# HPE Aruba Networking

## CX 10000 Collapsed Core

## CX IPFIX Telemetry

Aniruddha Jasu

Technical Marketing Engineer

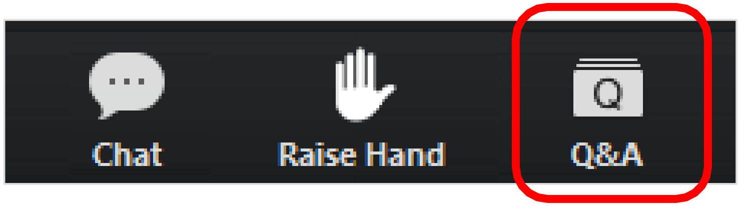
11th July 2024

# Before we begin…

- Listen by computer audio or dial-in

- All lines are muted during the webinar

- Ask *questions by selecting “Q&A”* and to report any webinar difficulties



- Webinar is being recorded & will be emailed to all attendees

# Agenda

Why we need CX 10000 in 2-tier architecture?

Solution Components

Configuration and deployment

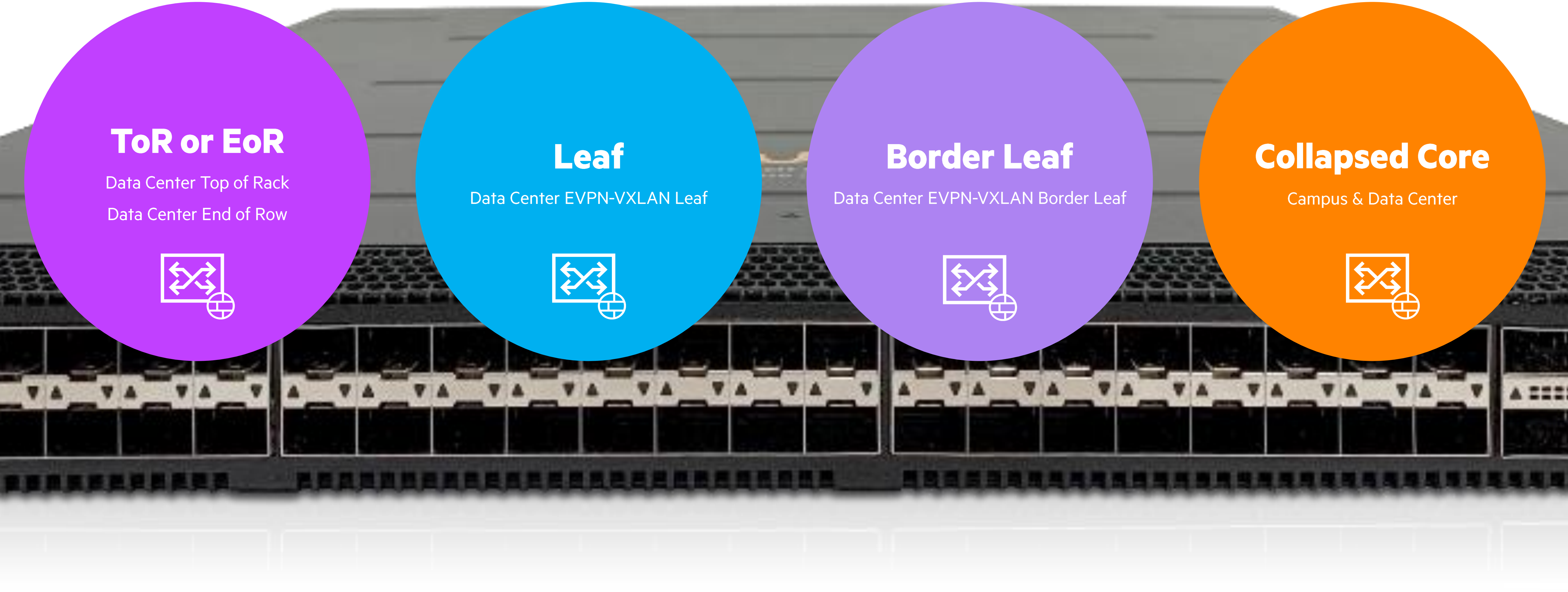
10K Collapsed Core Use Cases

CX 10K Telemetry(IPFIX) Demo

Partner Resources

# HPE Aruba Networking CX 10000 Series Switch

## Deploy software-defined stateful services



### ToR or EoR

Data Center Top of Rack

Data Center End of Row

### Leaf

Data Center EVPN-VXLAN Leaf

### Border Leaf

Data Center EVPN-VXLAN Border Leaf

### Collapsed Core

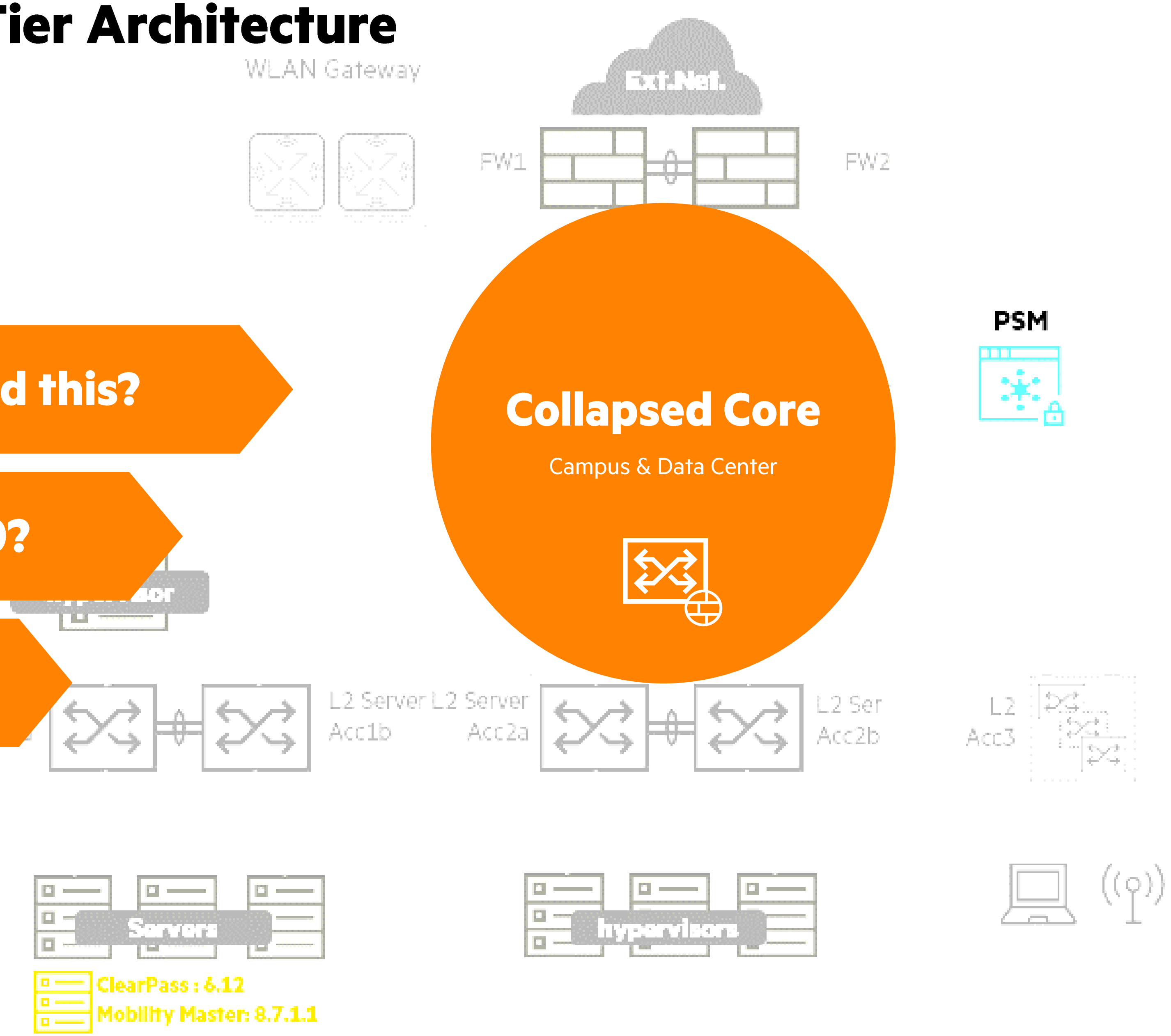
Campus & Data Center

# HPE Aruba Networking CX - 2-Tier Architecture

Why do we need this?

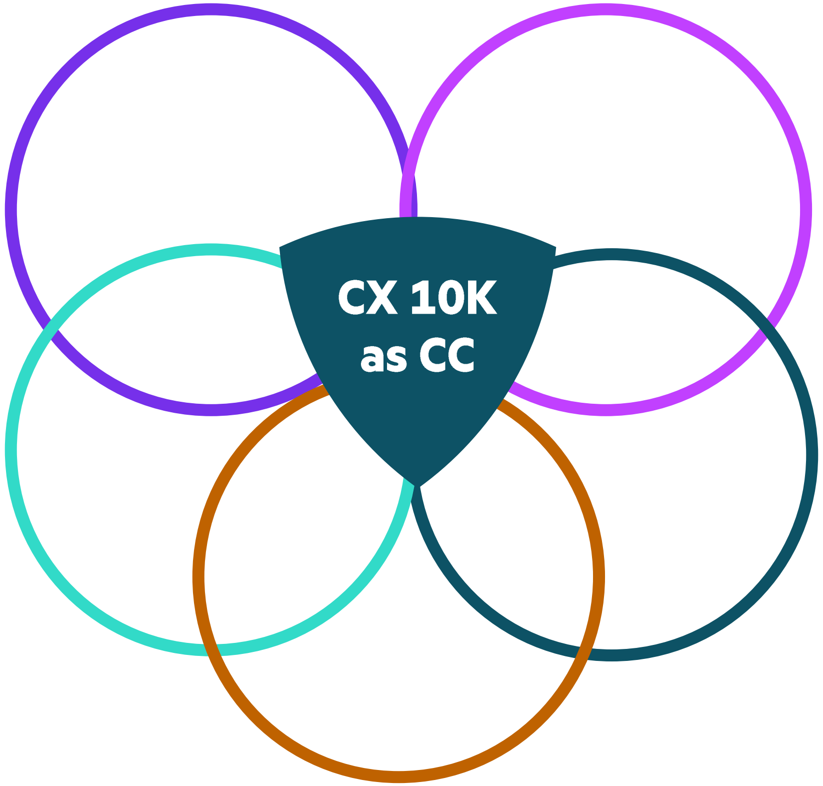
Why CX 10000?

How to achieve?



# Why we need 2-tier Collapsed Core architecture with CX 10000

**Telemetry:**
Improved visibility w/integrated telemetry. 10K Network flows and FW Syslog records can be exported to external collector.



**800G Stateful Firewall Inspection:**
Intra and Inter VRF -
Macro Segmentation,
Intra VRF -
Micro Segmentation

**No need for:**
Dedicated DC or Campus Core

**No need for:**
External firewalls for E-W traffic inspection

**Ability to limit Distributed Denial-of-Service(DDoS) attacks**

# Why CX 10000?

- Fully programmable Network OS and DPU.
- Distributed services architecture, stateful software-defined services inline.
- Security and Services offload at very high scale.
- Simple and efficient Provisioning, Operation and Flow visibility.

# How to achieve?

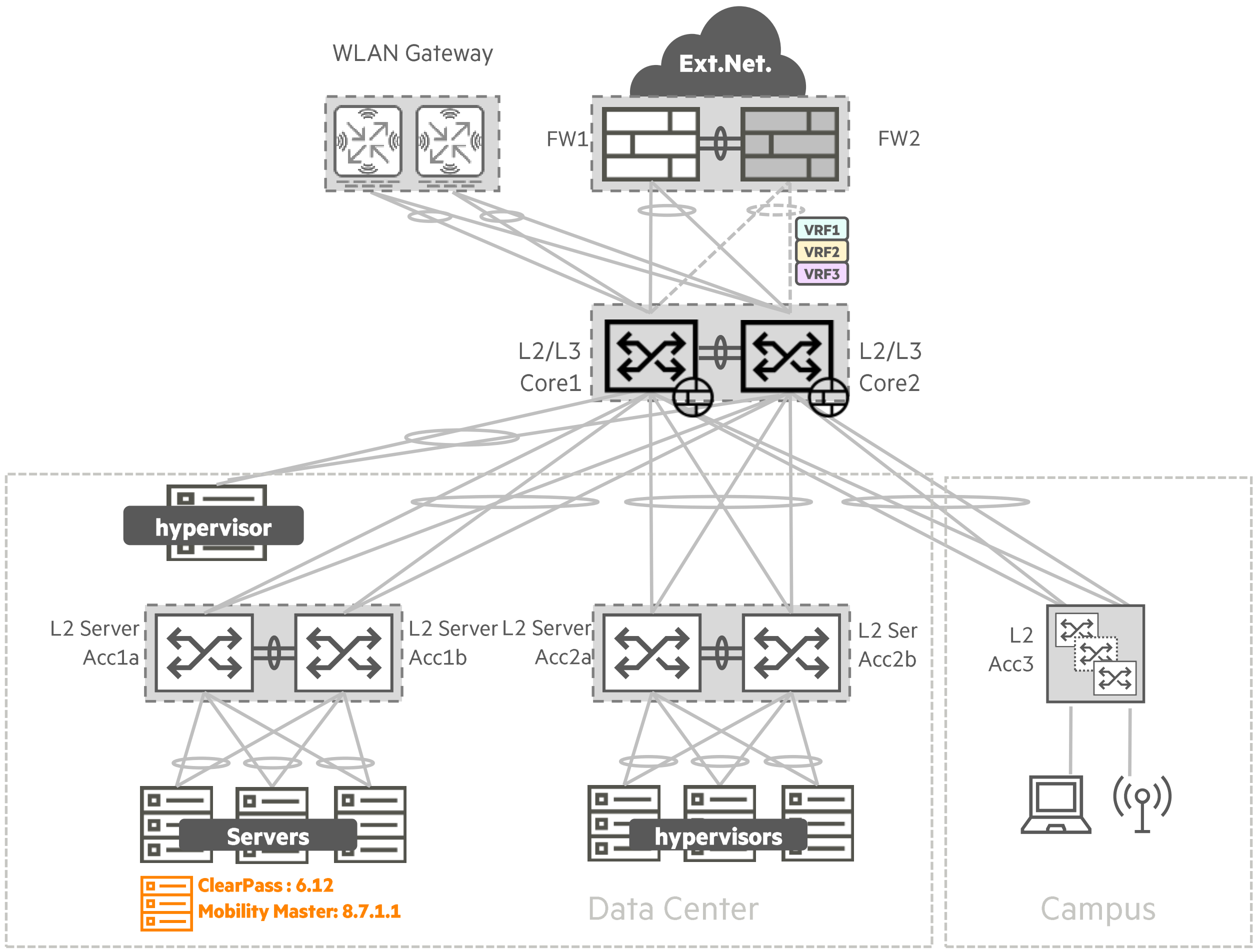
## Solution Components

- CX 10000 (VSX) functions as combined L2/L3 Core and L3 DG for all VLANs.
- Servers may have direct/indirect connection to Core.
- All traffic to Core gets inspected via Policy and Services Manager.
- WLAN Gateway and external FW connection to Core, ClearPass, WLAN MM could be on Server Access.

- DC Server Access(VSX or Standalone) and Campus Access(VSF or Standalone).
- Maximum of Four DC racks – CX8100, CX8360, CX8325.
- Maximum of eight to sixteen Campus Access switches – CX 6200, CX 6300.
- North-South L3-L7 Firewall may send default route to Core via OSPF, per VRF(4 VRFs).

# 10K Collapsed Core - Architecture

## 2 Tier (L2 server access / L3 core) Combined Campus and DC 10K Core with Stateful Firewall



— L2
— L3

Core: 10000-48Y6C - AOS-CX Version 10.13.1001, Profile L3-Agg, PSM: 1.80.1-T-7
Server Access: 8100-XX/8360-XX – With 8360 AOS-CX Version 10.13.1000, Profile-Agg-Leaf
Access: 6200-XX/6300-XX - 10.13.1000

### Campus Environment:

- Dynamic Segmentation (User-Based Tunneling) from switch to gateway inspected (tunnel traffic from gateway to Core is inspected) - Establish UBT between Campus access switches and wireless controllers and inspect the tunnelled traffic with DSM.
- Port access authentication from Campus access to ClearPass (EAP traffic is inspected. By DSM). **Caveat**: Any fragmented IP packet(for example: EAP-TLS) is dropped by DSM. Fix in-progress.

### DC Environment:

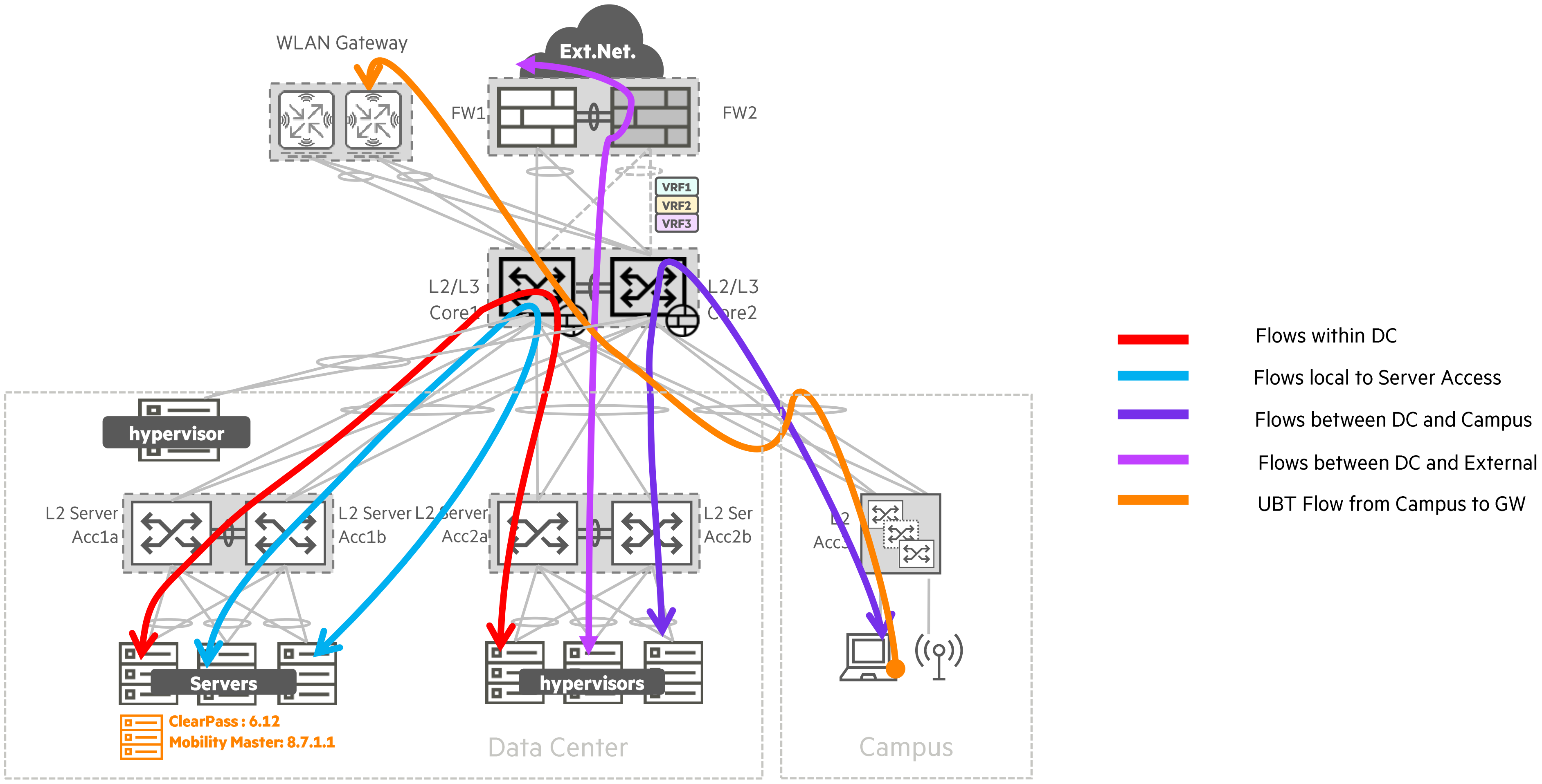
- Moving Workloads: Traffic is redirected to DSM, Using vMotion, move workloads within the rack and between server racks with traffic loss less than 1sec. TCP traffic should continue to pass traffic after moving back and forth. **Source and Destination CX 10Ks should be managed by same PSM.**
- Inter-VRF and Intra-VRF Macro Segmentation.
- Intra-VRF Micro Segmentation.

**Out of Scope: (from this presentation)**

- FW inspection for storage traffic (iSCSI etc),
- L3 default gateway on N/S firewall
- L2 external transparent firewall integration
- WLAN, GRE tunnels from AP to Gateway with firewall enabled.
- Micro segmentation, PVLAN from Core/Campus Access
- AFC/Central integration
- IPSec, NAT, IPv6
- External/Public Cloud connectivity

# 10K Collapsed Core

## Traffic Flows

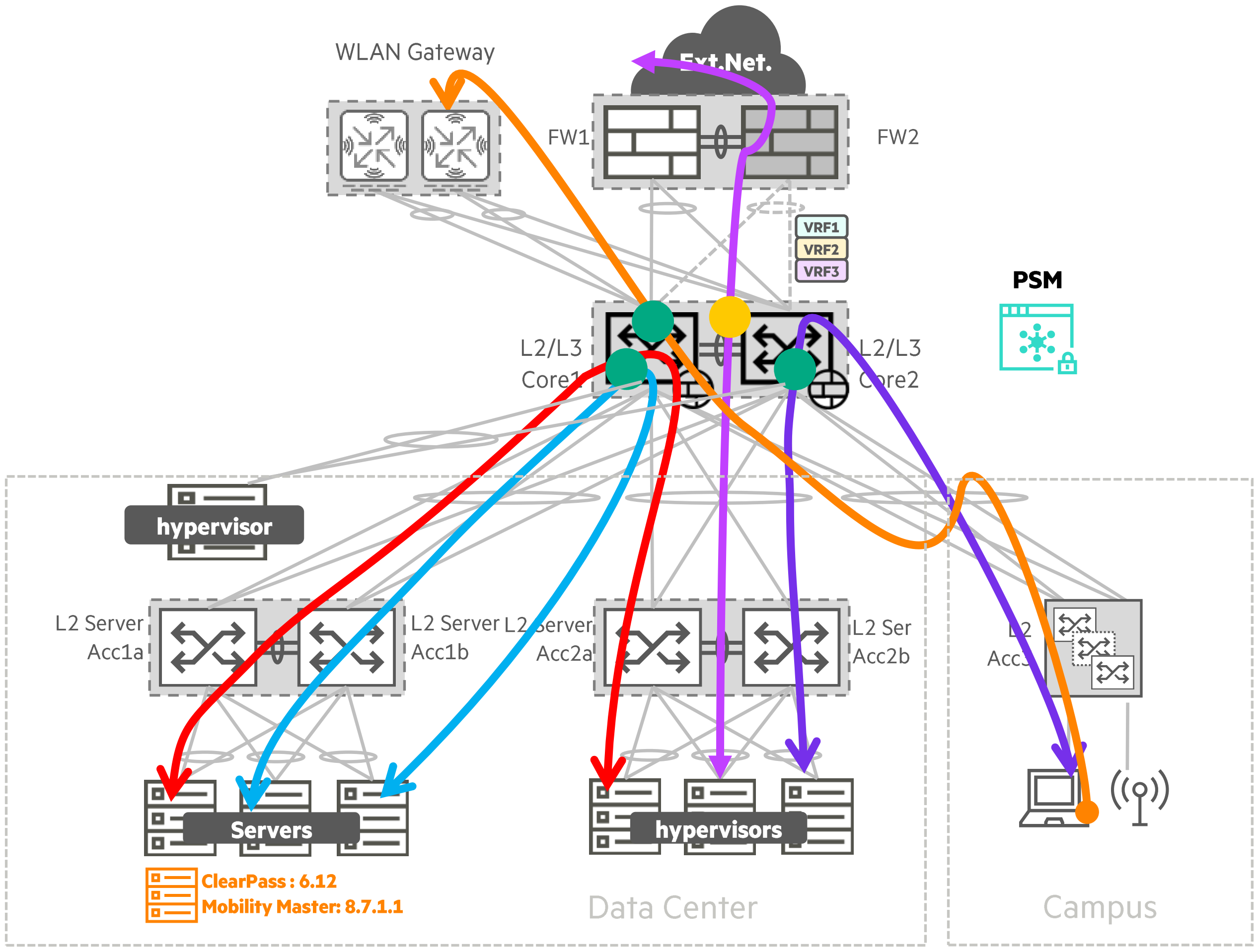


L2
L3

Core: 10000-48Y6C - AOS-CX Version 10.13.1001, Profile L3-Agg, PSM: 1.80.1-T-7
Server Access: 8100-XX/8360-XX – With 8360 AOS-CX Version 10.13.1000, Profile-Agg-Leaf
Access: 6200-XX/6300-XX - 10.13.1000

# 10K Collapsed Core

## Firewall Inspection Points



● Egress Policy on Ingress VLAN

● Ingress Policy on Egress VLAN

— L2
— L3

Core: 10000-48Y6C - AOS-CX Version 10.13.1001, Profile L3-Agg, PSM: 1.80.1-T-7
Server Access: 8100-XX/8360-XX – With 8360 AOS-CX Version 10.13.1000, Profile-Agg-Leaf
Access: 6200-XX/6300-XX - 10.13.1000

# 10K Collapsed Core- Use Case-1

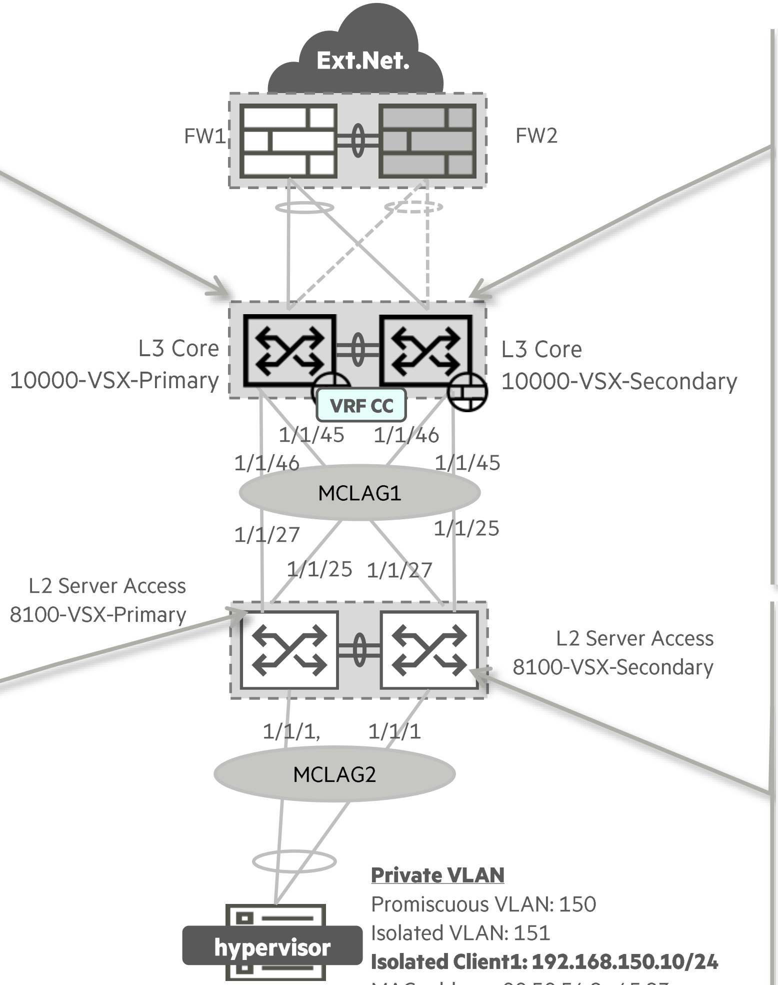
## Intra VRF Micro Segmentation – With Server Access

```
vlan 150
   private-vlan primary
vlan 151
   private-vlan isolated primary-vlan 150
interface vlan 150
   vrf attach CC
   ip address 192.168.150.1/24
   active-gateway ip mac 00:00:00:20:20:20
   active-gateway ip 192.168.150.254
   ip local-proxy-arp

interface lag 1 multi-chassis
   description LAG_TO_8100
   no shutdown
   no routing
   vlan trunk native 1
   vlan trunk allowed 150-151
   lacp mode active
   lacp rate fast
```

```
vlan 150
   private-vlan primary
vlan 151
   private-vlan isolated primary-vlan 150
interface vlan 150
   vrf attach CC
   ip address 192.168.150.2/24
   active-gateway ip mac 00:00:00:20:20:20
   active-gateway ip 192.168.150.254
   ip local-proxy-arp

interface lag 1 multi-chassis
   description LAG_TO_8100
   no shutdown
   no routing
   vlan trunk native 1
   vlan trunk allowed 150-151
   lacp mode active
   lacp rate fast
```



```
interface lag 1 multi-chassis
   description LAG_TO_10K
   no shutdown
   no routing
   vlan trunk native 1
   vlan trunk allowed 150-151
   lacp mode active
   lacp rate fast
interface lag 2 multi-chassis
   description
LAG_2_Server_ISOLATED_VLAN
   no shutdown
   no routing
   vlan trunk native 1
   vlan trunk allowed 150-151
   lacp mode active
   lacp rate fast
```

**Private VLAN**
Promiscuous VLAN: 150
Isolated VLAN: 151
**Isolated Client1: 192.168.150.10/24**
MAC address: 00:50:56:8e:65:83
**Isolated Client 2: 192.168.150.20/24**
MAC address: 00:50:56:8e:53:26
Gateway: 192.168.150.254

```
interface lag 1 multi-chassis
   description LAG_TO_10K
   no shutdown
   no routing
   vlan trunk native 1
   vlan trunk allowed 150-151
   lacp mode active
   lacp rate fast
interface lag 2 multi-chassis
   description
LAG_2_Server_ISOLATED_VLAN
   no shutdown
   no routing
   vlan trunk native 1
   vlan trunk allowed 150-151
   lacp mode active
   lacp rate fast
```

— L2
— L3

Core: 10000-48Y6C
Server Access: 8100-XX/8360-XX

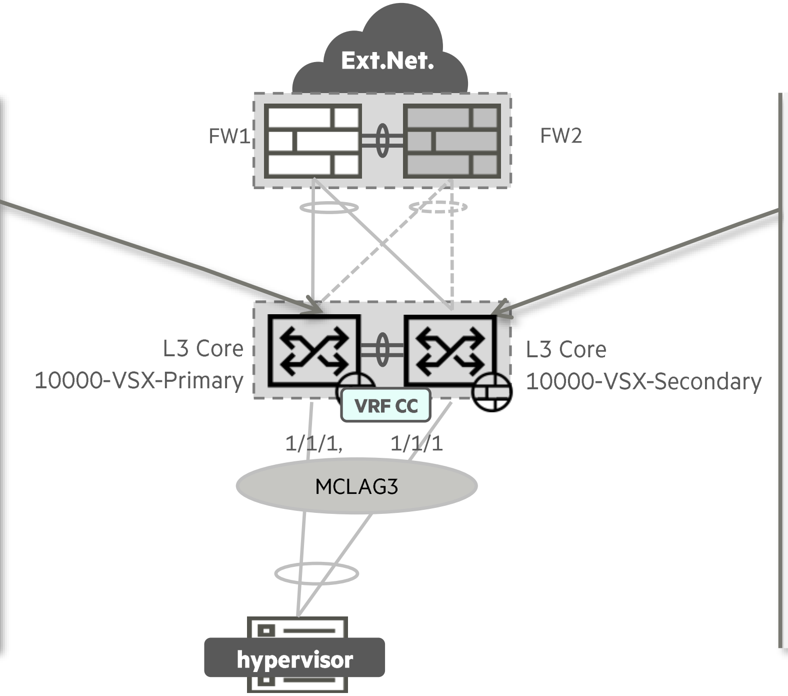
# 10K Collapsed Core- Use Case-2

## Intra VRF Micro Segmentation – Without Server Access

```
vlan 250
   private-vlan primary
vlan 251
   private-vlan isolated primary-vlan 250

interface vlan 250
   vrf attach CC
   ip address 192.168.250.1/24
   active-gateway ip mac 00:00:00:20:20:20
   active-gateway ip 192.168.250.254
   ip local-proxy-arp

interface lag 3 multi-chassis
   no shutdown
   no routing
   vlan trunk native 1 tag
   vlan trunk allowed 250-251
   lacp mode active
```



```
vlan 250
   private-vlan primary
vlan 251
   private-vlan isolated primary-vlan 250

interface vlan 250
   vrf attach CC
   ip address 192.168.250.2/24
   active-gateway ip mac 00:00:00:20:20:20
   active-gateway ip 192.168.250.254
   ip local-proxy-arp

interface lag 3 multi-chassis
   no shutdown
   no routing
   vlan trunk native 1 tag
   vlan trunk allowed  250-251
   lacp mode active
```

**Private VLAN**
Promiscuous VLAN: 250
Isolated VLAN: 251
**Isolated Client1: 192.168.250.10/24**
MAC address: 00:50:56:8e:9a:5b
**Isolated Client 2: 192.168.250.20/24**
MAC address: 00:50:56:8e:0f:37
Gateway: 192.168.250.254

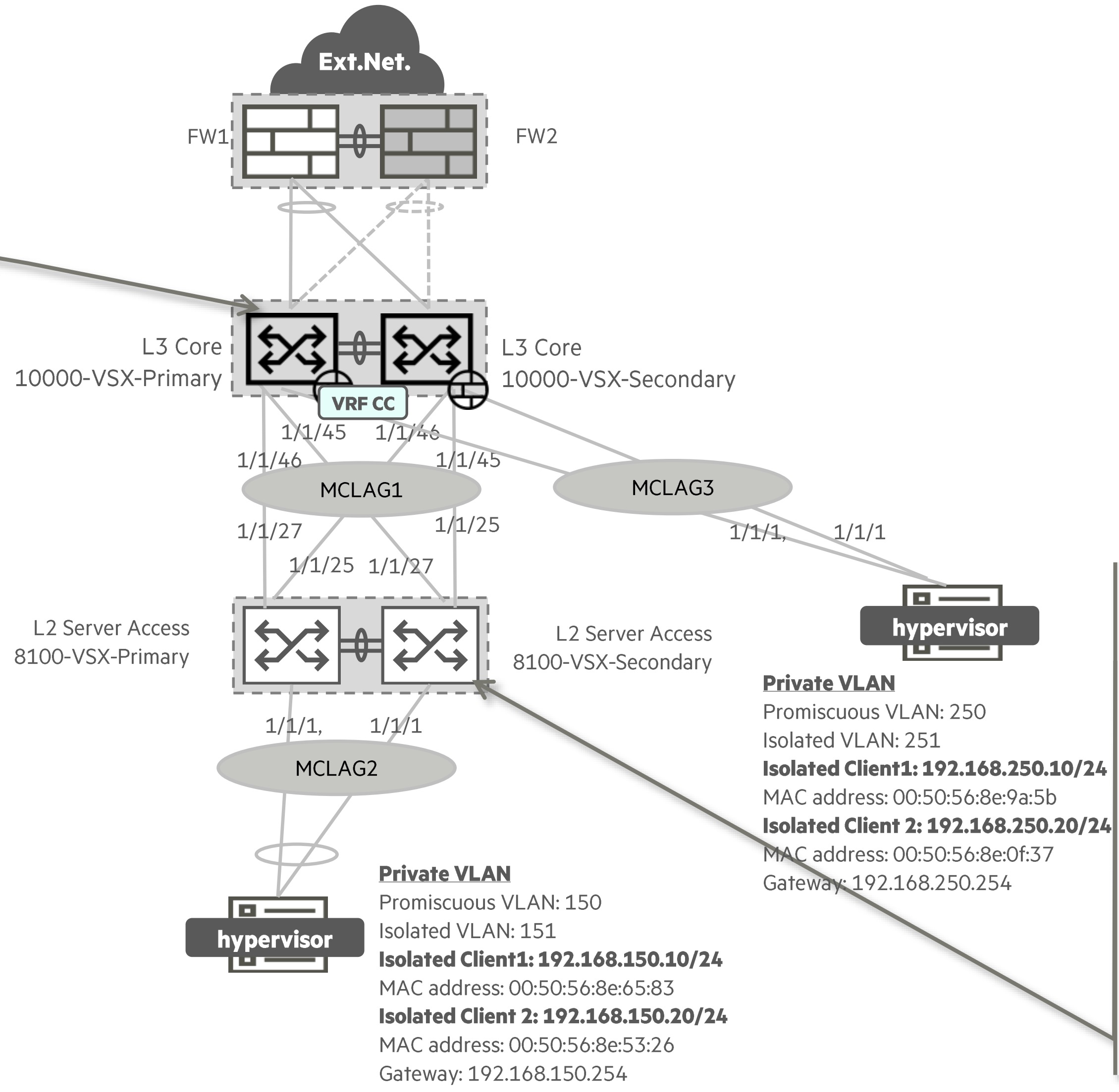
Core: 10000-48Y6C
Server Access: 8100-XX/8360-XX

— L2
— L3

# 10K Collapsed Core- Use Case-3

## Intra VRF Macro Segmentation

```
vlan 150
   private-vlan primary
vlan 151
   private-vlan isolated primary-vlan 150
vlan 250
   private-vlan primary
vlan 251
   private-vlan isolated primary-vlan 250
interface vlan 150
   vrf attach CC
   ip address 192.168.150.1/24
   active-gateway ip mac 00:00:00:20:20:20
   active-gateway ip 192.168.150.254
   ip local-proxy-arp
interface vlan 250
   vrf attach CC
   ip address 192.168.250.1/24
   active-gateway ip mac 00:00:00:20:20:20
   active-gateway ip 192.168.250.254
   ip local-proxy-arp
interface lag 1 multi-chassis
   description LAG_TO_8100
   no shutdown
   no routing
   vlan trunk native 1
   vlan trunk allowed 150-151
   lacp mode active
   lacp rate fast
interface lag 3 multi-chassis
   no shutdown
   no routing
   vlan trunk native 1 tag
   vlan trunk allowed 250-251
   lacp mode active
```



**Private VLAN**
Promiscuous VLAN: 250
Isolated VLAN: 251
**Isolated Client1: 192.168.250.10/24**
MAC address: 00:50:56:8e:9a:5b
**Isolated Client 2: 192.168.250.20/24**
MAC address: 00:50:56:8e:0f:37
Gateway: 192.168.250.254

**Private VLAN**
Promiscuous VLAN: 150
Isolated VLAN: 151
**Isolated Client1: 192.168.150.10/24**
MAC address: 00:50:56:8e:65:83
**Isolated Client 2: 192.168.150.20/24**
MAC address: 00:50:56:8e:53:26
Gateway: 192.168.150.254

```
interface lag 1 multi-chassis
   description LAG_TO_10K
   no shutdown
   no routing
   vlan trunk native 1
   vlan trunk allowed 150-151
   lacp mode active
   lacp rate fast
interface lag 2 multi-chassis
   description LAG_2_Server_ISOLATED_VLAN
   no shutdown
   no routing
   vlan trunk native 1
   vlan trunk allowed 150-151
   lacp mode active
   lacp rate fast
```

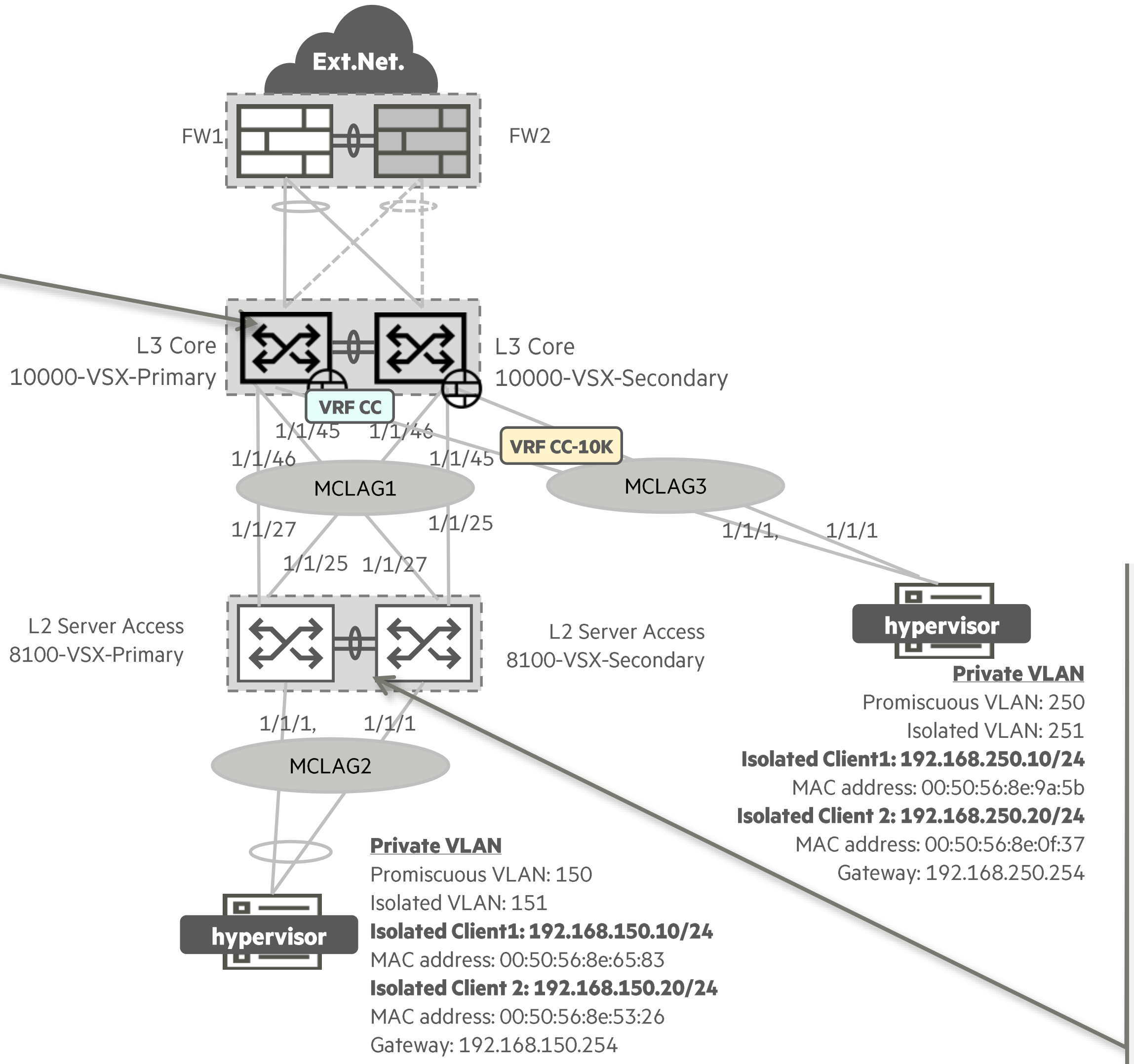
Core: 10000-48Y6C
Server Access: 8100-XX/8360-XX

L2
L3

# 10K Collapsed Core- Use Case-4

## Inter VRF Macro Segmentation

```
vlan 150
   private-vlan primary
vlan 151
   private-vlan isolated primary-vlan 150
vlan 250
   private-vlan primary
vlan 251
   private-vlan isolated primary-vlan 250
interface vlan 150
   vrf attach CC
   ip address 192.168.150.1/24
   active-gateway ip mac 00:00:00:20:20:20
   active-gateway ip 192.168.150.254
   ip local-proxy-arp
interface vlan 250
   vrf attach CC-10K
   ip address 192.168.250.1/24
   active-gateway ip mac 00:00:00:20:20:20
   active-gateway ip 192.168.250.254
   ip local-proxy-arp
interface lag 1 multi-chassis
   description LAG_TO_8100
   no shutdown
   no routing
   vlan trunk native 1
   vlan trunk allowed 150-151
   lacp mode active
   lacp rate fast
interface lag 3 multi-chassis
   no shutdown
   no routing
   vlan trunk native 1 tag
   vlan trunk allowed 250-251
   lacp mode active
```



**Private VLAN**
Promiscuous VLAN: 250
Isolated VLAN: 251
**Isolated Client1: 192.168.250.10/24**
MAC address: 00:50:56:8e:9a:5b
**Isolated Client 2: 192.168.250.20/24**
MAC address: 00:50:56:8e:0f:37
Gateway: 192.168.250.254

**Private VLAN**
Promiscuous VLAN: 150
Isolated VLAN: 151
**Isolated Client1: 192.168.150.10/24**
MAC address: 00:50:56:8e:65:83
**Isolated Client 2: 192.168.150.20/24**
MAC address: 00:50:56:8e:53:26
Gateway: 192.168.150.254

```
interface lag 1 multi-chassis
   description LAG_TO_10K
   no shutdown
   no routing
   vlan trunk native 1
   vlan trunk allowed 150-151
   lacp mode active
   lacp rate fast
interface lag 2 multi-chassis
   description LAG_2_Server_ISOLATED_VLAN
   no shutdown
   no routing
   vlan trunk native 1
   vlan trunk allowed 150-151
   lacp mode active
   lacp rate fast
```

Core: 10000-48Y6C
Server Access: 8100-XX/8360-XX

L2
L3

# PSM Configuration

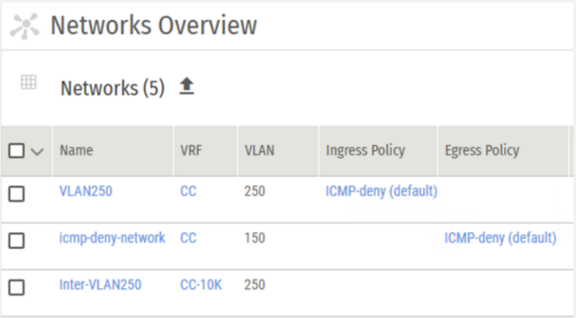
## Use-cases(1-4)

**PSM:**

Two VRFs in total:
1) CC
2) CC-10K

Networks Name:
1) *"icmp-deny-network"* attached to VRF *"CC"* with VLANID: *"150"*
2) *"VLAN250"* attached to VRF "CC" with VLANID: *"250"*
3) "Inter-VLAN250" attached to VRF *"CC-10K" with VLANID:* "250"

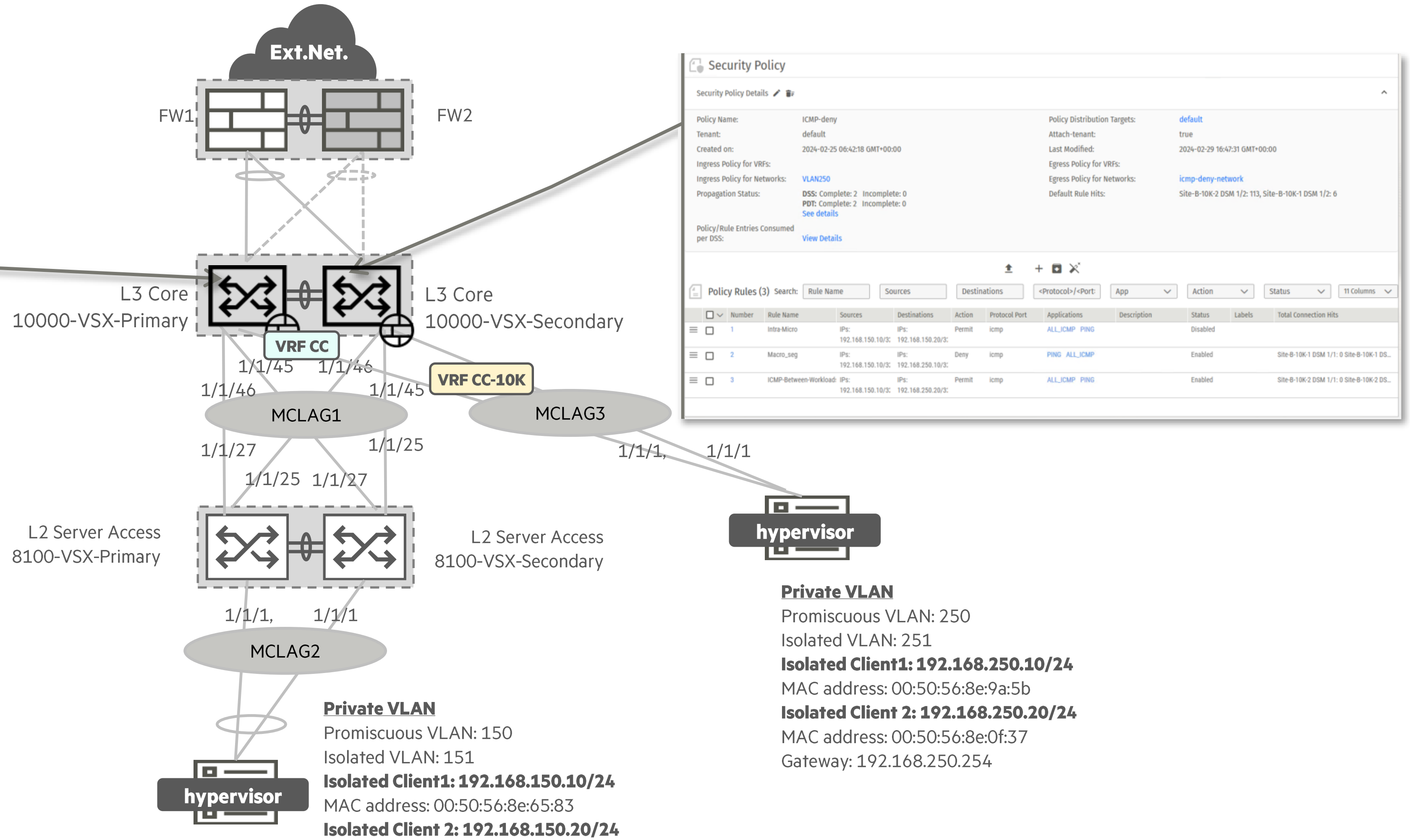
Policy Created:
Name: *"ICMP-deny"* with appropriate rules for each use-cases.



Networks Overview

Networks (5)

| ☐ | Name | VRF | VLAN | Ingress Policy | Egress Policy |
|---|---|---|---|---|---|
| ☐ | VLAN250 | CC | 250 | ICMP-deny (default) | |
| ☐ | icmp-deny-network | CC | 150 | | ICMP-deny (default) |
| ☐ | Inter-VLAN250 | CC-10K | 250 | | |



Security Policy

Security Policy Details

| | | | |
|---|---|---|---|
| Policy Name: | ICMP-deny | Policy Distribution Targets: | default |
| Tenant: | default | Attach-tenant: | true |
| Created on: | 2024-02-25 06:42:18 GMT+00:00 | Last Modified: | 2024-02-29 16:47:31 GMT+00:00 |
| Ingress Policy for VRFs: | | Egress Policy for VRFs: | |
| Ingress Policy for Networks: | VLAN250 | Egress Policy for Networks: | icmp-deny-network |
| Propagation Status: | **DSS:** Complete: 2 Incomplete: 0<br>**PDT:** Complete: 2 Incomplete: 0<br>See details | Default Rule Hits: | Site-B-10K-2 DSM 1/2: 113, Site-B-10K-1 DSM 1/2: 6 |
| Policy/Rule Entries Consumed per DSS: | View Details | | |

Policy Rules (3) Search: Rule Name Sources Destinations <Protocol>/<Port: App Action Status 11 Columns

| ☐ | Number | Rule Name | Sources | Destinations | Action | Protocol Port | Applications | Description | Status | Labels | Total Connection Hits |
|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | 1 | Intra-Micro | IPs:<br>192.168.150.10/3: | IPs:<br>192.168.150.20/3: | Permit | icmp | ALL_ICMP PING | | Disabled | | |
| ☐ | 2 | Macro_seg | IPs:<br>192.168.150.10/3: | IPs:<br>192.168.250.10/3: | Deny | icmp | PING ALL_ICMP | | Enabled | | Site-B-10K-1 DSM 1/1: 0 Site-B-10K-1 DS... |
| ☐ | 3 | ICMP-Between-Workload: | IPs:<br>192.168.150.10/3: | IPs:<br>192.168.250.20/3: | Permit | icmp | ALL_ICMP PING | | Enabled | | Site-B-10K-2 DSM 1/1: 0 Site-B-10K-2 DS... |

**Private VLAN**
Promiscuous VLAN: 250
Isolated VLAN: 251
**Isolated Client1: 192.168.250.10/24**
MAC address: 00:50:56:8e:9a:5b
**Isolated Client 2: 192.168.250.20/24**
MAC address: 00:50:56:8e:0f:37
Gateway: 192.168.250.254

**Private VLAN**
Promiscuous VLAN: 150
Isolated VLAN: 151
**Isolated Client1: 192.168.150.10/24**
MAC address: 00:50:56:8e:65:83
**Isolated Client 2: 192.168.150.20/24**
MAC address: 00:50:56:8e:53:26
Gateway: 192.168.150.254

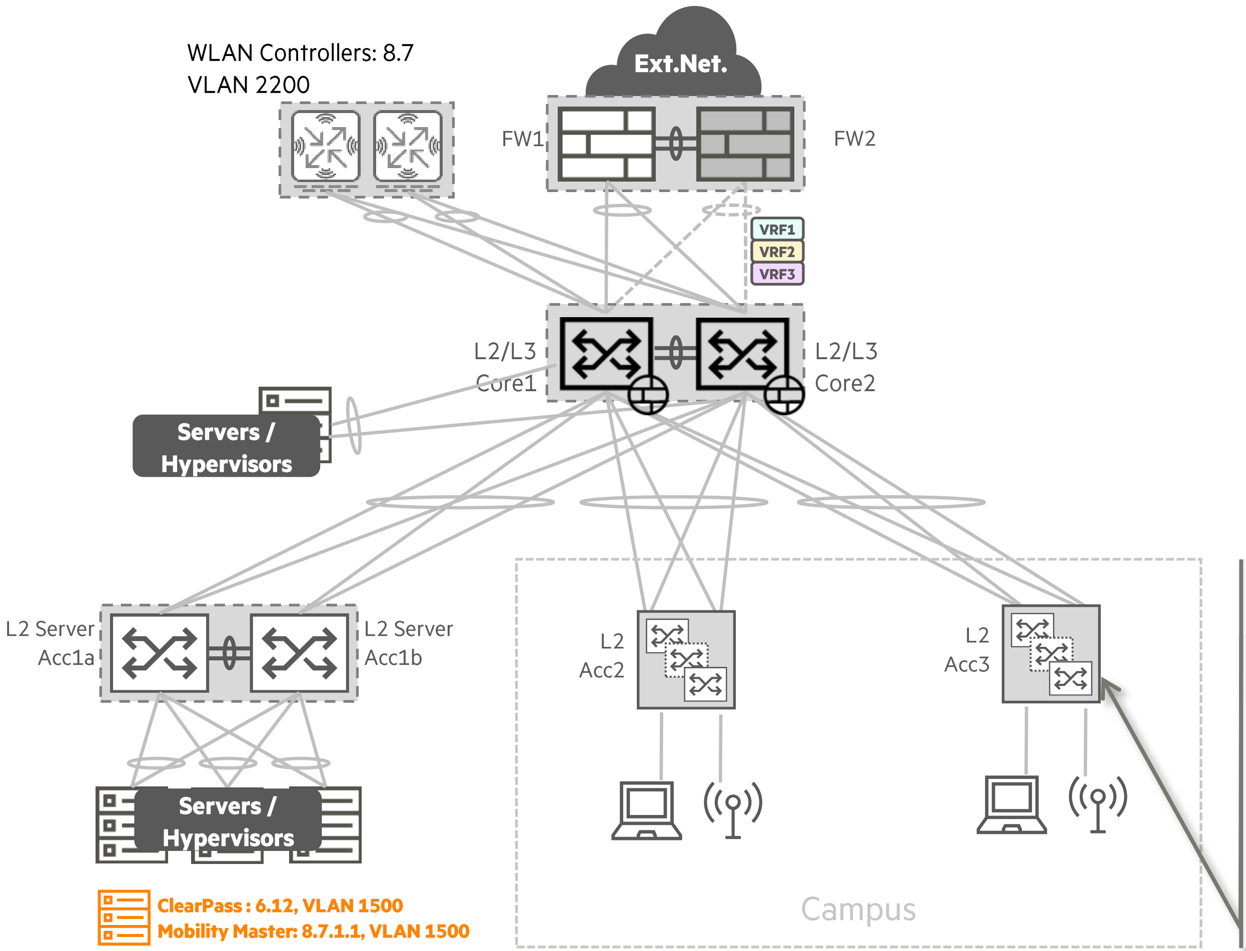
Core: 10000-48Y6C
Server Access: 8100-XX/8360-XX

L2
L3

# Demo

# 10K Collapsed Core – Use Case-5

## UBT from access switch to gateway (tunnel traffic from gateway to Core inspected)



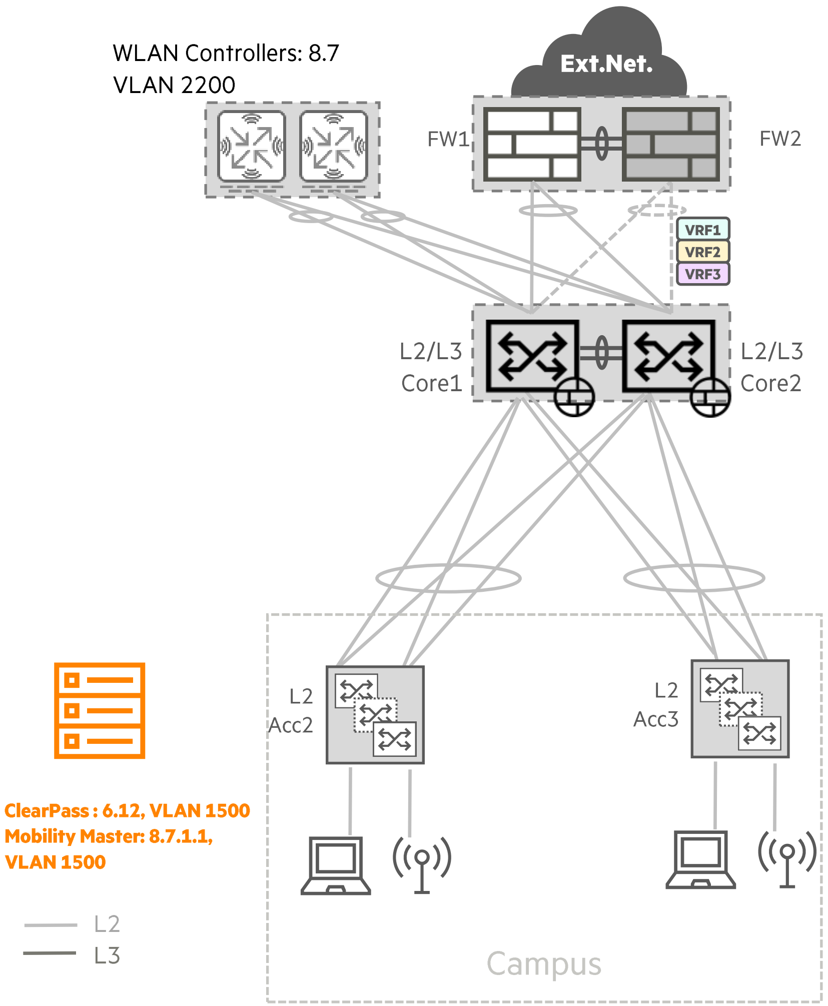
```
Campus 6200:
interface vlan 2200
   ip address 122.1.1.251/16
   ip mtu 9198

show running-config ubt
ubt-client-vlan 2500
ubt zone SE11-SVR vrf default
   primary-controller ip 122.1.1.10
   backup-controller ip 122.1.1.11
   enable
```

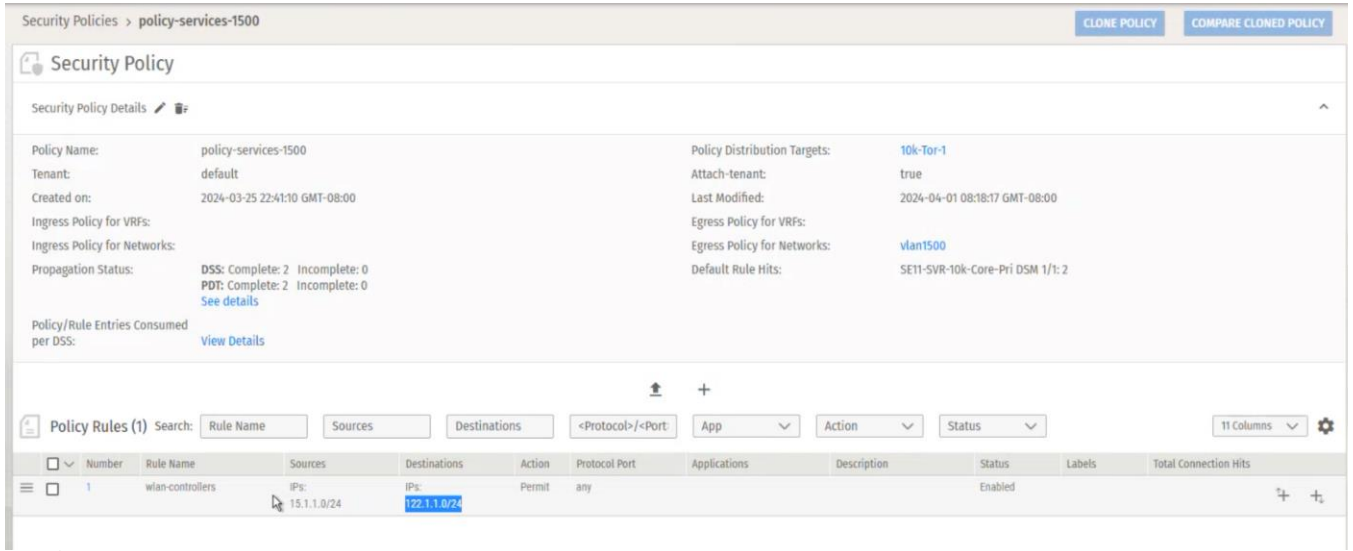
— L2
— L3

Core: 10000-48Y6C – 10.13.1001, PSM: 1.80.1-T-7
Server Access: 8100-XX/8360-XX
Access: 6200-XX/6300-XX
WLAN Gateway: 7240

# 10K Collapsed Core – Use Case-5



Core: 10000-48Y6C – 10.13.1001, PSM: 1.80.1-T-7
Server Access: 8100-XX/8360-XX
Access: 6200-XX/6300-XX
WLAN Gateway: 7240



Security Policies › policy-services-1500

Security Policy

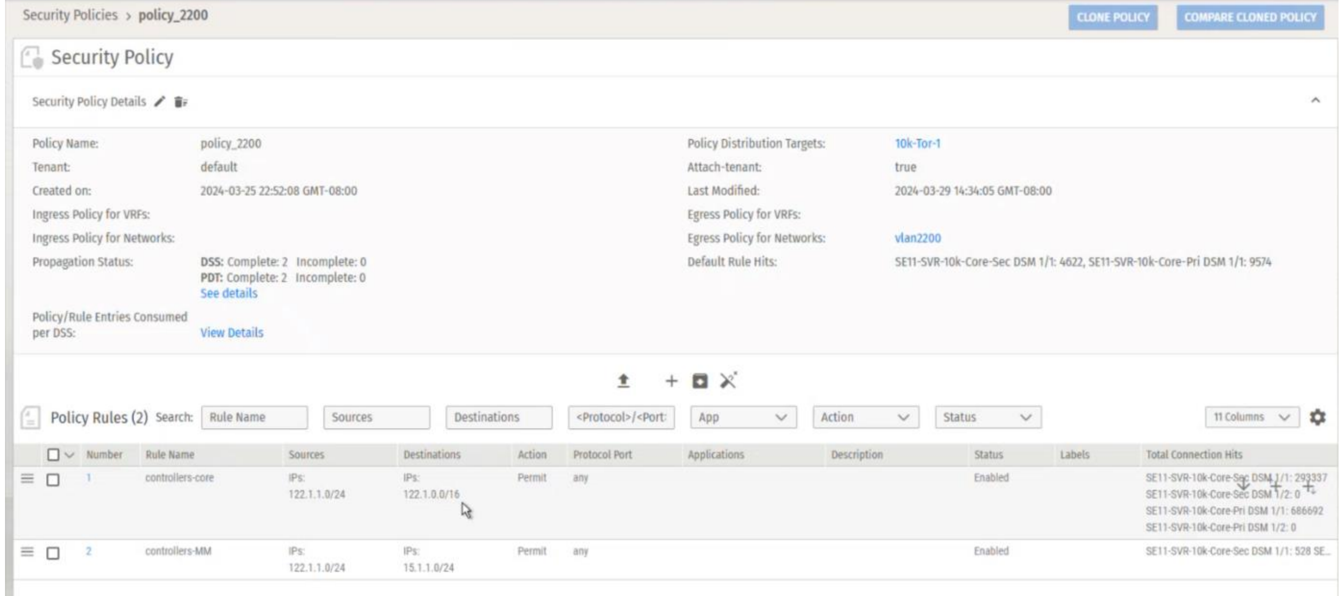
Security Policy Details

| | | | |
|---|---|---|---|
| Policy Name: | policy-services-1500 | Policy Distribution Targets: | 10k-Tor-1 |
| Tenant: | default | Attach-tenant: | true |
| Created on: | 2024-03-25 22:41:10 GMT-08:00 | Last Modified: | 2024-04-01 08:18:17 GMT-08:00 |
| Ingress Policy for VRFs: | | Egress Policy for VRFs: | |
| Ingress Policy for Networks: | | Egress Policy for Networks: | vlan1500 |
| Propagation Status: | DSS: Complete: 2 Incomplete: 0<br>PDT: Complete: 2 Incomplete: 0<br>See details | Default Rule Hits: | SE11-SVR-10k-Core-Pri DSM 1/1: 2 |
| Policy/Rule Entries Consumed per DSS: | View Details | | |

Policy Rules (1) Search: Rule Name Sources Destinations <Protocol>/<Port App Action Status 11 Columns

| Number | Rule Name | Sources | Destinations | Action | Protocol Port | Applications | Description | Status | Labels | Total Connection Hits |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | wlan-controllers | IPs:<br>15.1.1.0/24 | IPs:<br>122.1.1.0/24 | Permit | any | | | Enabled | | |

**Policy on PSM:** Source from ClearPass(15.1.1.x) to controllers(122.1.1.x) and Campus Switch. These are to be redirected to DSM and will be inspected.



Security Policies › policy_2200

Security Policy

Security Policy Details

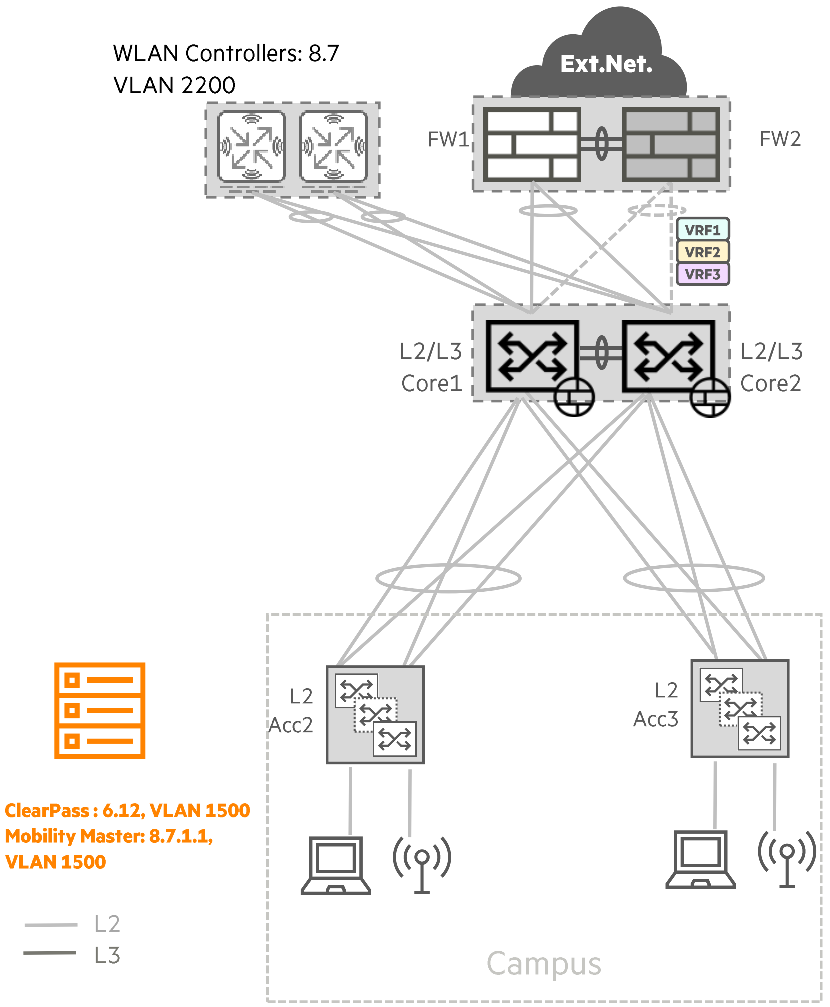
| | | | |
|---|---|---|---|
| Policy Name: | policy_2200 | Policy Distribution Targets: | 10k-Tor-1 |
| Tenant: | default | Attach-tenant: | true |
| Created on: | 2024-03-25 22:52:08 GMT-08:00 | Last Modified: | 2024-03-29 14:34:05 GMT-08:00 |
| Ingress Policy for VRFs: | | Egress Policy for VRFs: | |
| Ingress Policy for Networks: | | Egress Policy for Networks: | vlan2200 |
| Propagation Status: | DSS: Complete: 2 Incomplete: 0<br>PDT: Complete: 2 Incomplete: 0<br>See details | Default Rule Hits: | SE11-SVR-10k-Core-Sec DSM 1/1: 4622, SE11-SVR-10k-Core-Pri DSM 1/1: 9574 |
| Policy/Rule Entries Consumed per DSS: | View Details | | |

Policy Rules (2) Search: Rule Name Sources Destinations <Protocol>/<Port: App Action Status 11 Columns

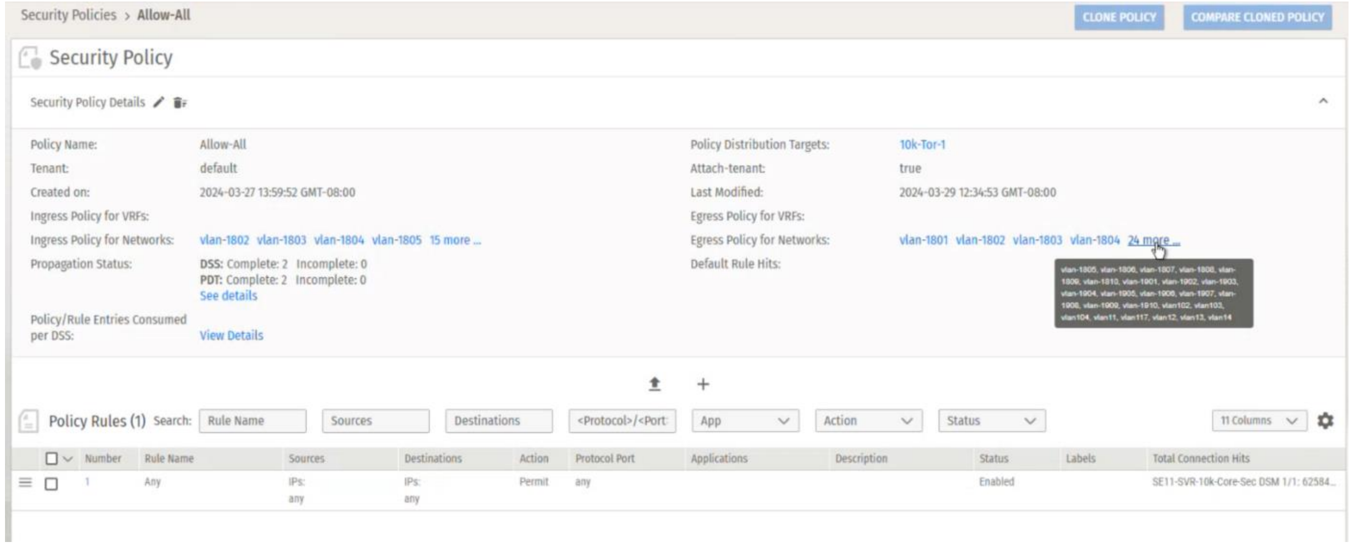
| Number | Rule Name | Sources | Destinations | Action | Protocol Port | Applications | Description | Status | Labels | Total Connection Hits |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | controllers-core | IPs:<br>122.1.1.0/24 | IPs:<br>122.1.0.0/16 | Permit | any | | | Enabled | | SE11-SVR-10k-Core-Sec DSM 1/1: 293337<br>SE11-SVR-10k-Core-Sec DSM 1/2: 0<br>SE11-SVR-10k-Core-Pri DSM 1/1: 686692<br>SE11-SVR-10k-Core-Pri DSM 1/2: 0 |
| 2 | controllers-MM | IPs:<br>122.1.1.0/24 | IPs:<br>15.1.1.0/24 | Permit | any | | | Enabled | | SE11-SVR-10k-Core-Sec DSM 1/1: 528 SE... |

**Policy on PSM:** Controllers to Core: Controllers are also on 122.1.1.x subnet → going to Core: 122.1.x.x(Campus)
Controllers to MM: Mobility Master is on 15.1.1.x. So, we allow traffic from controllers to MM.

# 10K Collapsed Core – Use Case-5



Core: 10000-48Y6C – 10.13.1001, PSM: 1.80.1-T-7
Server Access: 8100-XX/8360-XX
Access: 6200-XX/6300-XX
WLAN Gateway: 7240



Policy Name: Allow-All
Tenant: default
Created on: 2024-03-27 13:59:52 GMT-08:00
Ingress Policy for VRFs:
Ingress Policy for Networks: vlan-1802 vlan-1803 vlan-1804 vlan-1805 15 more ...
Propagation Status: **DSS:** Complete: 2 Incomplete: 0
**PDT:** Complete: 2 Incomplete: 0
See details
Policy/Rule Entries Consumed per DSS: View Details

Policy Distribution Targets: 10k-Tor-1
Attach-tenant: true
Last Modified: 2024-03-29 12:34:53 GMT-08:00
Egress Policy for VRFs:
Egress Policy for Networks: vlan-1801 vlan-1802 vlan-1803 vlan-1804 24 more ...
Default Rule Hits:

vlan-1805, vlan-1806, vlan-1807, vlan-1808, vlan-1809, vlan-1810, vlan-1901, vlan-1902, vlan-1903, vlan-1904, vlan-1905, vlan-1906, vlan-1907, vlan-1908, vlan-1909, vlan-1910, vlan102, vlan103, vlan104, vlan11, vlan117, vlan12, vlan13, vlan14

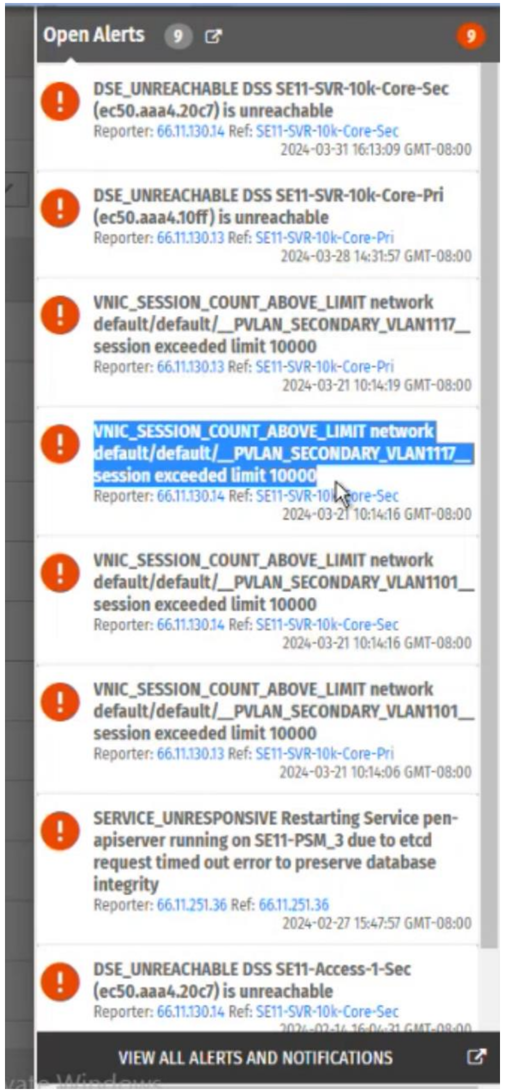
| | Number | Rule Name | Sources | Destinations | Action | Protocol Port | Applications | Description | Status | Labels | Total Connection Hits |
|---|---|---|---|---|---|---|---|---|---|---|---|
| □ | 1 | Any | IPs:<br>any | IPs:<br>any | Permit | any | | | Enabled | | SE11-SVR-10k-Core-Sec DSM 1/1: 62584... |

**Policy on PSM:**

UBT Clients are all allowed. For ex: VLAN 1801, after authentication(on management VLAN) to that UBT Client. UBT traffic being redirected and works well.

# 10K Collapsed Core- Use Case-6

DDoS enabled on 10K (session limit)



**Open Alerts** 9

**DSE_UNREACHABLE DSS SE11-SVR-10k-Core-Sec (ec50.aaa4.20c7) is unreachable**
Reporter: 66.11.130.14 Ref: SE11-SVR-10k-Core-Sec
2024-03-31 16:13:09 GMT-08:00

**DSE_UNREACHABLE DSS SE11-SVR-10k-Core-Pri (ec50.aaa4.10ff) is unreachable**
Reporter: 66.11.130.13 Ref: SE11-SVR-10k-Core-Pri
2024-03-28 14:31:57 GMT-08:00

**VNIC_SESSION_COUNT_ABOVE_LIMIT network default/default/__PVLAN_SECONDARY_VLAN1117__ session exceeded limit 10000**
Reporter: 66.11.130.13 Ref: SE11-SVR-10k-Core-Pri
2024-03-21 10:14:19 GMT-08:00

**VNIC_SESSION_COUNT_ABOVE_LIMIT network default/default/__PVLAN_SECONDARY_VLAN1117__ session exceeded limit 10000**
Reporter: 66.11.130.14 Ref: SE11-SVR-10k-Core-Sec
2024-03-21 10:14:16 GMT-08:00

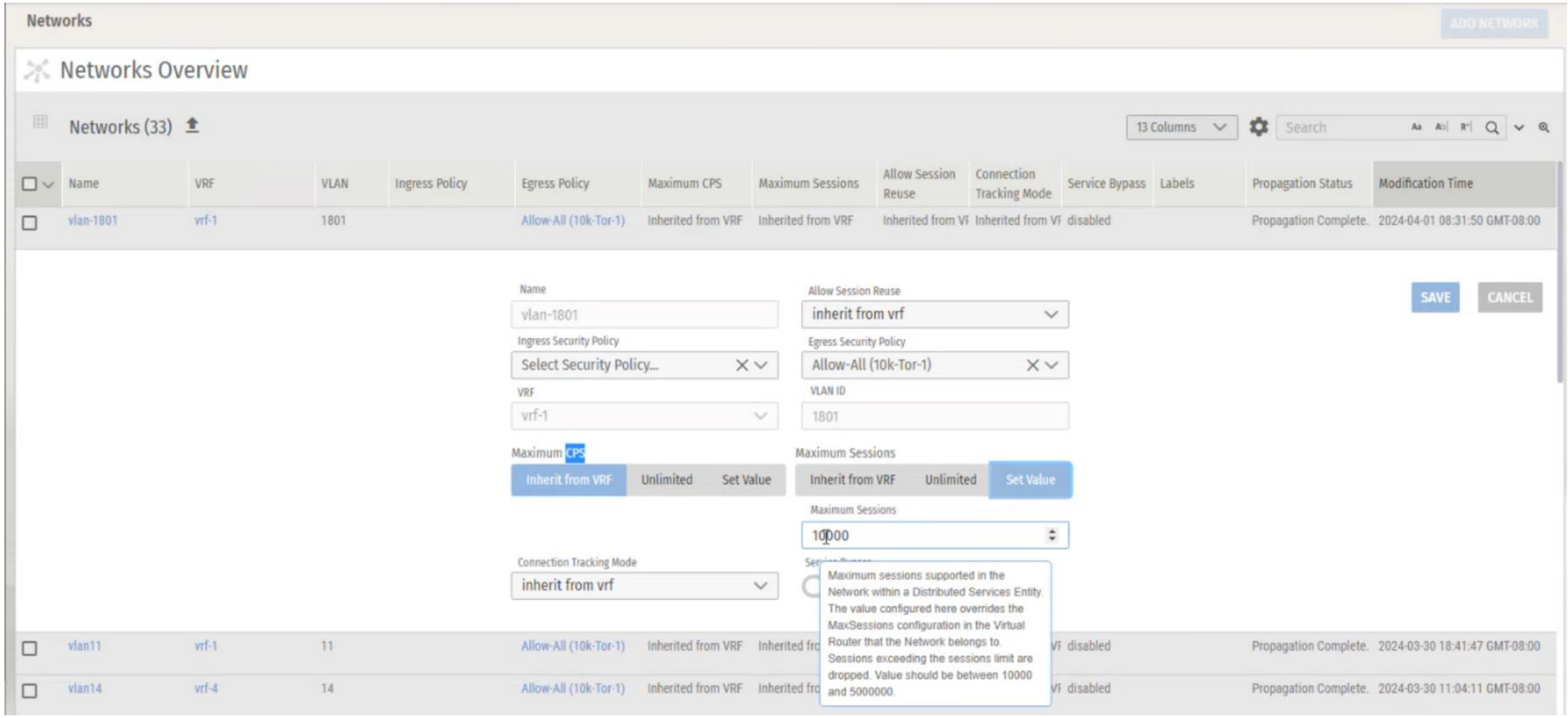
**VNIC_SESSION_COUNT_ABOVE_LIMIT network default/default/__PVLAN_SECONDARY_VLAN1101__ session exceeded limit 10000**
Reporter: 66.11.130.14 Ref: SE11-SVR-10k-Core-Sec
2024-03-21 10:14:16 GMT-08:00

**VNIC_SESSION_COUNT_ABOVE_LIMIT network default/default/__PVLAN_SECONDARY_VLAN1101__ session exceeded limit 10000**
Reporter: 66.11.130.13 Ref: SE11-SVR-10k-Core-Pri
2024-03-21 10:14:06 GMT-08:00

**SERVICE_UNRESPONSIVE Restarting Service pen-apiserver running on SE11-PSM_3 due to etcd request timed out error to preserve database integrity**
Reporter: 66.11.251.36 Ref: 66.11.251.36
2024-02-27 15:47:57 GMT-08:00

**DSE_UNREACHABLE DSS SE11-Access-1-Sec (ec50.aaa4.20c7) is unreachable**
Reporter: 66.11.130.14 Ref: SE11-SVR-10k-Core-Sec
2024-02-14 16:04:21 GMT-08:00

VIEW ALL ALERTS AND NOTIFICATIONS



| ☐ | Name | VRF | VLAN | Ingress Policy | Egress Policy | Maximum CPS | Maximum Sessions | Allow Session Reuse | Connection Tracking Mode | Service Bypass | Labels | Propagation Status | Modification Time |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ☐ | vlan-1801 | vrf-1 | 1801 | | Allow-All (10k-Tor-1) | Inherited from VRF | Inherited from VRF | Inherited from VI | Inherited from VI | disabled | | Propagation Complete. | 2024-04-01 08:31:50 GMT-08:00 |
| ☐ | vlan11 | vrf-1 | 11 | | Allow-All (10k-Tor-1) | Inherited from VRF | Inherited fro | | VF | disabled | | Propagation Complete. | 2024-03-30 18:41:47 GMT-08:00 |
| ☐ | vlan14 | vrf-4 | 14 | | Allow-All (10k-Tor-1) | Inherited from VRF | Inherited fro | | VF | disabled | | Propagation Complete. | 2024-03-30 11:04:11 GMT-08:00 |

Name: vlan-1801

Allow Session Reuse: inherit from vrf

Ingress Security Policy: Select Security Policy...

Egress Security Policy: Allow-All (10k-Tor-1)

VRF: vrf-1

VLAN ID: 1801

Maximum CPS: [✓ Inherit from VRF] Unlimited Set Value

Maximum Sessions: Inherit from VRF Unlimited [✓ Set Value]

Maximum Sessions: 10000

Connection Tracking Mode: inherit from vrf

Maximum sessions supported in the Network within a Distributed Services Entity. The value configured here overrides the MaxSessions configuration in the Virtual Router that the Network belongs to. Sessions exceeding the sessions limit are dropped. Value should be between 10000 and 5000000.

SAVE CANCEL

L2
L3

Core: 10000-48Y6C
Server Access: 8100-XX/8360-XX

**Resource**

**Location:**

# IPFIX

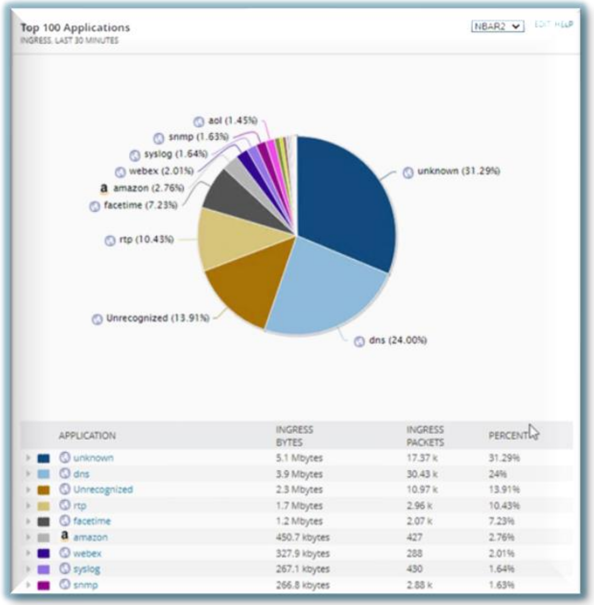
HPE ANW CX Switches

# Aruba CX Edge Insights

| Platforms | Application Recognition | IPFIX | Traffic Insight |
|---|---|---|---|
| 6300 | ✓ | ✓ | ✓ |
| 6400 | ✓ | ✓ | ✓ |

SolarWinds NTA

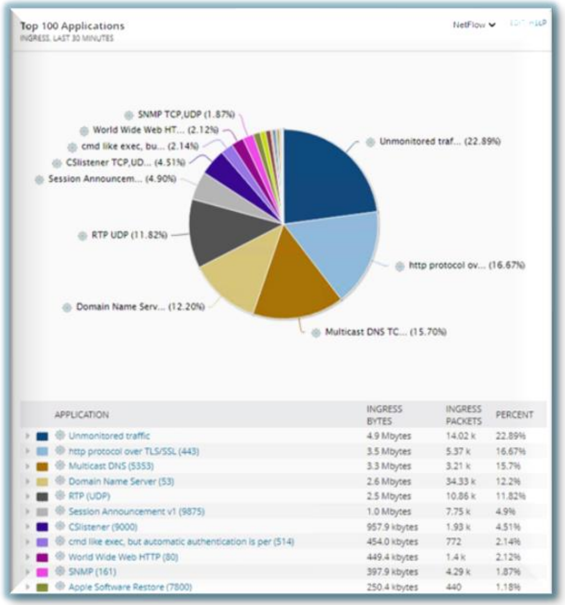
**Application Recognition providing edge insights**



| APPLICATION | INGRESS BYTES | INGRESS PACKETS | PERCENT |
|---|---|---|---|
| unknown | 5.1 Mbytes | 17.37 k | 31.29% |
| dns | 3.9 Mbytes | 30.43 k | 24% |
| Unrecognized | 2.3 Mbytes | 10.97 k | 13.91% |
| rtp | 1.7 Mbytes | 2.96 k | 10.43% |
| facetime | 1.2 Mbytes | 2.07 k | 7.23% |
| amazon | 450.7 kbytes | 427 | 2.76% |
| webex | 327.9 kbytes | 288 | 2.01% |
| syslog | 267.1 kbytes | 430 | 1.64% |
| snmp | 266.8 kbytes | 2.88 k | 1.63% |

**External Collector**

**IPFIX**
**providing flow analysis and report**


Top 100 Applications
INGRESS, LAST 30 MINUTES
NetFlow
EDIT HELP
SNMP TCP,UDP (1.87%)
World Wide Web HT... (2.12%)
cmd like exec, bu... (2.14%)
CSlistener TCP,UD... (4.51%)
Session Announcem... (4.90%)
RTP UDP (11.82%)
Domain Name Serv... (12.20%)
Multicast DNS TC... (15.70%)
http protocol ov... (16.67%)
Unmonitored traf... (22.89%)

| APPLICATION | INGRESS BYTES | INGRESS PACKETS | PERCENT |
|---|---|---|---|
| Unmonitored traffic | 4.9 Mbytes | 14.02 k | 22.89% |
| http protocol over TLS/SSL (443) | 3.5 Mbytes | 5.37 k | 16.67% |
| Multicast DNS (5353) | 3.3 Mbytes | 3.21 k | 15.7% |
| Domain Name Server (53) | 2.6 Mbytes | 34.33 k | 12.2% |
| RTP (UDP) | 2.5 Mbytes | 10.86 k | 11.82% |
| Session Announcement v1 (9875) | 1.0 Mbytes | 7.75 k | 4.9% |
| CSlistener (9000) | 957.9 kbytes | 1.93 k | 4.51% |
| cmd like exec, but automatic authentication is per (514) | 454.0 kbytes | 772 | 2.14% |
| World Wide Web HTTP (80) | 449.4 kbytes | 1.4 k | 2.12% |
| SNMP (161) | 397.9 kbytes | 4.29 k | 1.87% |
| Apple Software Restore (7800) | 250.4 kbytes | 440 | 1.18% |

NOTE: Aruba CX Edge Insights as a security solution is supported on 6300 and 6400 (for 6400 it is supported only for v2- default profile) switch series. AOS-CX Version 10.14.0001

# Aruba CX Edge Insights

| Platforms | Application Recognition | IPFIX | Traffic Insight |
|---|---|---|---|
| 6200 | | ✓ | ✓* |
| 6300 | ✓ | ✓ | ✓ |
| 6400 | ✓ | ✓ | ✓ |
| 8100 | | ✓ | |
| 8360 | | ✓ | ✓** |
| 8325 | | ✓ | |
| 10000 | | ✓ | ✓*** |

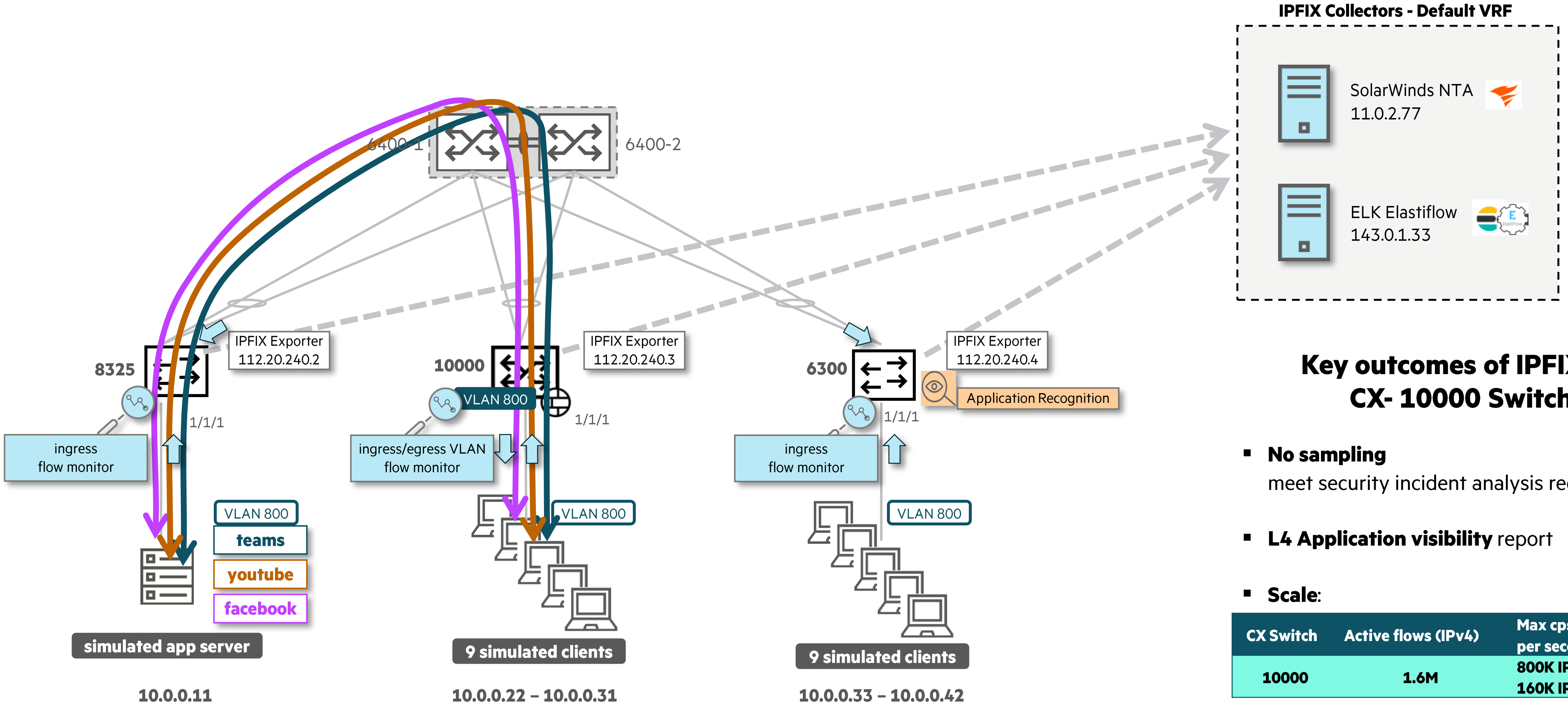
As on AOS-CX Version 10.14.0001

* TI on 6200 supports App and Raw Flow monitors.

** TI on CX8360 supports only DNS Average Latency monitor (requires client-insight to be enabled)

*** TI on CX10000 supports topN, flow & workload-flow monitors

# Telemetry Demonstration with CX Switching



## Key outcomes of IPFIX on CX- 10000 Switch

- **No sampling**
  meet security incident analysis requirements
- **L4 Application visibility** report
- **Scale**:

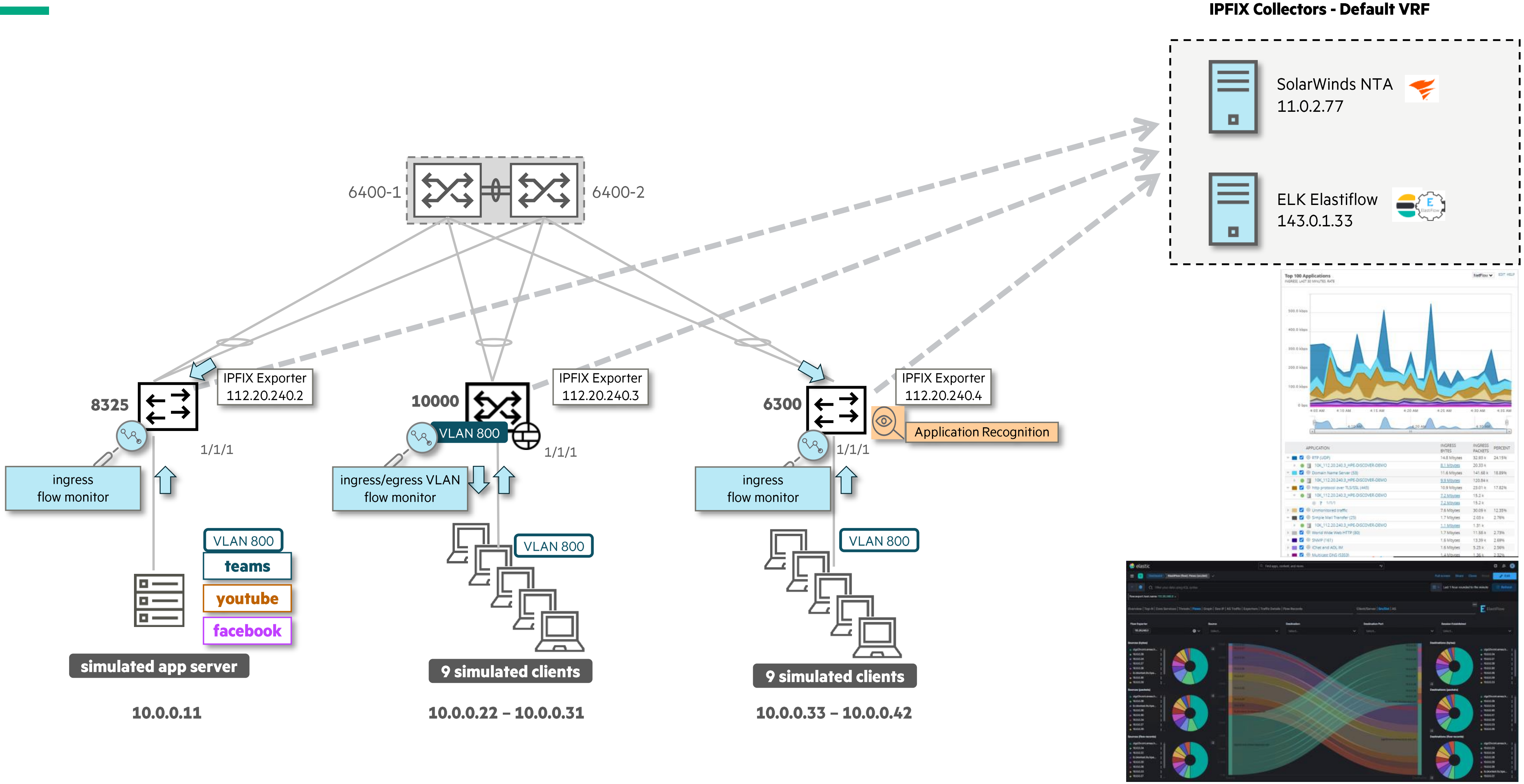
| CX Switch | Active flows (IPv4) | Max cps (Connections per second) FW/IPFIX |
|---|---|---|
| 10000 | 1.6M | 800K IPV4 (non-VSX)<br>160K IPV4 (VSX) |

— L2
— L3

As on AOS-CX Version 10.14.0001

Confidential | Authorized
HPE Partner Use Only

# Telemetry Demonstration with CX Switching



L2
L3

As on AOS-CX Version 10.14.0001

# CX-10K DPU FW Syslog vs IPFIX fields – Summary

## Unique FW sys log fields

- Allow or Deny action to session
- Flow session identifier
- Security Policy ID
- Rule-ID
- Rule-name
- Policy name ( to evaluate flow)
- Destination VLAN
- Product-type (DSS)
- Software version (AOS-CX)
- Serial number (device)
- Device name ( device MAC address)
- Post NAT translated source IP
- Post NAT translated destination IP
- Post NAT translated destination port
- Encryption – whether flow is IPsec encrypted
- Session flags – stateful or stateless

## Overlapping fields

- Flow record time stamp
- Flow role (initiator or responder)
- Source VRF
- Destination VRF
- Source IP
- Destination IP
- Source TCP/UDP Port
- Destination TCP/UDP port
- IP protocol
- Packet count ( initiator to responder- responder to Initiator)
- Flow bytes
- Permit packets
- Permit bytes
- Start flow timestamp
- End flow timestamp
- Visibility of source VLAN ID reference (or 802.1Q reference)
- DSM ID
- Policy Visibility ID (UUID relative to flow forwarding behaviour)
- Policy rule ID (UUID relative to flow forwarding behaviour)

## Unique IPFIX fields

- Drop packets
- Drop bytes
- Delta permit packets during flow lifespan
- Delta permit bytes during flow lifespan
- Flow last seen
- Last seen TCP sequence number
- Last seen TCP ACK number
- TCP retransmit count
- Drop TCP packets
- Drop TCP packets since last export
- Visibility of TCP transport options for flow life span
- Visibility of TCP flags for flow life span
- Visibility of abnormal IP events - ICMP
- TCP sender Transit capability – TCP acknowledgments
- TCP recipient receive capability - relation to TCP seq number
- IPv4 Diffserv value visibility
- Flow end reason ( Flow state clean up)
- Source subnet
- Destination subnet
- Source MAC
- Destination MAC
- Visibility of Ingress queue towards PEN ASIC
- Visibility of Egress queue towards PEN ASIC
- Visibility of 16-byte policy UUID relative to flow forwarding behaviour
- Visibility of 16-byte rule UUID relative to flows forwarding behaviour

**IP flow export**, implementing the IETF IPFIX standard, is used to gain visibility into network traffic usage patterns within data center networks(east-west), which can then be used as a basis for creating firewall policies. **Exporting Firewall Logs**, is used to gain visibility into activities processed by the firewall service. Mainly used by SecOps team.

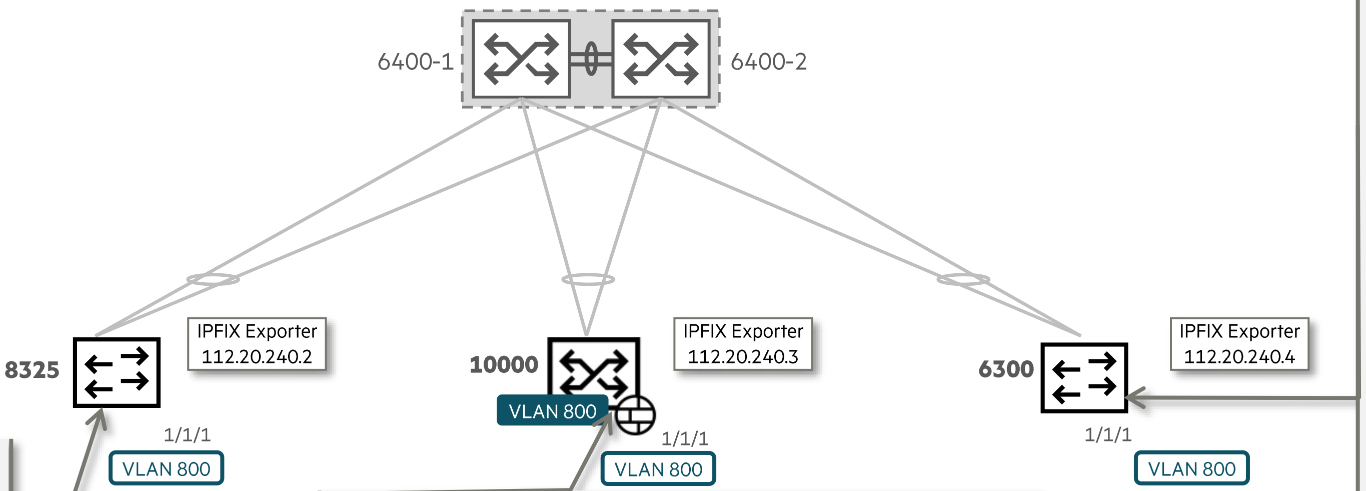
**Phase 1** Network team may want to use IPFIX to analyze network traffic flows in the Data Center.

**Phase 2** Security team may want to deploy FW policies, based on phase 1, to allow/block traffic and export and analyze firewall logs.

As on AOS-CX Version 10.14.0001

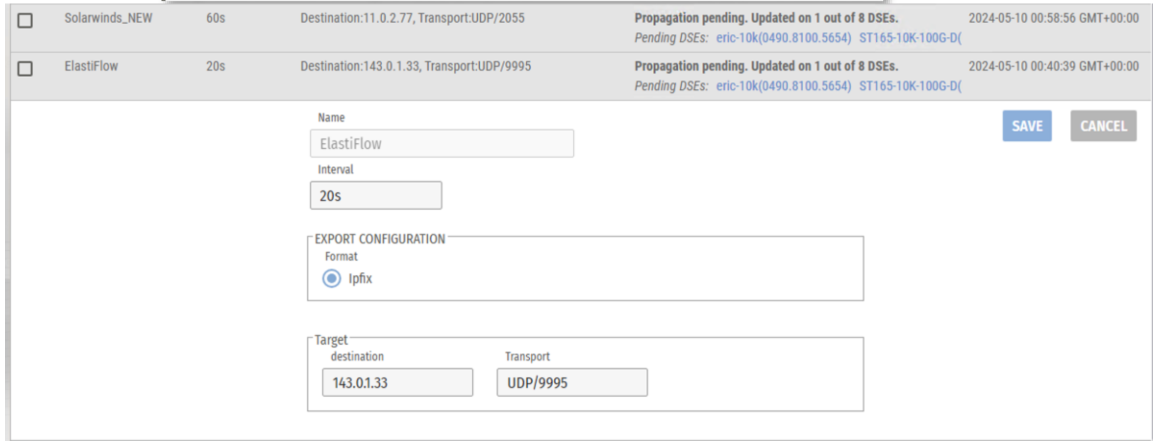
# Demo

# Telemetry Demonstration with CX Switching - Configuration


6400-1
6400-2
8325
IPFIX Exporter 112.20.240.2
10000
IPFIX Exporter 112.20.240.3
6300
IPFIX Exporter 112.20.240.4
VLAN 800
1/1/1
VLAN 800
1/1/1
VLAN 800
1/1/1
VLAN 800

```
flow exporter ElastiFlow
   destination 143.0.1.33
   transport udp 9995
flow record record-v4
   match ipv4 destination address
   match ipv4 protocol
   match ipv4 source address
   match transport destination port
   match transport source port
   collect counter bytes
   collect counter packets
   collect timestamp absolute first
flow monitor monitor-8325
   exporter ElastiFlow
   record record-v4
interface lag 1
   ip flow monitor monitor-8325 in
interface 1/1/1
   ip flow monitor monitor-8325 in
ip source-interface ipfix interface 1/1/24
```

```
dsm
   ipfix
ip source-interface ipfix 112.20.240.3      ---- Interface 1/1/24 to collector
```



| | | | | | |
|---|---|---|---|---|---|
| □ | Solarwinds_NEW | 60s | Destination:11.0.2.77, Transport:UDP/2055 | **Propagation pending. Updated on 1 out of 8 DSEs.**<br>*Pending DSEs:* eric-10k(0490.8100.5654) ST165-10K-100G-D( | 2024-05-10 00:58:56 GMT+00:00 |
| □ | ElastiFlow | 20s | Destination:143.0.1.33, Transport:UDP/9995 | **Propagation pending. Updated on 1 out of 8 DSEs.**<br>*Pending DSEs:* eric-10k(0490.8100.5654) ST165-10K-100G-D( | 2024-05-10 00:40:39 GMT+00:00 |

Name: ElastiFlow

Interval: 20s

EXPORT CONFIGURATION

Format: ● Ipfix

Target

destination: 143.0.1.33

Transport: UDP/9995

```
flow exporter ElastiFlow
   destination 143.0.1.33 vrf default
   transport udp 9995
flow exporter exporter-v4
   description SolarWinds
   destination 11.0.2.77 vrf default
   transport udp 2055
flow record record-v4
   match ipv4 destination address
   match ipv4 protocol
   match ipv4 source address
   match ipv4 version
   match transport destination port
   match transport source port
   collect application name
   collect counter bytes
   collect counter packets
   collect application dns response-code
   collect application https url
   collect timestamp absolute first
   collect timestamp absolute last
flow monitor monitor-v4
   cache timeout active 30
   exporter exporter-v4
   exporter ElastiFlow
   record record-v4
no ip source-lockdown resource-extended
flow-tracking
   enable
app-recognition
   enable
interface lag 3
   ip flow monitor monitor-v4 in
interface 1/1/1
   mtu 9198
   app-recognition enable
   no routing
   vlan access 800
   ip flow monitor monitor-v4 in
interface 1/1/2
   ip flow monitor monitor-v4 in
ip source-interface ipfix interface 1/1/24
6300#
```

L2
L3

AOS-CX Version 10.14.0001

# Useful Links

## Aruba Technical Enablement home page

https://arubapedia.arubanetworks.com/arubapedia/index.php/Technical_Enablement

## Aruba Data Center Information: Tons of great links!

https://arubapedia.arubanetworks.com/arubapedia/index.php/Category:Data_Center_Switches

## Aruba Fabric Composer Test Drive! Hands on!

https://www.arubanetworks.com/afc-demos/

## Data Center Evolution with Pensando

https://arubaversity.arubanetworks.com/student/path/1315140-data-center-evolution?sid_i=0

# Questions

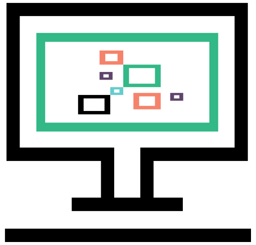
# Partner Resources

## Partner Portals

airheads COMMUNITY

Airheads Community

(Click Here)



Arubapedia for Partners

(Click Here)

Partner Ready for Networking portal

(Click Here)

## Live Support

Channel SEs (CSEs)

Regional channel support

# Thank you

aruba_switching_tme@hpe.com