

Lab 6 - Visibility and Troubleshooting

Contents

- Lab Overview
- Lab 6.1 - Add SVI to VLAN 10
- Lab 6.2 - Test Policies and SVI
- Lab 6.3 - View Flow Logs
- Lab 6.4 - Analyze Flow Graphs
- Lab 6.5 - Add Policy Rules
- Lab 6.6 - Test Policy Rules
- Lab 6.7 - Testing iPerf
- Lab 6.8 - Unique Flows
- Lab 6 Summary

Lab Overview

Lab time: 30 minutes

On top of the stateful services and microsegmentation, the CX 10000 also delivers visibility into each and every East / West flow. During this lab, we will test some basic traffic flows (ping, SSH, iPerf3), the firewalling policies and also explore the power of having complete visibility.

Lab 6.1 - Add SVI to VLAN 10

Description

In order to successfully redirect packets over the switch, we need to create a corresponding Switched Virtual Interface (SVI) for VLAN 10 to the switch.

Validate

1. In Fabric Composer, using the top menu, navigate to **Configuration / Routing** and then select **VRF**.
2. Click the 3 dots left of **default** and select **IP Interfaces**.

Configuration / Routing / **VRF**

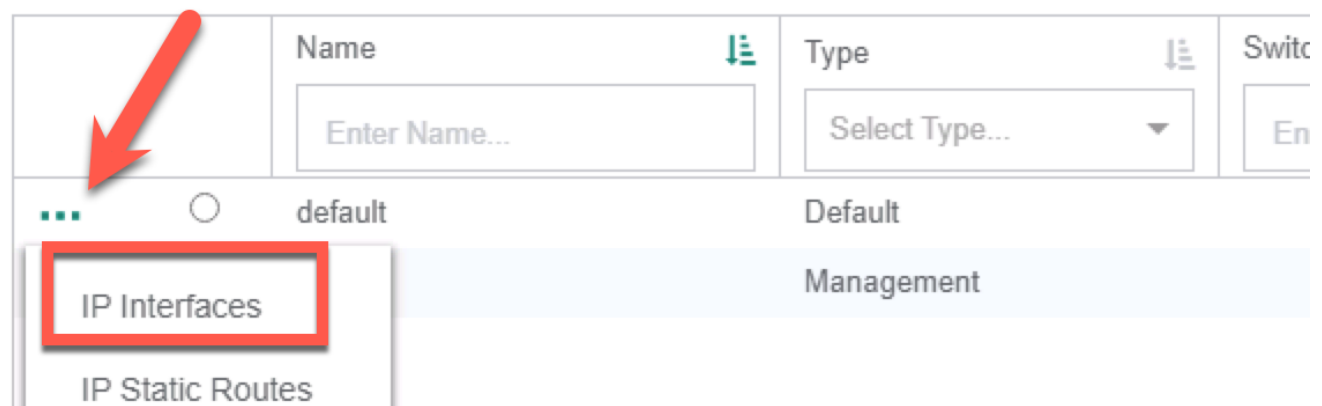


Fig. Lab 6 IP Interfaces

3. In the **IP Interfaces** context, select **Actions**, then **Add** and enter the following information in the form

Step 1 - Interfaces Type	
Enable this IP interface	Yes (select)
Type	SVI
VLAN	10
Switches	Select the VSX pair (dsf_LG01-Leaf01-A_LG01-Leaf...)
IP Subnet Address	10.0.10.0/24
IPv4 Addresses	10.0.10.2-10.0.10.6
Active Gateway IP Address	10.0.10.1
Active Gateway MAC Address	02:00:00:00:00:01
Enable VSX Shutdown on Split	Yes
Enable Local Proxy ARP	Yes
Click NEXT	

Step 2 - Name	
Name	SVI10
Description	(optional)
Click NEXT	
Review the Summary and APPLY	

Expected Results

1. Verify the new SVI in the AFC

IP INTERFACES IP STATIC ROUTES NETWORKS UNDERLAYS OVERLAYS ARP TABLES IP ROUTE TABLES							
	Type	Enabled	Switch	VLAN	Port/LAG	Active Gateway IP Address	Primary IPv4 Network
<input type="radio"/>	SVI	Yes	LG10-Leaf01-A	10		10.0.10.1	10.0.10.3/24
<input type="radio"/>	SVI	Yes	LG10-Leaf01-B	10		10.0.10.1	10.0.10.2/24

Fig. Lab 6 New SVI

2. Now let's ensure that the Network was added to the PSM by logging into the PSM:

URL	10.250.2 LG .31 (LG = Labgroup Number)
Username	admin
Password	Pensando0\$

3. Go to **Tenants / Networks** and you should see VLAN10 listed in your networks

Tenants					
Overview					
VRF					
Networks					
Networks (1)					
<input type="checkbox"/>	Name	VRF	VLAN	Ingress Policy	Egress Policy
<input type="checkbox"/>	VLAN10	default	10		dsf-leaf-01

Fig. Lab 6 PSM Networks

Lab 6.2 - Test Policies and SVI

Description

In the previous activity, you created a policy with a single `allow_all` rule, to allow all traffic between `Workload01` and `Workload02`.

Validate

To test the rule and visualize the flows, follow the following steps:

1. Using Putty or TeraTerm, open an SSH session with each workload

Workload	Address for SSH*	Username	Password	Hostname	VLAN 10 Address
1	10.250.2 LG .201	arubatm	admin	lg LG -wl01	10.0.10.101
2	10.250.2 LG .202	arubatm	admin	lg LG -wl01	10.0.10.102

2. From each workload, ping the VLAN 10 SVI 10.0.10.1 to verify connectivity between the VMs and the switches.

The image shows two terminal windows side-by-side. The left window is titled '10.250.201.201 - arubatm@lg01-wl01: ~ VT' and shows a series of ping results from 10.0.10.1 to 10.0.10.1. The right window is titled '10.250.201.202 - arubatm@lg01-wl02: ~ VT' and shows a series of ping results from 10.0.10.1 to 10.0.10.1. Both windows show successful pings with varying response times.

```

10.250.201.201 - arubatm@lg01-wl01: ~ VT
64 bytes from 10.0.10.1: icmp_seq=34 ttl=64 time=0.221 ms
64 bytes from 10.0.10.1: icmp_seq=35 ttl=64 time=0.303 ms
64 bytes from 10.0.10.1: icmp_seq=36 ttl=64 time=0.327 ms
64 bytes from 10.0.10.1: icmp_seq=37 ttl=64 time=0.276 ms
64 bytes from 10.0.10.1: icmp_seq=38 ttl=64 time=0.314 ms
64 bytes from 10.0.10.1: icmp_seq=39 ttl=64 time=0.290 ms
64 bytes from 10.0.10.1: icmp_seq=40 ttl=64 time=0.310 ms
64 bytes from 10.0.10.1: icmp_seq=41 ttl=64 time=0.340 ms
64 bytes from 10.0.10.1: icmp_seq=42 ttl=64 time=0.362 ms
64 bytes from 10.0.10.1: icmp_seq=43 ttl=64 time=0.323 ms
64 bytes from 10.0.10.1: icmp_seq=44 ttl=64 time=0.371 ms
64 bytes from 10.0.10.1: icmp_seq=45 ttl=64 time=0.313 ms
64 bytes from 10.0.10.1: icmp_seq=46 ttl=64 time=0.227 ms
64 bytes from 10.0.10.1: icmp_seq=47 ttl=64 time=0.270 ms
64 bytes from 10.0.10.1: icmp_seq=48 ttl=64 time=0.334 ms
64 bytes from 10.0.10.1: icmp_seq=49 ttl=64 time=0.312 ms
64 bytes from 10.0.10.1: icmp_seq=50 ttl=64 time=0.310 ms
64 bytes from 10.0.10.1: icmp_seq=51 ttl=64 time=0.256 ms

10.250.201.202 - arubatm@lg01-wl02: ~ VT
64 bytes from 10.0.10.1: icmp_seq=27 ttl=64 time=0.266 ms
64 bytes from 10.0.10.1: icmp_seq=28 ttl=64 time=0.290 ms
64 bytes from 10.0.10.1: icmp_seq=29 ttl=64 time=0.411 ms
64 bytes from 10.0.10.1: icmp_seq=30 ttl=64 time=0.283 ms
64 bytes from 10.0.10.1: icmp_seq=31 ttl=64 time=0.264 ms
64 bytes from 10.0.10.1: icmp_seq=32 ttl=64 time=0.312 ms
64 bytes from 10.0.10.1: icmp_seq=33 ttl=64 time=0.327 ms
64 bytes from 10.0.10.1: icmp_seq=34 ttl=64 time=0.297 ms
64 bytes from 10.0.10.1: icmp_seq=35 ttl=64 time=0.300 ms
64 bytes from 10.0.10.1: icmp_seq=36 ttl=64 time=0.289 ms
64 bytes from 10.0.10.1: icmp_seq=37 ttl=64 time=0.284 ms
64 bytes from 10.0.10.1: icmp_seq=38 ttl=64 time=0.345 ms
64 bytes from 10.0.10.1: icmp_seq=39 ttl=64 time=0.303 ms
64 bytes from 10.0.10.1: icmp_seq=40 ttl=64 time=0.345 ms
64 bytes from 10.0.10.1: icmp_seq=41 ttl=64 time=0.294 ms
64 bytes from 10.0.10.1: icmp_seq=42 ttl=64 time=0.335 ms
64 bytes from 10.0.10.1: icmp_seq=43 ttl=64 time=0.296 ms
64 bytes from 10.0.10.1: icmp_seq=44 ttl=64 time=0.335 ms

```

Fig. Lab 6 Ping SVI

Expected Results

Now have a look at the following network diagram to understand the flow. Both WL01 and WL2 have [10.0.10.xxx](#) IP Addresses and the Primary VLAN (VLAN 10) is paired with an Isolated VLAN (VLAN 11). The traffic on VLAN 11 is re-routed to the DSM chip on the CX10K for processing via the primary VLAN 10.

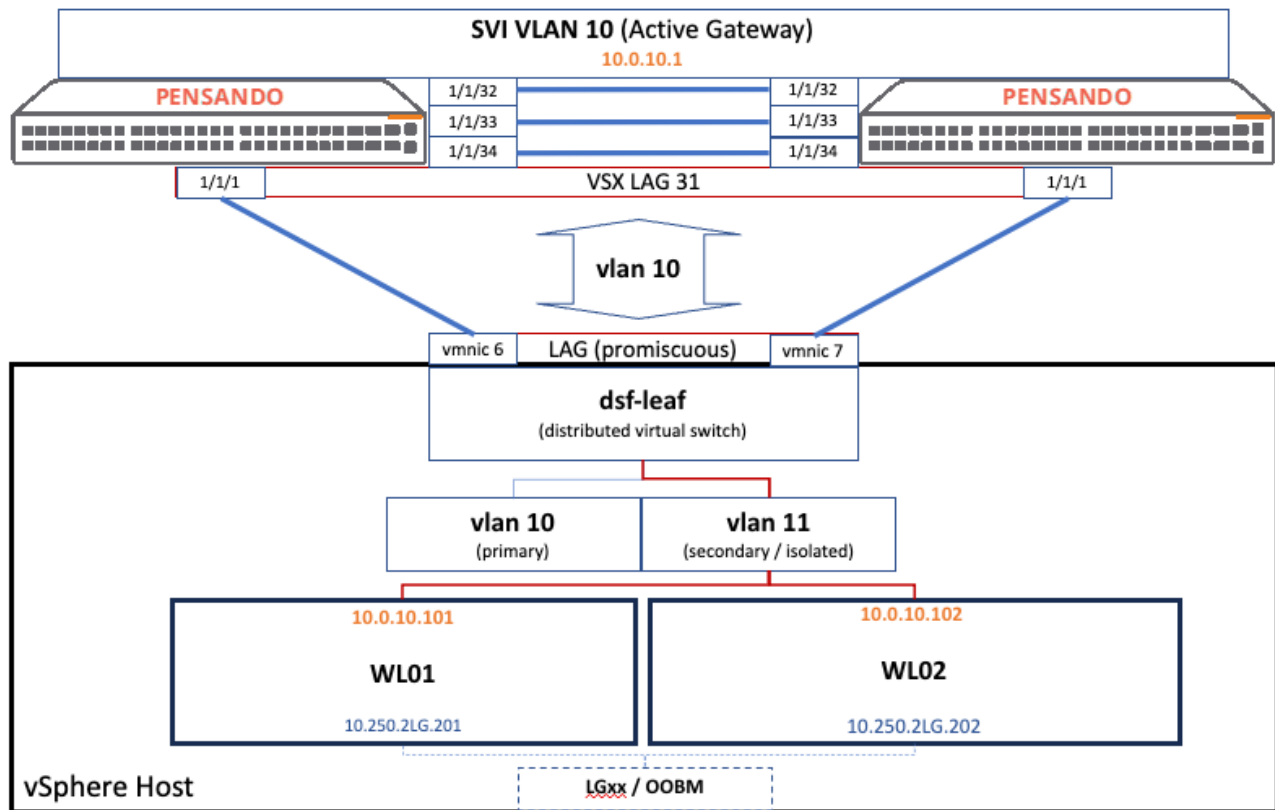


Fig. Lab 6 SVI Diagram

Policies will be defined using the AFC and sent, via automation, to the Pensando PSM. In turn, the PSM will program the enforcement on the DSM chips. A workload aware infrastructure built on top of a fully programmable, Automated, Scalable network pipeline.

Note

If you cannot ping the gateway, check to see that the switch ports are up! Enable port with no shut command.

10.250.203.101 - Tera Term VT

Port	Native VLAN	Mode	Type	Enabled	Status	Reason	Speed (Mb/s)	Description
1/1/1	1	trunk	10G-DAC3	yes	up		10000	
1/1/2	---	routed	---	yes	down	No XCVR installed	---	---
1/1/3	---	routed	---	yes	down	No XCVR installed	---	---
1/1/4	---	routed	---	yes	down	No XCVR installed	---	---
1/1/5	---	routed	---	yes	down	No XCVR installed	---	---
1/1/6	---	routed	---	yes	down	No XCVR installed	---	---
1/1/7	---	routed	---	yes	down	No XCVR installed	---	---
1/1/8	---	routed	---	yes	down	No XCVR installed	---	---
1/1/9	---	routed	---	yes	down	No XCVR installed	---	---
1/1/10	---	routed	---	yes	down	No XCVR installed	---	---
1/1/11	---	routed	---	yes	down	No XCVR installed	---	---
1/1/12	---	routed	---	yes	down	No XCVR installed	---	---
1/1/13	---	routed	---	yes	down	No XCVR installed	---	---
1/1/14	---	routed	---	yes	down	No XCVR installed	---	---
1/1/15	---	routed	---	yes	down	No XCVR installed	---	---
1/1/16	---	routed	---	yes	down	No XCVR installed	---	---
1/1/17	---	routed	---	yes	down	No XCVR installed	---	---
1/1/18	---	routed	---	yes	down	No XCVR installed	---	---
1/1/19	---	routed	---	yes	down	No XCVR installed	---	---
1/1/20	---	routed	---	yes	down	No XCVR installed	---	---

-- MORE --, next page: Space, next line: Enter, quit: q

Fig. Lab 6 Switch Port Up

Lab 6.3 - View Flow Logs

Description

Now that we have traffic on VLAN 10 being redirected over the DSM, we can start to look at some of the telemetry. During this lab, we will generate traffic between two VMs on the same ESXi host, and will view the live flow logs.

Validate

- Using the SSH sessions to Workload01 and Workload02 from the previous exercise, initiate a new continuous ping and do not interrupt it:

- From `Workload01`, ping `10.0.10.102`
- From `Workload02`, ping `10.0.10.101`

- Open two new SSH sessions, to each CX 10000 Switch:

Switch	Address for SSH	Username	Password
1	10.250.2 LG .101	<code>admin</code>	<code>admin</code>
2	10.250.2 LG .102	<code>admin</code>	<code>admin</code>

- On one of the switches, find which VLANs are being redirected to the DSM (Distributed Services Module = the Pensando Elba Packet Processor) for policy enforcement

Note

The CX 10000 Switch has two DSMs, and redirected VLANs are distributed between them using a hashing algorithm. In a CX 10000 VSX pair, all redirection and flow policing is synchronized across both switches

4. On each switch, run the following command and you should see an output similar to the screenshot below:

```
show dsm redirect
```

```
Distributed Services Modules 1/2
=====

No VLAN redirect configured to this Distributed Services module

Distributed Services Modules 1/1
=====

VLANs: 10-11
```

Fig. Lab 6 Show DSM Redirect

Note

In this example, VLAN 10 is redirected to DSM 1/1 on both switches, however in your lab, you may see redirection to DSM 1/2

5. To visualize the flows, enter diagnostics mode on the switch by entering the following commands:

- `diagnostics`
- `diag dsm console 1/1 or 1/2` (ensure you specify the DSM from the command above)
- `pdctl show flow`

Expected Results

After running the command `pdctl show flow`, you should a table showing the two flows, in each direction.


```

10.250.203.102 - Tera Term VT
File Edit Setup Control Window Help
$
$ pdsctl show flow
Legend
Handle      : Session Handle
Role        : I (Initiator), R (Responder)
Direction   : U (From Uplink), H (From Host)
BridId       : Bridge Domain ID or subnet ID
SIP          : Source IP address
Sport        : Source port for TCP/UDP
ID           : ICMP identifier
DIP          : Destination IP address
Dport        : Destination port for TCP/UDP
Proto        : IP Protocol
Action       : A (Allow), D (Drop), P (Pending evaluation)
-----
Flow-table-0
253      I/H      3      10.0.10.102      7      10.0.10.101      2048      ICMP      A
253      R/H      3      10.0.10.101      7      10.0.10.102      0          ICMP      A
254      I/H      3      10.0.10.101      7      10.0.10.102      2048      ICMP      A
254      R/H      3      10.0.10.102      7      10.0.10.101      0          ICMP      A
No. of flows: 4
Flow-table-1
Flow-table-2
Flow-table-3
Flow-table-4
Flow-table-5
Flow-table-6
Flow-table-7
$

```

Fig. Lab 6 pdsctl show flow

Note

Notice that the action is A (allow) for all 4 flows

Lab 6.4 - Analyze Flow Graphs

Description

The Switches forward flow data to the PSM and using the PSM, you can create different visualizations and dashboards based on that data. During this exercise, we will create some flow graphs to do just that.

Validate

1. In the PSM browser tab, goto **Sytem / DSS** and then click on the *first DSS-ID*

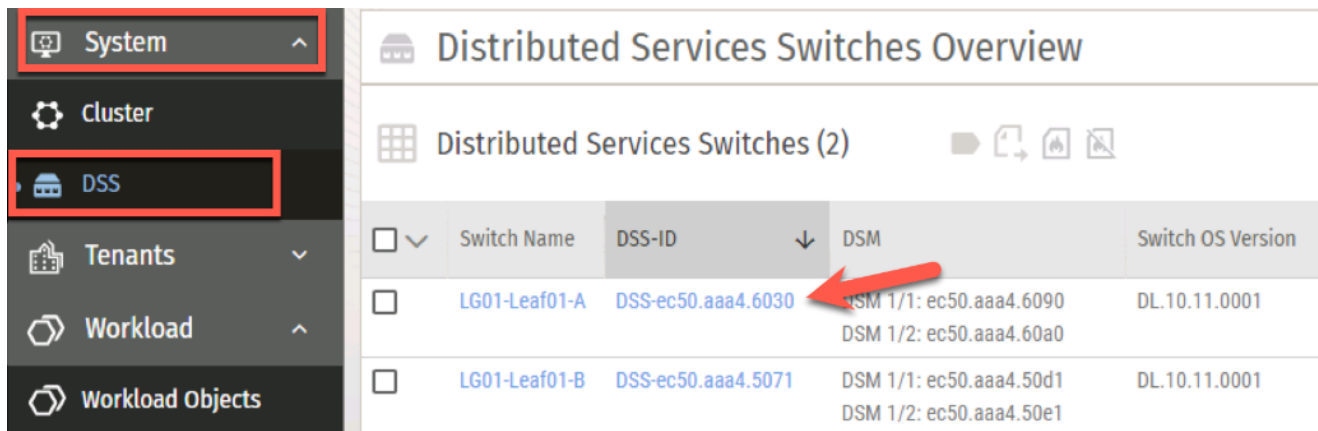


Fig. Lab 6 DSS Overview

2. Scroll down and look to the bottom right to see the graphs.

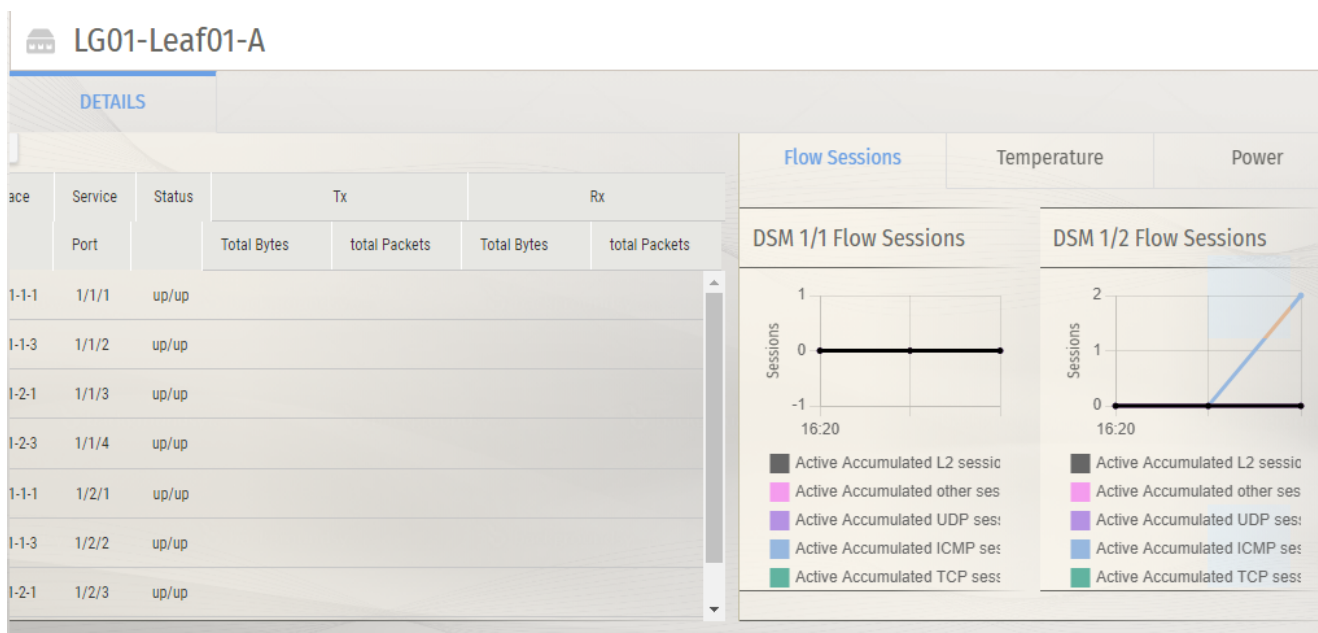


Fig. Lab 6 Flow Graphs

3. Go to **Monitoring / Metrics** and select **CREATE CHART** (top right)
4. Create a chart using the following paramters and save it. For the **Select DSSs** drop down, choose the **both switches**. Make sure to select the **DPU** you saw from the **PDSCCTL** command you ran earlier (should be either 1/1 or 1/2). Once completed, click **Save Chart**

Metrics

Pa

Statistics:

☐ Egress drops

☐ IPsec Decryption Statistics

☐ Ingress drops

☐ Uplink Interface Packet Statistics

☒ Flow Stats Summary

☐ IPsec Encryption Statistics

☐ Network drops

☐ Cluster

Fields:

☐ Accumulated Connection Tracking Disabled sessions over IPv4

☒ Accumulated ICMP sessions over IPv4

☒ Accumulated TCP sessions over IPv4

☒ Accumulated other sessions over IPv4

☐ Active ICMP sessions over IPv4

☐ Active TCP sessions over IPv4

☐ Active other sessions over IPv4

☐ Accumulated Connection Tracking Disabled sessions over IPv6

☐ Accumulated L2 sessions

☒ Accumulated UDP sessions over IPv4

☐ Accumulated session create errors

☐ Active L2 sessions over IPv4

☐ Active UDP sessions over IPv4

Select DSSs:

LG01-Leaf01-B (DSS-ec50.aaa4.5071), LG01-Leaf01-A (DSS-e...

Select Unit:

1/2

Group by:

reporterID & Unit

Fig. Create Chart

Expected Results

Since we should still have ping running between the workloads, we should see a graph similar to the following screenshot. You can use this reporting function from the PSM to visualize all traffic passing through the DSM chips.

my_chart Past day

Sessions

2

1

0

16:20

Accumulated ICMP sessions over IPv4 - LG01-Leaf01-B DSM 1/2

Accumulated UDP sessions over IPv4 - LG01-Leaf01-B DSM 1/2

Accumulated other sessions over IPv4 - LG01-Leaf01-B DSM 1/2

Accumulated TCP sessions over IPv4 - LG01-Leaf01-B DSM 1/2

Accumulated ICMP sessions over IPv4 - LG01-Leaf01-A DSM 1/2

Accumulated UDP sessions over IPv4 - LG01-Leaf01-A DSM 1/2

11 of 23

8/26/24, 18:55

Fig. New Flow Chart

Lab 6.5 - Add Policy Rules

Description

During this exercise, we will use the AFC to modify the policy that we created in an earlier step, and add the following rules between Workload01 and Workload02:

- Allow SSH
- Allow iPerf3 client/server flows (default using TCP port 5201) with the server on Workload02
- Deny All (block everything else, including ping)

Validate

1. Using the browser, navigate back to the Fabric Composer
2. Go to **Configuration / Policy / Rules**
3. Create the first `allow_ssh` Rule using the following settings:

Step 1 - Name	
Name	<code>allow_ssh</code>
Description	(optional)
Click NEXT	

Step 2 - Settings	
Type	Layer 3
Action	Allow
Click NEXT	

Step 3 - Endpoint Groups	
Source Endpoint Groups	<i>Select both Workload Groups</i>
Destination Endpoint Groups	<i>Select both Workload Groups</i>
Click NEXT	

Step 4 - Application and Service Qualifiers	
Applications	SSH
Service Qualifiers	(leave empty)
Click NEXT	
Review the Summary and Click APPLY	

4. Create the second `allow_iPerf_TCP_5201` Rule using the following settings:

Step 1 - Name	
Name	<code>allow_iPerf_TCP_5201</code>
Description	(optional)
Click NEXT	

Step 2 - Settings	
Type	Layer 3
Action	Allow
Click NEXT	

Step 3 - Endpoint Groups	
Source Endpoint Groups	<i>Select both Workload Groups</i>
Destination Endpoint Groups	<i>Select both Workload Groups</i>
Click NEXT	

Step 4 - Application and Service Qualifiers	
<i>Leave the Application box empty and click ADD at the bottom</i>	

Sub-step A - Name	
Name	TCP_5201
Description	(optional)
Click NEXT	

Sub-step B - Settings	
IP Protocol	tcp
Source Port	any
Destination Port	5201
Click ADD (bottom left), NEXT , review the Summary and APPLY	

5. Create the third `deny_all` rule using the following settings:

Note

There is an implicit deny all rule at the end of any policy, so this step is optional

Step 1 - Name	
Name	<code>deny_all</code>
Description	(optional)
Click NEXT	

Step 2 - Settings	
Type	Layer 3
Action	Drop
Click NEXT	

Step 3 - Endpoint Groups	
Source Endpoint Groups	(leave empty)
Destination Endpoint Groups	(leave empty)
Click NEXT	

Step 4 - Application and Service Qualifiers	
Applications	(leave empty)
Service Qualifiers	(leave empty)
Click NEXT	
Review the Summary and Click APPLY	

6. Go to **Policies**, find the **dsf-leafLG-01** policy, and click the **3 dots** to add/modify the rules
7. Select the `allow_all_vlan_10` rule and under **ACTIONS**, click **Remove**
8. Click the **ACTIONS** menu again, and now select **ADD > Existing** in order to add the rules from the previous step, to this policy
9. Select the new rules and click **APPLY**

Select Rules

Select one or more Rules to add to the Policy.

3 selected

Name	Source Endpoint Groups	Source Endpoint G...	Destination Endpoint Gr...	Destination Endpoi...	Applications	Servi
<input type="checkbox"/> allow_all_v10	WL-group-01 WL-group-02	10.0.10.101/32 10.0.10.102/32	WL-group-01 WL-group-02	10.0.10.101/32 10.0.10.102/32		all
<input checked="" type="checkbox"/> allow_iPerf_TCP_5120	10.250.0.50_AFC- integration:Workload01 10.250.0.50_AFC- integration:Workload03	10.0.10.101 10.0.20.201	10.250.0.50_AFC- integration:Workload01 10.250.0.50_AFC- integration:Workload02	10.0.10.101 10.0.10.102		TCP
<input checked="" type="checkbox"/> allow_ssh	10.250.0.50_AFC- integration:Workload01 10.250.0.50_AFC- integration:Workload02	10.0.10.101 10.0.10.102	10.250.0.50_AFC- integration:Workload01 10.250.0.50_AFC- integration:Workload02	10.0.10.101 10.0.10.102	SSH	ssh
<input checked="" type="checkbox"/> deny_all	Any		Any			all

(1 - 4 of 4 total) 25

* = Required

CANCEL APPLY

Fig. Add Rules

Note

Ensure the deny_all rule is the last rule in the policy - this will create a default deny scenario. If the deny all rule is not the last rule, you can change the order by editing the policy.

Expected Results

Our Firewall Policy should now have a zero trust type of behavior, where all East/West traffic on VLAN 10 is dropped, with the exception of SSH between two workloads, and iPerf.

Lab 6.6 - Test Policy Rules

Description

In the previous activity you created new rules for traffic between Workload011 and Workload02, as well as a deny_all rule. Now we will test the behavior of these new rules. Our pings between Workload01 and Workload02 should still be running in the background

as well.

Validate

1. Go back to the SSH session from one of your switches and rerun the command:

```
pdctl show flow
```

Note

In the flow table, notice that now the Action is D (deny) for all 4 flows.

2. Return to the SSH sessions of each workload and stop the ping. Restart the ping and according to the new ruleset, the ping should be blocked.
3. To test SSH on Workload01, run the following command using the credentials `arubadm` / `admin`:
 - `ssh 10.0.10.102`
4. Return to the SSH session of one of your switches. Enter the DSM diagnostics mode (similar to a previous exercise) by running:
 - `diagnostics`
 - `diag dsm console 1/x` (ensure you enter the diagnostics of the DSM which VLAN 10 is redirected to)
 - `pdctl show flow`

Handle	Role/Dir	BdId	SIP	Sport/Id	DIP	Dport/TyCo	Proto	Action
Flow-table-0								
253	I/H	3	10.0.10.102	5	10.0.10.101	2048	ICMP	D
253	R/H	3	10.0.10.101	5	10.0.10.102	0	ICMP	D
No. of flows: 2								
Flow-table-1								
524545	I/H	3	10.0.10.101	33080	10.0.10.102	22	TCP	A
524545	R/H	3	10.0.10.102	22	10.0.10.101	33080	TCP	A

Fig. Show Flow SSH

Note

Notice that the action for the flow to and from port 22 (SSH) is A (Allow)

5. Open the PSM browser tab and refresh the Metrics page. You should see a graph similar to the following screenshot.



Fig. Graph SSH

Expected Results

During this lab we tested the firewall policies that we created from the previous exercise. Ping should now be blocked on VLAN 10, however SSH between our two Workload VMs should still be allowed. The graphs and flow data available in PSM allows us to view all of the allowed and denied traffic patterns.

Lab 6.7 - Testing iPerf

Description

Other than SSH, we also added a rule to test iPerf which is a network performance testing tool. We will configure Workload02 as the iPerf3 server, and Workload01 as the iPerf3 client.

Validate

- Go back to your SSH session on **Workload02** and run the following command in order to start the **iPerf3 server**: `iperf3 -s`

```
-----+-----
Server listening on 5201
-----
```

Fig. iPerf Server

- Go back to the **Workload01** SSH session, and log out of SSH session from **Workload01** to **Workload02** (if still active)
- On **Workload01**, start the iPerf3 client using this command: `iperf3 -c 10.0.10.102 -t 1000`

```
Connecting to host 10.0.10.102, port 5201
[ 5] local 10.0.10.101 port 46200 connected to 10.0.10.102 port 5201
[ ID] Interval           Transfer     Bitrate      Retr  Cwnd
[ 5]  0.00-1.00   sec  1.09 GBytes  9.34 Gbits/sec    0   1.92 MBytes
[ 5]  1.00-2.00   sec  1.09 GBytes  9.36 Gbits/sec    0   1.92 MBytes
[ 5]  2.00-3.00   sec  1.09 GBytes  9.36 Gbits/sec    0   1.92 MBytes
[ 5]  3.00-4.00   sec  1.09 GBytes  9.33 Gbits/sec    0   2.02 MBytes
[ 5]  4.00-5.00   sec  1.09 GBytes  9.36 Gbits/sec    0   2.02 MBytes
[...]
```

Fig. iPerf Client

- Now let's look at the flow table on one of the switches again. On one of the switches, rerun the command: `pdctl show flow`

```
-----+-----
Handle  Role/Dir  BdId  SIP                               Sport|Id  DIP                               Dport|TyCo  Proto  Action
-----+-----
[. . .]
1048832  I/H       3     10.0.10.101                       58208    10.0.10.102                       5201        TCP     A
1048832  R/H       3     10.0.10.102                       5201     10.0.10.101                       58208       TCP     A
No. of flows: 2
[. . .]
3670273  I/H       3     10.0.10.101                       58210    10.0.10.102                       5201        TCP     A
3670273  R/H       3     10.0.10.102                       5201     10.0.10.101                       58210       TCP     A
No. of flows: 2
```

Fig. iPerf Flow Logs

- Go to the PSM UI and refresh the Metrics page one more time. You should see some updated graphs like the following.

HOL

Past day

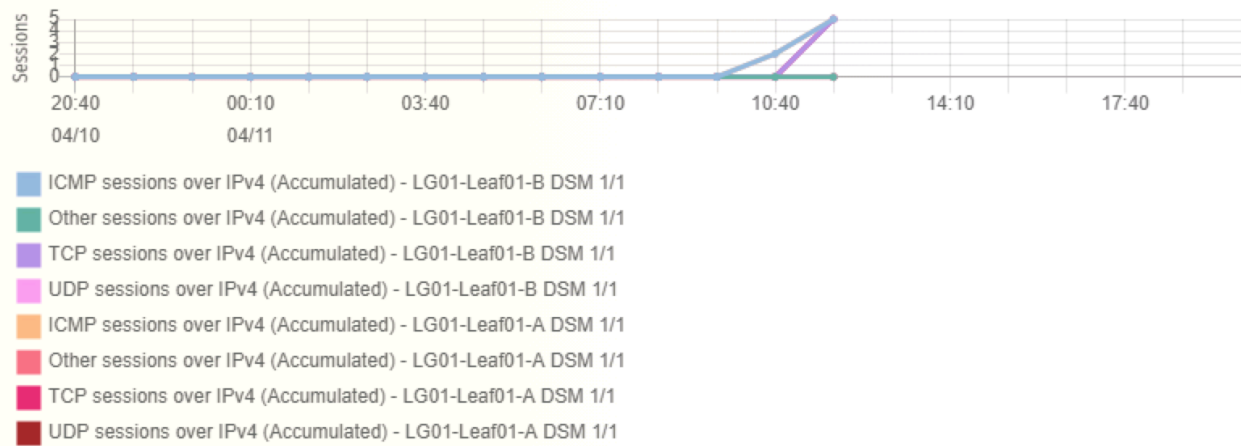


Fig. iPerf Graph

Expected Results

Just like in the previous lab, we should have the behavior that all traffic in VLAN 10 is denied, with the exception of SSH and iPerf. This lab should have confirmed this behavior.

Lab 6.8 - Unique Flows

Description

Enabling stateful services or microsegmentation in a brownfield environment, where little to no enforcement is in place, is not an easy task. This is where some of the built-in metrics to the CX 10000 help. We will look at how to find and analyze unique flows on a given network.

Validate

1. In the PSM UI, navigate to **Tenant / Security Policies**
2. Click the **Table View** menu from the top right corner, and select **Network Graph**

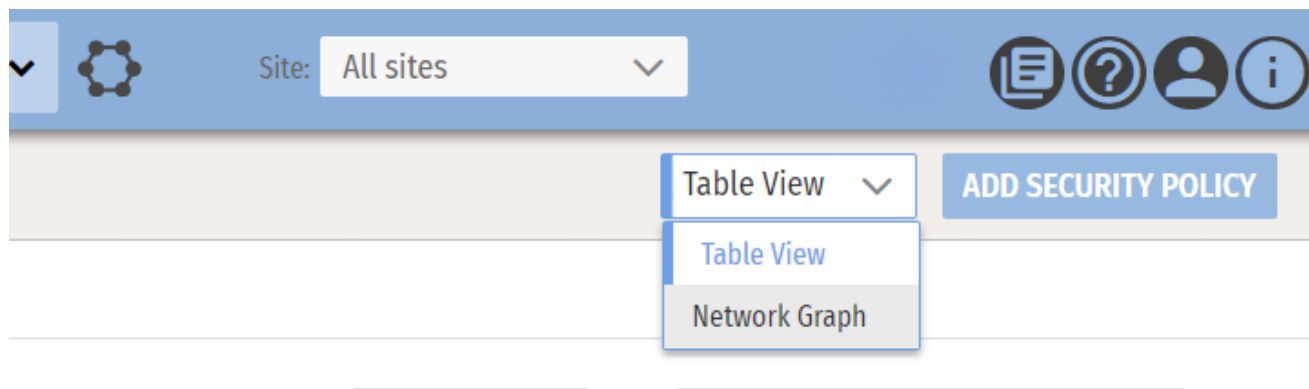


Fig. Network Graph Menu

3. Under the Security Policies filter, select the **default** VRF

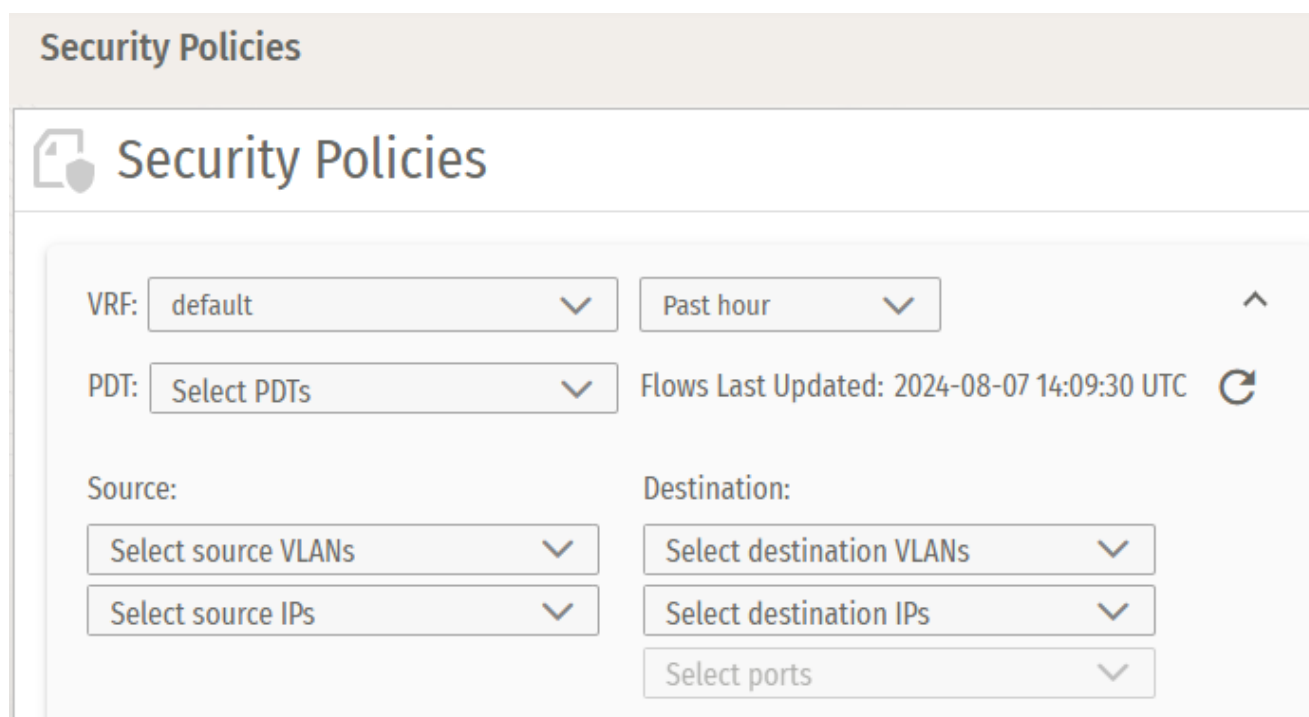


Fig. Security Policies Filter

4. Wait for the data to load and analyze the Unique Flows table on the right hand side.
5. Go to workload01 and stop the ipfer3 client.

Verify the ssh rule is working.

6. Open an SSH session from **workload01** to **workload02**

- `ssh arubadm@10.0.10.102`

Expected Results

The SSH session should connect, if not check the rules assigned to the policy.

Using the Unique Flows function from the PSM, we are able to see all of our unique flows on VLAN, over a specified time period. Having this level of data is crucial for implementing stateful services on your network.

Lab 6 Summary

- We added a Switched Virtual Interface to the switch for VLAN 10
- We verified that the traffic for VLAN 10 is successfully redirected over the AMD DSM, and become stateful
- We analyzed the DSM flow tables to see allowed or denied traffic
- We set up a zero trust and microsegmentation policy for VLAN 10, where all traffic is denied, with the exception of iPerf and SSH between two workloads
- We verified that the firewall policies that we defined for VLAN 10 are enforced
 - SSH (tcp 22) between Workload01 and Workload02 is open
 - iPerf3 (tcp 5201) between Workload01 and Workload02 is open
 - All other traffic patterns are denied - we verified this by attempting a ping from one workload to the other