Lab 5 - Microsegmentation

Contents

- Lab Overview
- Lab 5.1 - Create Endpoint Group for Workloads
- Lab 5.2 - Create Firewall Rule
- Lab 5.3 - Create Firewall Policy
- Lab 5.4 - Configure Microsegmentation
- Lab 5 Summary
- Lab 5 Learning Check

Lab Overview

Lab time: 40 minutes

In the previous labs, we built a fabric, attached switches, and added integrations with vSphere and the PSM. There are several workload VMs running in each lab and during this lab, we will levarage the integrations to build firewall policies to microsegment the workloads from each other.

Lab 5.1 - Create Endpoint Group for Workloads

Description

In this task, you will create 2 endpoint groups. An endpoint group in Fabric Composer is a set of VMs that have the same set of policy rules.

Validate

1. Using the AFC, select **Policy** and then **Enpoint Groups** from the top level menu

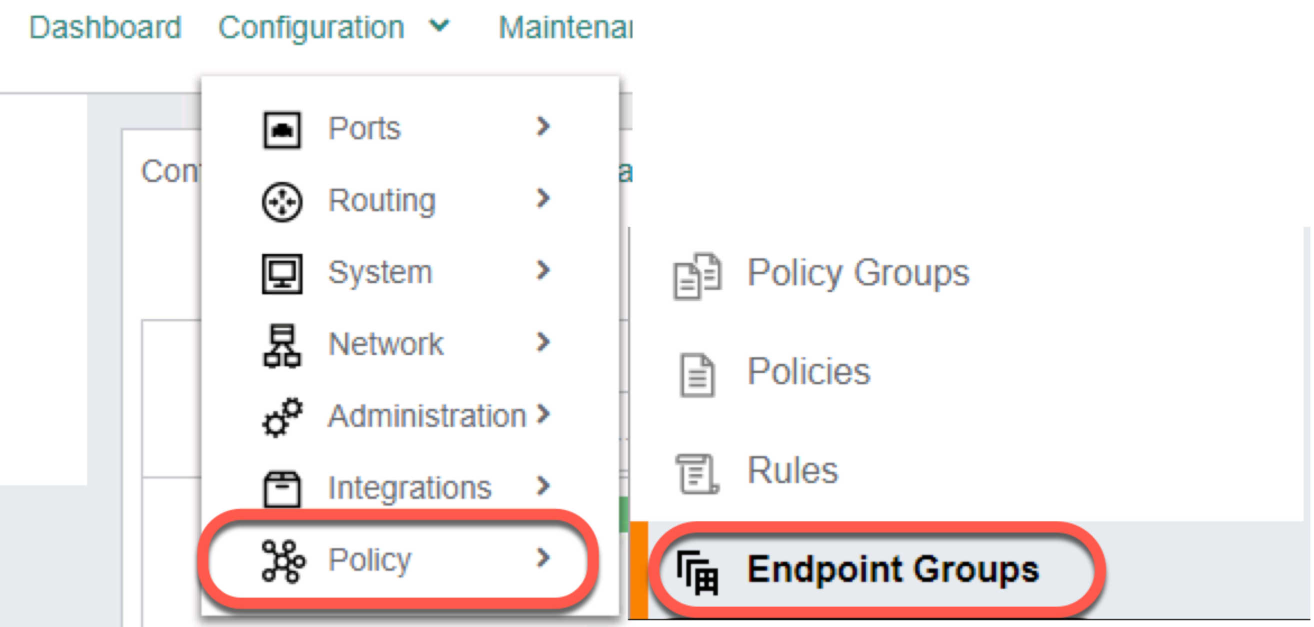


Fig. Lab 5 Endpoint Groups Menu

2. From the **ACTIONS** menu, select **Add**

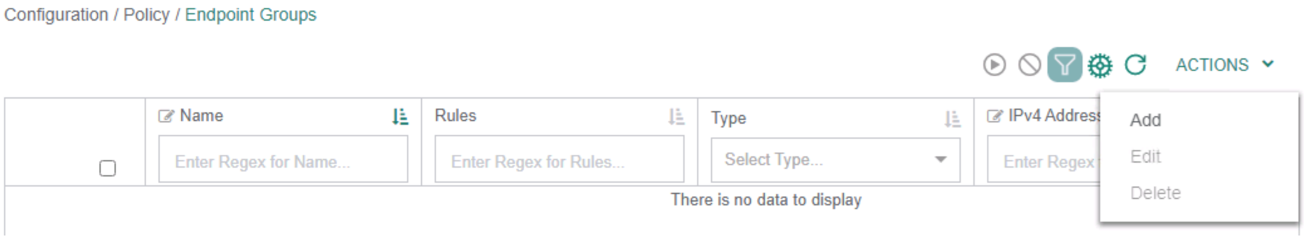


Fig. Lab 5 Add Endpoint Group

3. Create an Endpoint Group for Workload01

Step 1 - Name	
Name	WL-group-01
Description	(optional)
Click NEXT	

Step 2 - Type	
Type	Layer 3 - IP Address
Click NEXT	

Step 3 - Endpoints	
VM/VNIC/VMKernel Endpoint	Yes (selected)
Criteria	VM Tag* (select from the pull down menu)
VM Tag	`AFC-Integration.Workload01` (Look for your **Lab Group** Number)
VNIC	Select any ***Network Adapter 2*** with `10.0.10.101`
Scroll down, ***click ADD, NEXT and APPLY***	

4. Create an Endpoint Group for Workload02

Step 1 - Name	
Name	WL-group-02
Description	(optional)
Click NEXT	

Step 2 - Type	
Type	Layer 3 - IP Address
Click NEXT	

Step 3 - Endpoints	
VM/VNIC/VMKernel Endpoint	Yes (selected)
Criteria	VM Tag* (select from the pull down menu)
VM Tag	`AFC-Integration.Workload02` (Look for your **Lab Group** Number)
VNIC	Select any ***Network Adapter 2*** with `10.0.10.102`
Scroll down, ***click ADD, NEXT and APPLY***	

Expected Results

The Endpoint Groups should have been created based on VM Tag and visible in the list.

Lab 5.2 - Create Firewall Rule

Description

When enabling Microsegmentation, an explicit Deny All rule is placed at the bottom of the rule list, which acts as a catch all. For the purpose of these labs and in order to test the Switch Firewalling functionality, we will place an **Allow All** rule at the bottom, and add specific Deny rules above it.

Validate

1. Using the AFC, select **Policy** and then **Rules** from the top level menu, or if still visible, select **Rules** from the left menu.
2. From the **ACTIONS** menu, select **Add** to add a new Rule

Step 1 - Name	
Name	allow_all_v10
Description	(optional)
Click NEXT	

Step 2 - Settings	
Type	Layer 3
Action	Allow
Click NEXT	

Step 3 - Endpoint Groups	
Source Endpoint Groups	`WL-group-01` and `WL-group-02`
Destination Endpoint Groups	`WL-group-01` and `WL-group-02`
Click NEXT	

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

Expected Results

The Allow All rule should be successfully created and visible in the list of Rules.

Lab 5.3 - Create Firewall Policy

Description

Firewall Rules are placed in Policies and are enforced in a top to bottom fashion. We will create a Policy in this lab, and assign our Allow All rule to it.

Validate

1. Using the AFC, select **Policy** and then **Policies** from the top level menu, or if still visible, select **Policies** from the left menu.
2. From the **ACTIONS** menu, select **Add** to add a new Rule

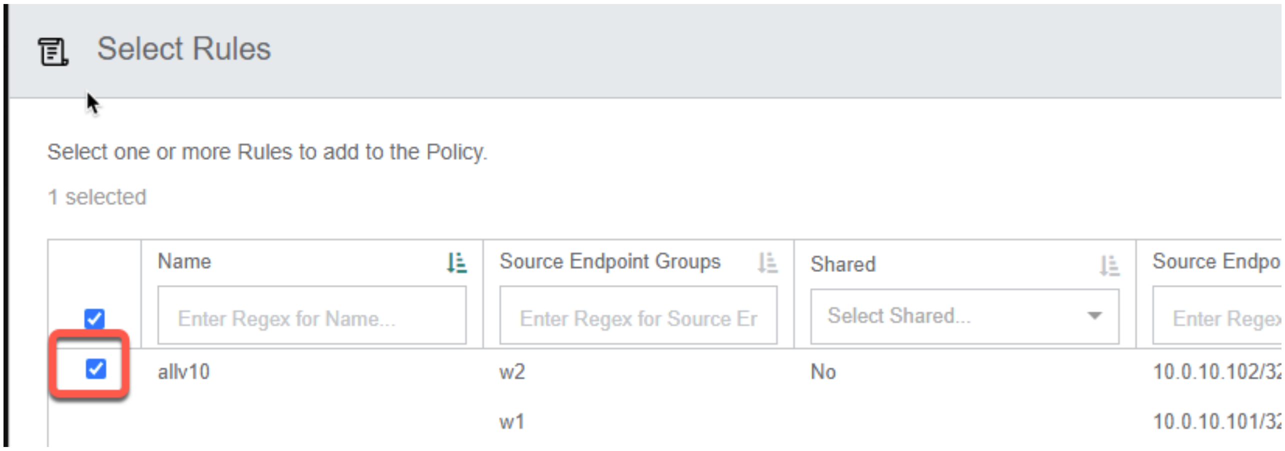
Step 1 - Name	
Name	dsf-leaf**LG**01
Description	(optional)
Click NEXT	

Step 2 - Settings	
Type	*Distributed Firewall **
Click NEXT	

> ℹ **Note**
>
> - For other CX switches, that are non CX-10K, you can use this same procedure to configure L2 or L3 ACLs

Step 3 - Rules

Go to **ACTIONS / ADD / Existing** (top right of this form)



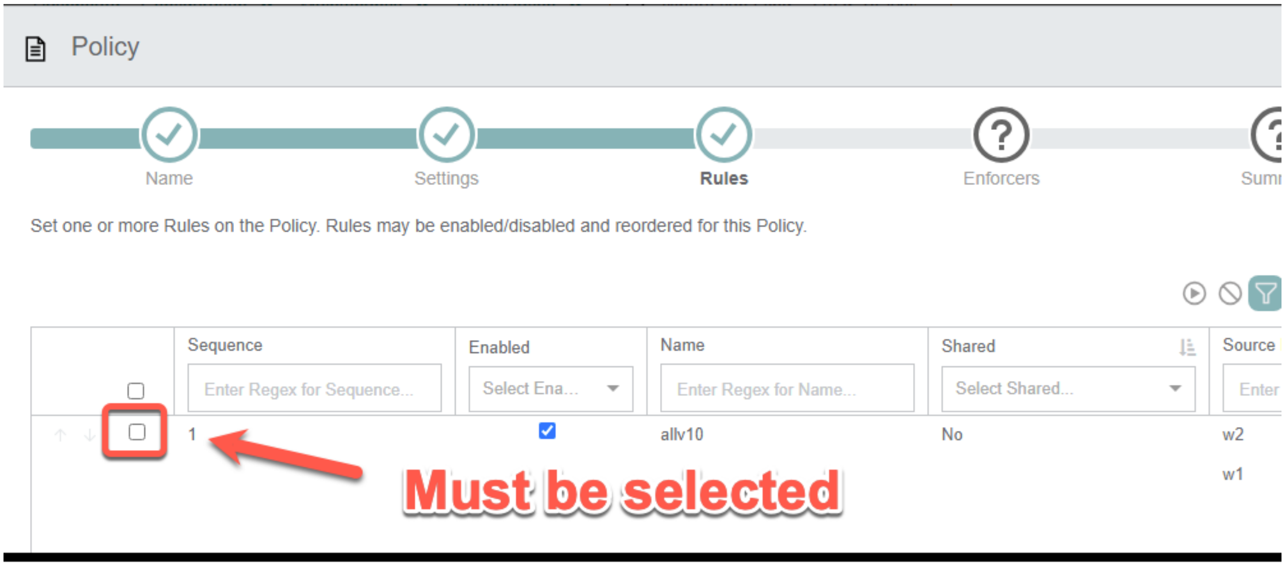
Select Rules

Select one or more Rules to add to the Policy.

1 selected

☑	Name	Source Endpoint Groups	Shared	Source Endpo
	Enter Regex for Name...	Enter Regex for Source Er	Select Shared...	Enter Regex
☑	allv10	w2 w1	No	10.0.10.102/32 10.0.10.101/32

Click APPLY



Policy

Set one or more Rules on the Policy. Rules may be enabled/disabled and reordered for this Policy.

□	Sequence	Enabled	Name	Shared	Source
	Enter Regex for Sequence...	Select Ena...	Enter Regex for Name...	Select Shared...	Enter
□	1	☑	allv10	No	w2 w1

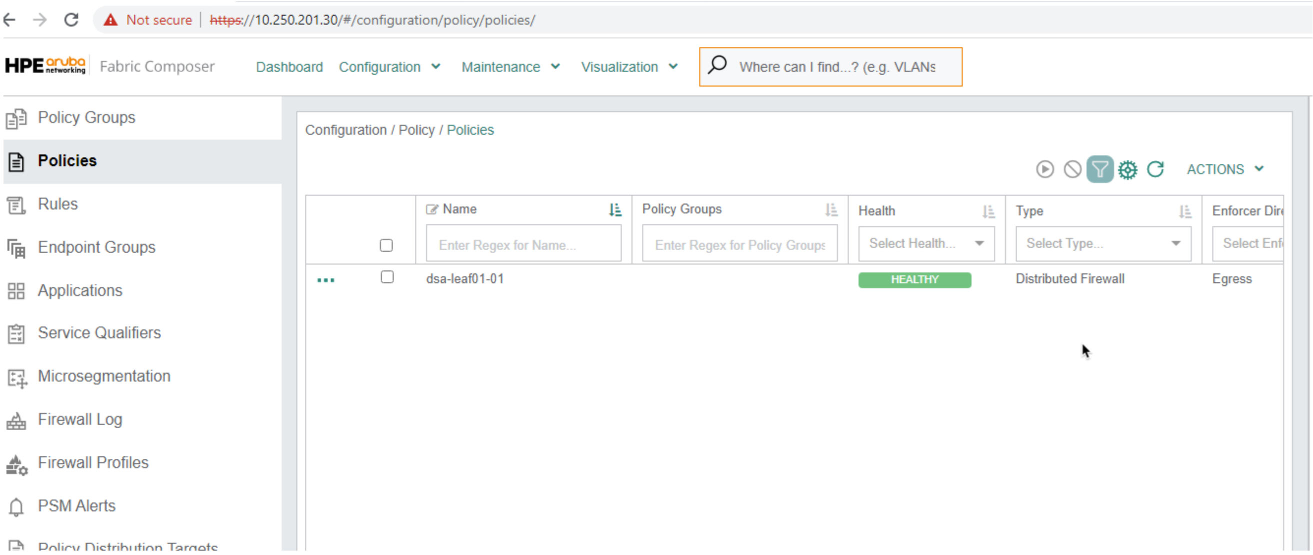
If you don’t select this there will only be an implicit deny all rule in the policy and nothing will ping!

Click NEXT

Step 4 - Enforcers		
Fabric	dsf	
Policy Distribution Target Type	Select **LEAF** from the dropdown	
Direction	Egress (direction is selected from the point of view of the workload/host)	
VRF	default	
Networks	Select **ADD** on the right side of this option to add the network (one or more VLANs)	
	Sub-step A - Name	
	Name	VLAN10
	Description	(optional)
	Click NEXT	
	Sub-step B - Settings	
	VLAN	10
	Click NEXT	
	Review the Summary and ***APPLY***	
Scroll down, click ***ADD*** (at bottom of dialog) and ***NEXT***		
Review the Summary and ***APPLY***		

Expected Results

The newly created Policy should appear in the Policy list (see screenshot below).


Not secure | https://10.250.201.30/#/configuration/policy/policies/
HPE aruba networking Fabric Composer
Dashboard
Configuration
Maintenance
Visualization
Where can I find...? (e.g. VLANs
Policy Groups
Policies
Rules
Endpoint Groups
Applications
Service Qualifiers
Microsegmentation
Firewall Log
Firewall Profiles
PSM Alerts
Policy Distribution Targets
Configuration / Policy / Policies
ACTIONS

Name	Policy Groups	Health	Type	Enforcer Dir
Enter Regex for Name...	Enter Regex for Policy Groups	Select Health...	Select Type...	Select Enf
dsa-leaf01-01		HEALTHY	Distributed Firewall	Egress

Fig. Lab 5 Policy List

Lab 5.4 - Configure Microsegmentation

Description

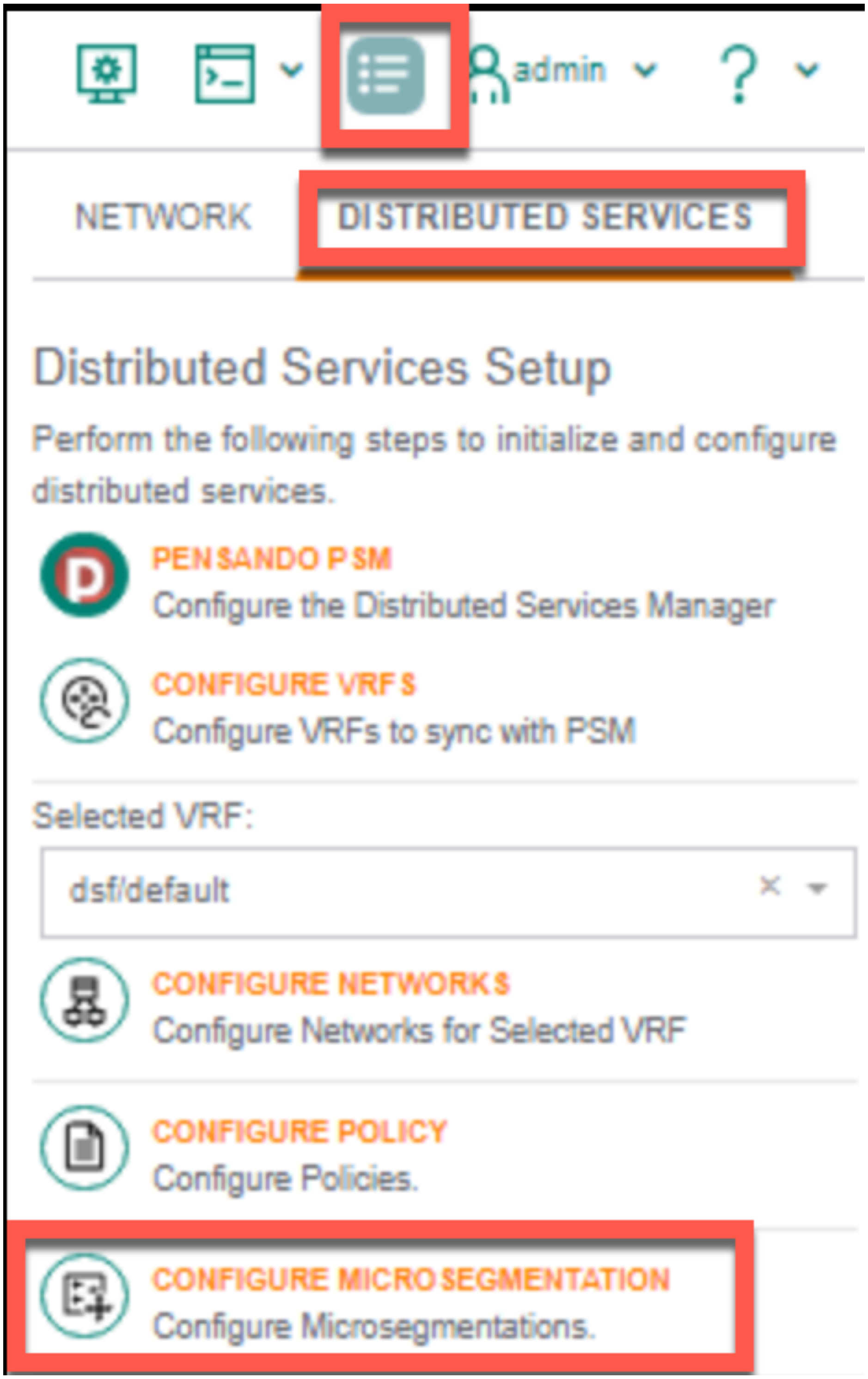
A microsegmentation is a set of configurations starting with a private/isolated VLAN on the host that extends to the switch. On the switch, that VLAN is redirected to the Pensando DSM processor for policy enforcement.

We will use the Microsegmentation Configuration in Fabric Composer which will:

- Creates, on the host:
  - A Distributed Virtual Switch
  - Two Port Groups: one for the private primary VLAN and another for the isolated VLAN
- Creates, between the host and the Switches:
  - A Link Aggregation Group transporting that VLAN (as a promiscuous port)

Validate

1. Using the AFC, we will use the Guided Setup menu on the right side. Go to **DISTRIBUTED SERVICES** and select **CONFIGURE MICROSEGMENTATION**



Distributed Services Setup

Perform the following steps to initialize and configure distributed services.

PENSANDO PSM
Configure the Distributed Services Manager

CONFIGURE VRFS
Configure VRFs to sync with PSM

Selected VRF:

dsf/default

CONFIGURE NETWORKS
Configure Networks for Selected VRF

CONFIGURE POLICY
Configure Policies.

CONFIGURE MICROSEGMENTATION
Configure Microsegmentations.

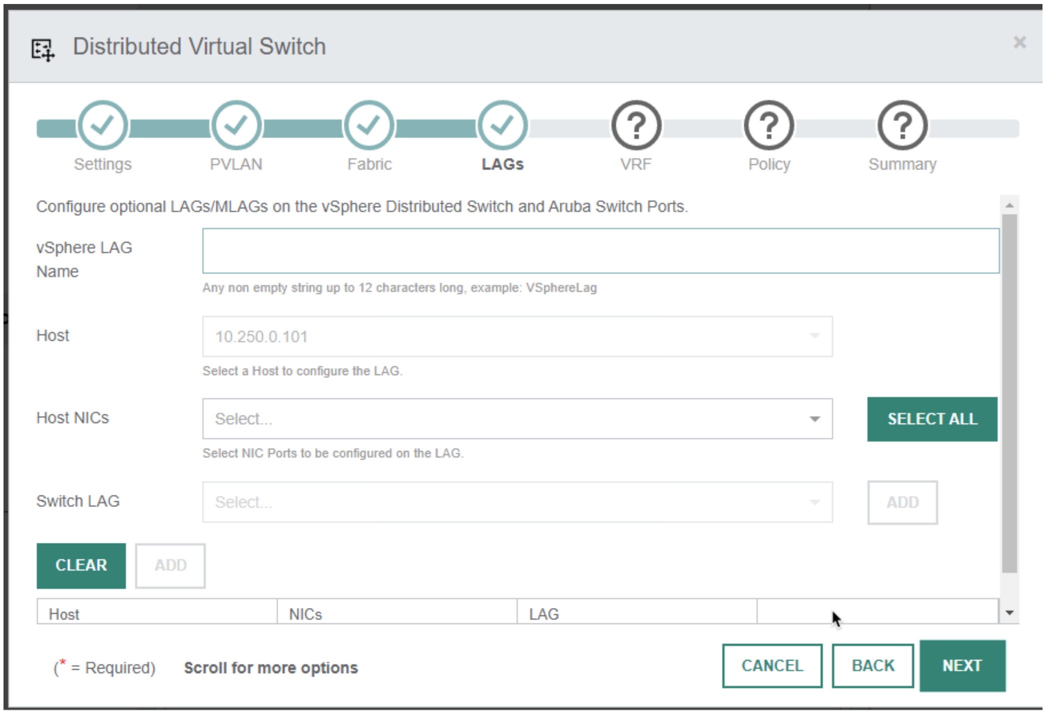
Fig. Lab 5 Configure Microsegmentation

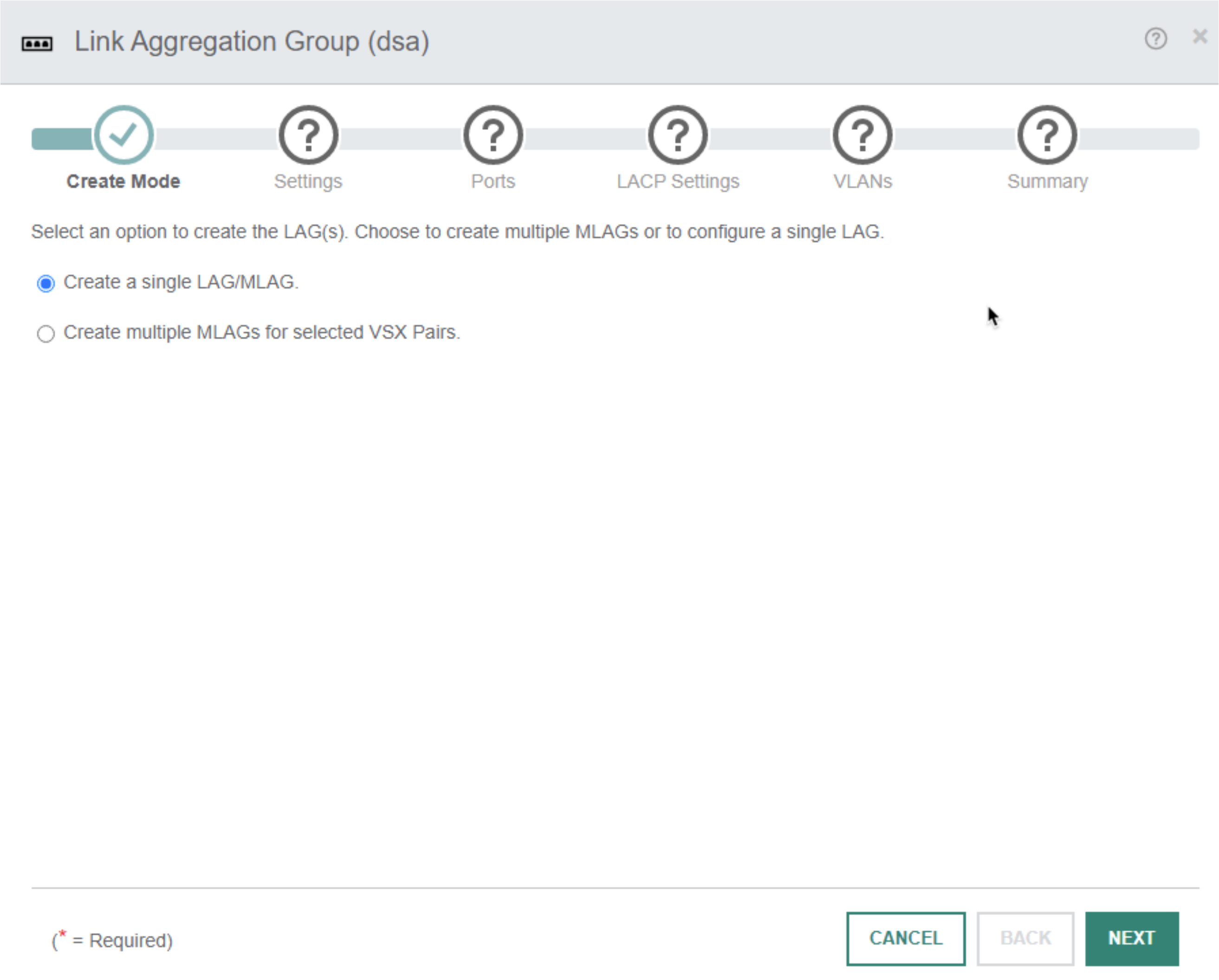
Step 1 - Settings	
Name (dvswitch)	dsf-leaf**LG** (LG = Lab Group Number)
Host	Enter the address of your host (see table below)
NICs	vmnic6 and vmnic7
Click ADD and NEXT	

Lab Group	vSphere Host	Lab Group	vSphere Host
01	10.250.0.101	06	10.250.0.106
02	10.250.0.102	07	10.250.0.107
03	10.250.0.103	08	10.250.0.108
04	10.250.0.104	09	10.250.0.109
05	10.250.0.105	10	10.250.0.110

Step 2 - PVLAN	
Portgroup Name Prefix	dsf-leaf**LG** (LG = Lab Group Number)
Primary VLAN	10
Primary VLAN NICS	**(do NOT select any)**
Isolated VLAN	11
Isolated VLAN NICS	Click **SELECT VNICS**
	Scroll down, select both Network Adapter 2 with IP address: `10.0.10.101` and `10.0.10.102`
	Note: workloads must be connected to the isolated VLAN
Click NEXT	

Step 3 - Fabric	
Fabric	dsf
Click NEXT	

Step 4 - LAGs	
	 Distributed Virtual Switch Settings · PVLAN · Fabric · **LAGs** · VRF · Policy · Summary Configure optional LAGs/MLAGs on the vSphere Distributed Switch and Aruba Switch Ports. vSphere LAG Name: Any non empty string up to 12 characters long, example: VSphereLag Host: 10.250.0.101 Select a Host to configure the LAG. Host NICs: Select... SELECT ALL Select NIC Ports to be configured on the LAG. Switch LAG: Select... ADD CLEAR ADD Host | NICs | LAG (* = Required) **Scroll for more options** CANCEL BACK NEXT
vSphere LAG Name	dsf_lag_lg**LG**
Host	(pull down menu and use the pre-populated address)
Host NICS	vmnic6 and vmnic7
Switch LAG	Click **ADD** on the right to configure the LAG on the CX10k VSX pair



Link Aggregation Group (dsa)

Select an option to create the LAG(s). Choose to create multiple MLAGs or to configure a single LAG.

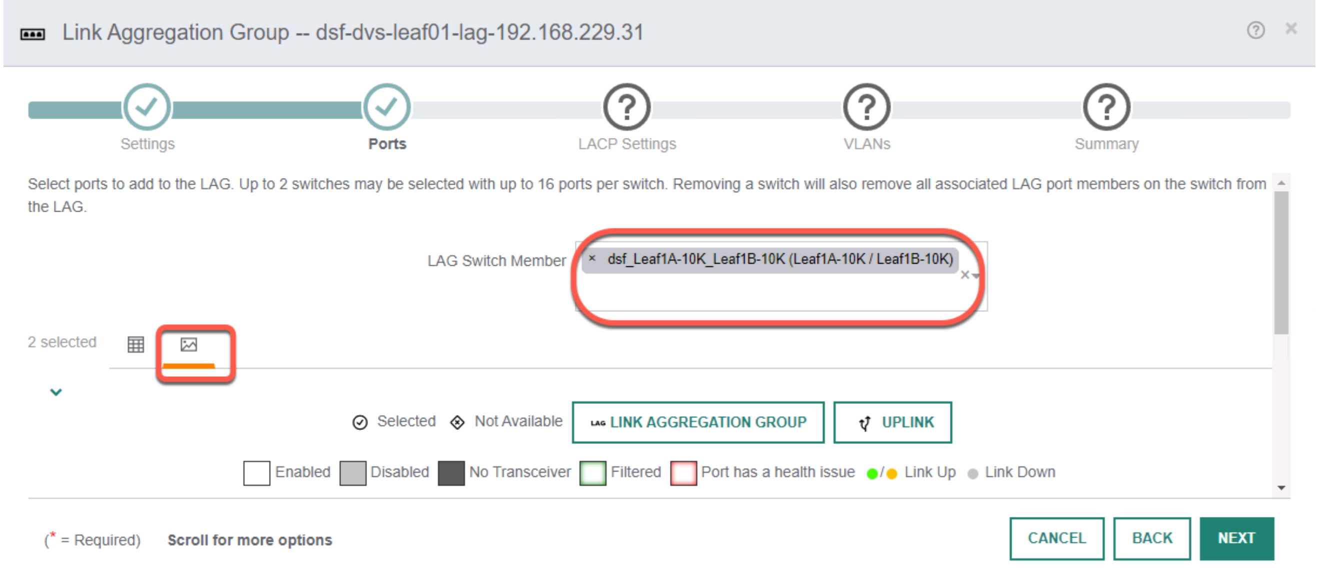
● Create a single LAG/MLAG.

○ Create multiple MLAGs for selected VSX Pairs.

(* = Required)

	Sub-step A - Settings	
	Create Mode	Create a single LAG/MLAG *(default)*
	Click NEXT	
	Name	`dsf_lag_lgLG-10.250.0.10LG` *(pre-populated)*
	Description	(optional)
	LAG Number	31
	Inter-Switch Link	**Check it! (if not greyed out)**
	Click NEXT	
	Sub-step B - Ports	
	LAG Switch Member	`dsf_LGLG-Leaf01A-Leaf01B`

> **Note**
>
> Select the LAG Switch Member and then click the small picture icon as highlighted in the following screenshot to view the port selection on the switches



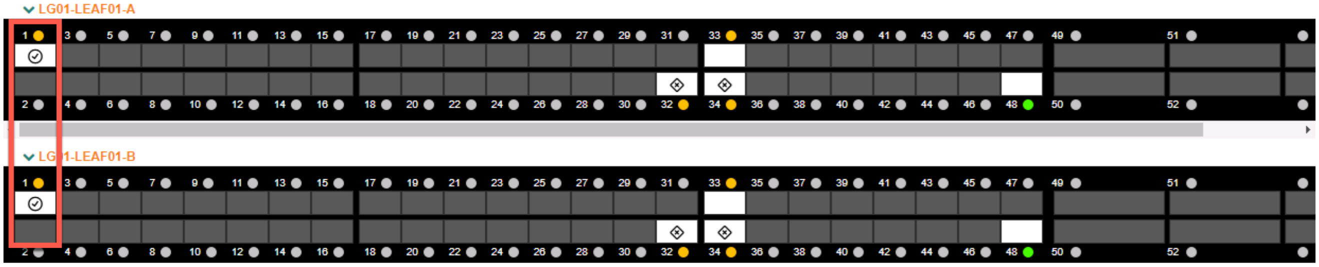
Link Aggregation Group -- dsf-dvs-leaf01-lag-192.168.229.31

Select ports to add to the LAG. Up to 2 switches may be selected with up to 16 ports per switch. Removing a switch will also remove all associated LAG port members on the switch from the LAG.

LAG Switch Member: dsf_Leaf1A-10K_Leaf1B-10K (Leaf1A-10K / Leaf1B-10K)

2 selected

> **Note**
>
> Select the switch ports as highlighted in the following screenshot



	Click ***NEXT*** after port selection *(see screenshots above)*	
	Sub-step C - LACP Settings	
	Review and ***click NEXT***	
	Sub-step D - VLANs	
	VLANs	**10,11** (should be populated)
	Click NEXT and APPLY	
	In the DVS Task main window, ***click ADD*** at the bottom left	

Step 5 - VRF
Leave emtpy and click ***NEXT***

Step 6 - Policy
Leave emtpy and click ***NEXT***

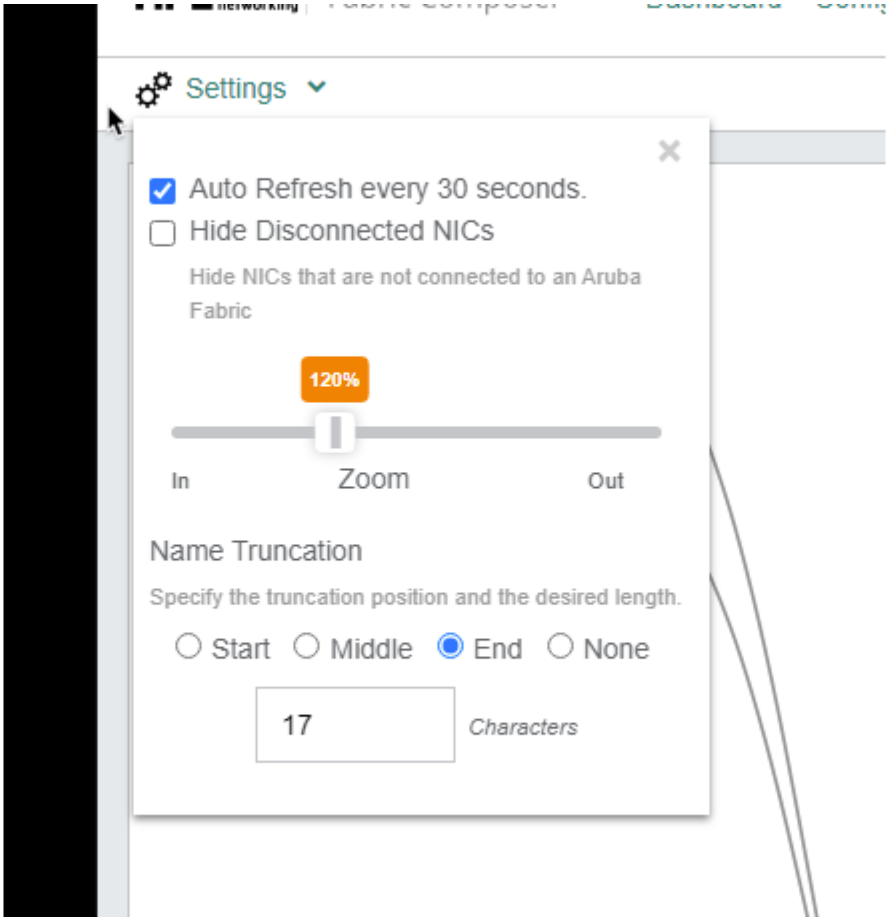
Step 7 - Summary

Review the Summary and click ***APPLY***

Expected Results

To confirm that Microsegmentation has been properly configured, click ***Visualization / Hosts*** from the top menu.

On the left side fo the map, under **Settings**, you can use the **Zoom Out** function until you can see the whole diagram. Also under **Settings**, select **Name Truncation: None**



☑ Auto Refresh every 30 seconds.

□ Hide Disconnected NICs

Hide NICs that are not connected to an Aruba Fabric

Zoom: 120% (In — Out)

Name Truncation

Specify the truncation position and the desired length.

○ Start ○ Middle ● End ○ None

17 Characters

Fig. Lab 5 Diagram Settings

Check the diagram to verify the connections and make sure you are looking at your specific Lab Group.

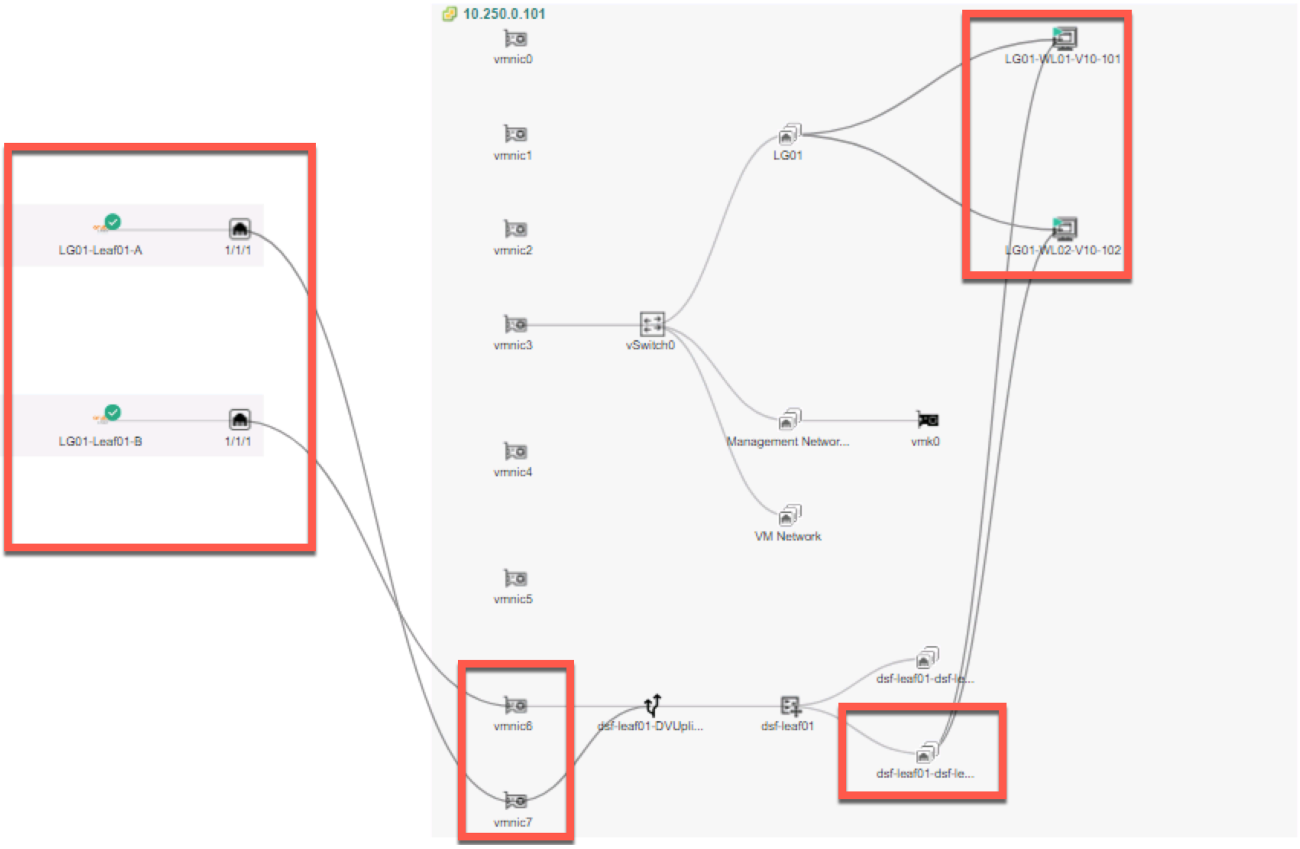


Fig. Lab 5 Host Visualization

> **Note**
>
> The VMs are connected to the Isolated VLAN 11 port group. And now you see the switch connections

Lab 5 Summary

- During this lab, we enabled microsegmentation on the CX 10000 switches
- We created Endpoint Groups for each of the workloads running in the lab
    - We used VM Tags for matching to demostrate how to create dynamic firewall rules
- We created an Allow All firewall rule
- We created a firewall policy and added the Allow All rule to that policy
- We use the AFC to activate Microsegmentation
    - We created a Private VLAN and added our test workload vNICs to this new Private VLAN to ensure VM isolation

Lab 5 Learning Check

- Endpoint Groups can be created manually or automatically learned from VMware
- Rules are added to policies.
- Policies are atuomatically sent to the AMD Pensando Policy Services Manager(PSM)
- PSM programs the DPU chips on the HPE Aruba CX 10000 switch