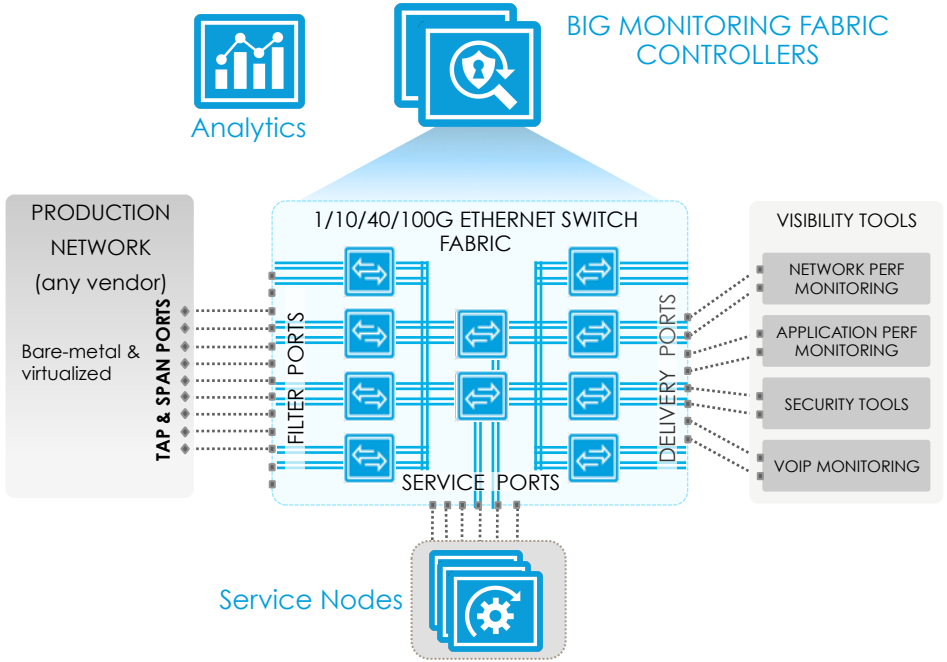
This Hands-on lab introduces Big Monitoring Fabric's out-of-band mode

- Use Big Mon's Graphical User Interface (GUI) client to
  - On-board fabric switches
  - Assign filter and delivery roles to fabric interfaces
  - Create policies to aggregate, filter and deliver traffic from SPAN/TAPs to monitoring tools
- Big Monitoring Fabric can be configured using the Controller's REST API. Internally, both the CLI and the GUI clients use the same REST API calls to configure Big Monitoring Fabric

You will be using actual software in a sandbox environment. Feel free to experiment

BIG MONITORING FABRIC INTRODUCTION

Big Monitoring Fabric out-of-band allows you to monitor <u>all</u> of your bare-metal and virtualized workloads, east-west traffic included, selectively delivering mirrored traffic to security, monitoring, and performance measurement tools in centralized tool farms

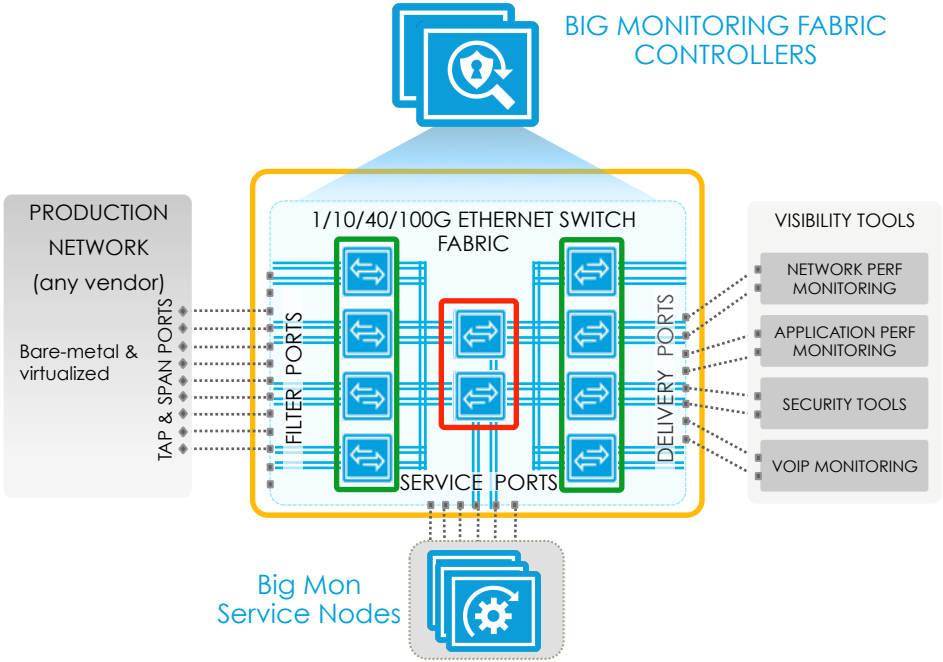


big switch networks

BIG MONITORING FABRIC BUILDING BLOCKS

Fabric scales out to admit additional SPAN/TAP & tool ports

Big Mon is based on a centrally-managed **leaf-spine** fabric built out of high-performance 1/10/40/100G **Open Networking** data center switches.

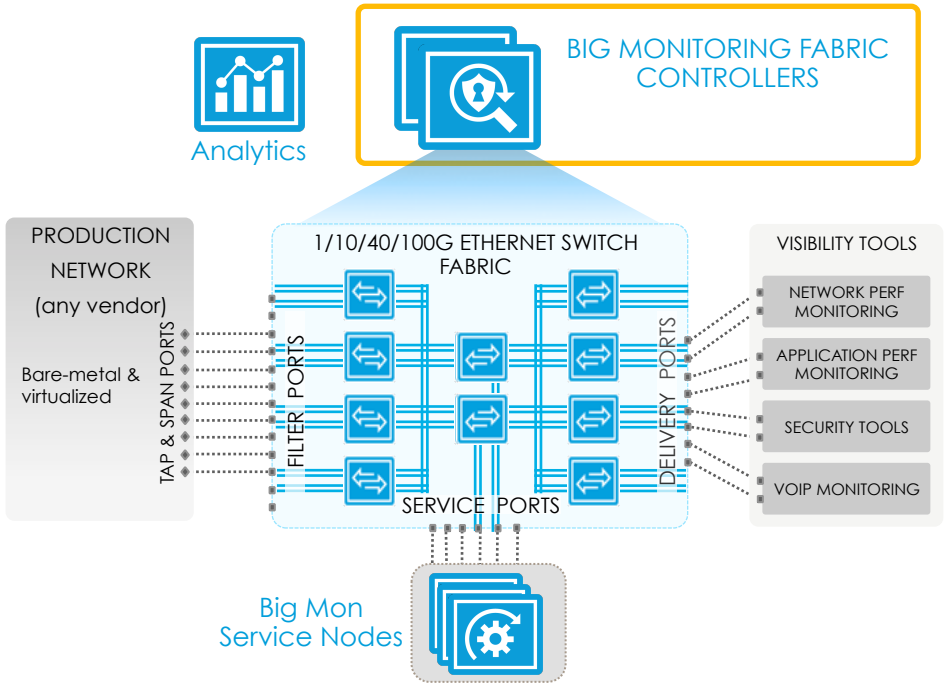


big switch networks

BIG MONITORING FABRIC BUILDING BLOCKS

SDN-style management for unprecedented operational simplicity

HA cluster of Big Mon controllers enables single pane of glass configuration, monitoring and troubleshooting

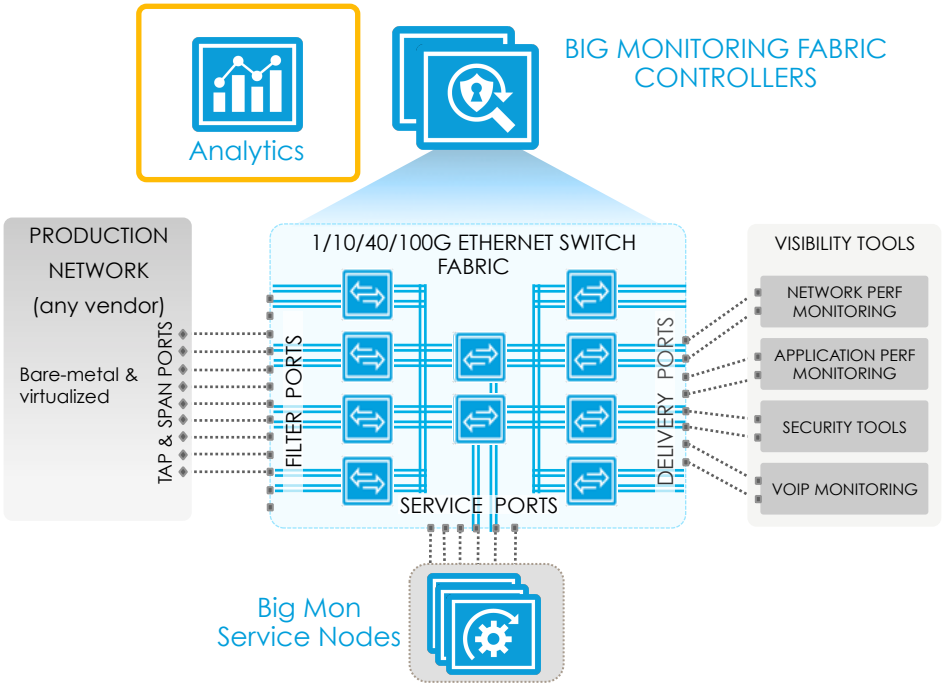


big switch networks

BIG MONITORING FABRIC BUILDING BLOCKS

Big Monitoring Fabric Analytics

Big Monitoring Fabric Analytics

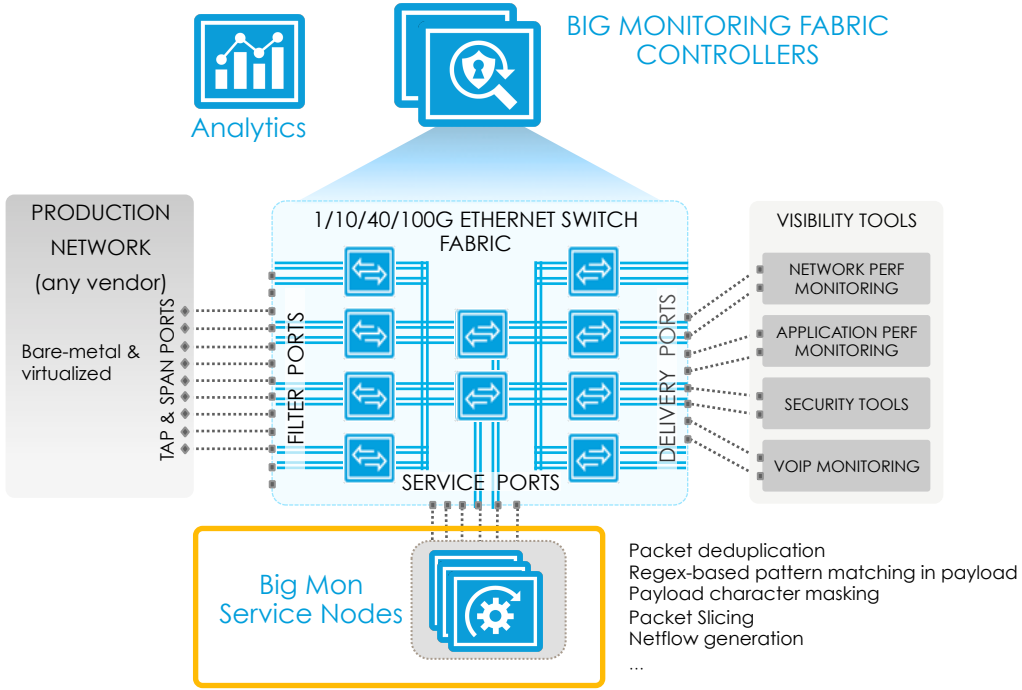


big switch networks

BIG MONITORING FABRIC BUILDING BLOCKS

Big Mon Managed Service Nodes for advanced packet functions *

Big Monitoring Fabric's Managed Service Nodes allow the insertion of advanced packet services within policies that you define over the monitoring fabric

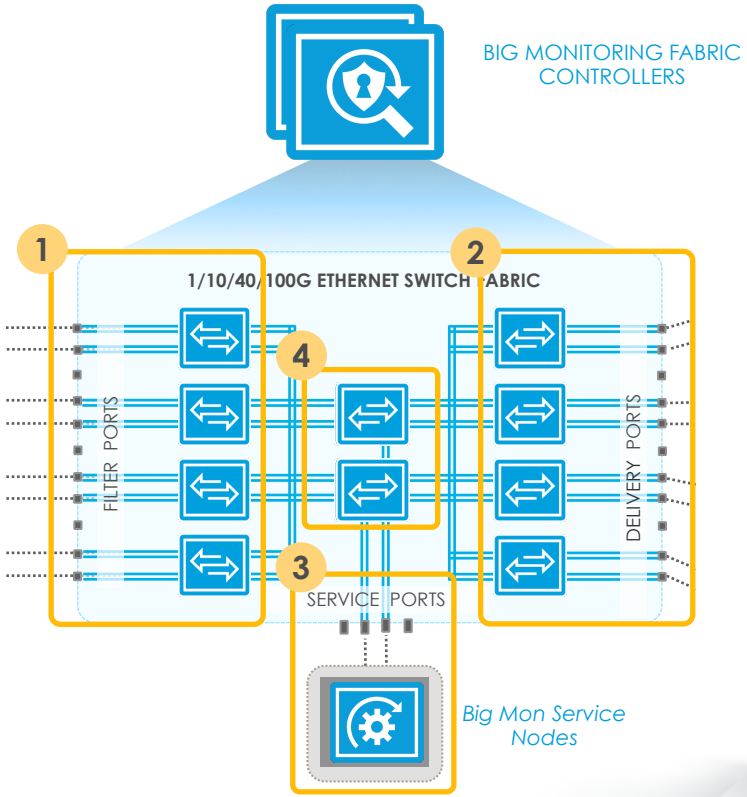


* Service Node Covered in the Big Monitoring Fabric Service Node lab

big switch networks

BIG MONITORING FABRIC TERMINOLOGY

1. **Filter Ports**: Mirrored traffic comes into the monitoring fabric on interfaces that you configure as *filter ports*
2. **Delivery Ports**: Tools connect to interfaces configured as *delivery ports*. In this module we use Wireshark and Snort as delivery tools
3. **Service Ports** (optional): Big Mon's Managed Service Nodes can be connected to fabric interfaces which then become *service ports*. Alternatively, fabric interfaces may be assigned the *service role* allowing third party services to be attached to the fabric
4. **Core Switches & Ports** (optional): In scale-out designs, core switches are typically attached to aggregate traffic from multiple leaf switches



big switch networks

MODULE OUTLINE

INTRODUCTION

* Demo Setup & Terminology

HANDS-ON LAB SECTIONS

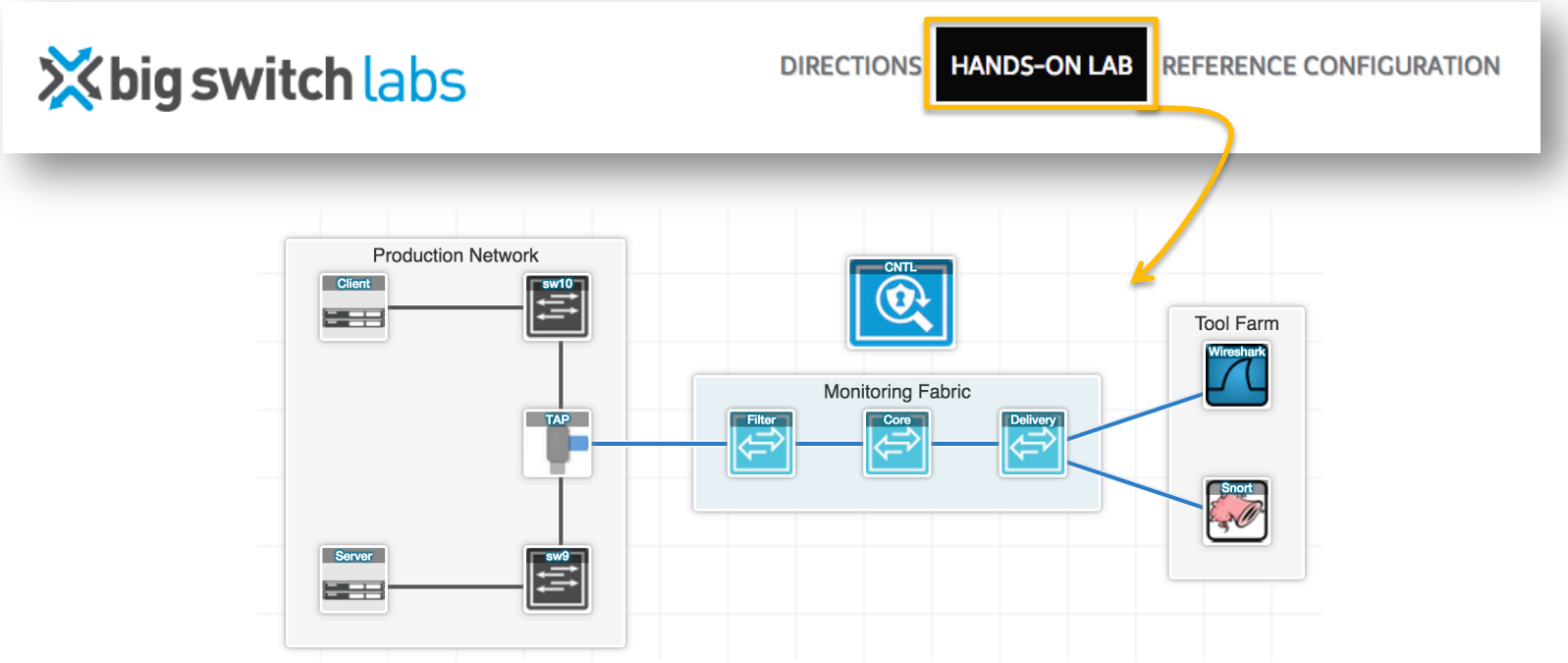
1. Fabric Configuration
2. Create a First Policy
3. Create a Second Policy

big switch networks

Demo Setup & Terminology

LAB TOPOLOGY

Click Hands-on Lab on the menu bar to view the topology and access the controller



big switch networks

LAB TOPOLOGY: BIG TAP CONTROLLER

The Big Monitoring Fabric Controller is the single pane of glass for configuring and troubleshooting the monitoring fabric

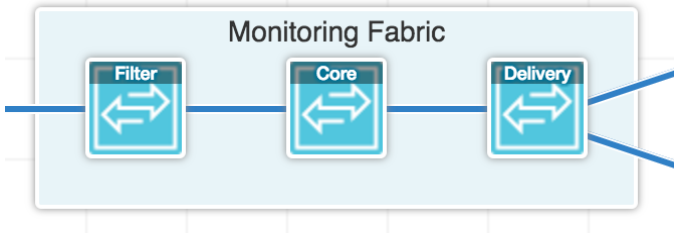
- You will only need access to the Big Monitoring Fabric controller
- Right click on the controller icon and select Controller GUI

Tip: Default controller username/password for initial access is: **admin/bsn123**

LAB TOPOLOGY: ETHERNET SWITCH FABRIC

In this module, the Fabric topology consists of 3 switches running Switch Light™ OS:

- Filter Switch – **Filter**
- Core Switch – **Core**
- Delivery Switch – **Delivery**



Note on the Design of Fabric Topologies:

– To highlight the scale-out fabric design, the topology used in this module depicts Filter Ports to be configured on the Filter Switch, Delivery Ports to be configured on the Delivery Switch and Service Ports on the Core Switch. This is not a design requirement.

– For smaller deployments, a single Ethernet switch can have Filter, Delivery and Service ports. For very large deployments, a multi-tier topology with Filter, Core and Delivery Switches is recommended.

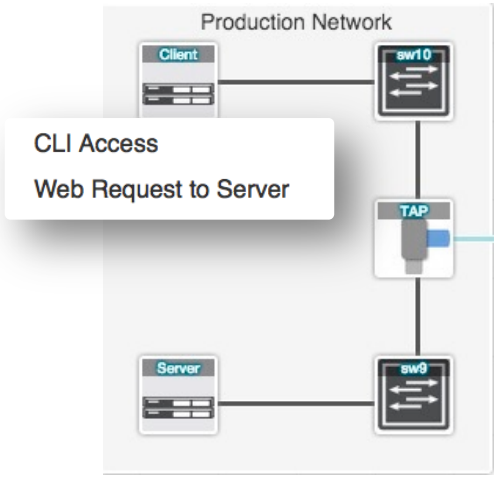
big switch networks

LAB TOPOLOGY: PRODUCTION NETWORK

Production network traffic is simulated by sending requests from the Client to the Server.

Use Case – Tap Every Rack or Location

In a large data center, enterprise or campus network, SPAN and TAP traffic from multiple physical or virtual switches can be fed to the monitoring fabric.



PRODUCTION NETWORK
(Data Center, Campus)

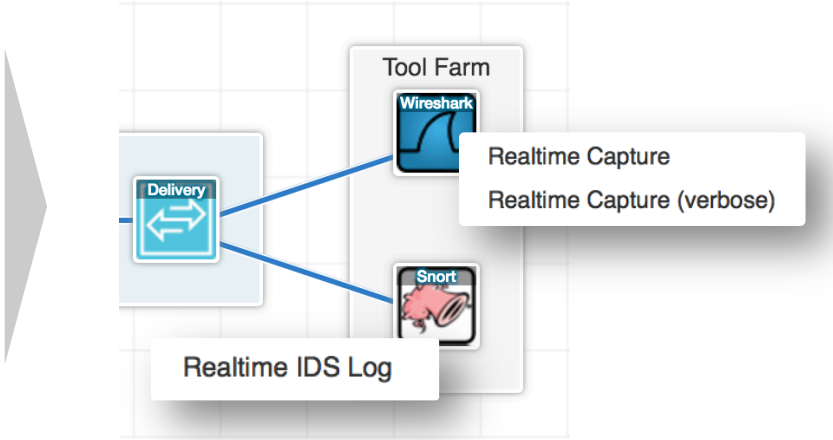
Tip: Right click a topology icon (e.g. Client) to open shell access to that node.

big switch networks

LAB TOPOLOGY: CENTRALIZED TOOLS

Two tools are used in this module:

- **Wireshark** as a network traffic analyzer (packet capture)
- **Snort** as the intrusion detection and prevention system (IDS/IPS)



Hyperscale Design – Centralized Tool Farms

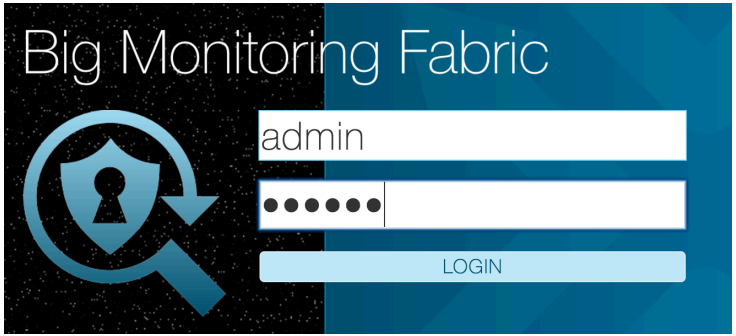
Big Monitoring Fabric selectively filters and optimally replicates traffic to a pool of shared services. Which traffic flows are sent to which tools is determined by the policies configured via the Controller

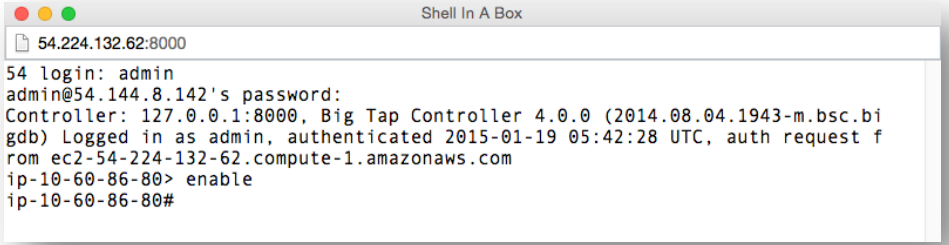
big switch networks

1. Fabric Configuration

1.1 ACCESS BIG MONITORING FABRIC CONTROLLER

Right click the Big Mon controller icon and select the **Controller GUI** and **CLI Access**



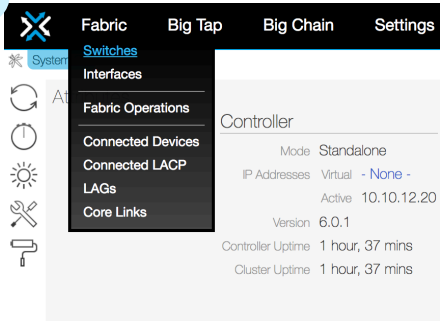


Tip: Default Controller username/password for initial access is **admin/bsn123**

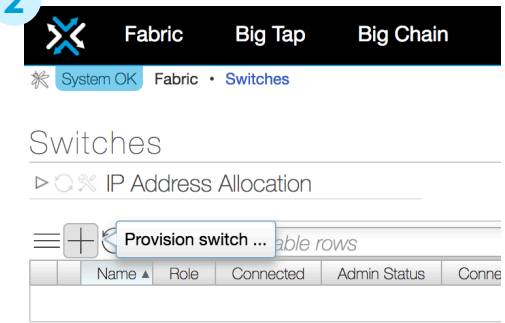
1.2 ADD FABRIC SWITCHES

1. Navigate to Fabric > Switches
2. Click + to provision a switch
3. Configure the Filter-Switch using MAC address 00:00:00:00:00:0A & Save

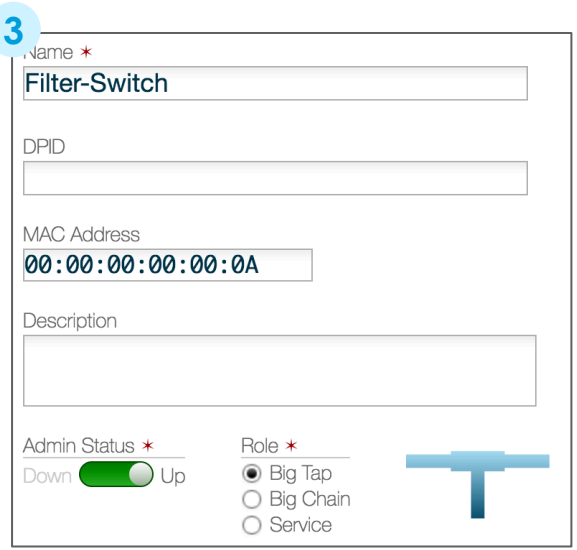
1



2



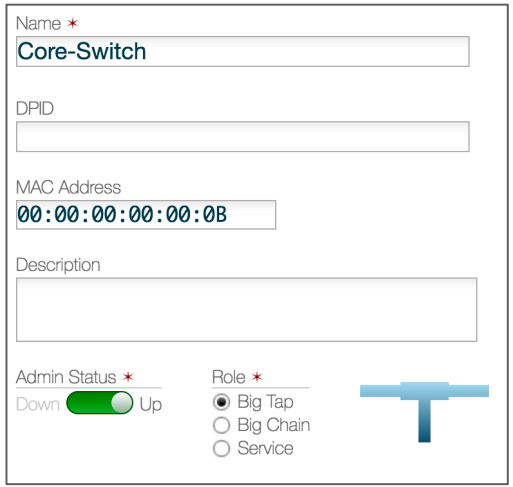
3

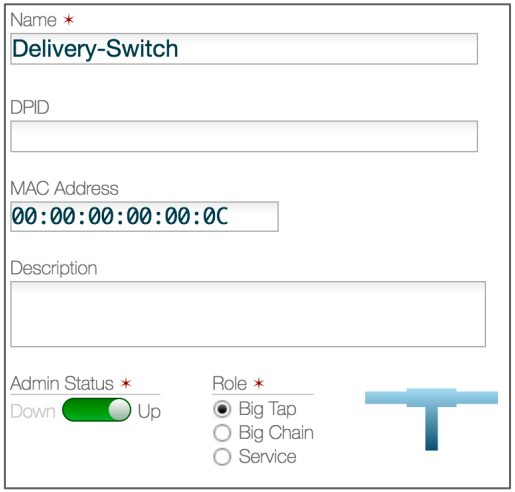


big switch networks

1.3 ADD CORE AND DELIVERY SWITCHES TO THE FABRIC

- Under Fabric > Switches, repeat the same steps to add Core-Switch 00:00:00:00:00:0B & Delivery-Switch 00:00:00:00:00:0C

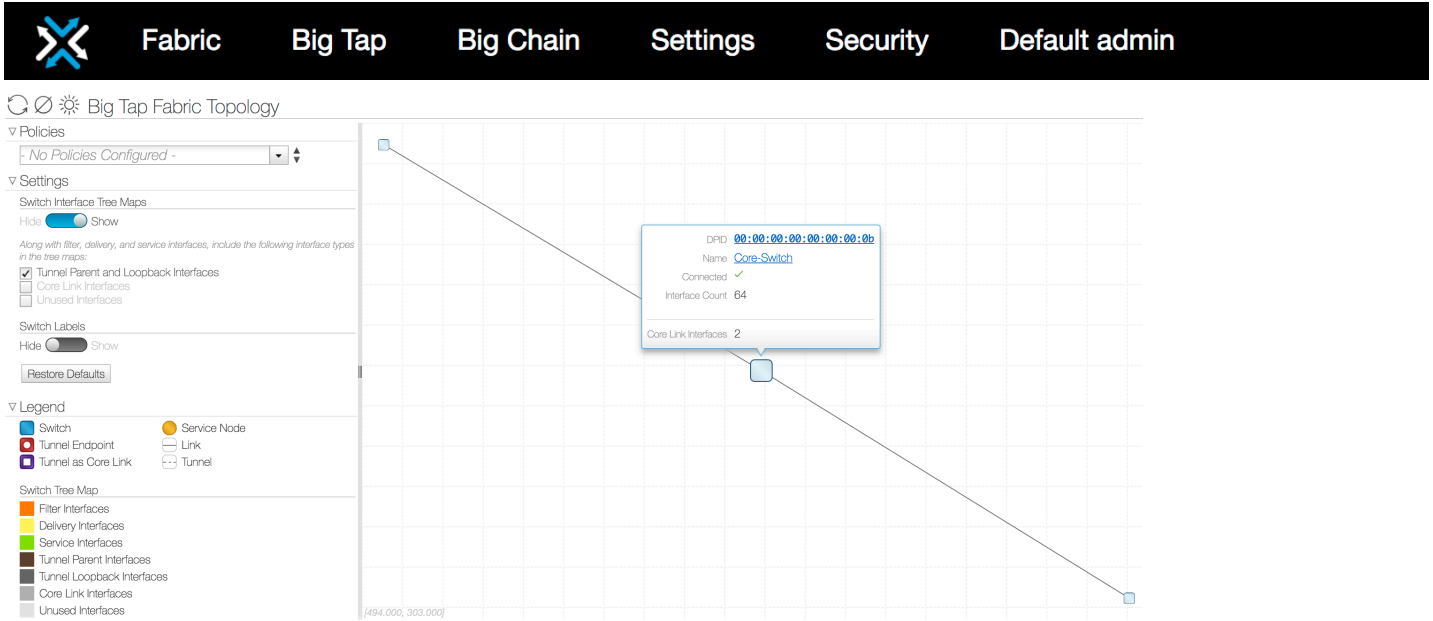




Note: To highlight the scale-out fabric design, the topology used in this module depicts Filter Ports to be configured on the Filter Switch, Delivery Ports to be configured on the Delivery Switch. This is not a design requirement. A leaf switch of the fabric can be configured with a mix of filter & delivery ports

1.4 VERIFY FABRIC TOPOLOGY

Click Fabric to show a graphical summary of your fabric

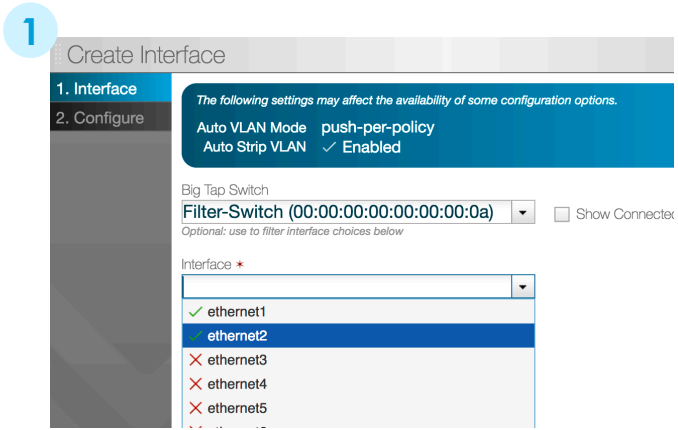


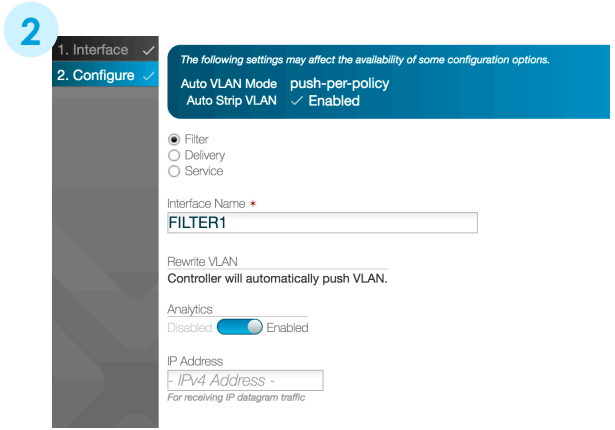
Leaf switches (filter & delivery) are not directly connected to each other. On the other hand, a spine switch (core) is a switch that is physically connected to every leaf switch, and core switches do not connect to each other

big switch networks

1.5 ASSIGN FILTER ROLE TO INTERFACE

- In this lab's topology *ethernet2* of the *Filter-Switch* is connected to a TAP in the production network
- Navigate to Big Tap > Interfaces, click + to add an interface
- Choose Filter-Switch & ethernet2, then hit next, select Filter and name the interface FILTER1. Save to apply the configuration

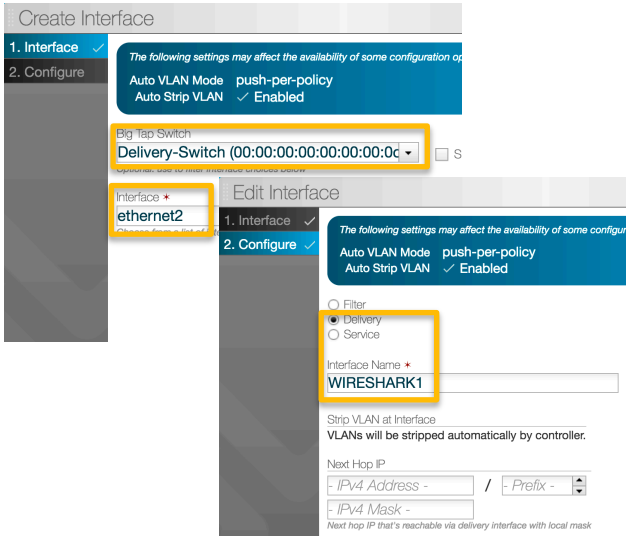


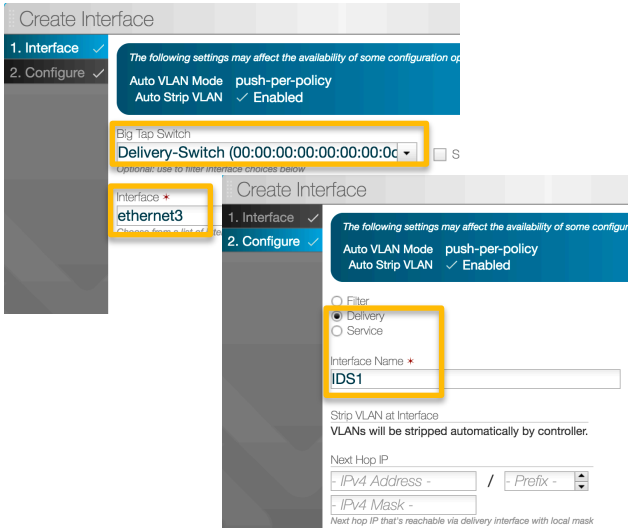


big switch networks

1.6 ASSIGN DELIVERY ROLE TO INTERFACES

- *ethernet2* of *Delivery-Switch* is physically connected to a Wireshark tool, and ethernet3 of the same switch is connected to the Snort IDS
- Repeat the same steps to add two delivery interfaces as shown below, making sure you set the role of the interfaces to Delivery

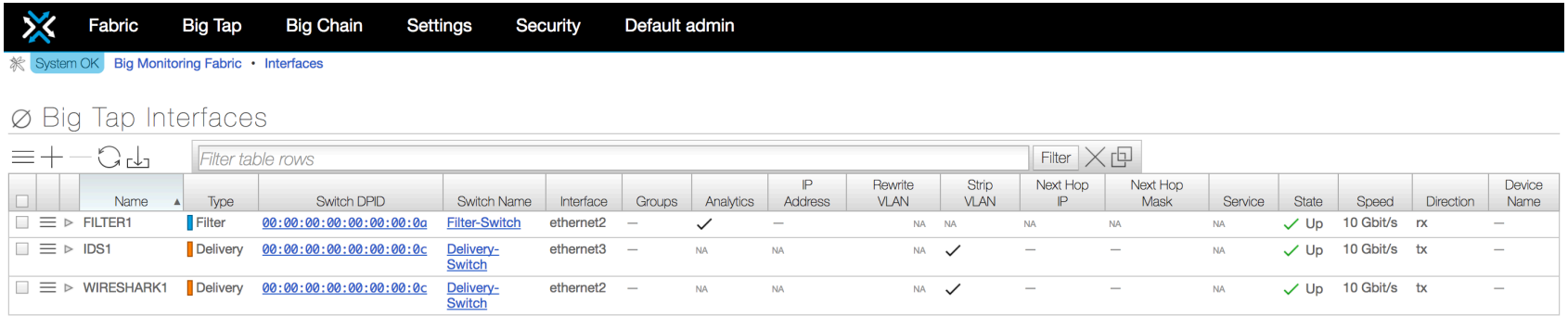




big switch networks

1.7 VERIFY FABRIC INTERFACE ROLES

Review the **roles** (filter or delivery) assigned to the interfaces of the Fabric under *Big Tap > Interfaces*



Name	Type	Switch DPID	Switch Name	Interface	Groups	Analytics	IP Address	Rewrite VLAN	Strip VLAN	Next Hop IP	Next Hop Mask	Service	State	Speed	Direction	Device Name
FILTER1	Filter	00:00:00:00:00:00:00:0a	Filter-Switch	ethernet2	—	✓	—	NA	NA	NA	NA	NA	Up	10 Gbit/s	rx	—
IDS1	Delivery	00:00:00:00:00:00:00:0c	Delivery-Switch	ethernet3	—	NA	NA	NA	✓	—	—	NA	Up	10 Gbit/s	tx	—
WIRESHARK1	Delivery	00:00:00:00:00:00:00:0c	Delivery-Switch	ethernet2	—	NA	NA	NA	✓	—	—	NA	Up	10 Gbit/s	tx	—

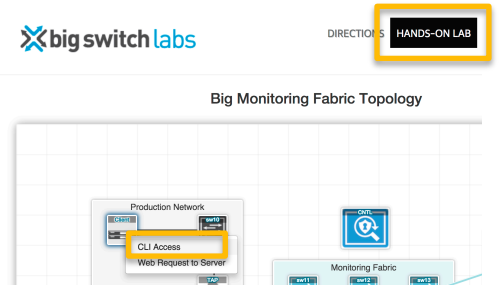
big switch networks

2. Create a First Policy

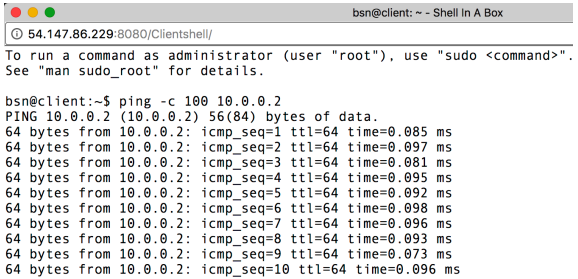
2.1 GENERATE PRODUCTION TRAFFIC

1. Generate production network traffic by sending Ping traffic from the Client to the Server.
   - Go to HANDS-ON LAB tab and right click on the Client icon in the topology
   - Select CLI Access and start a ping to the Server

     ping –c 100 10.0.0.2



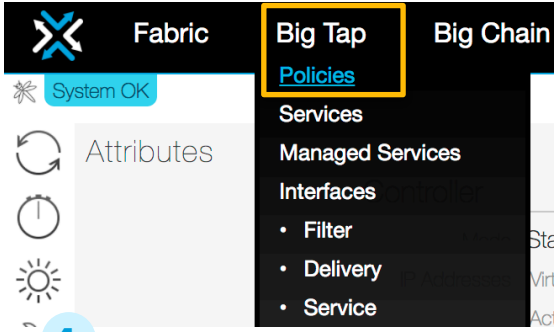
2. Verify that Big Monitoring Fabric is <u>not</u> capturing any traffic. This is the default drop behavior for packets not matching any policies.
   - Right click on any of the delivery tool icons (Wireshark, Snort) and access their Realtime logs. You should find them empty.



Tip: Client IP Address: 10.0.0.3 Server IP Address: 10.0.0.2

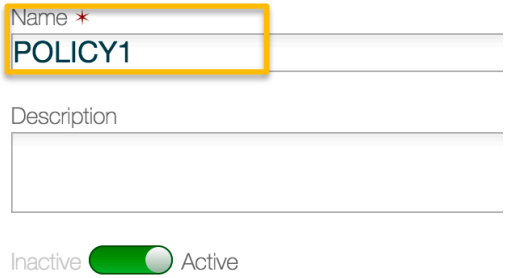
2.2 DELIVER PRODUCTION TRAFFIC TO TOOLS

Create the 1st Policy



Click on "Policies" under Big Tap

Click on + to add a new policy

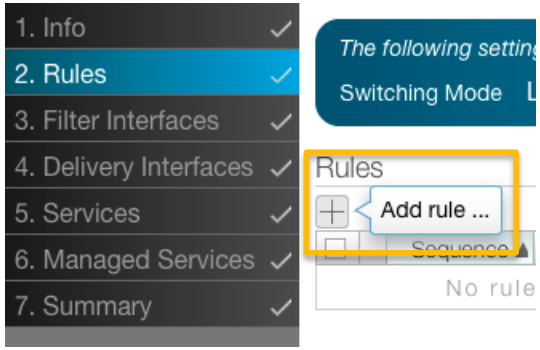


In the **1. Info** menu name your policy "POLICY1", and set the **Action** field to value "**Forward**"

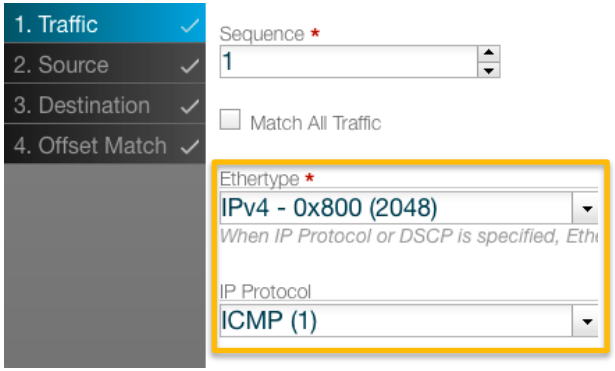
big switch networks

2.3 DELIVER PRODUCTION TRAFFIC TO TOOLS

Create the 1st Policy



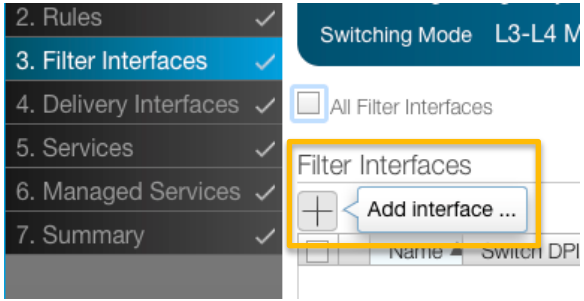
4 Click on the + symbol to add a rule for your policy



5 Select **IPv4** as Ethertype and **ICMP (1)** as the IP Protocol

Leave all other fields set to their default values

Skip Source, Destination and Offset match settings, then **Append** the rule

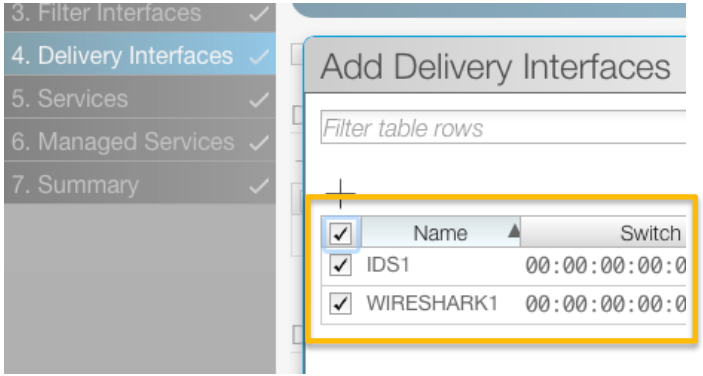


6 Under Filter Interfaces, click to add an interface and **select FILTER1**, submit with **Append Selected**

big switch networks

2.4 DELIVER PRODUCTION TRAFFIC TO TOOLS

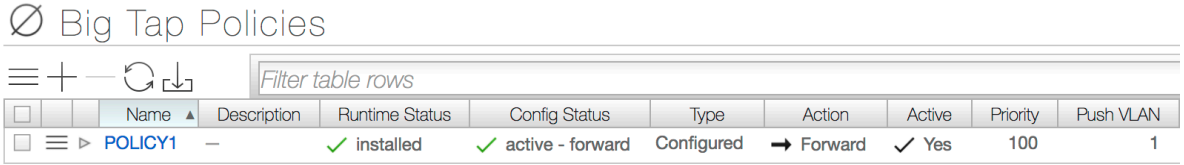
Create the 1st Policy



7 Under **Delivery Interfaces** click the + symbol and **select both IDS1 and WIRESHARK1** then click **Append Selected**

8 Leave the fields under Services, Managed Services and Summary set to their default value

Then click **Save** to install to the policy



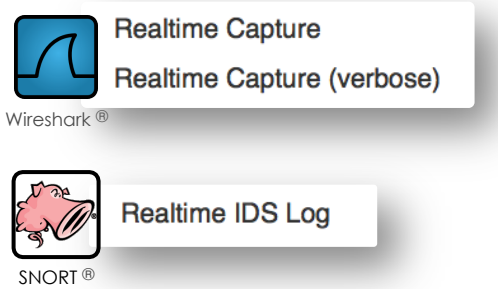
big switch networks

2.5 DELIVER PRODUCTION TRAFFIC TO TOOLS

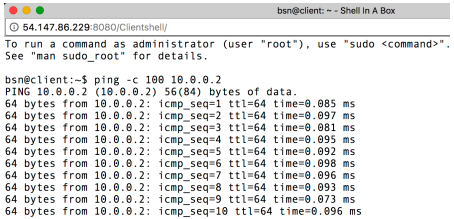
Test the 1st Policy

1. Right click on the "Wireshark" icon and select "**Realtime Capture**".
   - *A real-time capture CLI window should appear.*

2. Right click on the "SNORT®" icon, and select "**Realtime IDS Log**".
   - *A real-time IDS log window should appear.*



3. Right click on the "Client" icon, and select "**CLI Access**".
   - *In the CLI issue the command "ping 10.0.0.2".*
   - *This command will send ICMP traffic to Server. Press CTRL-C after a few seconds to stop the test.*



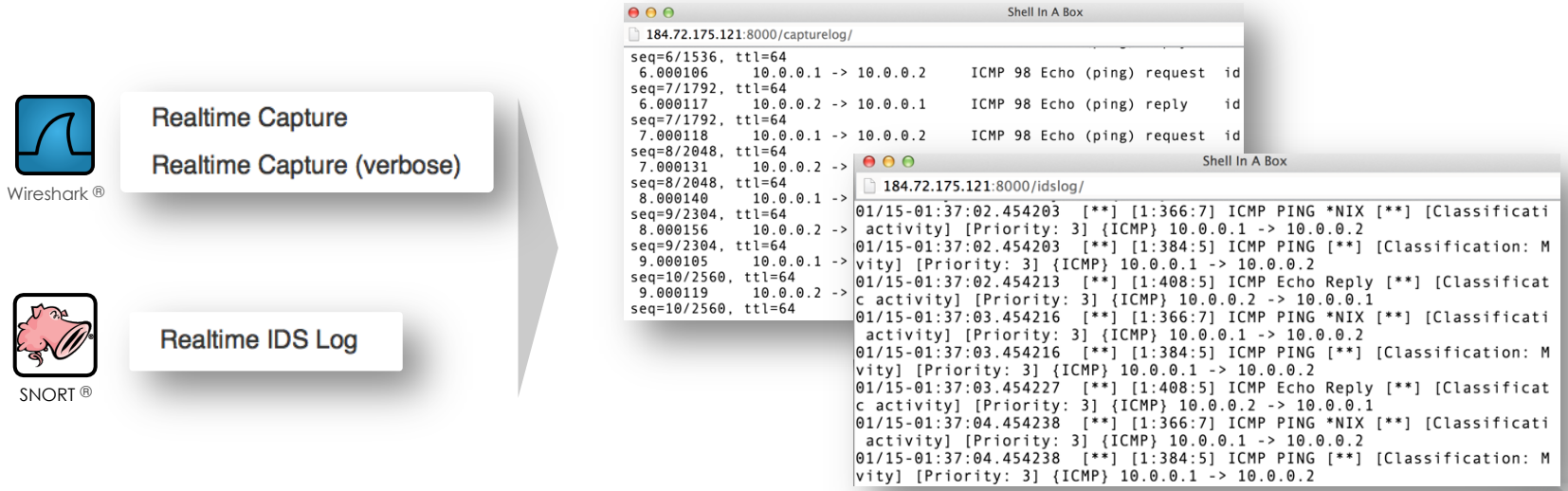
big switch networks

2.6 DELIVER PRODUCTION TRAFFIC TO TOOLS

Test the 1st Policy

Verify that Ping traffic from the Client to the Server is mirrored onto the Monitoring Fabric. After configuring POLICY1, the traffic should be forwarded from the filter ports to the delivery ports where the tools (Wireshark & Snort) are connected.

Note: Big Mon replicates traffic on the common switch closest to the delivery ports to optimize fabric resource utilization



big switch networks

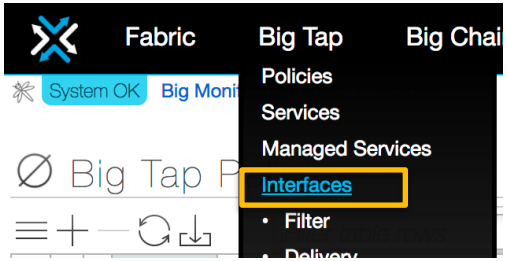
big switch networks

3. Create a Second Policy

3.1 CREATE THE 2ND POLICY

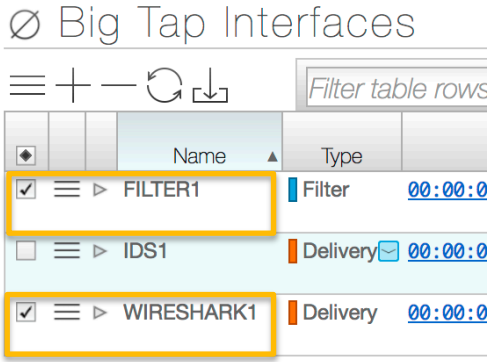
Create the 2nd Policy

Goal: Add a second policy for one tool (Wireshark) to monitor TCP traffic in addition to the ICMP*



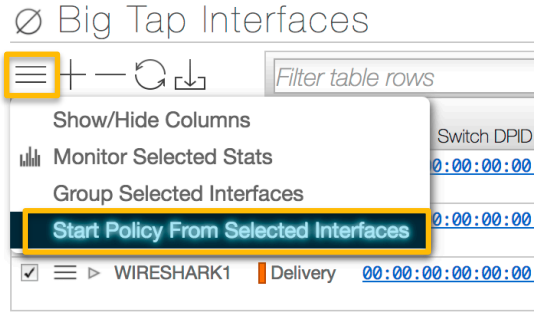
1

Go to Interfaces under Big Tap



2

Select FILTER1 and WIRESHARK1

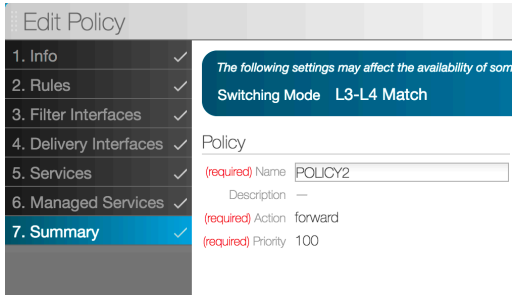


3

Click on the drop-down icon and choose Start Policy From Selected Interfaces. A policy menu gets automatically created and populated

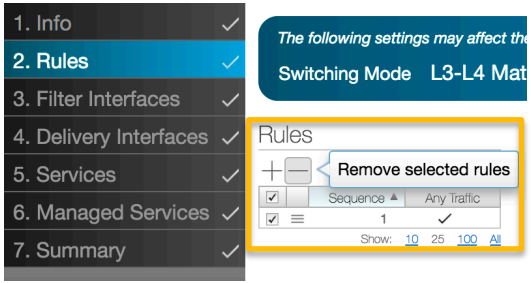
* Note this time we use a slightly different workflow for creating a policy, starting from Big Tap interfaces

3.2 CREATE THE 2ND POLICY



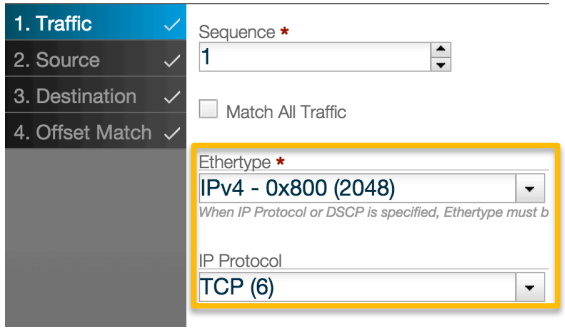
4

Set policy name to POLICY2



5

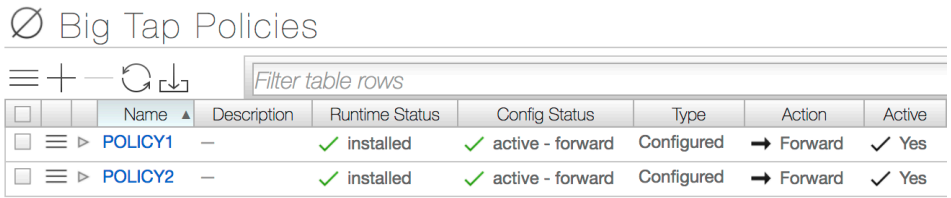
Under Rules, select & remove the default All Traffic rule



6

Add a new rules to match on IPv4 TCP traffic. Click Append, then Save to create the policy.

Optional: Navigate to Big Tap > Policies to verify policy creation

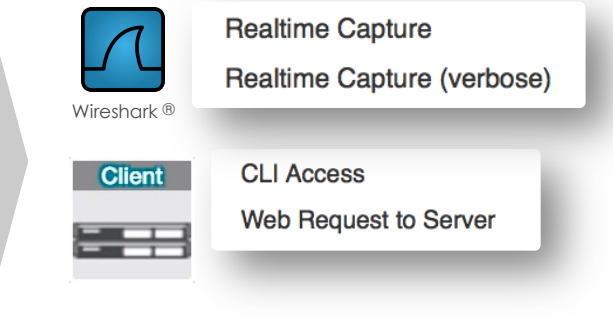


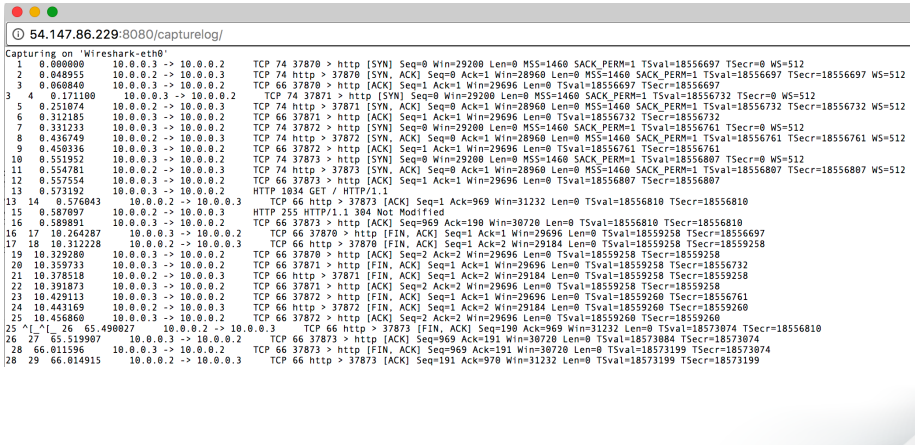
big switch networks

3.3 TEST THE 2ND POLICY

To verify the policy perform the following steps

- *Right click on the "Wireshark" icon, and select "**Realtime Capture**". A real-time capture CLI window should appear.*
- *Right click on the "Client" icon, and select "**Web Request to Server**". This should open the website on the Server in a new browser window. The request for this website by the browser is proxied via Client to the Server.*





big switch networks

Thank You

FOR MORE INFORMATION, PLEASE CONTACT INFO@BIGSWITCH.COM.